A Text Book Of

NETWORK AND INFORMATION SECURITY

(22620)

Semester - VI

THIRD YEAR DIPLOMA IN COMPUTER ENGINEERING AND INFORMATION TECHNOLOGY GROUP

As Per MSBTE's 'I' Scheme Syllabus

Mrs. Mrunal P. Fatangare

M. E. (Computer)
HOD, Information Technology Department
MAEER,s MIT Polytechnic, Pune

Mrs. Pallavi U. Nehete

M.E. (I.T.)
Lecturer, Information Technology Department
MAEER,s MIT Polytechnic, Pune

Price ₹ 150.00

NIRALI PRAKASHAN
ADVANCEMENT OF KNOWLEDGE

N4399

NETWORK AND INFORMATION SECURITY **ISBN 978-93-89825-46-6**

First Edition : December 2019

© : Author

The text of this publication, or any part thereof, should not be reproduced or transmitted in any form or stored in any computer storage system or device for distribution including photocopy, recording, taping or information retrieval system or reproduced on any disc, tape, perforated media or other information storage device etc., without the written permission of Author with whom the rights are reserved. Breach of this condition is liable for legal action.

Every effort has been made to avoid errors or omissions in this publication. In spite of this, errors may have crept in. Any mistake, error or discrepancy so noted and shall be brought to our notice shall be taken care of in the next edition. It is notified that neither the publisher nor the author or seller shall be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom.

Published By :
NIRALI PRAKASHAN
Abhyudaya Pragati, 1312, Shivaji Nagar
Off J.M. Road, PUNE – 411005
Tel - (020) 25512336/37/39, Fax - (020) 25511379
Email : niralipune@pragationline.com

Polyplate

Printed By :
YOGIRAJ PRINTERS AND BINDERS
Survey No. 10/1A, Ghule Industrial Estate
Nanded Gaon Road
Nanded, Pune - 411041
Mobile No. 9404233041/9850046517

➢ DISTRIBUTION CENTRES

PUNE

Nirali Prakashan (For orders within Pune) : 119, Budhwar Peth, Jogeshwari Mandir Lane, Pune 411002, Maharashtra
Tel : (020) 2445 2044, Fax : (020) 2445 1538; Mobile : 9657703145
Email : niralilocal@pragationline.com

Nirali Prakashan (For orders outside Pune) : S. No. 28/27, Dhayari, Near Asian College Pune 411041
Tel : (020) 24690204 Fax : (020) 24690316; Mobile : 9657703143
Email : bookorder@pragationline.com

MUMBAI

Nirali Prakashan : 385, S.V.P. Road, Rasdhara Co-op. Hsg. Society Ltd.,
Girgaum, Mumbai 400004, Maharashtra; Mobile : 9320129587
Tel : (022) 2385 6339 / 2386 9976, Fax : (022) 2386 9976
Email : niralimumbai@pragationline.com

➢ DISTRIBUTION BRANCHES

JALGAON

Nirali Prakashan : 34, V. V. Golani Market, Navi Peth, Jalgaon 425001, Maharashtra,
Tel : (0257) 222 0395, Mob : 94234 91860; Email : niralijalgaon@pragationline.com

KOLHAPUR

Nirali Prakashan : New Mahadvar Road, Kedar Plaza, 1st Floor Opp. IDBI Bank, Kolhapur 416 012
Maharashtra. Mob : 9850046155; Email : niralikolhapur@pragationline.com

NAGPUR

Nirali Prakashan : Above Maratha Mandir, Shop No. 3, First Floor,
Rani Jhanshi Square, Sitabuldi, Nagpur 440012, Maharashtra
Tel : (0712) 254 7129; Email : niralinagpur@pragationline.com

DELHI

Nirali Prakashan : 4593/15, Basement, Agarwal Lane, Ansari Road, Daryaganj
Near Times of India Building, New Delhi 110002 Mob : 08505972553
Email : niralidelhi@pragationline.com

BENGALURU

Nirali Prakashan : Maitri Ground Floor, Jaya Apartments, No. 99, 6th Cross, 6th Main,
Malleswaram, Bengaluru 560003, Karnataka; Mob : 9449043034
Email: niralibangalore@pragationline.com

Other Branches : Hyderabad, Chennai

Note : Every possible effort has been made to avoid errors or omissions in this book. In spite this, errors may have crept in. Any type of error or mistake so noted, and shall be brought to our notice, shall be taken care of in the next edition. It is notified that neither the publisher, nor the author or book seller shall be responsible for any damage or loss of action to any one of any kind, in any manner, therefrom. The reader must cross check all the facts and contents with original Government notification or publications.

Preface ...

We take an opportunity to present this book entitled as "**Network and Information Security**" to the students of Sixth Semester (Third Year Diploma in Computer Engineering and Information Technology Group). The object of this book is to present the subject matter in a most concise and simple manner. The book is written strictly according to the Revised Syllabus (I-Scheme) prepared by Maharashtra State Board of Technical Education (MSBTE).

This book contains five constructive chapters.

- First chapter gives an introduction to computer and information security.
- Second chapter focuses on concepts of user authentication and access control.
- Third chapter covers cryptography.
- Fourth chapter introduces firewall and intrusion detection system.
- Network security, cyber laws and compliance standards are covered in Fifth chapter.

A special words of thank to Shri. Dineshbhai Furia, Mr. Jignesh Furia for showing full faith in us to write this text book. We also thank to entire staff of M/s Nirali Prakashan for their excellent co-operation.

We welcome constructive suggestions from our colleagues and students.

Authors

■■■

Syllabus ...

1. Introduction to Computer and Information Security

1.1 Foundations of Computer Security: Definition and Need of Computer Security, Security Basics: Confidentiality, Integrity, Availability, Accountability, Non-Repudiation and Reliability.

1.2 Risk and Threat Analysis: Assets, Vulnerability, Threats, Risks, Counter Measures.

1.3 Threat to Security: Viruses, Phases of Viruses, Types of Virus, Dealing with Viruses, Worms, Trojan Horse, Intruders, Insiders.

1.4 Type of Attacks: Active and Passive Attacks, Denial of Service, DDOS, Backdoors and Trapdoors, Sniffing, Spoofing, Man in the Middle, Replay, TCP/IP Hacking, Encryption Attacks.

1.5 Operating System Security: Operating System Updates HotFix, Patch, Service Pack.

1.6 Information, Need and Importance of Information, Information Classification, Criteria for Information Classification, Security, Need of Security, Basics Principles of Information Security.

2. User Authentication and Access Control

2.1 Identification and Authentication: User Name and Password, Guessing Password, Password Attacks - Piggybacking, Shoulder Surfing, Dumpster Diving.

2.2 Biometrics: Finger Prints, Hand Prints, Retina, Patterns, Voice Patterns, Signature and Writing Patterns, Keystrokes.

2.3 Access Controls: Definition, Authentication Mechanism, Principle - Authentication, Authorization, Audit, Policies: DAC, MAC, RBAC.

3. Cryptography

3.1 Introduction: Plain Text, Cipher Text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption.

3.2 Substitution Techniques: Caesar's Cipher, Modified Caesar's Cipher, Transposition Techniques: Simple Columnar Transposition.

3.3 Steganography: Procedure.

3.4 Symmetric and Asymmetric Cryptography: Introduction to Symmetric Encryption, DES (Data Encryption Standard) Algorithm, Asymmetric Key Cryptography: Digital Signature.

4. Firewall and Intrusion Detection System

4.1 Firewall: Need of Firewall, Types of Firewall - Packet Filters, Stateful Packet Filters, Application Gateways, Circuit Gateways.

4.2 Firewall Policies, Configuration, Limitations, DMZ.

4.3 Intrusion Detection System: Vulnerability Assessment, Misuse Detection, Anomaly Detection, Network - Based IDS, Host-Based IDS, Honeypots.

5. Network Security, Cyber Laws and Compliance Standards

5.1 Kerberos: Working, AS, TGS, SS.

5.2 IP Security - Overview, Protocols - AH, ESP, Modes - Transport and Tunnel.

5.3 Email Security - SMTP, PEM, PGP.

5.4 Public Key Infrastructure (PKI): Introduction, Certificates, Certificate Authority, Registration Authority, X.509/PKIX Certificate Format.

5.5 Cyber Crime: Introduction, Hacking, Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography, Identity Theft and Terrorism, Cyber Terrorism, Cyber Defamation.

5 6 Cyber Laws: Introduction, Need, Categories: Crime Against Individual, Government, Property.

5.7 Compliance Standards: Implementing and Information Security Management System, ISO 27001, ISO 20000, BS 25999, PCI DSS, ITIL Framework, COBIT Framework.

■■■

Contents ...

1. Introduction to Computer and Information Security	**1.1 – 1.40**
2. User Authentication and Access Control	**2.1 – 2.26**
3. Cryptography	**3.1 – 3.24**
4. Firewall and Intrusion Detection System	**4.1 – 4.22**
5. Network Security, Cyber Laws and Compliance Standards	**5.1 – 5.36**

■■■

1... Introduction to Computer and Information Security

Chapter Outcomes...

- Explain the importance of the given component of computer security.
- Explain the characteristics of the given type of threat.
- Explain the given type of attacks related with security.
- Describe the features of given type of update of operating system.
- Classify information.
- Explain principles of information security.

Learning Objectives...

- To understand Basic Concepts in Computer Security and Information Security
- To learn Risk and Threat Analysis
- To study Concepts in Operating System Security
- To understand Threats in Security
- To learn Types of Attacks in Security
- To learn Information (Classification, Criteria) and Principles of Information Security

1.0 INTRODUCTION [S-16]

- The term 'security' means protection from danger or unauthorized actions. There are various types of security like project security, personal security, operating system security, information security, national security, operations security, communication security, computer security and so on.
- In a general sense, security means protecting the assets. Security is a state of freedom or protection from a danger, risk or attack.
- With the rapid advances in networked computer technology during the last few decades and the unprecedented growth of the Internet, the public has become increasingly aware of the threats to personal and security through computer crime.
- Identity theft, pirated bank accounts, forgery - the list of electronic crimes is as unlimited as the imaginations of those who use technology in harmful and dangerous ways.
- Information security or computer security is concerned with the control of threats related to the use of information or computer. To achieve this objective, one should develop a secure computing platform so that he/she can restrict the users to perform only particular actions that is permitted to him or her.

- Computer security, is the protection of computer systems and information from harm, theft and unauthorized use. Computer security is the protection of the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data and so on).
- Information security is the task of guarding information which is processed by a server, stored on a storage device and transmitted over a network like Local Area Network (LAN) or the Internet.
- Information security means protecting information and Information Systems (IS) from unauthorized access, use, disclosure, disruption, modification or destruction.
- An Information System (IS) is a set of interrelated components that collect, process, store and disseminate data and information. An information system provides a feedback mechanism to monitor and control its operations to make sure it continues to meet its goals and objectives.
- Information systems are made up of the major components of hardware, software, data, people, procedures and networks.
- The critical characteristics of information including Confidentiality, Integrity and Availability (CIA), must be protected at all times. This protection is implemented by multiple measures that include policies, education, training and awareness and technology.
- The objective of information system security is to optimize the performance of an organization with respect to the risks to which it is exposed.
- In computer security, a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat refers, to anything that has the potential to cause serious harm to a computer system.
- A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.
- An attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.
- Risk is the intersection of assets, threats and vulnerabilities. Risk is defined as, change of injury, damage, or loss. Thus, risk has two elements namely, chance (an element of uncertainty) and potential loss or damage.
- Security measures cannot assure 100% protection against all threats. Therefore risk analysis which is the process of evaluating system vulnerabilities and the threats facing it is an essential part of any risk management program.
- The analysis process identifies the probable consequences or risks associated with the vulnerabilities and provide the basis for establishing a cost-effective security program.
- Risk management is the process of implementing and maintaining counter measures that reduce the effects of risk to an acceptable level.
- The risk analysis process gives management the information it needs to make educated judgments concerning information security. The procedure identifies the existing security controls, calculates vulnerabilities, and evaluates the effect of threats on each area of vulnerability.

1.1 FOUNDATION OF COMPUTER SECURITY [S-16]

- The foundations of computer security include answers to the superficially simple question "What is this all about?" This section gives us detailed knowledge about the concepts of computer security. This section also defines a few of the most important terms of computer security.
- Security is about the protection of assets. The assets of a computer system can be categorized as hardware, software, data and communication lines and networks.
- Security is the technique which makes the accessibility of information/system more reliable. Security means to protect information or computer system from unauthorized user like attackers, hackers who damage to system purposely.

- Cyberspace (computer networks and Internet) is becoming a dangerous place for all organizations and individuals to protect their sensitive data or information. Security is not only to protect information or network, but also allow authorized user to access the system or network.
- Computer security can be viewed as a set of mechanisms that protect computer systems from unauthorized access, theft, damage and disruption of the services they provide.
- Computer security includes protection from both internal and external threats. Internal threats can be flaws in a software program or operating system. External threats are unauthorized access or human error.
- Computer security is the protection of information systems from theft or damage to the hardware, the software and to the information on them, as well as from disruption or misdirection of the services they provide.
- The objective of computer security includes protection of information from theft, corruption, or natural disaster, while allowing the information to remain accessible and productive to its intended users.

Terms related to Computer Security:

1. The term **Computer System Security** means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. Example, a security system protects our house, warning the neighbors or the police, if an unauthorized intruder tries to get in. We speak of a child's "physical security", hoping he or she is safe from any potential harm.
2. **Computer Security and Information Security** is the protection of computers and data that the computers hold. This can be anything from placing passwords on computers to setting up firewalls. Information security deals with protection of information.
3. **Data Security** means ensuring the data which is kept safe from corruption and access to it is suitably controlled. Thus, data security helps to ensure privacy. Data security refers to the protective measures which ensure that data or computer is kept safe from modification or corruption. It also prevents unauthorised access to data or computer. Thus, data security helps to provide privacy to the data. Thus, data security and privacy help the organisation to prevent data breaches, ensure the integrity of data and protect the important information from disclosure.
4. In the field of networking, the **network security** comprises of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security means protection of data on the network during transmission. It consists of different policies and provisions adopted by the administrator. It involves the authorisation and access control of the network. Network administrator is responsible for the proper implementation of access control and authentication to provide the security.

1.1.1 Definition of Computer Security [S-16, 17, 18, 19, W-16]

- Internet is most required thing in today's life. The Internet has changed our lives. Unfortunately, this huge network and its associated technologies will leads to the increasing number of security threats.
- Awareness of standard cyber security practices is the most effective way to protect our self from these threats and attacks.
- Computer security includes the protection, prevention and detection of unauthorized use of computer systems as well as data stored in the computer.
- "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" like hardware, software. **OR**

- Computer security is, defined as, "the protection of computing systems and the data/information that system will access". **OR**
- Computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

1.1.2 Need of Computer Security [S-17, 18, W-17]

- The growth of computers and Information Technology (IT) has been explosive. Never before an entirely new technology has been propagated around the world with such speed and with so great a penetration of virtually every human activity.
- Today, the use of computer with internet is increasing rapidly. At the same time security challenges are also increasing. A number of software tools are available which help the attackers to attack easily without much knowledge of computer field.
- Therefore, today's information security is an emerging field which helps to protect the computer from various attacks and also provides the awareness about security among the common people. Information security supports to protect the information from unauthorised persons.
- Information security not only confined to computer security but it includes the security of data or information in different forms.
- We use computer for various applications so it is very important to protect our computer so that unauthorised person cannot access the system and modify or delete or read the data.
- Computer security is the process of preventing and detecting unauthorized use of the computer system. Computer security needed for information security (securing information from unauthorized access, modification and deletion).
- Computer security is important because it keeps information protected. Computer security is needed in many areas such as:
  1. **To Preserve Company/Organizations Assets:** Company assets such as information of organization kept in the computer networks, which is useful as the physical assets of the company.
  2. **To Confirm with Governing Requirements and Moral Responsibilities:** Each organization creates policies and procedures which deal with the security requirements of the organization in question.
  3. **For Competitive Benefit**: Financial services and e-commerce considers network security to be of prime importance.
  4. **Protecting Data/Information that Organization Use and Collect:** Without data an organization losses its records of transaction and ability to deliver a value to its customer. Protecting data at motion and at rest are both critical aspects of information security. The value of data motivates attackers to steal and corrupt the data.
  5. **Enabling the Safe Operation of Application:** A modern organization need to create an environment that safeguards these Applications, specially operating system platform, e-mail, instant messaging application etc.
  6. **Safeguarding Technology Assets in Organization:** To perform effectively, organizations must employ secure infrastructure service which appropriate to the size and the scope of the organization. For example, a small business uses an email service and secure with the personal encryption tool. When an organization grows, it must develop additional security service that uses system of software, encryption methodology and legal agreement that support entire information infrastructure.

1.1.3 Security Basics [S-16, 18]

- Computer security means to protect information or data. In simple words, security is defined as, protecting information system from unintended access.

- It deals with prevention and detection of unauthorized actions by users of a computer. Basic security concepts important to information on the Internet also called as principles of security are confidentiality, integrity, and availability.
- Concepts relating to the people who use the information are accountability, reliability and non-repudiation.

1. Confidentiality:

- Confidentiality is the protection of information or resources. Also, there is a need to keep data/information secret from unauthorized users that want to have access to it, so just the right people can access it.
- It is used as an attempt to prevent the unauthorized disclosure of message contents. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality.
- For some types of information confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies.
- Loss of confidentiality can occur in many ways such as through the intentional release of private company information.

Example in Real Life:

- Consider that there are two people interacting via an email (encrypted) they know the decryption keys of each other and they read the email by entering these keys into the email program.
- If someone else can read these decryption keys when they are entered into the program, then the confidentiality of that email is compromised.
- Consider user A sends message to user B. Other user C gets access to this message which is not desired; hence it leads to loss of confidentiality. When user C access message without permission of A and B, This type of attack is called as Interception.

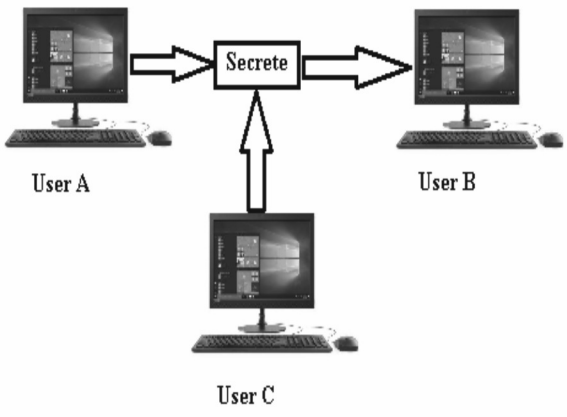


Fig. 1.1: Loss of Confidentiality

2. Integrity: **[S-16]**

- Integrity refers to the trustworthiness of data or resources, in terms of preventing improper or unauthorized change/modification.
- It means unauthorized person are not allowed to make modifications to data. It means ensuring that information remains unaltered. Only authorized person can edit or change information.
- It includes two variations of integrity as "data integrity" - that data have not been changed inappropriately, whether by accidentally harmful action.
- It also includes "origin" or "source integrity"- that the data actually came from the person or entity we think it did, rather than an unauthorized person.

- Information can be corrupted when it is present on an insecure network. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information whether by human error.

Example in Real Life:

- Consider online payment system in which user A want to send 100 USD to user B, but information is modified without permission of user A.
- User C can make changes in information by sending 1000 USD to user B. So information is modified hence integrity is loosed.

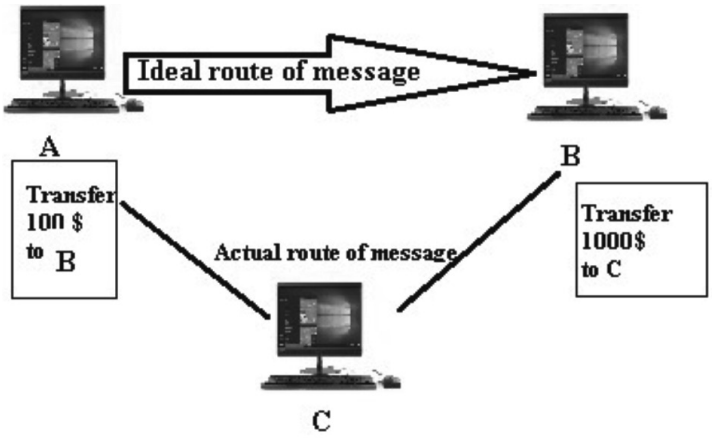


Fig. 1.2: Loss of Integrity

3. Availability:

- Availability refers to the ability to access data of a resource when it is needed to authorized person/users. Only authorized individual can create or change information.
- The concept of availability ensures the reliable and timely access to data or by the authorised person. Availability guarantees that the systems are up and running when they are needed.
- Information can be erased or become unavailable, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need.
- To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization.

Example in Real Life:

- Consider hacker has hacked web server of a bank and put it down. We as an authenticated user want to perform an e-banking transfer but it is difficult to access it, the undone transfer is a money lost for the bank.
- Consider user A is authorized user and he wants to access data from server computer B. Due to the intentional actions of unauthorized user C, an authorized user A cannot be able to access server computer B. This would breach the concept of availability, hence such type of attack is called as Interruption.

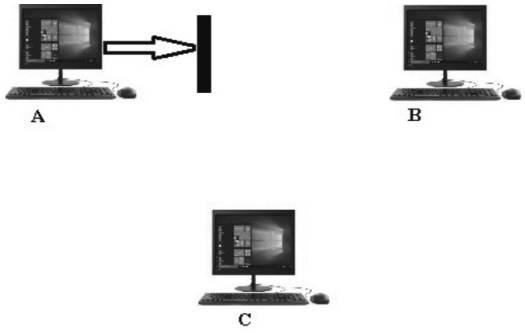


Fig. 1.3: Loss of Availability

4. Non-Repudiation:

- Security is strong when the means of authentication cannot later be contradicted the user cannot later deny that he or she performed the activity. This is known as non-repudiation.
- There are some situations where a user sends a message and later on he refuses that she/he had sent that message. Principle of non-repudiation defeats such possibilities of denying something, having done it.

Example:

- Consider user A sends fund transfer request to bank B using internet. After bank performs the fund transfer as per user A's requirement.
- A could claim that she/he never sent the fund transfer instruction to the bank. Thus A repudiates her fund transfer instruction.



Fig. 1.4: Non Repudiation

5. Accountability:

- Accountability is an essential part of an information security plan. It means that every individual who works with an information system should have specific responsibilities for information assurance.
- The tasks for which an individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance.

Example:

- Consider policy statement in any organization that all employees must avoid installing outside software on a company-owned information infrastructure.
- The person in charge of information security should perform periodic checks to be certain that the policy is being followed. Individuals must be aware of what is expected of them and guide continual improvement.

6. Reliability:

- Reliability is an attribute of any computer-related component (software, hardware or a network) that consistently performs according to its specifications. Reliability is the property of leading to consistent intended behavior and results.
- Reliability is also defined as the property of trustworthiness. Data are frequently considered reliable when they are exact and precise, and when they can be reproduced.
- It has been long considered one of three related attributes that must be considered when making, buying, or using a computer product or component.
- Reliability, availability, and serviceability considered to be important aspects to design into any system. If we say product is Reliable then that product is totally free from technical errors. Vendors frequently express a product's reliability quotient as a percentage.
- For example, IBM's z/OS (an operating system for their S/390 server series), has a reputation for reliability because it evolved from a long line of earlier MVS and OS/390 operating system versions.

1.2 RISK AND THREAT ANALYSIS

- A risk is any event or action that could cause a loss or damage to computer hardware, software data/information or processing capability.
- Threat analysis is the analysis of probability of occurrences and consequences of damaging actions/ events to a system. Threat analysis identifies possible threats in computer security process.
- In this section we will study risk and threat analysis.