UNIT 1 SECURITY CONCEPTS

Structure

1.0 INTRODUCTION

Computer Security can be defined as technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of the information managed by the computer. It means the protection of Integrity, Availability and Confidentiality of Computer Assets and Services from associated Threats and vulnerabilities.

Security is divided into two categories; (a) computer security and (b) network security. In generic terms, computer security is the process of securing a single, standalone computer; while network security is the process of securing an entire network of computers.

a) **Computer Security:** Technology and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of the data managed by the computer.

(b) **Network Security:** Protection of networks and their services from unauthorised modification, destruction, or disclosureand provision of assurance that the network performs its critical functions correctly and there are no harmful side effects.

The major weakneses in a computer system pertain to hardware, software, and data. However, other components of the computer systems may also be targeted.

1.1 OBJECTIVES

After going through this unit you will be able to:

- know of the threats to computer security;
- understand what causes these threats, and
- know various security techniques.

1.2 GOALS OF COMPUTER SECURITY

The goals of computer security are integrity, confidentiality, and availability of the information managed by the computer system. The relationship among the three is shown in *Figure 1*.

1.2.1 Integrity

The data Integrity in computer security deals with the knowledge that data has not been modified. Data Integrity is related to data accuracy, but integrity and accuracy are not the same. For example, if information is entered incorrectly, it will remain incorrect. So, it is possible to have Data Integrity without Data Accuracy.

Integrity means preventing unauthorised modification. To preserve the integrity of an item means that the item is unmodified, precise, accurate, modified in an acceptable way by authorised people, or consistent.

1.2.2 Confidentiality

Confidentiality means preventing unauthorised access. It ensures that only the authorised person accesses the computer system. Not all data available on the computer falls in the category of confidential data. There is data that can be made public and there is data that is considered sensitive. It is this critical or sensitive data that will require confidentiality. Data confidentiality cannot be enforced unless data integrity is present. The following items could require data confidentiality: credit card files, medical records, personnel data, mission-critical data, and R&D data etc.

1.2.3 Availability

There is no point in making the computer system so secure that no users can access the data they need to perform their jobs effectively.

The system should be accessible to authorised persons at appropriate times.

A computer system is available if:

- The response time is acceptable
- There is a fair allocation of resources
- Fault tolerance exists
- It is user friendly
- Concurrency control and deadlock management exists. Terms like concurrency

control and deadlock manbgement will be discussed in the operating system course.

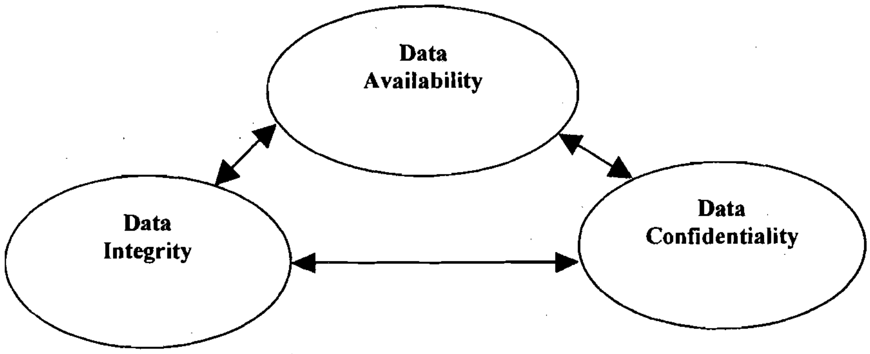

Figure 1: Relationship between Confidentiality, Integrity, and Availability

1.3 SECURITY PROBLEM AND REQUIREMENTS

Protection of information has been a major challenge since the beginning of the computer age. The computer security problem has grown with the computer industry, the computer itself was not really part of the security problem or its solution.

Connecting computers introduces a need for communication security (often utilising cryptography) to prevent the possibility of an attack. Connecting computers gives them greater accessibility, which increases computer security problems.

Computer security attempts to ensure the confidentiality, integrity, and availability of the computing system's components. The principal components of a computing system subject to attacks are: hardware, software and data. These three components and the communications among them is the basis of computer vulnerabilities. Attackers can devise attacks that exploit these vulnerabilities. There are basically four kinds of attacks on computing systems: **interception**, **interruption**, **modification**, and **fabrication**. These terms will be explained later.

One of the ways to identify security problems is by means of risk analysis. Risk analysis involves determining:

- What you need to protect,
- What you need to protect it from,
- And how to protect it.

It is the process of examining all of your risks, and ranking those risks by level of severity.

There are three major steps in risk analysis, namely:

- Identifying the assets (what are you protecting)
- Identifying the threats (against what)
- Identifying impact.

1.3.1 Identifying the Assets

List all the things that are subject to security threats. These include:

- **Hardware:** CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers, hubs, gateways, servers, modems, etc.

- **Software:** source programs, object programs, utilities, diagnostic programs, operating systems, communications program, firewall software, IDS (Intrusion Detection System) software etc.
- **Data:** during execution, store on-line, archive off-line, backup, audit logs, databases, in transit over communication media etc.
- **People:** user, people needed to run systems.
- **Documentation:** on programs, hardware, systems, local administrative procedures.
- **Supplies:** paper, forms, ribbons, floppy diskettes, magnetic media.

Based on the above, asset inventory can be created with the following component for each asset:

- Designated owner
- General support system or critical/major application
- Physical/logical location.

1.3.2 Identifying the Threats

Once the assets requiring protection are identified, it is necessary to identify threats to those assets. The threats can be then evaluated to determine what potential for loss exists.

There are two basic type of threats: accidental threats and intentional threats.

Accidental threats can lead to exposure of confidential information or causing an illegal system state to occur due to modification of information. An intentional threat is an action performed by an entity with the intention to violate security. And this includes destruction, modification, fabrication, interruption or interception of data.

In general, threats to an asset should be considered in terms of the availability, confidentiality and integrity of the asset. The possible threats to a computer system can be:

- Unauthorised Access
- Disclosure of information
- Denial of service.

1.3.3 Identifying the Impact

After identifying the assets and threats, the impact of security attack should be assessed. The process includes the following tasks.

- Identifying the vulnerabilities of the system;
- Analysing the possibility of threats to exploit these vulnerabilities;
- Assessing the consequences of each threat;
- Estimating the cost`of each attack;
- Estimating the cost of potential counter measure, and
- Selecting the optimum and cost effective security system.

The consequence of a threat materialised in an organisation could result in one or more impacts. For example, an impact can be:

- Infringement of privacy
- Financial loss
- Disruption of activities.

1.4 THREATS AND VULNERABILITIES

With the rise of multiprogramming, the several aspects of a computing system requiring protection are system software, memory, sharable I/O devices such as disk, printers, tape drivers, shared programs/procedures, networks, shared data, files, and execution environment.A threat is a set of instances that has the capability of causing loss or harm to the computer system. There are many threats to a computer system and can be (a) Human initiated, (b) Computer initiated, and (c) Natural disasters like flood or earthquake.

A threat can be accidental or deliberate and the various types of security breaches can be classified as (a) interruption, (b) interception, (c) modification and (d) fabrication.

- Interruption: An asset of the system becomes lost, unavailable, or unusable.
  - Malicious destruction of a hardware device
  - Deletion of program or data file
  - Malfunctioning of an Operating system.
- Interception: Some unauthorised entity can gain access to a computer asset. This unauthorised entity can be a person, a program, or a computer system.
  - Illicit copying of program or data files
  - Wiretapping to obtain data.
- Modification: Some unauthorised party not only accesses but also tampers with the computer asset.
  - Change in the values in the database
  - Alter a program
  - Modify data being transmitted electronically
  - Modification in hardware.
- Fabrication: Some unauthorised party creates a fabrication of counterfeit object of a system. The intruder may put spurious transaction in the computer system or modify the existing database.

An attacker needs three things (1) method, (2) opportunity and (c) motive.

- A method: It comprises the tools, skills, knowledge etc.
- Opportunity: Opportunity means the right time and right access to perform the attack.
- Motive: Motive is the reason to carry out the attack.

A **threat** can be blocked by control of vulnerability. We can use a control as a protective measure. A control can be in action, device, procedure and technique that limits or eliminates vulnerability.

A computer system has three valuable components as pointed out earlier: hardware, software and data. Vulnerability is a weakness in the system. This weakness may be exploited by threats causing loss/damage or harm to the system. Vulnerability does not cause any harm until exploited. It can be a weakness in: (a) Procedures, (b) Design and (c) Implementation.

The various vulnerability examples are: insufficient security training, lack of security awareness, inadequate recruitment procedures, insufficient preventive maintenance, lack of identification and authentication mechanisms, transfer of password in readable form (clear text), unprotected public network connections, poor password management, well-known flaws in the software, unsupervised work by external staff, no security policy, exposed/unprotected communication lines, poor cable joint, inadequate system management, no audit-trail, wrong allocation of access rights or permissions, lack of documentation and dialup connections, etc.

The computing system vulnerabilities are:

- Software vulnerabilities: software vulnerability can be due to interruption, interception, modification, or fabrication. The examples of software vulnerabilities are: (a) destroyed/deleted software, (b) stolen or pirated software, (c) unexpected behaviour and flaws, (d) non-malicious program errors, (e) altered (but still run) software.
- Hardware vulnerabilities: hardware vulnerability is caused due to interruption (denial of service), modification, fabrication (substitution) and interception (theft).
- Data vulnerabilities: Data vulnerability is caused by interruption (results in loss of data), interception of data, modification of data and fabrication of data.
- Human vulnerabilities: The various human generated vulnerabilities are break-ins, virus generation, security violation, inadequate training.

☞ Check Your Progress 1

1) What are the Goals of Computer Security?

....

....

....

2) Justify the following statement:

“ There is no confidentiality without integrity”

....

....

....

....

1.5 USER AUTHENTICATION

Authentication in a computer system uses any of three qualities to authenticate the user:

- Something the user knows, like password, PIN numbers; pass phrases, a secret handshake etc.

- Something the user has: Identity badges, physical keys, a driver's license, or a uniform.

- Something the user is: This is based on the physical characteristic of the user (Biometrics), such as a finger print, face recognition, voice recognition etc.

Two or more methods can be combined for more solid authentication; for example, an identity card and PIN combination.

The computer system needs a system in place to be sure that only authorised users have access to its resources. On the computer system, one of the critical areas of security is who has access to what.

There are two types of access control that can be implemented:

- Mandatory Access Control (MAC) : MAC is an access control policy that supports a system with highly secret or sensitive information. Government agencies typically use a MAC.

- Discretionary Access Control (DAC) : DAC is an access control policy that uses the identity of the user or group that they belong to allow authorised access. It is discretionary in that the administrator can control who has access, to what and what type of access will they have, such as create or write, read, update, or delete.

Authentication occurs when a user provides the requested information to an authentication verification authority. The traditional method of authentication is to provide a password.

To increase the level of reliability, biometric authentication can be introduced. The user is not only identified digitally, but by their physical characteristics such as fingerprint scan, iris scans or hand geometry.

Authentication Token: It is a portable device used for authenticating a user. The tokens are devices that operate by using systems such as:

Hardware Tokens

- **Challenge and response:** It is an authentication technique using a calculator type of token that contains identical security keys or algorithms as Access Server, which sends an unpredictable challenge to the user, who computes a response using their authentication response token.

- **Time-based challenge response Token:** The Time-based Token utilises an authentication method where the security token and server use an identical algorithm. To gain access, the user takes the code generated by the token and adds his or her user name and PIN to create a pass code. The pass code is combined with a seed value and the current time, encrypted with an algorithm and sent to the server. The server authenticates the user by generating its own version of the valid code by accessing the pre-registered PIN and using the same seed value and algorithm for validation.

Software Token

If an organisation does not wish to purchase hardware tokens, it may opt for a software type instead. A software token is an authentication process using portable devices such as a Palm Pilot, Palm PC, or wireless telephone to carry the embedded software.

1.6 SECURITY SYSTEM AND FACILITIES

Security controls should be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.

System software and resources should be accessible after being authenticated by access control system.

1.6.1 System Access Control

- Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted on "need-to-use" basis.
- The access control software or operating system should be providing features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game", etc,. to protect access to the system and data resources should be avoided.
- Guidelines and procedures governing access authorisation shall be developed, documented and implemented.
- Each user shall be assigned a unique user ID.
- Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised access.
- Automatic time-out for terminal inactivity should be implemented.
- Audit trail of security sensitive access and actions shall be logged.
- Audit trails must be protected against modification or deletion.
- Activities of all remote users shall be logged and monitored closely.
- The startup and shutdown procedure of the security software must be automated.
- Sensitive operating system files must be protected using proven tools and techniques.

1.6.2 Password Management

Certain minimum quality standards for password shall be enforced. The following control features shall be implemented for passwords:

- Minimum of 8 characters without leading or trailing blanks;
- Shall be different from existing passwords;
- To be changed at least once every 90 days and for sensitive systems it should be changed every 30 days;
- Should not be shared, displayed or printed;
- Password retries should be limited to a maximum of 3 attempted logons after which the user ID shall then be revoked for sensitive systems;

- Passwords, which are easy to guess, should be avoided;
- Password shall always be of encrypted form to avoid disclosure, and
- All passwords must be resistant to dictionary attacks and all known password cracking algorithms.

1.6.3 Privileged User Management

The following points must be taken into account while granting privilege to users.

- Privileges shall be granted only on a need-to-use basis.
- Login available only from console.
- Audit log should be maintained.

1.6.4 User Account Management

Procedures for user account management should be established to control access to application and data. It should include:

- Should be an authorised user.
- A written statement of access rights should be given to all users.
- A formal record of all registered users shall be maintained.
- Access rights of users who have been transferred, or left the organisation, shall be removed immediately.
- A periodic check/review shall be carried out for redundant user accounts and access right that is no longer required.
- Redundant user accounts should not be reissued to another user.

1.6.5 Data and Resource Protection

All information shall be assigned an owner responsible for integrity of data and resource. This will help in protection of data and resources to a great extent. And this assignment of responsibility should be formal and top management must supervise the whole process of allocation of responsibilities.

1.6.6 Sensitive System Protection

- Security token/smart cards/bio-metric technologies such as iris recognition, finger print verification technologies, etc,. shall be used to complement the usage of password to access the computer system.
- Encryption should be used to protect the integrity and confidentiality of sensitive data. In this unit we will discuss various techniques used in the protection of sensitive computer systems and networks.

Data backup and Off-site Retention

- Backup procedures shall be documented, scheduled and monitored.
- Upto date backup of critical items shall be maintained. These items include: data files, utilities/programmes, databases, operating system code, encryption keys, documentation, full/incremental backup frequencies as per schedule.

Firewall

The firewall is the first line of defense for any computer system or network. All packets that enter the network should come through this point. A modern firewall is a system of applications and hardware working together. A sophisticated firewall performs a combination of packet filtering, network address translation (NAT), and proxy services. These applications are depicted in *Figures 2, 3* and *4* respectively.

Firewalls have two general methods of implementing security for a network. Although variations between these two exist, most modifications belongs to one or the other of the following:

— packet filtering and

— proxy server (Application Gateway)

Packet Filtering were designed to look at header information of the packet. Packet Filtering, shown in *Figure 2*, was the first type of firewall used by many organisations to protect their network. The general method of implementing a packet filter was to use a router. These routers had the ability to either permit or deny packets based on simple rules.

Proxy Servers use software to intercept network traffic that is destined for a given application. The proxy server, shown in *Figure 3*, recognises the request, and on behalf of the client makes the request to the server. In this, the internal client never makes a direct connection to the external server. Instead, the proxy functions as man-in-the-middle and speaks to both the client and server, relaying the message back and forth. The addition of proxy server capabilities added to the firewalls created a much more solid security product than a pure packet filter. Proxy software can make decisions based on more than the header information of a packet.

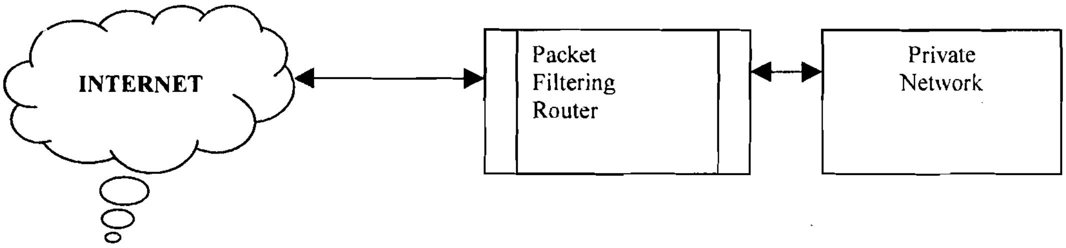

Figure 2: Packet Filtering Router

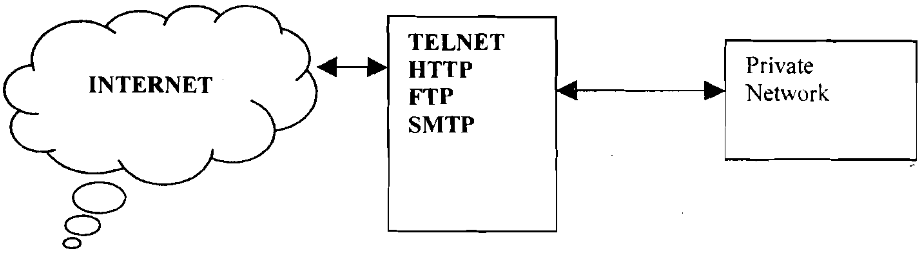

Figure 3: Application level gateway or Proxy server

A firewall can have a negative impact on the network by blocking access to the desired resources. This is due to improper configuration of a firewall that makes the desired resource unavailable. Additionally, if an ordinary PC has been configured to be the firewall (a multi-homed computer) it may not have the internal speed to perform all the functions of the firewall fast enough, resulting in increased latency.

Encryption

- Central to all security mechanism
- Confidentiality of data

- Some protocols rely on encryption to ensure availability of resources.

The encryption process as a whole is taking data that is plain text (readable form), and using a mathematical technique to make the text unreadable. The receiver then performs a similar technique to decrypt the message. The process of encrypton and decrypton is shown in *Figure 4*.

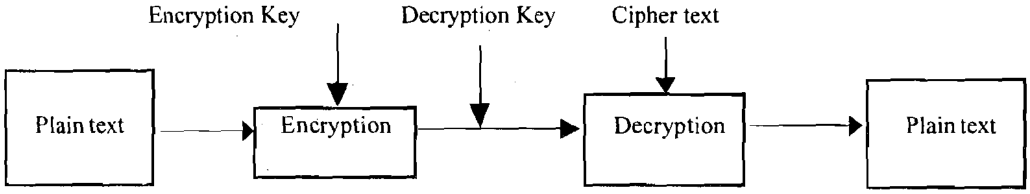

Figure 4: Encryption/ Decryption Mechanism

The performance hit is much more obvious in encryption. If the data packets are encrypted, the information that must be transmitted is bigger, and more bandwidth will be required. Additionally there will be more overheads on devices for performing encryption and decryption.

The computer that is asked to perform encryption and decryption must be able to handle extra workload.

Intrusion Detection System (IDS)

Intrusion Detection Systems are a combination of hardware and software systems that monitor and collect information and analyse it to detect attacks or intrusions. Some IDSs can automatically respond to an intrusion based on collected library of attack signatures. IDSs uses software based scanners, such as an Internet scanner, for vulnerability analysis.

Intrusion detection software builds patterns of normal system usage; triggering an alarm any time when abnormal patterns occur.

What IDS can do?

- By using various techniques it attempt to detection of intrusion into a computer or network by observation of actions, security logs, or audit data.
- Detection of break-ins or attempts via software systems that operate on logs or alert information.
- Cannot stop crime, only prevent and provide evidence for investigations.

Software Controls

- Internal program controls
- OS controls
- Development controls.

Hardware controls

- Locks or blocks limiting access
- Hardware or smart card based encryption
- Devices for user's authentication
- Mechanism to control access to storage media.

Policies

The security policies and procedures must be properly implemented to ensure their proper use.

Physical Controls

- Easy to implement, effective and less costly
- Include locks on doors, guards at entry/exit points
- Backup copies of critical software and data
- Access Control
- Media Control
- Precautions against water and fire damage
- Air conditioning
- Physical site planning that minimizes the risk of natural disasters.

System Security

- International Security Standards: Most computer vendors nowadays adopt international standards into building security facilities into their system.

Computer Virus

- Computer should be equipped with updated virus protection and detection software.
- Virus detection software must check storage drives both internal and external to the system on a regular basis.
- All diskettes and software shall be screened and verified by virus scanner software before being loaded onto the computer system.

Personnel Security

Personnel security is everything involving employees, who are potential elements of breaches of security.

- Hiring them
- Training them
- Monitoring them
- Handling their departure

Why personnel Security?

- Most of the Security breaches are caused by people only like, break-ins, virus generation etc.
- Statistics reveal that the most common perpetrators of significant computer crime are the legitimate users of the computer system.
- Some studies show that over 80% of incidents are due to internal users.

Auditing

Auditing is a tedious process and requires a good eye for details.

- Track everyone who logs on and off the computer system.
- Audit movement of critical files, attempted deletion or access to mission-critical data.
- Some of the common red flags to watch for in auditing are – multiple bad logon attempts, or same account trying to log in from many locations at the same time, and attempted shutdown of critical servers.

It is due to time-consuming process of reading the logs that many companies avoid auditing of log files. The organisation that takes the log files for granted will end up as one that is unable to inform the legal agencies that an incident has really happened.

☞ Check Your Progress 2

1) Identify computer assets in your organisation.

....

....

....

....

2) Identify threats to assets listed in progress 1 above.

....

....

....

....

3) Identify the impact of security attack listed in 2 above.

....

....

....

....

1.7 CRYPTOGRAPHY

A cryptosystem is an algorithm, plus all possible plaintexts, cipher texts, and keys.

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption (E) and decryption (D). The key is a large number. The range of possible values of the key is called the key space. Both encryption and decryption use this key space.

$E_K[M] = C$

$D_K[C] = M$

or, $D_K[E_K[M]] = M$

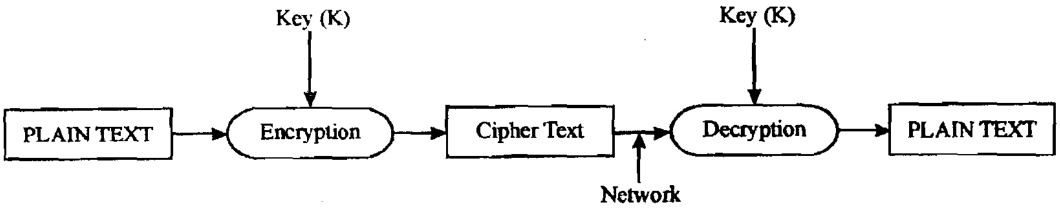

Figure 5: Encryption & Decryption using same key

Sometimes algorithms use a different encryption and decryption key. The encryption key K1 is different from decryption key K2 (Figure 6).

$$E_{K1}[M] = C$$

$$D_{K2}[C] = M$$

$$\text{Or } D_{K2}[E_{K1}[M]] = M$$

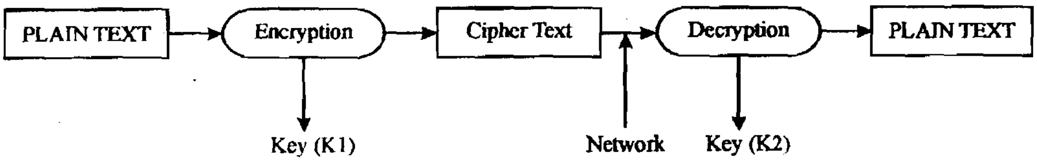

Figure 6: Encryption & Decryption using different keys

There are two general types of key-based algorithms: symmetric and public-key (asymmetric algorithm). The universally accepted modern method of electronic authentication is the one based on asymmetric cryptosystems. This is also known as public key cryptography, and is the basis for creating digital signatures. However rapid advancements and technological changes are challenging the supremacy of digital signatures as the only method of electronic authentication. Biometrics and dynamic signature analysis, among other technologies, are expected to be equally important in the years to come. It is also expected that some of the biometric techniques may prove to be more reliable and less susceptible to compromise than digital signatures. In view of the pace of technological development, no single technology may prevail for a long time as the sole means of electronic authentication.

1.8 INTRUSION DETECTION

ID stands for Intrusion Detection, which is the art of detecting inappropriate, incorrect, or anomalous activity. ID systems that operate on a host to detect malicious activity on that host are called host-based ID systems, and ID systems that operate on network data flows are called network-based ID systems.

Sometimes, a distinction is made between misuse and intrusion detection. The term intrusion is used to describe attacks from the outside; whereas, misuse is used to describe an attack that originates from inside the organisation's network. However, most people don't draw such distinctions.

The most common approaches to ID are statistical anomaly detection and pattern-matching detection.

Increased usage and consequent exposure have led to the need to develop security components for the Web interface architecture. One such component is Intrusion Detection system. Intrusion Detection systems are however complex to implement, especially on large networks, because they generate vast quantities of data and require significant configuration and management. IDS's come in many forms and implementation models. Some rule-based systems rely on preset rules. Anomaly-based systems generate their own baseline overtime by building a database of recorded network usage. When network usage moves outside of the developed pattern, the IDS sounds an alarm.

In addition, IDS can be either host or network based or a combination thereof. A host based IDS is installed on and looks for potential malicious authority on a specific computer. A network based IDS records network traffic and scans for suspicious activity using sensors and agents installed throughout a network often through a tap off of a hub or a switch with a spanner port. It looks for malicious commandos, repeated failed login attempts, traffic peaking at odd hours or other evidence of possible mischief.

1.9 COMPUTER – SECURITY CLASSIFICATIONS

The "Trusted Computer System Evaluation Criteria (TCSEC or orange book)" is the most widely accepted standard in the industry. The TCSEC model was developed based on a hierarchical model of security classifications.

The classes of systems recognised under the TCSEC are as follows. They are represented in the order of increasing desirability from computer system security point of view.

Class D (Minimal Protection)

A system with a Class D rating does not have to pass any tests to be rated as a class D system.

Class C1 (Discretionary Security Protection)

For a system to have C1 level security, it must provide a separation of users from data. Discretionary access controls need to be available to allow a user to limit access to data. Users must be identified and authenticated.

Class C2 (Controlled Access Protection)

For a system to have C2 level security, a user must be able to protect data so that it is available to only one user at a time. An audit trail that tracks access and attempted access to objects, such as files, must be kept. Further C2 security requires that all the residual data generated in temporary memory or register is erased.

Class B1 (Labeled Security Protection)

Systems at the B1 level of security must have mandatory access control capabilities. Mandatory access controls limit access to objects based on the sensitivity of the information contained in the objects and formal authorisation of subjects to access information. The subject and objects that are controlled must be individually labeled with a security level. Labels must include both hierarchical security level such as "unclassified", "secret", and "top secret", and categories. Discretionary access control must also be present.

Class B2 (Structured Protection)

For a computer system to meet the B2 level of security, there must be a formal security model. Covert channels used to transmit data must be constrained. There must be a verifiable top-level design, and testing must confirm that this design has been implemented. A security officer is designated to implement access control policies.

Class B3 (Security Domains)

The security of systems at B3 level is based on a complete and conceptually simple model. The capability of specifying access protection for each object, and specifying allowed subjects, the access allowed for each, and disallowed subjects must be included. A reference monitor for accessing user's requests and allows or disallows access based on access control policies, must be implemented. The system must be tamper proof and highly resistant to penetration. Auditing must be available for detection of security violations.

Class A1 (Verified Design)

The capabilities of a class A1 system are identical to those of a B3 system. However, the formal model for a class A1 system must be formally verified as secure.

☞ Check Your Progress 3

1) Distinguish between vulnerability and threat.

....

....

....

2) List any three recent computer security failures.

....

....

....

3) Do you currently apply any computer security control measures? If so, what?Against what attacks are you trying to protect?

....

....

....

4) Discuss various security systems and facilities.

....

....

....

5) What is computer-security classification?

....

....

....

6) What do you understand by symmetric and asymmetric cryptography?

....

....

....

1.10 SUMMARY

Computer security attempts to ensure the integrity, confidentiality, and availability of computer system. Computer systems are subject to attacks: hardware, software, and data. These three components and communication equipment associated with the computer constitute the basis of computer security vulnerabilities. Further, the people and systems interested in compromising a system can devise attacks that exploit the vulnerabilities. Four kinds of attacks on a computer system–interception, interruption, modification, and fabrication–have been discussed.

Controls can be applied at the level of the data, the programs, the system, the physical devices, the communication lines, the environment, and the personnel.

1.11 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) The goals of computer security are:

   a) Data integrity

   b) Data confidentiality

   c) Data availability

2) Confidentiality ensures that the information in a computer system and transmitted information are accessible only for reading by authorised parties. This includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object. And without integrity of data, this is not possible.

Check Your Progress 2

1) This includes hardware, software, data, people related to system operation and management, documentations, and supplies, etc.

2) Threats are of two types: (1) accidental threats, (2) intentional threats.

3) The impact of security attacks could be: (1) infringement of privacy, (2) financial loss, or (3) disruption of activities.

Check Your Progress 3

1) a) A threat is a set of instances that has the capability of causing loss or harm to the computer system. There are many threats to a computer system and can be (a) Human initiated, (b) Computer initiated, and (c) Natural disasters like flood or earthquake. A threat can be accidental or deliberate and the various types of security breaches can be classified as (a) interruption, (b) interception, (c) modification, and (d) fabrication.

   b) A computer system has three valuable components: hardware, software, and data. Vulnerability is a weakness in the system. This weakness may be exploited by threats causing loss/damage or harm to the system. Vulnerability does not cause any harm until exploited. It can be a weakness in: (a) procedures, (b) design, and (c) implementation.

2) "Trusted Computer System Evaluation Criteria (TCSEC or orange book)" is the most widely accepted standard in the industry. The TCSEC model was developed

based on a hierarchical model of security classifications. It includes various classes like Class D, C1, C2, B1,B2, B3, and A1.

3) In the case of symmetric cryptography encryption key is same as the decryption key. But, in asymmetric cryptography, also known as public key cryptography, encryption key is different from the decryption key.

1.12 FURTHER READINGS

1) http://www.mit.gov.in/it-bill.asp Information Technology Act 2000, India.

2) *Cryptography and Network Security, Principles and Practice*, William Stallings –SE, PE.

3) *RSA Security's Official Guide to Cryptography*, Steve Burnett and Stephen Paine – RSA Press.

4) http://www.cca.gov.in Controller of Certifying Authorities, Web Site.

5) *Security in Computer*, Charles P. Pfleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education.