CW3551 DATA AND Information Security

Cryptography and Network Security (Panimalar Institute of Technology)

CW3551 DATA AND INFORMATION SECURITY

COURSE OBJECTIVES:

- To understand the basics of Information Security
- To know the legal, ethical and professional issues in Information Security
- To equip the students' knowledge on digital signature, email security and web security

UNIT I INTRODUCTION 9

History, What is Information Security?, Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

UNIT II SECURITY INVESTIGATION 9

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues - An Overview of Computer Security - Access Control Matrix, Policy-Security policies, Confidentiality policies, Integrity policies and Hybrid policies

UNIT III DIGITAL SIGNATURE AND AUTHENTICATION 9

Digital Signature and Authentication Schemes: Digital signature-Digital Signature Schemes and their Variants- Digital Signature Standards-Authentication: Overview- Requirements Protocols - Applications - Kerberos -X.509 Directory Services

UNIT IV E-MAIL AND IP SECURITY 9

E-mail and IP Security: Electronic mail security: Email Architecture -PGP – Operational Descriptions- Key management- Trust Model- S/MIME.IP Security: Overview- Architecture - ESP, AH Protocols IPSec Modes – Security association - Key management.

UNIT V WEB SECURITY 9

Web Security: Requirements- Secure Sockets Layer- Objectives-Layers -SSL secure communication- Protocols - Transport Level Security. Secure Electronic Transaction- Entities DS Verification-SET processing.

COURSE OUTCOMES:

Upon successful completion of this course, students will be able to:

CO1: Understand the basics of data and information security
CO2:Understand the legal, ethical and professional issues in information security
CO3: Understand the various authentication schemes to simulate different applications.
CO4:Understand various security practices and system security standards
CO5:Understand the Web security protocols for E-Commerce applications

TOTAL :45 PERIODS

TEXT BOOKS:

1. Michael E Whitman and Herbert J Mattord, "Principles of Information Security, Course Technology, 6th Edition, 2017.

2. Stallings William. Cryptography and Network Security: Principles and Practice, Seventh Edition, Pearson Education, 2017.

REFERENCES

1. Harold F. Tipton, Micki Krause Nozaki,, "Information Security Management Handbook, Volume 6, 6th Edition, 2016.

2. Stuart McClure, Joel Scrambray, George Kurtz, "Hacking Exposed", McGraw- Hill, Seventh Edition, 2012.

3. Matt Bishop, "Computer Security Art and Science, Addison Wesley Reprint Edition, 2015.

4. Behrouz A Forouzan, Debdeep Mukhopadhyay, Cryptography And network security, 3rd Edition, . McGraw-Hill Education, 2015.

WHAT IS SECURITY?

Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts. In general, security is defined as "the quality or state of being secure—to be free from danger."

Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another.

Specialized areas of security

- **Physical security**, which encompasses strategies to protect people, physical assets, and the workplace from various threats including fire, unauthorized access, or natural disasters
- **Personal security**, which overlaps with physical security in the protection of the people within the organization
- **Operations security**, which focuses on securing the organization's ability to carry out its operational activities without interruption or compromise
- **Communications security**, which encompasses the protection of an organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives
- **Network security**, which addresses the protection of an organization's data networking devices, connections, and contents, and the ability to use that network to accomplish the organization's data communication functions
- **Information security** includes the broad areas of information security management, computer and data security, and network security.

Where it has been used?

- Governments, military, financial institutions, hospitals, and private businesses.

- Protecting confidential information is a business requirement.

Information Security components:

- Confidentiality
- Integrity
- Availability(CIA)

CIA Triangle

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.

CRITICAL CHARACTERISTICS OF INFORMATION

- Confidentiality

  Integrity

- Availability

  Privacy

  Identification

  Authentication

  Authorization

  Accountability

- Accuracy

Utility

Possession

1 Confidentiality

Confidentiality of information ensures that only those with sufficient privileges may access certain information. When unauthorized individuals or systems can access information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users Example, a credit card transaction on the Internet.
    - The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored.
    - Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information, it could result in a breach of confidentiality.

Integrity

Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted.

- Integrity means that data cannot be modified without authorization.

- Eg: Integrity is violated when an employee deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast a very large number of votes in an online poll, and so on.

2 Availability

Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format. A user in this definition may be either a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users.

- For any information system to serve its purpose, the information must be available when it is needed.

- Eg: High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Privacy

The information that is collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected. This definition of privacy does focus on freedom from observation (the meaning usually associated with the word), but rather means that information will be used only in ways known to the person providing it.

Identification

An information system possesses the characteristic of identification when it is able to recognize individual users. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted.

Authentication

Authentication occurs when a control provides proof that a user possesses the identity that he or she claims.

- In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents(electronic or physical) are genuine(i.e. they have not been forged or fabricated)

Authorization

After the identity of a user is authenticated, a process called authorization provides assurance that the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

Accountability

The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process. For example, audit logs that track user activity on an information system provide accountability.

3 Accuracy

Information should have accuracy. Information has accuracy when it is free from mistakes or errors and it has the value that the end users expects. If information contains a value different from the user's expectations, due to the intentional or unintentional modification of its content, it is no longer accurate.

Utility

Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful. Thus, the value of information depends on its utility.

Possession

The possession of Information security is the quality or state of having ownership or control of some object or item.

NSTISSC SECURITY MODEL

‘National Security Telecommunications & Information systems security committee’ document.

It is now called **the National Training Standard for Information security professionals.**

The NSTISSC Security Model provides a more detailed perspective on security.

While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.

Another weakness of using this model with too limited an approach is to view it from a single perspective.

- The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today’s Information systems.

- To ensure system security, each of the 27 cells must be properly addressed during the security process.

- For example, the intersection between technology, Integrity & storage areas requires a control or safeguard that addresses the need to use technology to protect the Integrity of information while in storage.

NSTISSC SECURITY MODEL

‘National Security Telecommunications & Information systems security committee’ document.

It is now called **the National Training Standard for Information security professionals.**

The NSTISSC Security Model provides a more detailed perspective on security.

While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.

Another weakness of using this model with too limited an approach is to view it from a single perspective.

- The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's Information systems.

- To ensure system security, each of the 27 cells must be properly addressed during the security process.

- For example, the intersection between technology, Integrity & storage areas requires a control or safeguard that addresses the need to use technology to protect the Integrity of information while in storage.

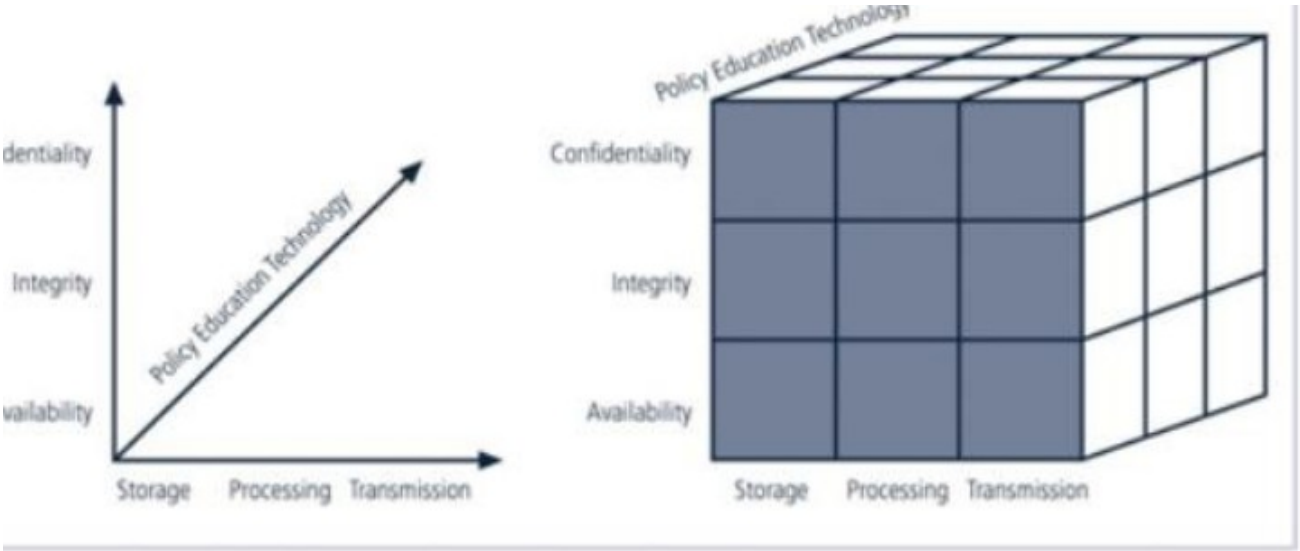

Figure 1.4.1 NSTISSC Security Model

Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts. In general, security is defined as "the quality or state of being secure—to be free from danger."

Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another.

COMPONENTS OF AN INFORMATION SYSTEM

- Software
- Hardware
- Data

- People
- Procedures
- Networks
-

ü **Software**

The software components of IS comprises applications, operating systems, and assorted command utilities.

Software programs are the vessels that carry the lifeblood of information through an organization. These are often created under the demanding constraints of project management, which limit time, cost, and manpower.

ü **Hardware**

Hardware is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system.

Physical security policies deal with hardware as a physical asset and with the protection of these physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system.

Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

-

ü **Data**

Data stored, processed, and transmitted through a computer system must be protected.

-

Data is often the most valuable asset possessed by an organization and is the main target of intentional attacks.

-

The raw, unorganized, discrete(separate, isolated) potentially-useful facts and figures that are later processed(manipulated) to produce information.

ü **People**

There are many roles for people in information systems. Common ones include

Systems Analyst

Programmer

Technician

Engineer

Network Manager

MIS (Manager of Information Systems)

Data entry operator

ü **Procedures**

A procedure is a series of documented actions taken to achieve something. A procedure is more than a single simple task. A procedure can be quite complex and involved, such as performing a backup, shutting down a system, patching software.

ü **Networks**

When information systems are connected to each other to form Local Area Network (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.

Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

SECURING COMPONENTS

Protecting the components from potential misuse and abuse by unauthorized users.

Subject of an attack

Computer is used as an active tool to conduct the attack.

Object of an attack

Computer itself is the entity being attacked

Two types of attacks:

1. **Direct attack**
2. **Indirect attack**

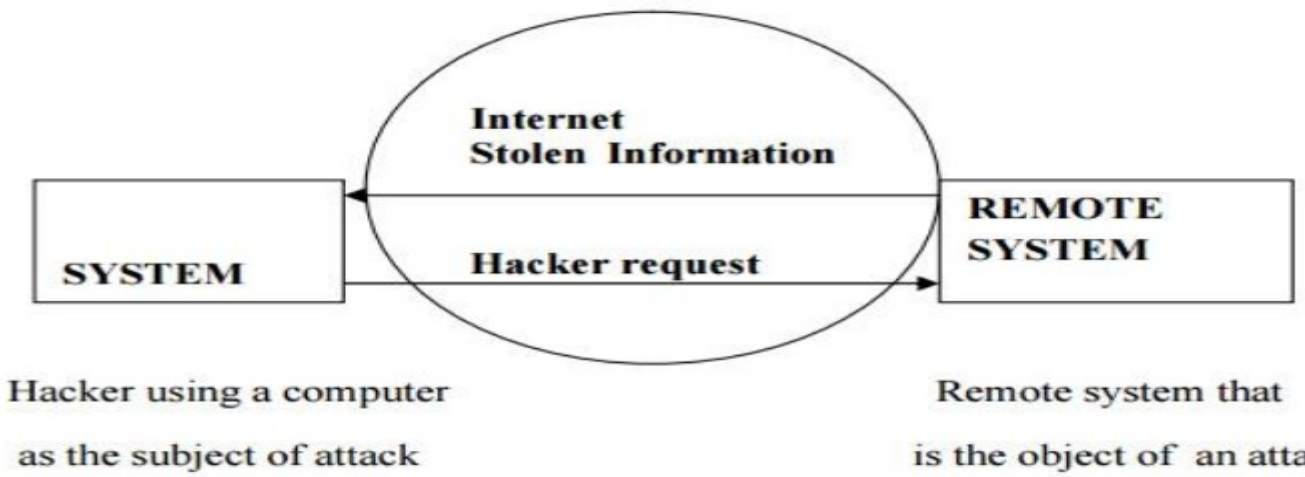

Figure 1.6.1 Attack

1. Direct attack

When a Hacker uses his personal computer to break into a system.[Originate from the threat itself]

2. Indirect attack

When a system is compromised and used to attack other system.

[Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

A computer can, therefore, be both the subject and object of an attack when ,for example, it is first the object of an attack and then compromised and used to attack other systems, at which point it becomes the subject of an attack.

BALANCING INFORMATION SECURITY AND ACCESS

Has to provide the security and is also feasible to access the information for its application.

Information Security cannot be an absolute: it is a process, not a goal.

Should balance protection and availability.

Approaches to Information Security Implementation

- Bottom- up- approach.
- Top-down-approach
  - Has higher probability of success.
  - Project is initiated by upper level managers who issue policy & procedures & processes.
  - Dictate the goals & expected outcomes of the project.

˜ Determine who is suitable for each of the required action.

THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

SDLC Waterfall Methodology

SDLC-is a methodology for the design and implementation of an information system in an organization.

- A methodology is a formal approach to solving a problem based on a structured sequence of procedures.
- SDLC consists of 6 phases.

Investigation

It is the most important phase and it begins with an examination of the event or plan that initiates the process.

During this phase, the objectives, constraints, and scope of the project are specified.

At the conclusion of this phase, a feasibility analysis is performed, which assesses the economic, technical and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

Analysis

It begins with the information gained during the investigation phase.

It consists of assessments (quality) of the organization, the status of current systems, and the capability to support the proposed systems.

Analysts begin by determining what the new system is expected to do, and how it will interact with existing systems.

This phase ends with the documentation of the findings and an update of the feasibility analysis.

Logical Design

In this phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem.

Based on the business need, applications are selected that are capable of providing needed services.

Based on the applications needed, data support and structures capable of providing the needed inputs are then chosen.

In this phase, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits.

At the end of this phase, another feasibility analysis is performed.

Physical design

In this phase, specific technologies are selected to support the solutions developed in the logical design.

The selected components are evaluated based on a make-or-buy decision.

Final designs integrate various components and technologies.

Implementation

In this phase, any needed software is created.

Components are ordered, received and tested.

Afterwards, users are trained and supporting documentation created.

Once all the components are tested individually, they are installed and tested as a system.

Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

Maintenance and change

It is the longest and most expensive phase of the process.

It consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle.

Periodically, the system is tested for compliance, with business needs.

Upgrades, updates, and patches are managed.

As the needs of the organization change, the systems that support the organization must also change.

When a current system can no longer support the organization, the project is terminated and a new project is implemented.

THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE (SEC SDLC)

The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project.

1 Sec SDLC phases

Investigation

- This phase begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints.
- Frequently, this phase begins with an **enterprise information security policy**, which outlines the implementation of a security program within the organization.

- Teams of responsible managers, employees, and contractors are organized.
- Problems are analyzed.
- Scope of the project, as well as specific goals and objectives, and any additional constraints not covered in the program policy, are defined.
- Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

Analysis

- In this phase, the documents from the investigation phase are studied.
- The developed team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls.
- The risk management task also begins in this phase.

Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the

information stored and processed by the organization.

Logical design

- This phase creates and develops the blueprints for information security, and examines and implements key policies.
- The team plans the incident response actions.
- Plans business response to disaster.

- Determines feasibility of continuing and outsourcing the project.

Physical design

- In this phase, the information security technology needed to support the blueprint outlined in the logical design is evaluated.
- Alternative solutions are generated.
- Designs for physical security measures to support the proposed technological solutions are created.
- At the end of this phase, a feasibility study should determine the readiness of the organization for the proposed project.
- At this phase, all parties involved have a chance to approve the project before implementation begins.

Implementation

- Similar to traditional SDLC
- The security solutions are acquired (made or bought), tested, implemented, and tested again
- Personnel issues are evaluated and specific training and education programs are conducted.
- Finally, the entire tested package is presented to upper management for final approval.

Maintenance and change

- Constant monitoring, testing, modification, updating, and repairing to meet changing threats have been done in this phase.

Security Professionals and the organization

Senior management

Chief information Officer (CIO) is the responsible for

- Assessment
- Management
- And implementation of information security in the organization

Information Security Project Team

Champion

- ü Promotes the project
- ü Ensures its support, both financially & administratively.

Team Leader

- ü Understands project management
- ü Personnel management
- ü And information Security technical requirements.

Security policy developers

individuals who understand the organizational culture,

existing policies

Requirements for developing & implementing successful policies.

- **Risk assessment specialists**

Individuals who understand financial risk assessment techniques.

The value of organizational assets,

and the security methods to be used.

- **Security Professionals**

Dedicated

Trained, and well educated specialists in all aspects of information security from both a technical and non technical stand point.

- **System Administrators**

Administrating the systems that house the information used by the organization.

- **End users**

Data Owners

1. Responsible for the security and use of a particular set of information.

2. Determine the level of data classification

3. Work with subordinate managers to oversee the day-to-day administration of the data.

Data Custodians

1 Responsible for the storage, maintenance, and protection of the information.

2 Overseeing data storage and backups

3 Implementing the specific procedures and policies.

Data Users (End users)

· Work with the information to perform their daily jobs supporting the mission of the organization.

· Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

4. Key Terms in Information Security Terminology

- **Asset**

-An asset is the organizational resource that is being protected. -An Asset can be logical ,such a

Website, information or data

Asset can be physical, such as person , computer system

Attack

- An attack is an intentional or unintentional attempt to cause damage to or otherwise compromise the information and /or the systems that support it. If someone casually reads sensitive information not intended for his use, this is considered a passive attack. If a hacker attempts to break into an information system, the attack is considered active.

Risk

- Risk is the probability that something can happen. In information security, it could be the probability of a threat to a system.

Security Blueprint

- It is the plan for the implementation of new security measures in the organization. Sometimes called a frame work, the blueprint presents an organized approach to the security planning process.

Security Model

A security model is a collection of specific security rules that represents the implementation of a security policy.

Threats

1. A threat is a category of objects, persons, or other entities that pose a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences, while others are purposeful. For example, all hackers represent potential danger or threat to an unprotected information system. Severe storms are also a threat to buildings and their contents.

Threat agent

1. A threat agent is the specific instance or component of a threat. For example, you can think of all hackers in the world as a collective threat, and Kevin Mitnick, who was convicted for hacking into phone systems, as a specific threat agent. Likewise, a specific lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

Vulnerability

1. Weaknesses or faults in a system or protection mechanism that expose information to attack or damage are known as vulnerabilities. Vulnerabilities that have been examined, documented, and published are referred to as **well-known vulnerabilities.**

Exposure

The exposure of an information system is a single instance when the system is open to damage. Vulnerabilities can cause an exposure to potential damage or attack from a threat. Total exposure is the degree to which an organization's assets are at risk of attack from a threat..