Principles of Information Security

Course Code: CS 472 L-T-P-Credits

3-0-0-3

Dr. Abdul Gafur M
CSE Dept. MEA Engineering College, Perinthalmanna

Course Objective

- To introduce fundamental concepts of security
- To introduce and discuss the relevance of security in operating system, web services etc.
- To introduce fundamental concepts of secure electronic transactions

Expected Course Outcome

i. Appreciate the common threats faced today
ii. Interpret the foundational theory behind information security
iii. Design a secure system
iv. Identify the potential vulnerabilities in software
v. Appreciate the relevance of security in various domains
vi. Develop secure web services and perform secure e-transactions

Basic components: Confidentiality, Integrity, Availability

Confidentiality

Confidentiality: Concealment of Information or resources

Applies the “need to know” principle (Military, car design)

Access control mechanism supports confidentiality

Eg. cryptography (if key is not protected, fails)

System dependent mechanism: protect the security of data more completely than cryptography, but if they fail data becomes visible

Confidentiality (Contd..)

- Confidentiality also applies to the existence of data

Eg. Suvey on trust/distrust by politician

Resource hiding is another important aspects of confidentiality- eg. equipment hiding

Assumption and trust is the basis of confidentiality mechanism (eg can rely on kernel)

Integrity

Integrity refers to trustworthiness of data or resources (Preventing improper or unauthorized change]

Integrity includes data integrity and origin integrity [source of data or authentication]

Eg. printing a statement in news paper as it is but source is unauthentic]

Integrity [Contd..]

- Integrity mechanism fall in two classes

Prevention mechanism, Detection Mechanism

Prevention: Blocking unauthorized attempt to change data or Blocking attempt to change data unauthorized way

Detection mechanism may analyze system events to detect problems. This mechanism may report the actual cause of the integrity violations or may simply report that the file is now corrupt.

Availability

- Availability refers to the ability to use the information or resource desired
- Attempt to block availability is called Denial of Service (DoS) attack.
- DoS is most difficult to detect, because the analyst must determine if the unusual access patterns are attributable to deliberate manipulation of resources or of environment.

The need for security

Computer security V/S Information security

Information security includes all the things we use to do business: computers, s/w, procedures, data and people.

Information security primary mission: To ensure things remain same.

Business needs first, Technology needs last

Information security: Four important Functions

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization’s IT systems
3. Protects the data the organisation collects and uses
4. Safeguards the technology assets in use at the organization

Threats

- A threat is an object, person or other entity that represents a constant danger to an asset.
- Threat is a potential violation of security

Deliberate Software Attacks

- Deliberate software attacks occur when an individual or group designs software to attack an unsuspecting system
- Most of this software is referred to as malicious code or malicious software or malware
- Eg. virus., worms, Trojan horses, logic-bombs and back doors

[instances of high impact software attack]

Deliberate Software Attacks (Contd.)

- Virus:- segments of code that perform malicious actions
- The code attaches itself to the existing program and takes control of that program's access to the targeted computer.
- Virus controlled target program then carries out the virus plan, by replicating itself into additional targeted system.

Deliberate Software Attacks (Contd.)

Macro virus: embedded in automatically executing macro code, common in word processors, spreadsheets and database applications.

Boot virus: infects the key operating systems files located in a computer's boot sector

Worms: replicate themselves constantly without requiring another program to provide a safe environment for replication.

Deliberate Software Attacks (Contd.)

- Trojan horses: hide their true nature, and reveal their designed behavior only when activated.
- Back door or Trap door: malicious computer program used to provide the attacker with unauthorized remote access to a compromised PC by exploiting security vulnerabilities. This **backdoor virus** works in the background and hides from the user. It is quite difficult to detect as it is very similar to other malware **viruses**

Deliberate Software Attacks (Contd.)

- Virus and worm Hoaxes: A **computer virus/worm hoax** is a message warning the recipients of a non-existent computer virsus/worm. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know.

Deliberate Software Attacks (Contd.)

Password crack: attempting to reverse calculate a password is often called cracking

[demonstration].

Brute force: applications which try every possible combination of a password, also called password attack.

Control the limit the number of attempts allowed per unit of elapsed time are very effective to prevent such attack

Deliberate Software Attacks (Contd.)

Timing attack: A **timing attack** is **security** exploit that allows an attacker to discover vulnerabilities in the **security** of a computer or network system by studying how long it takes the system to respond to different inputs.

Another timing attack is the exploring the contents of a web browser's cache.

Deliberate Software Attacks (Contd.)

- Sniffers: a program or device that can monitor data travelling over a network
- It can be used both for legitimate network management functions and for stealing information from a network.
- Virtually impossible to detect and can be inserted anywhere
- They often work on TCP/IP networks (called packet sniffers)