FIT2093
INTRODUCTION TO CYBER SECURITY

Exam Date: 14/06/2017

Week 1 - Introduction to Cyber Security

What is cyber security?

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Ways of Protection

- Prevention - preventing a breach of security.
- Detection - investigating a security breach.
- Recover - recovering the system after an attack.

We need to protect data in order to preserve **confidentiality, integrity** and **availability** of information.

Security Mechanisms are designed to detect, prevent or recover from a security attack. Hence multiple mechanisms are required.

Level of Impact

- Low: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- Moderate: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

- High: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

———

Confidentiality

- Sensitive information can only be accessed by authorised parties.
- Access can be in the form of reading, copying & distributing.
- **Tools used:** *Encryption, Authentication & Access Control*

Integrity

- Protecting information from unauthorised modification.
- To ensure authenticity of data. (It should be genuine, and not just appear genuine)
- Ensuring **non-repudiation**,prevents the sender and the receiver from denying a transmitted message.
- **Tools used:** *Backups, Checksums & Digital Signatures*

Availability

- The information should be accessible and useable (without delay) upon demand by an authorised entity.
- **Tools used:** *Physical protections & Computational Redundancies* (Computers and Servers as fallbacks in case of failure)

———

Security Attacks

Interruption (Denial-of-Service)

Information resources (hardware, software and data) are deliberately made unavailable, lost or unusable, usually through malicious destruction.
Example: Cutting your home phone/cable modem line, disabling a file management system, email spam to fill up the mail queue and slow down an email server, etc..

Interception (Unauthorised Access)

Difficult to trace as no traces of intrusion might be left.
Example: Illegal eavesdropping or wiretapping or sniffing, illegal copying.

Modification (Tampering a Resource)

Resources can be data, programs, hardware devices, etc.

Example: man-in-the-middle attack where a network stream is intercepted, modified and retransmitted.

Fabrication (Counterfeiting)

Allows to bypass the authenticity checks.

Impersonating/Masquerading in-order to gain access to data/services/etc by pretending to be a different entity.

Example: Insertion of spurious messages in a network, adding a record to a file, counterfeit banknotes, fake cheque, etc.

Repudiation

The denial of a commitment or data receipt.

This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.

Tools used: Digital Signatures

Network Security Attacks

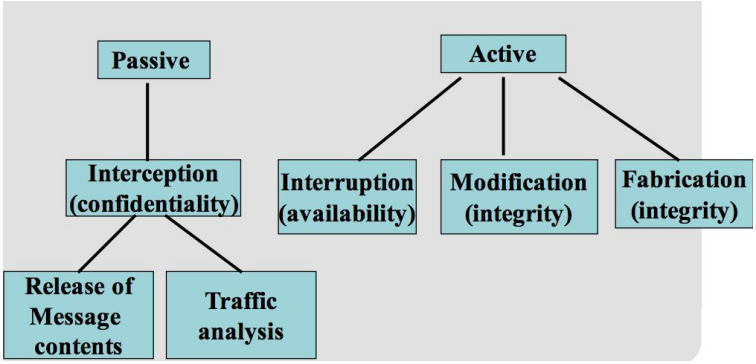
- **Passive Attacks** - Eavesdropping
    - Release of message contents
    - Traffic analysis
    - Are hard to detect so aim to prevent
- **Active Attacks** - Modify / Fake data
    - Masquerade
    - Replay
    - Modification
    - Denial of service
    - Hard to prevent so aim to detect

Passive Attacks

- Release of message contents - opponent learns contents of sensitive transmissions.
- Traffic analysis - can occur even when contents of messages are masked (e.g encryption)
- The goal is to obtain information to breach **confidentiality** property.

Active Attacks

- Active attacks involve modification of data stream or creation of false data.
- Masquerade - when one entity pretends to be another.
- Replay - passive capture of data and subsequent retransmission.
- Modification of messages - a legitimate message is altered, delayed or reordered.
- Denial of service prevents or inhibits the normal use or management of communications facilities, or the disruption of an entire network.
- Violating **integrity, availability** properties.



Principles of Security

- Principle of **easiest penetration** – an intruder will use any means of penetration.
- Principles of **timeliness** – items only need to be protected until they lose their value.
- Principles of **effectiveness** – controls must work, and they should be efficient, easy to use, and appropriate.

X.800 Security Architecture

Systematic way of defining requirements for security and characterizing approaches to satisfying them.

———

Week 2 - Authentication

User Authentication is the process of verifying an identity claimed by or for a system entity. It has two steps:

- Identification - specify identifier
- Verification - bind entity (person) and identifier

4 means of user authentication, based on something you:

➔ **Know** - e.g. password, PIN (SYK)
➔ **Possess** - e.g. key, token, smartcard (SYH)
➔ **Are (static biometrics)** - e.g. fingerprint, retina (SYA)
➔ **Do (dynamic biometrics)** - e.g. voice, sign (SYA)

They can be used alone or combined. All of them have their own issues.

———

Password Vulnerabilities

- Offline dictionary attack • specific account attack • popular password attack • password guessing against single user • workstation hijacking • exploiting user mistakes • exploiting multiple password use • electronic monitoring

Countermeasures

- Controls to prevent unauthorized access to password file • intrusion detection measures • Rapid reissuance of compromised passwords • account lockout mechanisms • policies against using common passwords but rather hard to guess

passwords • training & enforcement of password policies • automatic workstation logout • encrypted network links

———

Two strategies to store passwords:

- Transform the password into something else. (Encryption) **Windows**
- Use the password itself to transform into something else. (Hashing) **Unix**

———

A **hash function** is a function that can be used to turn data into relatively smaller format that may serve as digital representation of the data; however you will not be able to derive the data from its derivative.

The derivative is called a **message digest**.

A good hashing algorithm will produce small (almost negligible) number of collisions.

Increasing the length of the hash code can reduce the probability of collision.

———

In the Linux operating system, a **shadow password** file is a system file in which encryption user password are stored so that they aren't available to people who try to break into the system. Ordinarily, user information, including passwords, is kept in a system file called /etc/passwd .

———

Stable Biometric
Does not change from one session to another.
Relatively static.
Fingerprint, Face, Hand, Iris, Retina.

Alterable Biometric
Can be altered easily if necessary.
Voice, Keystrokes pattern.