Week 2: Information System Security Fundamentals

Ayman El Hajjar

6COSC002W - Security and Forensics

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

25 January 2021

University of Westminster

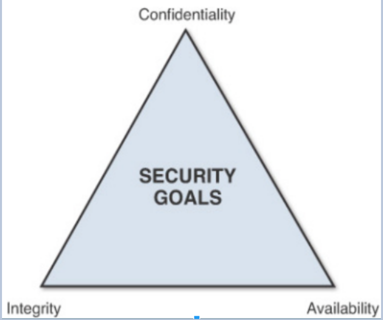
Session Overview

1. Security Fundamentals
2. Information systems security
3. Domains of an IT infrastructure
4. The Ten Security Principles

Security Definition

- What is Computer Security?
  - The protection of computing systems and the data that they store or access, including defense against attack, interference, espionage, etc.
- Why is Computer Security Important?
  - Enable people to carry out their jobs, education, and research.
  - Support critical business process.
  - Protecting personal and sensitive information.
- Why do I need to learn about Computer Security? Isn't this just an I.T. problem?
  - 10% of security safeguards are technical.
  - 90% of security safeguards rely on the computer user ("YOU") to adhere to good computing practices

Security Goals



- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

Goal: Integrity

- Availability models keep data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:
  - Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)
  - Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
  - Equipment failures during normal use

Goal: Confidentiality

- Keep data and communication secret
- Privacy of personal financial/health records, etc
- Military and commercial relevance

A succinct definition

Security is ensuring that only authorised people can perform authorised actions, without interference from others and without risk of data interception.

Security – who is responsible?

- So who is responsible for security in a system/network? and What issues are important with respect to security?
  - The programmers who designed the software?
  - The hardware designers?
  - The users?
- Everybody is responsible for security
- Security is like a chain... it is only as strong as the weakest link
- What is the point of having all kinds of fancy protection if the culture is such that users "lend" account details to others, and compromise the network from inside?
- So what are the general principles of (reasonable) security?

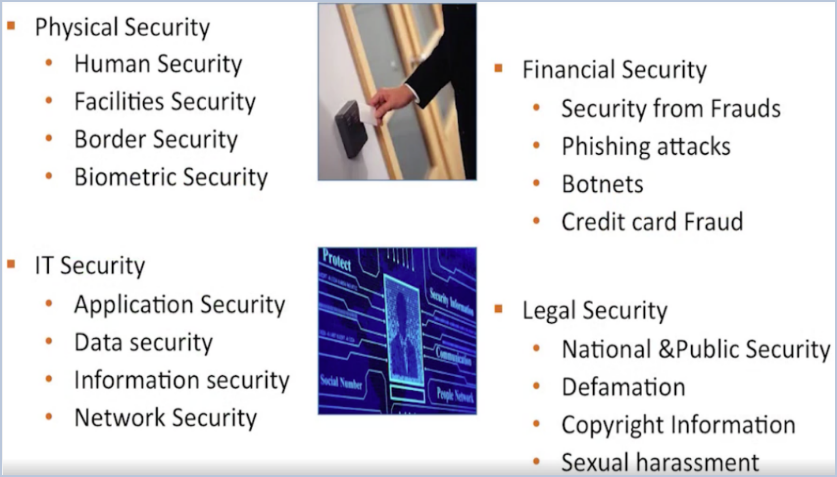
Security principles

- Security is not an "add-on" or an extra; It should be considered from the very beginning upwards.
- No security can make a system 100
  - The only way to do that would be to take a totally secure machine, with no external connections of any kind (network, mouse, keyboard) and lock it in a safe
  - Not very useful, and even that wouldn't quite be 100% uncrackable!
- security is a trade-off between total security and usability.
- Security should not rely on keeping the inner workings "secret" - this is security by obscurity, and as soon as the "cat is out of the bag" it is not much better than having no security at all.

Security Policy

- Security policy is a written statement describing what assets are to be protected and why, who is responsible, which behaviours are acceptable or not.
- The policy address
  - Physical security
  - Network security
  - Access authorisations
  - Virus protection
  - Disaster recovery

Aspects of organizational security



- Physical Security
  - Human Security
  - Facilities Security
  - Border Security
  - Biometric Security
- IT Security
  - Application Security
  - Data security
  - Information security
  - Network Security
- Financial Security
  - Security from Frauds
  - Phishing attacks
  - Botnets
  - Credit card Fraud
- Legal Security
  - National &Public Security
  - Defamation
  - Copyright Information
  - Sexual harassment

Risks, Threats, and Vulnerabilities

Risk

Likelihood that something bad will happen to an asset

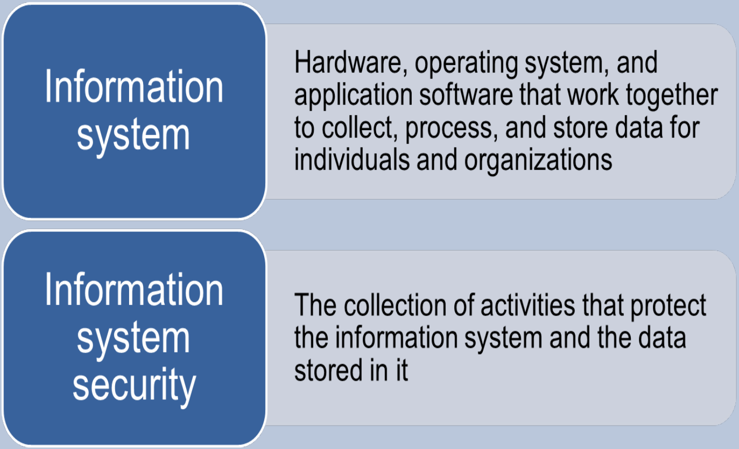
Threat

Any action that could damage an asset

Vulnerability

A weakness that allows a threat to be realized or to have an effect on an asset

What Is Information Systems Security?



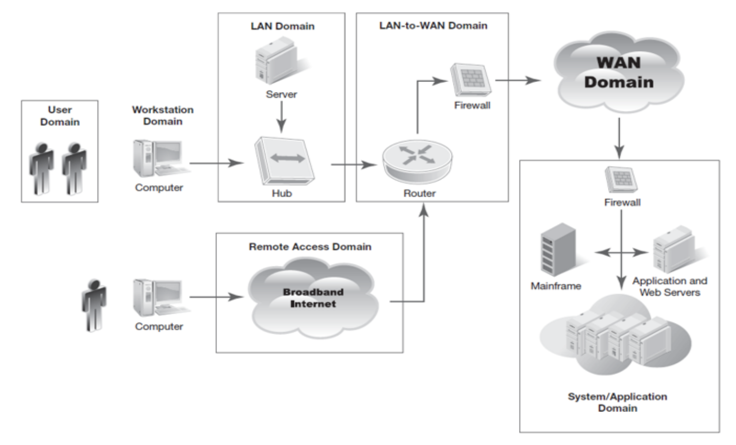
Information system

Hardware, operating system, and application software that work together to collect, process, and store data for individuals and organizations

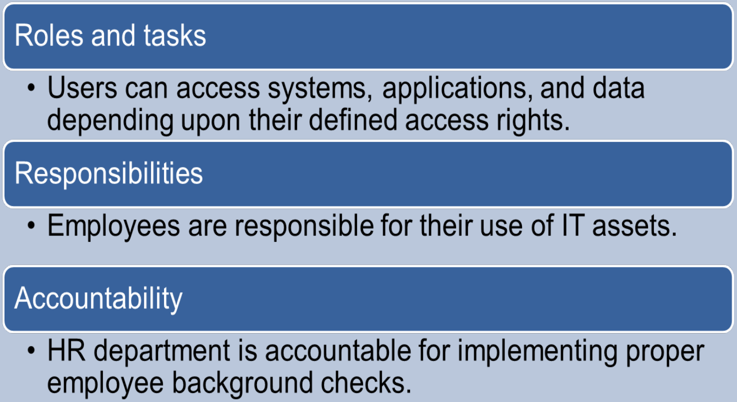
Information system security

The collection of activities that protect the information system and the data stored in it

Seven Domains of a Typical IT Infrastructure



User Domain



Roles and tasks

- Users can access systems, applications, and data depending upon their defined access rights.

Responsibilities

- Employees are responsible for their use of IT assets.

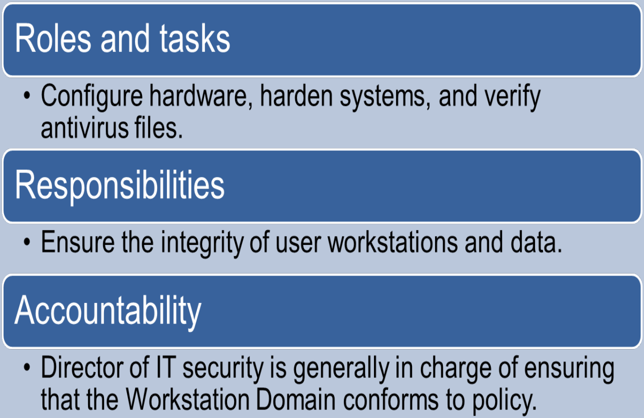
Accountability

- HR department is accountable for implementing proper employee background checks.

Common Threats in the User Domain

- Lack of user awareness
- User apathy toward policies
- User violating security policy
- User inserting CD/USB with personal files
- User downloading photos, music, or videos
- User destructing systems, applications, and data
- Disgruntled employee attacking organization or committing sabotage
- Employee blackmail or extortion

Workstation Domain



Roles and tasks

- Configure hardware, harden systems, and verify antivirus files.

Responsibilities

- Ensure the integrity of user workstations and data.

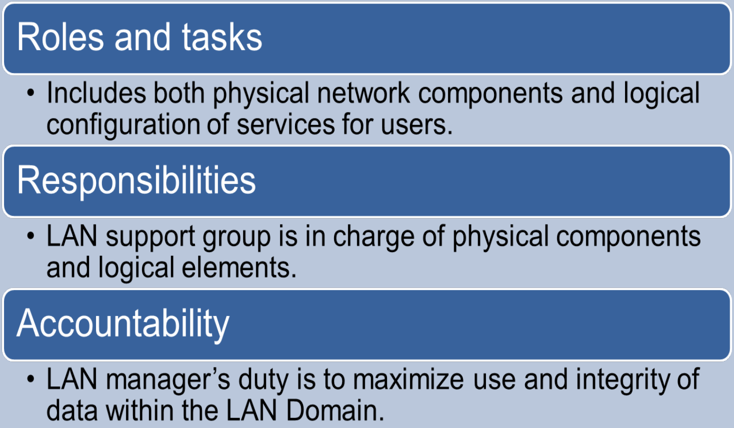
Accountability

- Director of IT security is generally in charge of ensuring that the Workstation Domain conforms to policy.

Common Threats in the Workstation Domain

- Unauthorized workstation access
- Unauthorized access to systems, applications, and data
- Desktop or laptop operating system vulnerabilities
- Desktop or laptop application software vulnerabilities or patches
- Viruses, malicious code, and other malware
- User inserting CD/DVD/USB with personal files
- User downloading photos, music, or videos

LAN Domain



Roles and tasks

- Includes both physical network components and logical configuration of services for users.

Responsibilities

- LAN support group is in charge of physical components and logical elements.

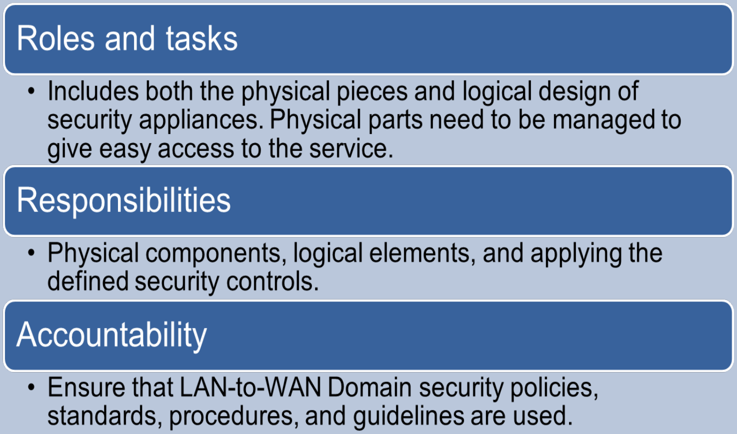
Accountability

- LAN manager's duty is to maximize use and integrity of data within the LAN Domain.

Common Threats in the LAN Domain

- Unauthorized physical access to LAN
- Unauthorized access to systems, applications, and data
- LAN server operating system vulnerabilities
- LAN server application software vulnerabilities and software patch updates
- Rogue users on WLANs
- Confidentiality of data on WLANs
- LAN server configuration guidelines and standards

LAN-to-WAN Domain



Roles and tasks

- Includes both the physical pieces and logical design of security appliances. Physical parts need to be managed to give easy access to the service.

Responsibilities

- Physical components, logical elements, and applying the defined security controls.

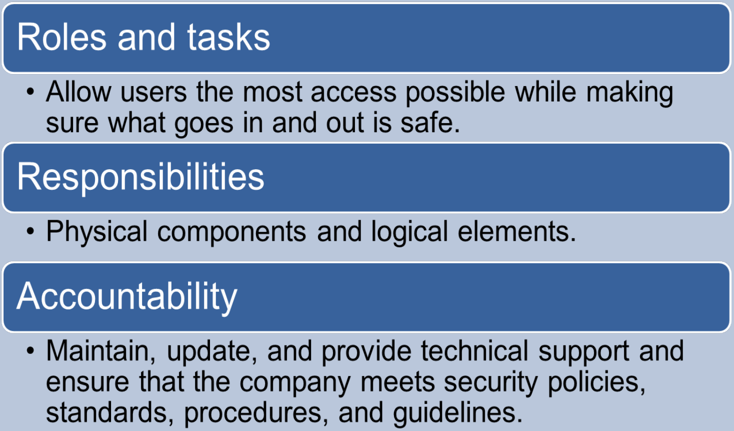
Accountability

- Ensure that LAN-to-WAN Domain security policies, standards, procedures, and guidelines are used.

Common Threats in the LAN-to-WAN Domain

- Unauthorized probing and port scanning
- Unauthorized access
- IP router, firewall, and network appliance operating system vulnerability
- Download of unknown file type attachments from unknown sources
- Unknown email attachments and embedded URL links received by local users

WAN Domain



Roles and tasks

- Allow users the most access possible while making sure what goes in and out is safe.

Responsibilities

- Physical components and logical elements.

Accountability

- Maintain, update, and provide technical support and ensure that the company meets security policies, standards, procedures, and guidelines.

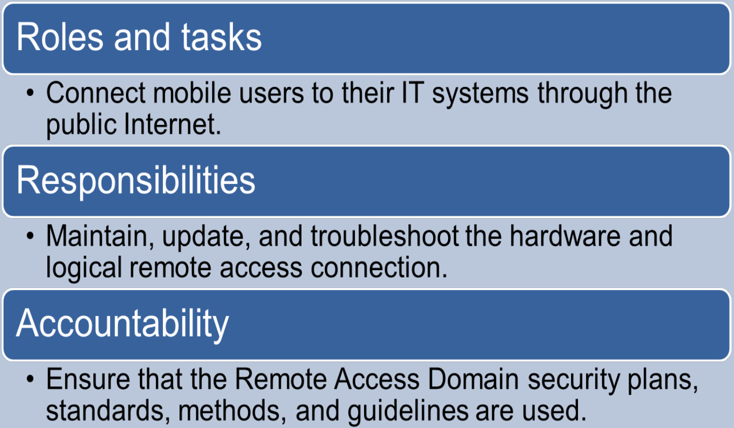
Common Threats in the WAN Domain (Internet)

- Open, public, and accessible data
- Most traffic being sent as cleartext
- Vulnerable to eavesdropping
- Vulnerable to malicious attacks
- Vulnerable to denial of service (DoS) and distributed denial of service (DDoS) attacks
- Vulnerable to corruption of information/data
- Insecure TCP/IP applications

Common Threats in the WAN Domain (Connectivity)

- WAN IP traffic on the same service provider router and infrastructure from different people getting mixed
- Maintaining high WAN service availability
- Using SNMP network management applications and protocols maliciously (ICMP, Telnet, SNMP, DNS, etc.)
- SNMP alarms and security monitoring 24 X 7 X 365

Remote Access Domain



Roles and tasks

- Connect mobile users to their IT systems through the public Internet.

Responsibilities

- Maintain, update, and troubleshoot the hardware and logical remote access connection.

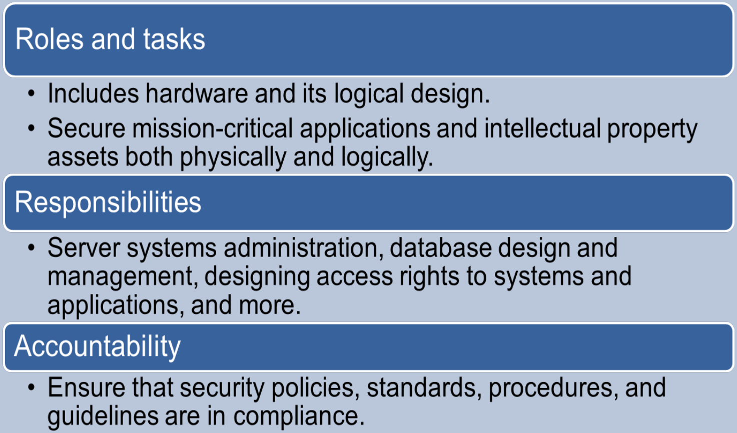
Accountability

- Ensure that the Remote Access Domain security plans, standards, methods, and guidelines are used.

Common Threats in the Remote Access Domain

- Brute-force user ID and password attacks
- Multiple logon retries and access control attacks
- Unauthorized remote access to IT systems, applications, and data
- Confidential data compromised remotely
- Data leakage in violation of data classification standards

System/Application Domain



Roles and tasks

- Includes hardware and its logical design.
- Secure mission-critical applications and intellectual property assets both physically and logically.

Responsibilities

- Server systems administration, database design and management, designing access rights to systems and applications, and more.

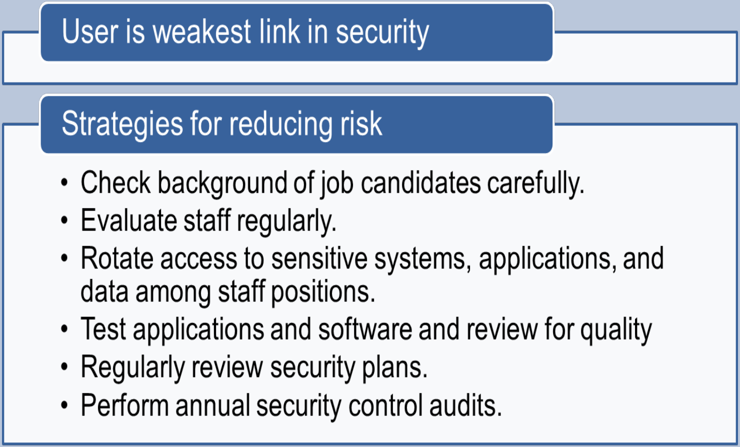
Accountability

- Ensure that security policies, standards, procedures, and guidelines are in compliance.

Common Threats in the System/Application Domain

- Unauthorized access to data centers, computer rooms, and wiring closets
- Downtime of servers to perform maintenance
- Server operating systems software vulnerability
- Insecure cloud computing virtual environments by default
- Corrupt or lost data
- Loss of backed-up data as backup media are reused

Weakest Link in the Security of an IT Infrastructure

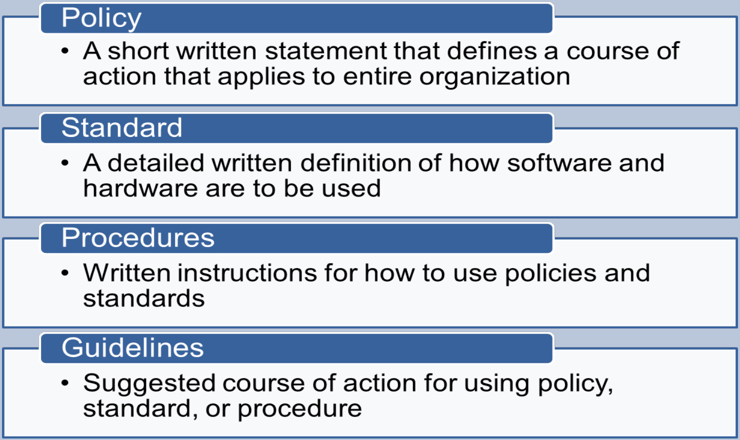


User is weakest link in security

Strategies for reducing risk

- Check background of job candidates carefully.
- Evaluate staff regularly.
- Rotate access to sensitive systems, applications, and data among staff positions.
- Test applications and software and review for quality
- Regularly review security plans.
- Perform annual security control audits.

IT Security Policy Framework



Policy

- A short written statement that defines a course of action that applies to entire organization

Standard

- A detailed written definition of how software and hardware are to be used

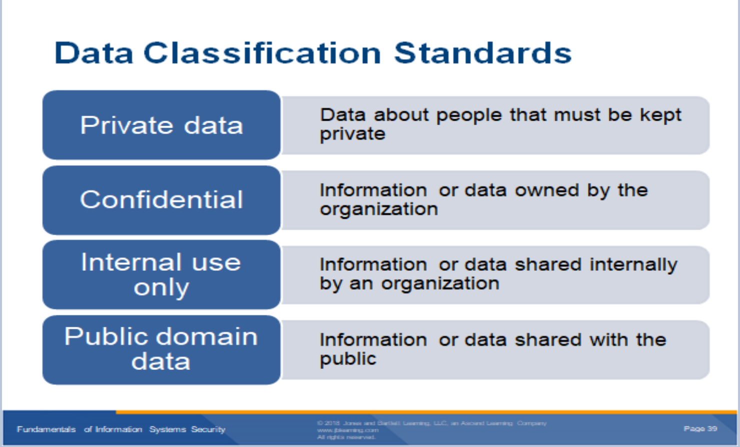
Procedures

- Written instructions for how to use policies and standards

Guidelines

- Suggested course of action for using policy, standard, or procedure

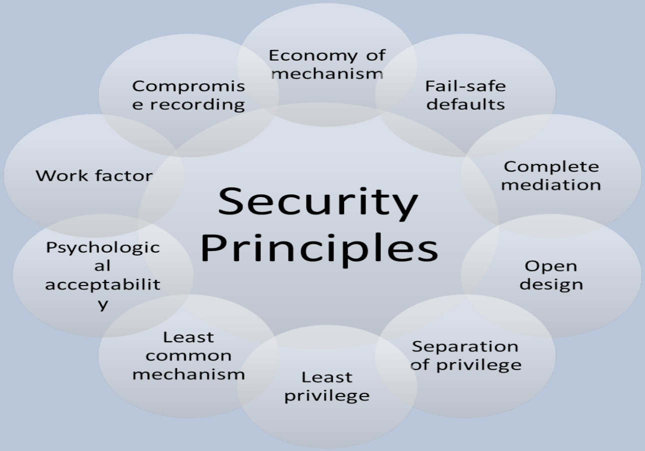
Data Classification Standards



Data Classification Standards

Private data	Data about people that must be kept private
Confidential	Information or data owned by the organization
Internal use only	Information or data shared internally by an organization
Public domain data	Information or data shared with the public

The Ten Security Principles



Security Principles

Economy of mechanism

Fail-safe defaults

Complete mediation

Open design

Separation of privilege

Least privilege

Least common mechanism

Psychologic al acceptabilit y

Work factor

Compromis e recording

Economy of mechanism

- This principle stresses simplicity in the design and implementation of security measures.
    - While applicable to most engineering endeavors, the notion of simplicity is especially important in the security domain, since a simple security framework facilitates its understanding by developers and users and enables the efficient development and verification of enforcement methods for it.

Fail-safe defaults

- This principle states that the default configuration of a system should have a conservative protection scheme.
  - For example, when adding a new user to an operating system, the default group of the user should have minimal access rights to files and services. Unfortunately, operating systems and applications often have default options that favor usability over security.
  - This has been historically the case for a number of popular applications, such as web browsers that allow the execution of code downloaded from the web server.

Complete mediation

- The idea behind this principle is that every access to a resource must be checked for compliance with a protection scheme.
  - As a consequence, one should be wary of performance improvement techniques that save the results of previous authorization checks, since permissions can change over time.
  - For example, an online banking web site should require users to sign on again after a certain amount of time, say, 15 minutes, has elapsed.

Open design

- According to this principle, the security architecture and design of a system should be made publicly available.
  - Security should rely only on keeping cryptographic keys secret.
  - Open design allows for a system to be scrutinized by multiple parties, which leads to the early discovery and correction of security vulnerabilities caused by design errors.
  - The open design principle is the opposite of the approach known as security by obscurity, which tries to achieve security by keeping cryptographic algorithms secret and which has been historically used without success by several organizations.

Separation of privilege

- This principle dictates that multiple conditions should be required to achieve access to restricted resources or have a program perform some action.

Least privilege

- Each program and user of a computer system should operate with the bare minimum privileges necessary to function properly.
    - If this principle is enforced, abuse of privileges is restricted, and the damage caused by the compromise of a particular application or user account is minimized.
    - The military concept of need-to-know information is an example of this principle.

Least common mechanism

- In systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized.
    - For example, if a file or application needs to be accessed by more than one user, then these users should have separate channels by which to access these resources, to prevent unforeseen consequences that could cause security problems.

Psychological acceptability

- This principle states that user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.

Work factor

- According to this principle, the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.
    - A system developed to protect student grades in a university database, which may be attacked by snoopers or students trying to change their grades, probably needs less sophisticated security measures than a system built to protect military secrets, which may be attacked by government intelligence organizations.

Compromise recording

- This principle states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent it.
    - Internet-connected surveillance cameras are a typical example of an effective compromise record system that can be deployed to protect a building in lieu of reinforcing doors and windows.
    - The servers in an office network may maintain logs for all accesses to files, all emails sent and received, and all web browsing sessions.

Summary

- Information systems security concepts
- Confidentiality, integrity, and availability (CIA)
- The seven domains of an IT infrastructure
- The weakest link in the security of an IT infrastructure
- IT security policy framework and data classification standard

Tasks for next week

- Research hackers and crackers
- List different types of hackers – script kiddies to suicide hackers
- Research Information harvesting
- Research Social Engineering Attacks

References

- Resources used:
  - Chapter 1 of the book CEHv10 Certified Ethical Hacker study guide Networks by Ric Messier, published by Sybex 2019. Click here for the online book Library link
- Chapter 1 of the book Fundamentals of Information Systems's Security, 3rd edition, Kim, Jones & Bartlett Learning publisher, October 2016 Click here for the online book library link