CSF3404 Cyber Security

Chapter 1
Security Fundamentals

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli

Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

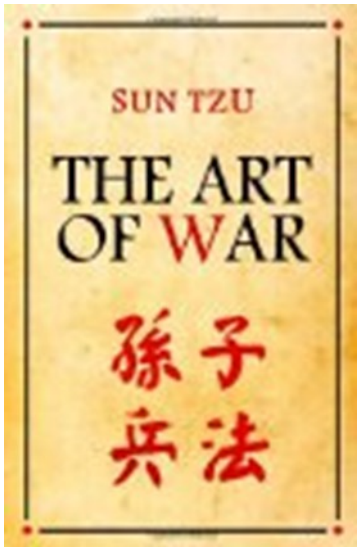
The Art of War

We lead

This quote is from The Art of War.

The art of war teaches us to rely not on the likelihood of the enemy's not coming,
but on our own readiness to receive him;
not on the chance of his not attacking,
but rather on the fact that we have made our position unassailable.

The Art of War, Sun Tzu



What is “Security”

- Dictionary.com says: https://www.dictionary.com/browse/security
  1. Freedom from risk or danger ➔ Safety.
  2. Freedom from doubt, anxiety, or fear ➔ Confidence.
  3. Something that secures or makes safe ➔ Protection ➔ Defense.
  4. Something that gives or assures safety, as:
     - A group or department of private guards: Call building security if a visitor acts suspicious.
     - Measures adopted by a government to prevent espionage, sabotage, or attack.
     - Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.
- …etc.

Common Terminologies

ECSS Common Terminologies (cont'd)

ECSS™ EC-Council Certified Security Specialist

Security:

- A state of well-being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services are kept low or tolerable

Threat:

- An action or event that might compromise security
- A threat is a potential violation of security

Vulnerability:

- Existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system

EC-Council

Information Security

ECSS Information Security

EC-Council Certified Security Specialist

Information security refers to securing the data or information and information systems from the unauthorized access, unauthorized use, misuse, destruction, or alteration

It plays a vital role in protecting the interests of individuals who depend on information or data

The goal of information security is to protect the confidentiality, integrity, and availability of information

EC-Council

Other Definitions

- **Computer Security**

  The protection of computer systems from the theft or damage to the hardware, software or the information on them.

- **Network Security**

  Process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

- **Cyber (Internet) Security**

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

Ref.: Taylor, P. J. & Nufryk, J. (2014) CompTIA Security+, (SY0-401) Logical Operation Choice New York

Security Fundamentals

- There are many different tasks, concepts, and skills involved in the pursuit of computer security. But most of these tasks, concepts, and skills share a few **fundamental principles**.
- Each security implementation starts with a series of fundamental building blocks.
- As a **security professional**, it is your responsibility to understand these fundamental concepts so you can build the appropriate security structure for your organization.

- TOPICS:
  - The Information Security Cycle
  - Information Security Controls
  - Authentication Methods
  - Security Policy Fundamentals
  - Cryptography Fundamentals

What Is Information Security?

UMT
We lead

What Is Information Security?

Information security refers to the protection of available information or information resources from **unauthorized access**, **attacks**, **thefts**, or **data damage**.

Responsible **individuals** and **organizations** must secure their confidential information.

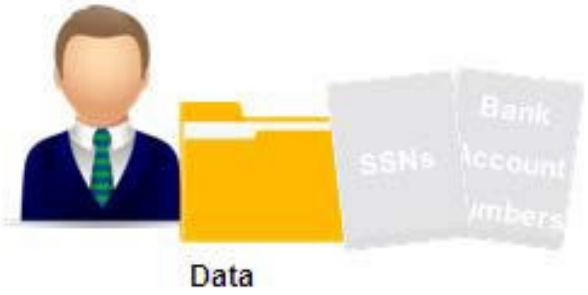
Due to the presence of a widely connected business environment, data is now available in a variety of forms such as **digital media** and **print**. Therefore, every **bit** of data that is being used, shared, or transmitted must be protected to minimize business risks and other consequences of losing crucial data.

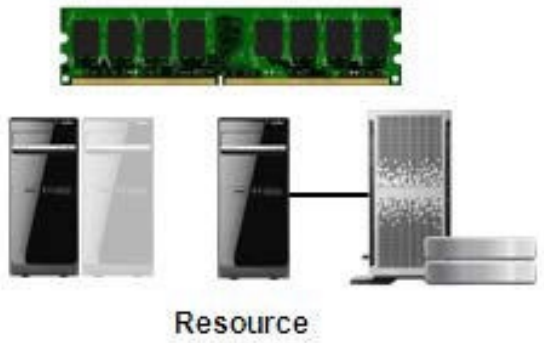
Summary:

- ✓ Protection of available information or information resources.
- ✓ Necessary for a responsible individual or organization to secure confidential information.
- ✓ Minimize business risks and other consequences of losing crucial data.

What to Protect

- As an information security professional, you need to know **what information to secure** in an organization and **why those assets** need protection.
- **Data**
  - This is a general term that relates to the information assets of a person, customer, or organization.
  - In a computer system, the files are the data.
  - You need to protect data from getting corrupt or from being accessed without authorization.
- **Resources**
  - These are any virtual or physical system components that have limited availability.
  - A physical resource is any device connected directly to a computer system.
  - A virtual resource refers to types of files, memory locations, or network connections



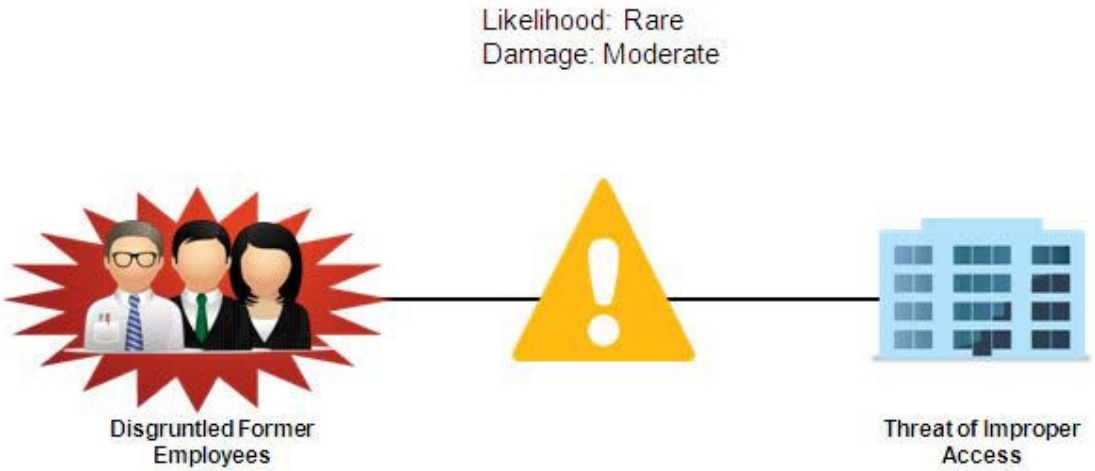


Goals of Security

- **Prevention:**
  - Personal information, company information, and information about intellectual property must be **protected**.
  - If there is a breach in security in any of these areas, then the organization may have to put a lot of effort into recovering losses.
  - Preventing users from gaining **unauthorized access** to confidential information should be the number one priority of information security professionals.
- **Detection:**
  - Detection occurs when a user is discovered trying to access unauthorized data or after information has been lost.
  - It can be accomplished by **investigating individuals** or by **scanning the data and networks** for any traces left by the **intruder** in any attack against the system.
- **Recovery:**
  - When there is a disaster or an intrusion by unauthorized users, system data is sometimes compromised or damaged.
  - It is in these cases that you need to employ a process to recover vital data from a crashed system or data storage devices.
  - Recovery can also pertain to physical resources.

Risk

- As applied to information systems,
  - Risk is a concept that indicates exposure to the chance of damage or loss.
  - It signifies the likelihood of a hazard or dangerous threat occurring.
- In information technology,
  - Risk is often associated with the loss of a system, power, or network, and other physical losses.
- Risk also affects people, practices, and processes.
  - **For example,**
    - A disgruntled former employee is a threat.
    - The amount of risk this threat represents depends on the likelihood that the employee will access his or her previous place of business and remove or damage data.
    - It also depends on the extent of harm that could result.

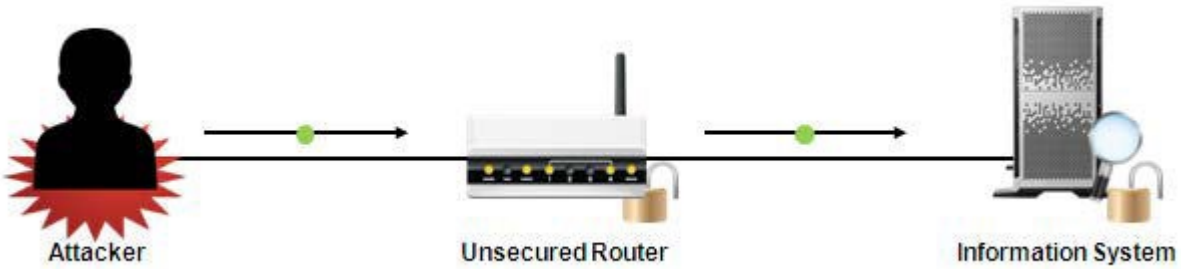


Threats

- In the realm of computer security, a **threat** is any **event** or **action** that could potentially cause damage to an asset.
- Threats are often in violation of a security requirement, policy, or procedure.
- Regardless of whether a violation is intentional or unintentional, malicious or not, it is considered a threat.

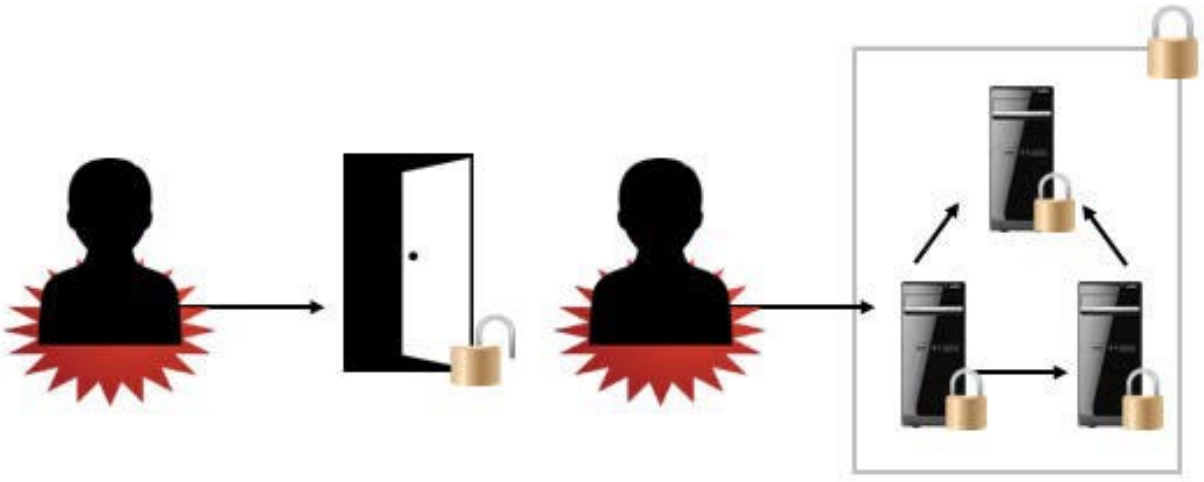
Vulnerabilities

- A vulnerability is any condition that leaves a system open to harm.
- Vulnerabilities can come in a wide variety of forms, including:
  - ✓ Improperly configured or installed hardware or software.
  - ✓ Untested software and firmware patches.
  - ✓ Bugs in software or operating systems.
  - ✓ The misuse of software or communication protocols.
  - ✓ Poorly designed networks.
  - ✓ Poor physical security.
  - ✓ Insecure passwords.
  - ✓ Design flaws in software or operating systems.
  - ✓ Unchecked user input.



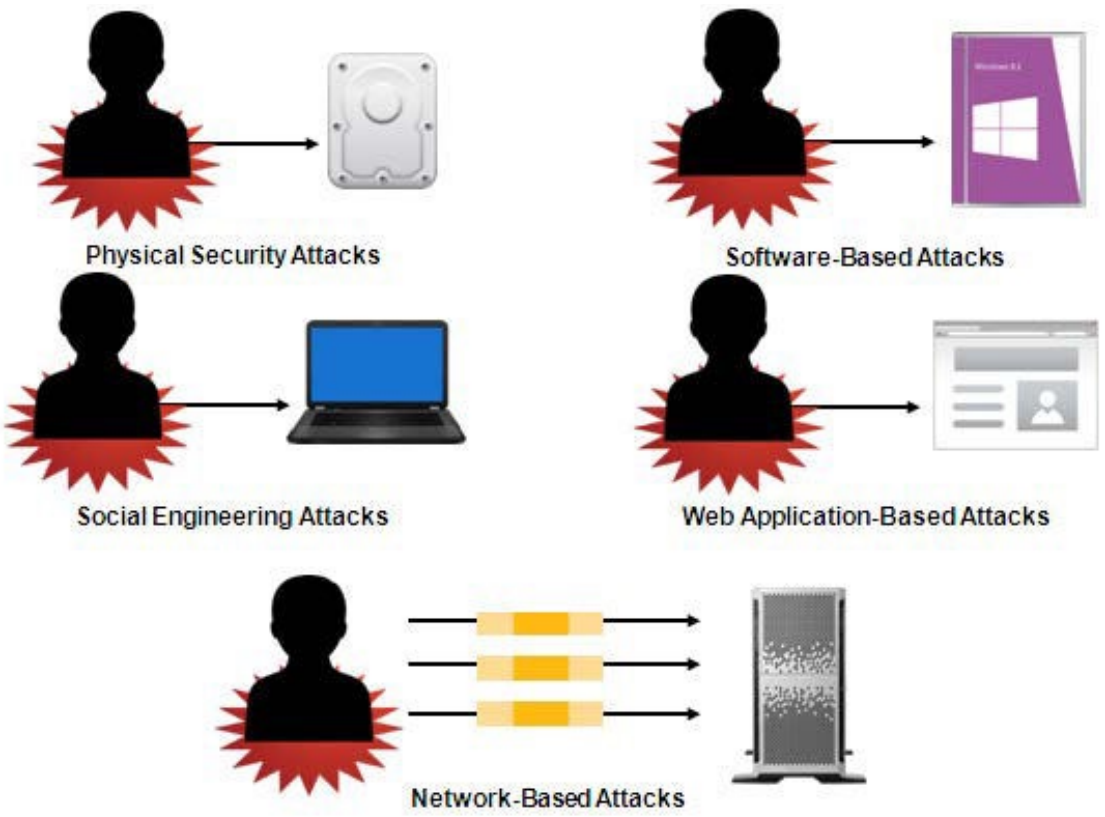
Intrusions

- In the realm of computer security,
  - An intrusion occurs when an attacker accesses a computer system without the authorization to do so.
  - An intrusion occurs when the system is vulnerable to attacks, and may include:
    - Physical intrusions.
    - Host-based intrusions.
    - Network-based intrusions.

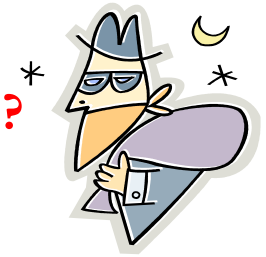


Attacks

- An attack is a technique that is used to exploit a vulnerability in any application or physical computer system without the authorization to do so.
- Attacks on a computer system and network security include:
  - ✓ Software-Based Attacks.
  - ✓ Web Application-Based Attacks.
  - ✓ Network-Based Attacks.
  - ✓ Social Engineering Attacks.
  - ✓ Physical Security Attacks.



Attacking the Network



What's wrong with the infrastructure?

The Internet

Border Router/Firewall

DMZ

Network Servers

WLAN

Firewall

Inter Network

Intra Network

Controls

- Controls are the countermeasures that you need to put in place to avoid, mitigate, or counteract security risks due to threats or attacks.
- Controls are solutions and activities that enable an organization to meet the objectives of an information security strategy.
- Controls can be safeguards and countermeasures that are logical or physical.
- Controls are broadly classified as prevention, detection, and correction controls.

Prevention Control

Detection Control

Correction Control

Types of Controls

UMT
We lead

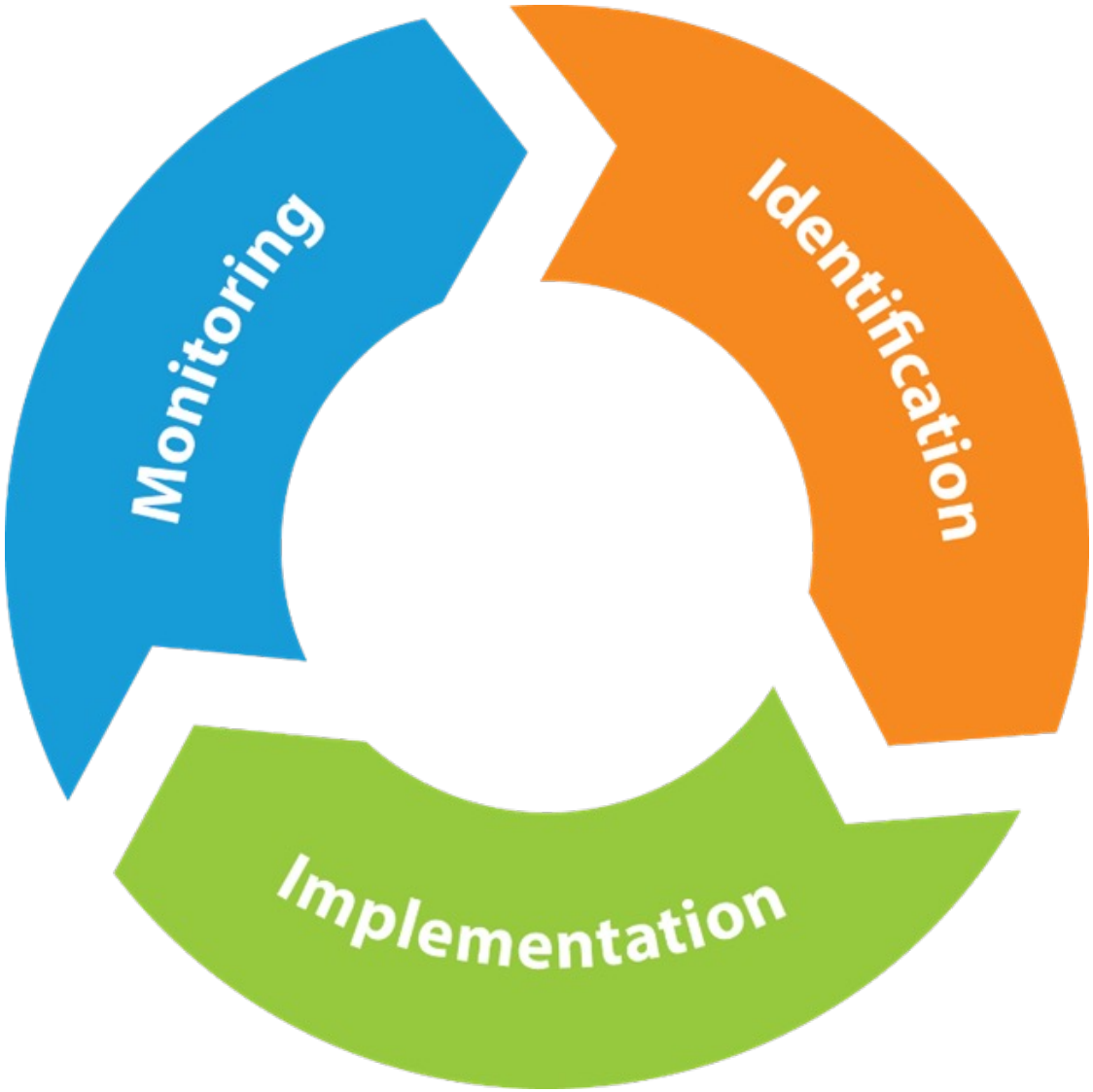
The different types of controls include:

- **Prevention controls:**
  These help to prevent a threat or attack from exposing a vulnerability in the computer system.
  For example, a security lock on a building's access door is a prevention control.

- **Detection controls:**
  These help to discover if a threat or vulnerability has entered into the computer system.
  For example, surveillance cameras that record everything that happens in and around a building are detection controls.

- **Correction controls:**
  These help to mitigate the consequences of a threat or attack from adversely affecting the computer system.
  For example, a security officer who responds to a silent alarm detecting an intrusion and who then stops the intruder is a correction control.

The Security Management Process



The Security Management Process

Identify security controls:

This involves detecting problems and determining how best to protect a system:

- ✓ Find out when and where security breaches occur.
- ✓ Log details of the breaches, showing information regarding the failed attempts, such as typing a wrong user name or password.
- ✓ Select the appropriate identification technique, such as a network intrusion detection system (NIDS).

The Security Management Process

Implement security controls:

This involves installing control mechanisms to prevent problems in a system:

- ✓ Authenticate users appropriately or control access to data and resources.
- ✓ Match implementation security controls with the management requirements in any organization.
- ✓ Install a security mechanism such as an intrusion detection system (IDS) or an intrusion prevention system (IPS) to prevent any attacks on the system.

Monitor security controls

This involves detecting and solving any security issues that arise after security controls are implemented:

- ✓ Run tests on the various controls installed to see if they are working correctly and will remain effective against further attacks on the system.
- ✓ Analyze important steps that improve the performance of controls.
- ✓ Document each control failure and determine if a control needs to be upgraded or removed.

The CIA Triad

- Information security seeks to address three specific principles: **confidentiality**, **integrity**, and **availability**.
- This is called the **CIA** triad.
- If one of the principles is compromised, the security of the organization is threatened.

The CIA Triad

UMT
We lead

- **Confidentiality:**
  - This is the fundamental principle of keeping information and communications private and protecting them from unauthorized access.
  - Confidential information includes trade secrets, personnel records, health records, tax records, and military secrets.
  - Confidentiality is typically controlled through encryption, access controls, and steganography.

- **Integrity:**
  - This is the fundamental principle of keeping organization information accurate, free of errors, and without unauthorized modifications.
  - For example, if an attack on a school system's server occurred and student test scores were modified, the integrity of the grade information was compromised by unauthorized modification.
  - Integrity is typically controlled through hashing, digital signatures, certificates, and non-repudiation.

The CIA Triad

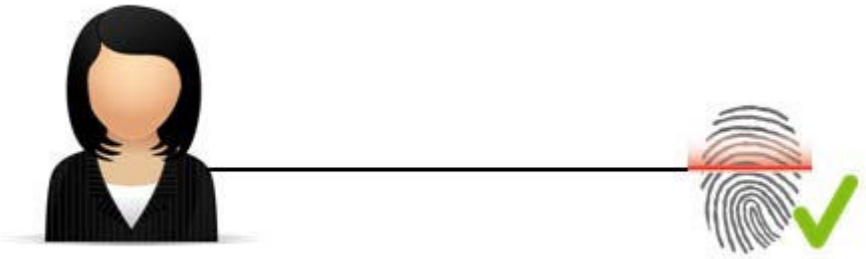
- **Availability:**
  - This is the fundamental principle of ensuring that systems operate continuously and that authorized persons can access the data that they need.
  - Information available on a computer system is useless unless the users can get to it.
  - Consider what would happen if the Federal Aviation Administration's air traffic control system failed. Radar images would be captured but not distributed to those who need the information.
  - Availability is typically controlled through redundancy, fault tolerance, and patching.

Non-repudiation

- **Non-repudiation:**
  - Is the goal of ensuring that the party that sent a transmission or created data remains associated with that data and cannot deny sending or creating that data.
  - You should be able to independently verify the identity of a message sender, and the sender should be responsible for the message and its data.
- **Non-repudiation** is one way to determine accountability, which is the process of determining who to hold responsible for a particular activity or event, such as a log on.

Identification

- **Identification** is a method that ensures that an entity requesting access to resources by using a certain set of credentials is the true owner of the credentials.
- The investment and effort that goes into implementing a method of identification varies depending on the degree of security or protection that is needed in an organization.



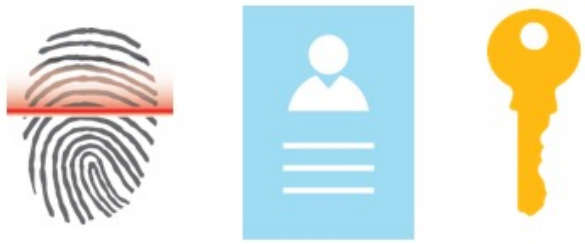
- When a request for access to resources involves providing credentials such as an email address or user name together with a password, identification ascertains whether or not the individual who enters the credentials is also the owner of those assigned, particular credentials.

Authentication

- **Authentication** is the method of validating a particular entity or individual's unique credentials.
- Authentication concentrates on identifying if a particular individual has the right credentials to enter a system or secure site.
- Authentication credentials should be kept secret to keep unauthorized individuals from gaining access to confidential information.

Authentication Factors

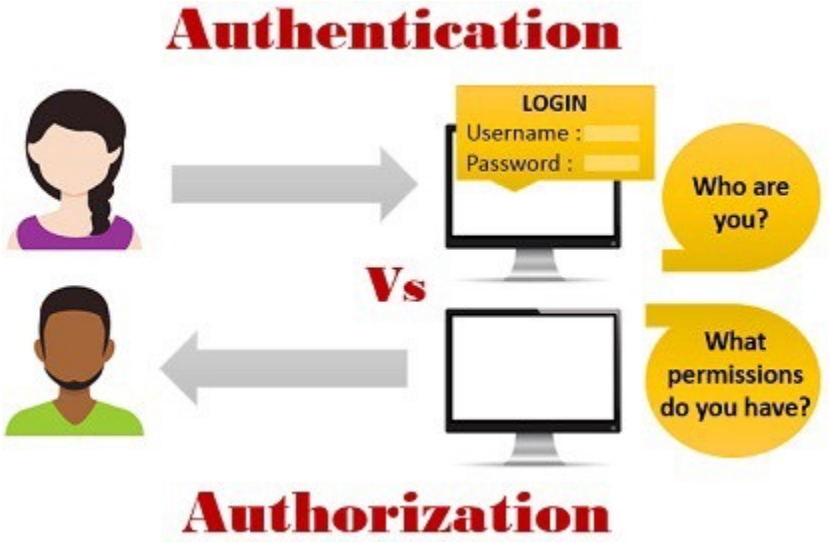
- Most authentication schemes are based on the use of one or more authentication factors.
- The factors include:
  - ✓ Something you are (Fingerprints, handprints, or retinal patterns).
  - ✓ Something you have (Key or ID card).
  - ✓ Something you know (Password or PIN).
  - ✓ Somewhere you are or are not (IP address or GPS).
  - ✓ Something you do (Keystroke patterns).



Note: The keystroke pattern factor is also referred to as keystroke biometrics **or** dynamic biometrics.

Authorization

- In security terms,
  - Authorization is the process of determining what rights and privileges a particular entity has.
  - Authorization is equivalent to a security guard checking the guest list at an exclusive gathering, or checking for your ticket when you go to the movies.
  - After a user has been identified and authenticated, a system can then determine what rights and privileges that user should have to various resources.



- **Summary:**
  - ✓ Determining the rights and privileges of a user or entity.
  - ✓ Comes after identification and authentication.

Common Security Practices

UMT
We lead

- Common security practices help implement access controls in ways that provide effective measures for the **protection** of data and resources.
- The following is a list of common security practices:

  - ✓ Implicit deny
  - ✓ Least privilege
  - ✓ Separation of duties
  - ✓ Job rotation
  - ✓ Mandatory vacation
  - ✓ Time of day restrictions
  - ✓ Privilege management

Implicit Deny

- Implicit Deny:
  - The principle of implicit deny dictates that everything that is not explicitly allowed is denied.
  - Users and software should only be allowed to access data and perform actions when permissions are specifically granted to them.
  - No other action is allowed.

Least Privilege

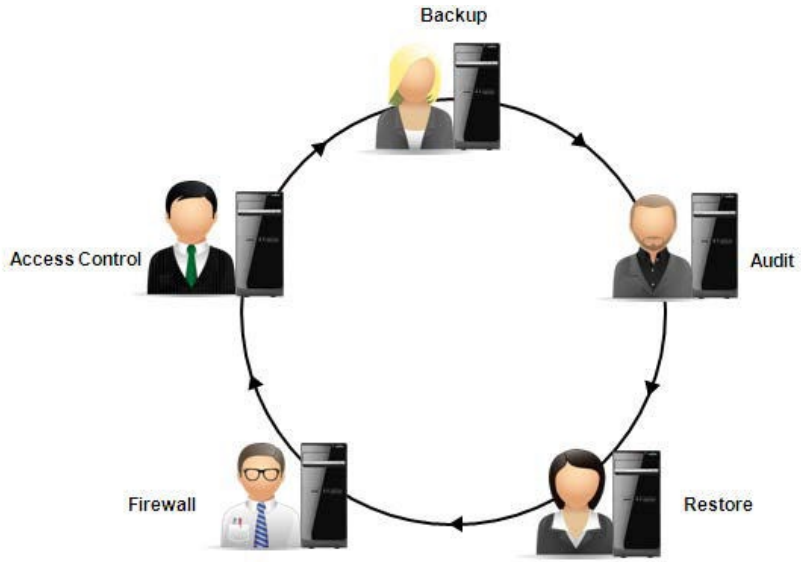
- The principle of **least privilege** dictates that users and software should only have the **minimal level of access** that is necessary for them to perform the duties required of them.
- This level of minimal access includes facilities, computing hardware, software, and information.
- When a user or system is given access, that access should still be only at the level required to perform the necessary task.

Separation of Duties

- **Separation of duties** states that no one person should have too much power or responsibility.
- Duties and responsibilities should be divided among individuals to prevent **ethical conflicts** or **abuse of powers**.
- Duties such as authorization and approval, and design and development should not be held by the same individual, because it would be far too easy for that individual to exploit an organization.

Job Rotation

- The idea of **job rotation** is that no one person stays in a vital job role for too long.
- Rotating individuals into and out of roles, such as the firewall administrator or access control specialist, helps an organization ensure that it is not tied too firmly to any one individual because vital institutional knowledge is spread among trusted employees.
- **Job rotation** also helps prevent abuse of power, reduces boredom, and enhances individuals' professional skills.

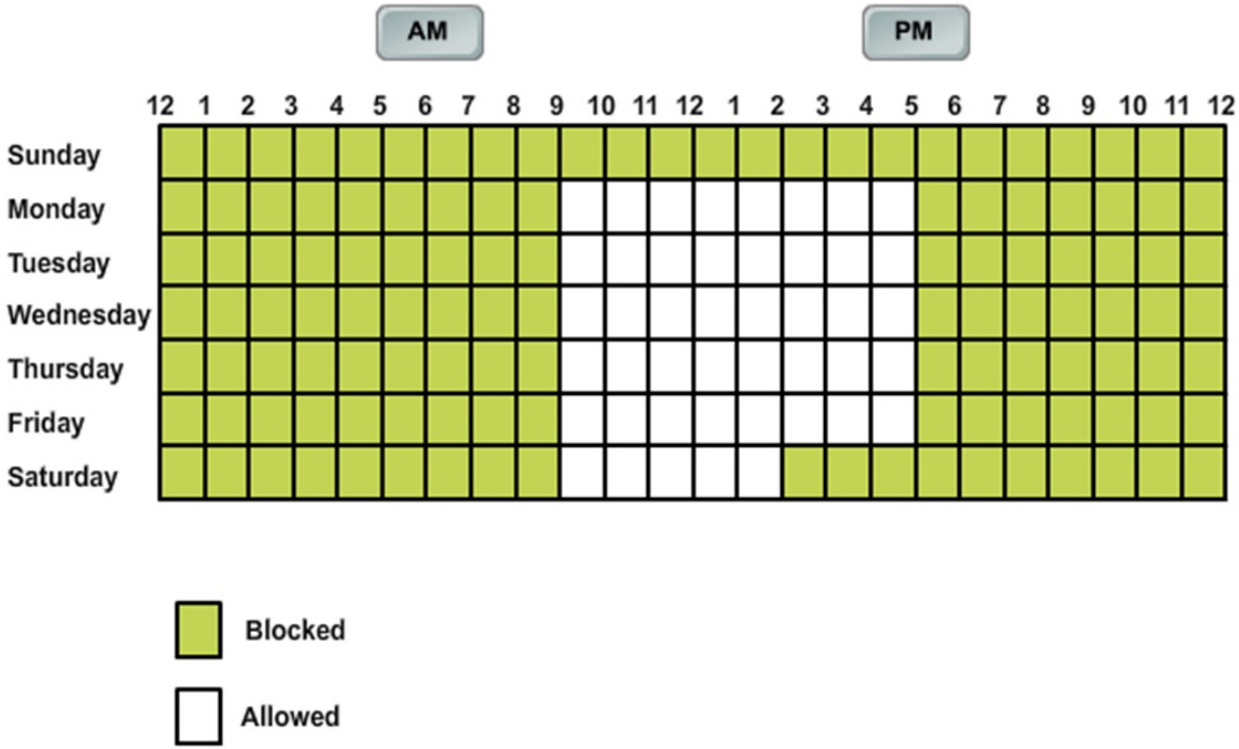


Mandatory Vacation

- **Mandating employee** vacations is a personnel management issue that has security implications.
- From a security standpoint, **mandatory vacations** provide an opportunity to review employees' activities.
- The typical mandatory vacation policy requires that employees take at least one vacation a year in a full week increment so that they are away from work for at least five days in a row.
- During that time, the corporate audit and security employees have time to investigate and discover any discrepancies in employee activity.
- When employees understand the security focus of the **mandatory vacation** policy, the chance of fraudulent activities decreases.

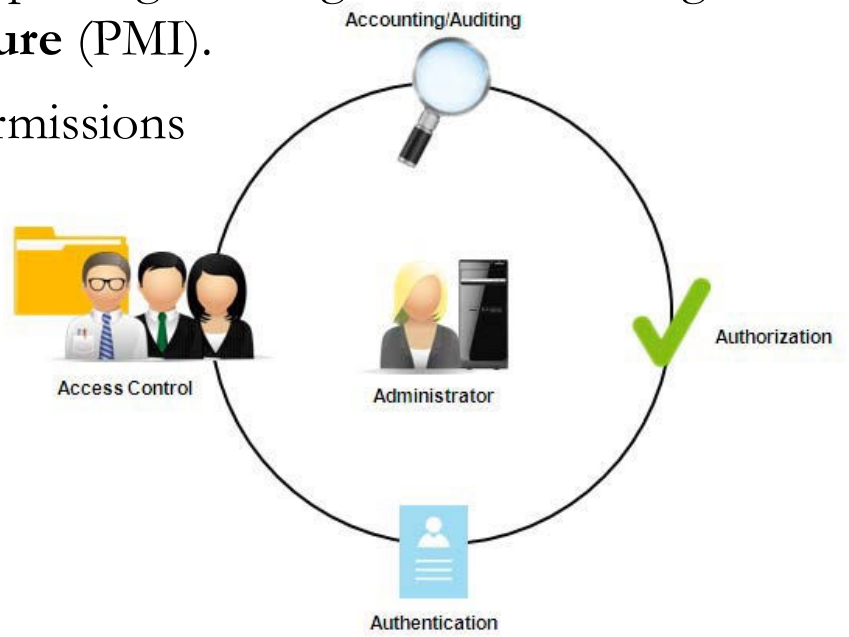
Mandatory Vacation

- **Time of day restrictions** are controls that restrict the periods of time when users are allowed to access systems, which can be set using a group policy.
- You can also apply **time of day restrictions** to individual systems and to wireless access points.



Privilege Management

- **Privilege management** is the use of authentication and authorization mechanisms to provide centralized or decentralized administration of user and group access control.
- **Privilege management** should include an auditing component to track privilege use and privilege escalation.
- **Single sign-on** (SSO) can offer privilege management capabilities by providing users with one-time authentication for browsing resources such as multiple servers or sites.
- An implementation of a particular set of privilege management technologies is called a **Privilege Management Infrastructure** (PMI).
- The purpose of a **PMI** is to issue specific permissions and rights to users within the infrastructure.



Authentication Methods

- The information security controls include authentication which is one of the primary controls in use.

- Authentication is not a single process.

- The primary authentication methods in use today:
  - User Name/Password Authentication.
  - Tokens.
  - Smart Cards.
  - Biometrics.
  - Geolocation.
  - Keystroke Authentication.
  - Multi-factor Authentication.
  - Mutual Authentication.

Authentication Methods

- User Name/Password Authentication.
  - The combination of a user name and password is one of the most basic and widely used authentication schemes.
- Tokens.
  - Tokens are physical or virtual objects, such as smart cards, ID badges, or data packets, that store authentication information.
  - Tokens can store personal identification numbers (PINs).
- Smart Cards.
  - Smart cards are a common example of token-based authentication.
  - A smart card is a plastic card containing an embedded computer chip that can store different types of electronic information.
- Biometrics.
  - Biometrics are authentication schemes based on the identification of individuals by their physical characteristics.
- Geolocation.
  - Geolocation refers to the use of location technologies such as GPS or IP addresses to identify and track the whereabouts of connected electronic devices.

Authentication Methods

- Keystroke Authentication.
  - Keystroke authentication is a type of authentication that relies on detailed information that describes exactly when a keyboard key is pressed and released as someone types information into a computer or other electronic device.
- Multi-factor Authentication.
  - Multi-factor authentication is any authentication scheme that requires validation of two or more authentication factors.
  - It can be any combination of who you are, what you have, what you know, where you are or are not, and what you do.
- Mutual Authentication.
  - Mutual authentication is a security mechanism that requires that each party in a communication verifies each other's identity.

A Security Policy

We lead

Develetech Industries Password Policy ← **Individual Policy**

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the company's entire corporate network. As such, all employees (including contractors and vendors with access to corporate systems) are responsible for taking the appropriate steps, as outlined in the following, to select and secure their passwords. ← **Resources to Protect**

2.0 Purpose

The purpose of this policy is to establish a standard for creating strong passwords, protecting those passwords, and setting the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Develetech facility, has access to the corporate network, or stores any non-public company information.

Formal Policy Statement

4.0 Policy Specifications

4.1 General

- All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.) must be changed on at least a monthly basis.
- All production system-level passwords must be part of the company administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least once every three months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described in the following section.

Implementation Measures

Security Policy Fundamentals

UMT
We lead

- A **security policy** is a formalized statement that defines how security will be implemented within a particular organization.

- It describes the means the organization will take;
  - ✓ To protect the confidentiality, availability, and integrity of sensitive data and resources.
  - ✓ To protect the network infrastructure, physical and electronic data, applications, and the physical environment.

- It often consists of multiple individual policies.

Security Policy Components

- **Policy Statement**
  - Outlines the plan for the individual security component.
- **Standards**
  - Define how to measure the level of adherence to the policy.
- **Guidelines**
  - Suggestions, recommendations, or best practices for how to meet the policy standard.
- **Procedures**
  - Step-by-step instructions that detail how to implement components of the policy.

Common Security Policy Types

- There are several common security policy types that are included in most corporate security policies

  - ✓ **Acceptable Use Policy (AUP).**
    - ✓ States the limits and guidelines that are set for users and others to make use of an organization's physical and intellectual resources.
    - ✓ The policy should define what use of organizational assets,
      - ✓ such as **computers** and **telecommunications** equipment.
  - ✓ **Privacy Policy.**
    - ✓ Defines standards for divulging organizational or personal information to other parties.
  - ✓ **Audit Policy.**
    - ✓ Details the requirements and parameters for risk assessment and audits of the organization's information and resources.

Common Security Policy Types

- There are several common security policy types that are included in most corporate security policies.

  - ✓ **Extranet Policy.**
    - ✓ Sets the requirements for third-party entities that desire access to an organization's networks.
  - ✓ **Password Policy.**
    - ✓ Defines standards for creating password complexity.
  - ✓ **Wireless Standards Policy.**
    - ✓ Defines which wireless devices can connect to an organization's network and how to use them in a safe manner that protects the organization's security.
  - ✓ **Social Media Policy**
    - ✓ Defines how the organization and its employees use social media such as blogs, Facebook, Twitter, LinkedIn, and others.

Thank you