Chapter 7

Always A Pioneer, Always Ahead

Physical Access Control

Dr Zaheera Zainal Abidin
zaheera@utem.edu.my

MyUTeM

By the end of the lesson, the student will be able to:

a. Understand difference between identification and authentication
b. Understand the centralized and decentralized physical access control
c. Identify the attacks in physical access control

OVERVIEW

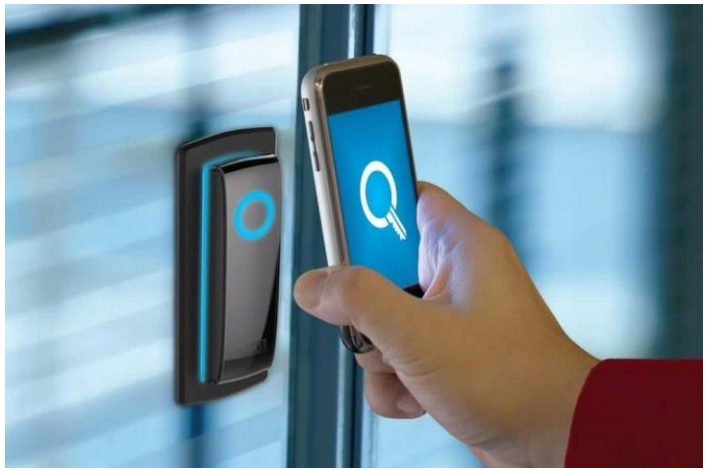
- Introduction
- Identification and Authentication
- Centralized Physical Access Control
- Decentralized Physical Access Control
- Physical Access Control Attacks
- Testing the Physical Access Control

INTRODUCTION

INTRODUCTION

- Physical Access Control is a collection of mechanism tools that permits and restricts the manager of a system to exercise a giving and limiting influence over the use and content of a system. Example such as controlled gate and RFID door.
- It permits the management to specify the type of users to access the system, whose user is allowed to access, and operations that user is allowed to perform in the system.

Examples of Physical Access Control



INTRODUCTION

- The goals of implementing the physical access control system are:
  - Permit or deny the subject's to access the information
  - Reliability check about the user's profiler or user identity
  - Identify the user's purpose of using the system
  - Grant an access to an eligible user

CONCEPT OF PHYSICAL ACCESS CONTROL

- Principles of Physical Access Control
  - Deciding which persons have access to what systems, data and functions
  - Designing, configuring and operating the technology
- Types of Physical Access Control
  - Control is an activity, process or apparatus to ensure the confidentiality, integrity or availability of an asset
- Categories of Physical Access Control
  - Know how access to the Information System is controlled

PRINCIPLES OF PHYSICAL ACCESS CONTROL

- Separation of duties:
  - No single individual should have so many privileges to complete any functions
  - The function should be divided into individual tasks that performed by separate individuals or groups
  - Eg: Financial payments, software changes, creation of computer user accounts
  - Least privileges
  - Any individual should have access to only the system, data and function
- Least Privileges and Server Application : privileges not only to people but to application and service processes
  - User Permissions on File Servers and Applications : give user access by assign on file server
  - Least Privileges on Workstations : vitally in end-user workstations such administrative privileges

TYPES OF PHYSICAL ACCESS CONTROL

- Technical Control
  - The programs and mechanisms on Information System that control system behavior and user access
  - Authentication, ACL, Firewall, Remote access, anti-virus, encryption, configuration management
- Physical Control
  - Used to manage physical access to Information System such as application servers and network devices
  - Video surveillance, key card, no trespassing signs, fencing
- Administrative Control
  - Represent a broad set of actions, policies, procedures and standards to govern the actions of people, Information System, Policies, Processes and Procedures; and Standard.

CATEGORY OF PHYSICAL ACCESS CONTROL

- Detective
  - Record events that occur
  - They detect but do nothing else
  - Only effective if the controls are monitored video surveillance, access logs, transaction logs, IDS
- Deterrent
  - Designed to highly visible and give persons the impression that any unauthorized activities will be stopped
  - Consists sign that alert person of controls
  - Signs, guards, guard dogs, barbed wire or razor wire
- Preventive
  - Designed to prevent unwanted activities
  - Firewalls, anti-virus and anti-soy software, encryption, IPS, bollards

CATEGORY OF PHYSICAL ACCESS CONTROL

- Corrective
  - Events that occur after a security event has occurred
  - Undertaken in order to prevent the recurrence of unwanted event
- Recovery
  - Take place after an incident has occurred
  - Activities that enable the restoration to normal operations after some event
- Compensating
  - It compensates for the lack or failure of another control

Identification and Authentication

INDENTIFICATION & AUTHENTICATION

- Identification means comparison of a genuine user from one to many user profiles in the databases.
- Example of identification, the face of an employee who is passing by at the corridor of the building is compared with the image of a face in the database to find the successful match. Then, the group of employee is identified as operation, manager or CEO.
- After, the employee as been identified, then the respective employee needs to perform authentication to prove the actual identity / user profiler.
- Authentication means a system requests identifying information from user in order to permit access to legitimate a user and deny access to invalid user. Example of authentication is password.

IDENTIFICATION METHOD

- The identification in this chapter is referring to the user identification.
- User identification is based on several methods:
  - Software agents – a program inside user PC collects information about the user information and share with a server using protocol.
  - Log in and log out – user activity about going in and out of PC, access Email, browsing website etc. The pattern of attendance, availability at working place and working behavior is obtained from logins activity.
  - Enhanced proxy servers – User who bypass the proxy server can be identified since an improved settings have been done at the server
  - Cookies – Cookies saves the IP address of a user in user's PC that visit same websites
  - Session IDs – similar as cookies but has no storage to keep user id between visits.

USER IDENTIFICATION ISSUE

- Falsely Accepted Identification
- High Noise Rate in User Template or User Data
- Data Collection:
  - User collects browsing caches on periodic basis
  - User installs a proxy server to get Internet access
  - User uses multiple computer so difficult to get the browsing cache
  - User login using same user password in multiple computer in the same software application
- User data privacy and security

IDENTIFICATION TECHNOLOGY

- Keyword-based profiles – keyword is extracted from web pages collected. Example: tf*idf from Information retrieval theory.
  - Latent Semantic Indexing (LSI) and Linear Least Squares Fit (LLSF) – LSI and LLSF is the extension of tf*idf for creating the keyword-based feature vectors. Only the top N most highly weighted terms in the page contributes to the profile.
- Semantic Network profiles – The added keyword score is increased based on user feedback or decreased as negative feedback. If keyword exist then new node is created. Thus, set of keywords are used to update weights on the co-occurrence arcs.
  - SiteIF – Keyword is extracted from web page and mapped using Wordnet. Polysemous words are disambiguated by analyzing their synsets to identify the most likely sense given the other words in the document. The synsets are combined to a user profile that is a semantic whose nodes a sunsets and between nodes that co-occurrence relation. The weight of the net is updated and nodes and arcs that are no longer updated may be removed from the network.

AUTHENTICATION METHOD

- Information systems authenticate users by challenging the user in three ways:
- What the user knows,
  - Method requires user to input information
  - Consist of userid and password (PIN)
- What the user has
  - Relies on something that the user has
  - Often called as two-factor authentication because user should know the userid and password + physical object
  - Eg: smart card, token, USB key
- What the user is
  - Involves some form of biometric device to measure a characteristic of user body such fingerprint, hand scan, iris scan, signature, facial scan and etc
  - Considered as two factor authentication –relies on what user knows and what user is

AUTHENTICATION METHOD

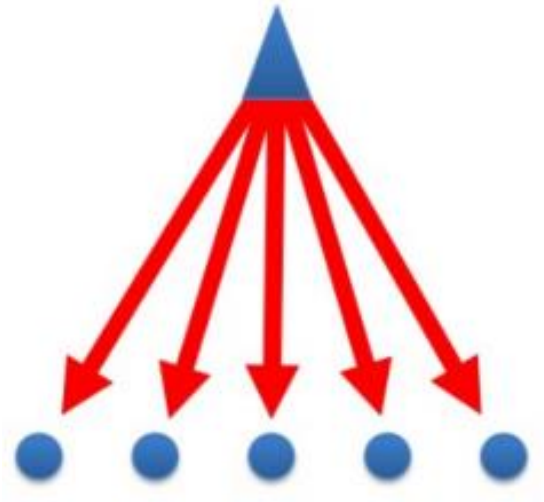
- Single Factor Authentication
- Two Factor Authentication – 2FA - Strong Authentication
- Tokens
- Public Key Interchange (PKI)
- Block Chain
- CAPTCHAs

AUTHENTICATION ISSUE

- Some significant issues:
  - Password quality
  - Forgotten credentials
  - Compromised credentials
  - Staff terminations
  - Multiple access using same password

AUTHENTICATION TECHNOLOGY

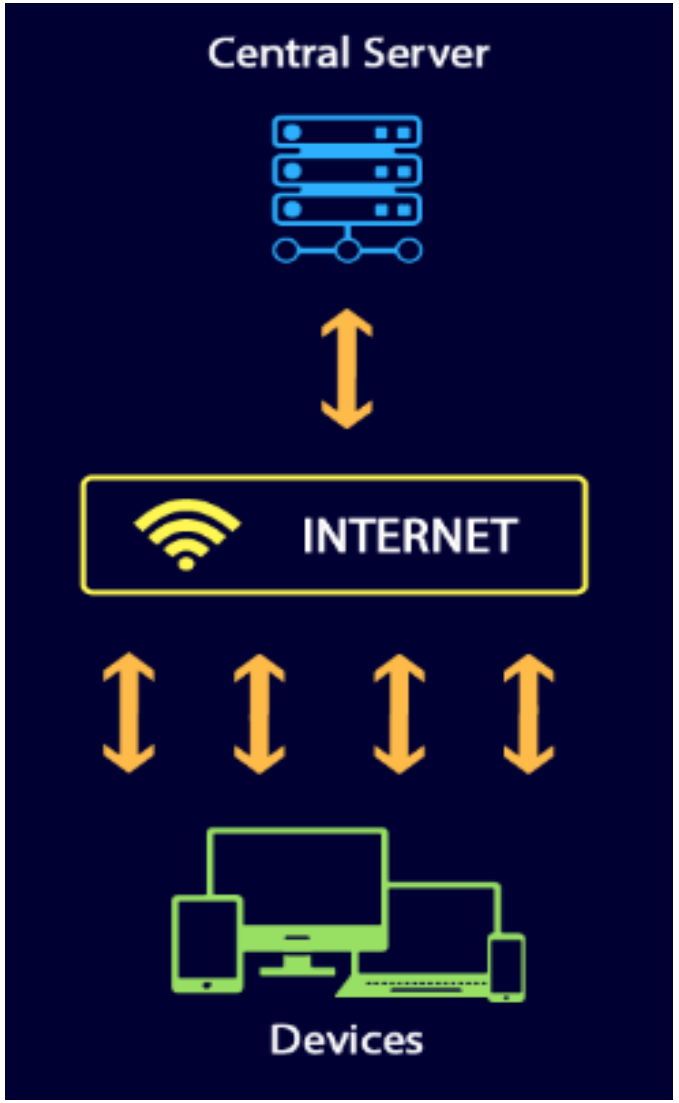
- Common use for authenticating users to systems and applications:
  - LDAP
  - RADIUS
  - TACACS
  - Kerberos
  - Single Sign-On and Reduced Sign-On
  - Secure Socket Layer (SSL)
  - Transport Layer Security (TLS)

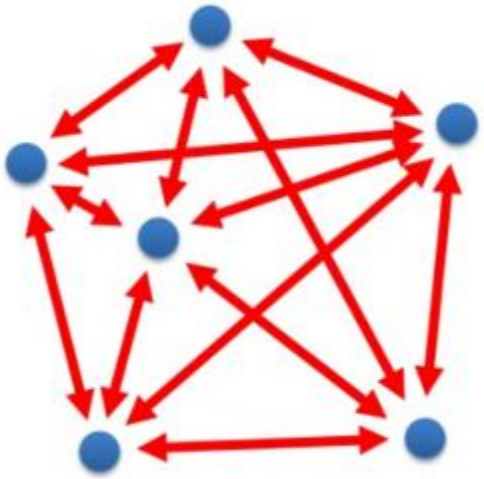


Centralized Physical Access Control

Centralized Physical Access Control

- Data flows through a central point such as server
- The data communication flows is vertical
- Systematic reservation of authority in a network
- Subject to effect of single point failure

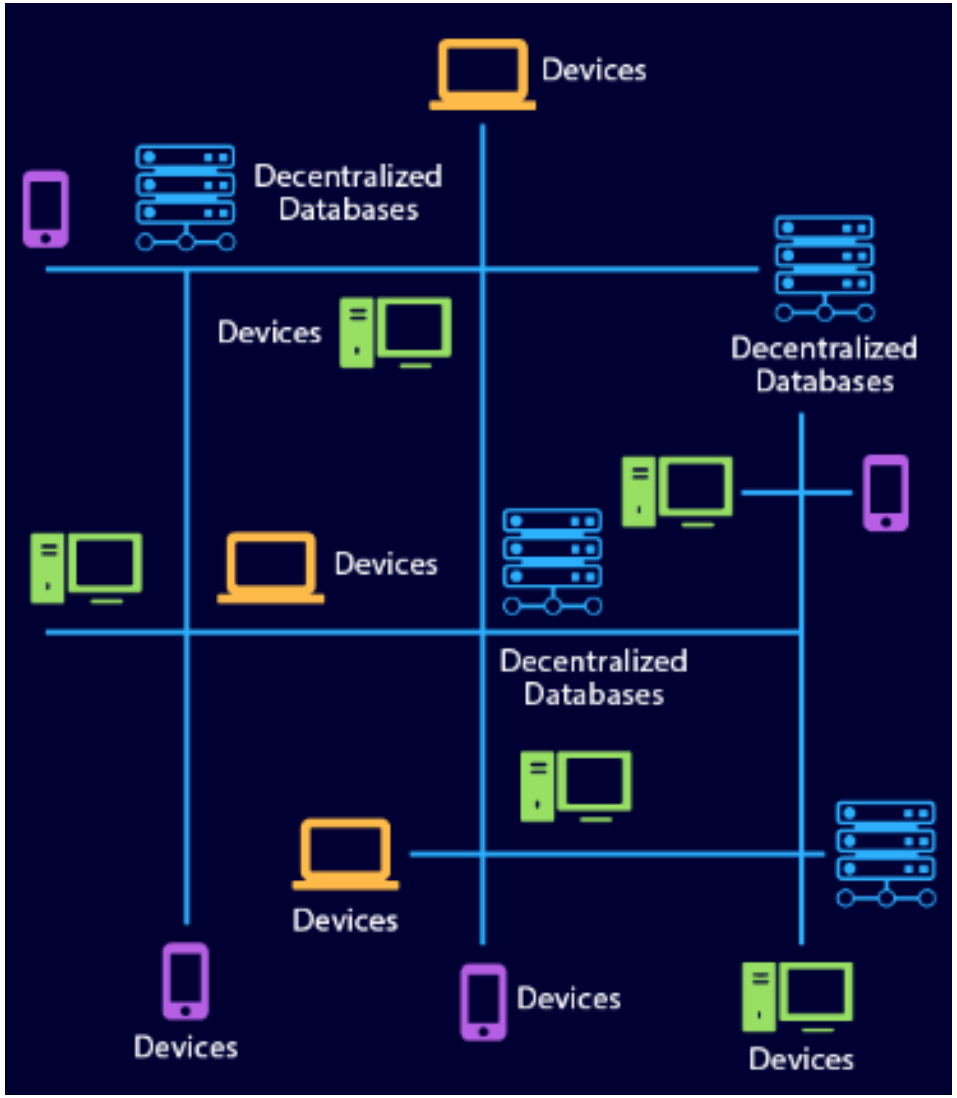




Decentralized Physical Access Control

Decentralized Physical Access Control

- Data flows through various point without any specific point which it must go through before access is granted
- Data flows in open and free
- Network involves a systematic dispersal of authority to various access point
- A variety of access points or nodes in the network that data freely moves and prevents the risks of single point failure.



ATTACKS OF PHYSICAL ACCESS CONTROL

PHYSICAL ACCESS CONTROL ATTACKS

- Several methods used to attack a system's access control mechanism to steal information and gain access to system
- Buffer Overflow, Script Injection, Data Remanence, Denial of Service, Dumpster Diving, Eavesdropping, Emanations, Spoofing and Masquerading, Phishing, Pharming, Spamming, Password Guessing & Password Cracking, Malicious Code and Social Engineering.

TESTING THE PHYSICAL ACCESS CONTROL AGAINST ATTACKS

PHYSICAL ACCESS CONTROL TESTING

- Log Analysis Audit Testing
  - Number of attempted break-in – log in and log out attempts
  - System malfunctions – system error logs
  - Account abuse – concurrent log in
- Penetration Testing
  - Discover the defects at server or operating system level
  - Scanning and analyzing using tools such as Nessus, Nikto, GFI LANguard, Superscan and Microsoft Baseline Security Analyzer
- Application Vulnerability Testing
  - Web-based application to steal or damage information such as online banking
  - Tools: WebInspect, Nessus, HP SPI Dynamic and IBM Watchfire AppScan

CONCLUSION

Conclusion

- Physical access control is an automated and mechanical form system that manages the people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
- The idea of physical access control is to enter a room using a key. When the physical access is controlled by software, the chip on an access card and an electric lock grants access through software, which is called as logical access control.

Thank You

MyUTeM

www.utem.edu.my