

Chapter 8

Always A Pioneer, Always Ahead



Physical Access Control Techniques

Dr Zaheera Zainal Abidin
zaheera@utem.edu.my

- By the end of the lesson, the student will be able to:
 - Understand about critical data in physical access control
 - Understand the types of access control
 - Understand the technique use in physical access control

- Introduction
- The emerging of information security technology in physical access control system
- The sensitive data or critical data in physical access control
- Types of access control (why? to study existing techniques)
 - role-based access control (RBAC)
 - discretionary access control (DAC)
 - mandatory access control (MAC)
- Techniques in physical access control (Previous and Current Technology)
 - Smartcard, Radio Frequency Identification (RFID) and Biometrics.

INTRODUCTION

INTRODUCTION

- A physical access control system is an integration of electronic door readers, control panels, intelligent databases, identification card (i.e.: smartcards, RFID tag or biometric template data), CCTV and ESM through access control points.
- The purpose of access control in physical security system is to provide a friendly working environment, convenient to the employee and secure the place against burglar or intruder.
- Thus, to make the goal a reality, steps are taken to increase convenience and secure work place.

INTRODUCTION

- The basic steps to obtain a safe and convenient working place are :
 1. Study the architecture of the working place. Use SWOT technique (Strength, Weakness, Opportunity and Threat) to gather information. List the assets, vulnerabilities, threats and potential risks.
 2. Identify the current electronic surveillance system available and improve the use for better security implementation for example new arrangement or setup.
 3. Design an integration of new technology in the physical access control to overcome the limitation in the existing access control system such as IoT or block chain.
 4. Audit the physical access control system.
 5. Testing the functionality of physical₆ access control system.

INTRODUCTION

- The pre-requisite to design a good physical access control system, is to learn a new technology available in the market and identify ways to improve the system.
- A new or emerging technology in physical access control is further explained in the next section.

THE EMERGING TECHNOLOGY FOR PHYSICAL ACCESS CONTROL

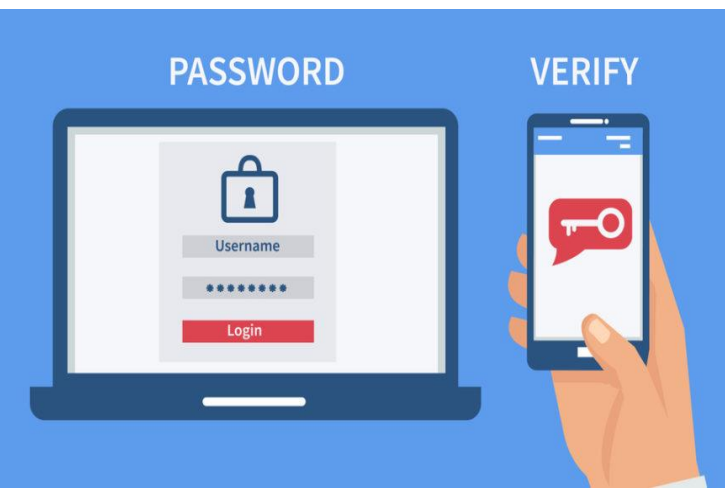
THE EMERGING TECHNOLOGY

- **The integration of smartphone application with physical access control system** — A mobile application of a smartphone is used as a security badge instead of having a separate key or ID that might get lost. Employee needs to enable the Near Field Communications (NFC) feature in the smartphone and performs some settings to activate the security feature. Employee uses software key generated and access the door using NFC inside the smartphone.
- **The integration of biometrics with physical access control system** — Employee uses fingerprint, facial or iris identification to access to the physical system such as thumbprint to switch on the computer or face recognition to access the door.



THE EMERGING TECHNOLOGY

- **The integration of multiple devices into a single platform** – In a company or multiple offices, CCTV monitoring not only monitoring employee movements but also monitors the fire or temperature in a room. Also, CCTV is combined with VoIP for better security services.
- **The combination of access control technologies** – A combination of two factor authentication (2FA) with three factor authentication (3FA) in a badge application for better security.



THE EMERGING TECHNOLOGY




- **Other example of emerging technology in physical access control are such as:**
 - **Blockchain Access Control**
 - **Charge-coupled device (CCD) Camera**
 - **Bluetooth Access Control**
 - **Ingress and Egress**
 - **Single sign-on (SSO) in active directory (AC)**
 - **Power over Ethernet (PoE) Access Control**
 - **Internet-of-Things (IoT) Access Control**
 - **Physical Access Control System (PACS)**
 - **Internet Protocol (IP) Access Control**
 - **Wireless Access Control**

THE CRITICAL DATA IN PHYSICAL ACCESS CONTROL SYSTEM

THE CRITICAL OR SENSITIVE DATA

- The critical or sensitive data is a data or information about a person or an organization that cannot be shared to others without the permission or agreement of the respective person or organization body.

THE CRITICAL OR SENSITIVE DATA

- The critical or sensitive is categorized as
 - Personal data: employee ID, phone number, medical records, physical address
 - Business-related data: financial and accounting info
 - Transactional-data : credit card, bank account, identification card no
 - Governmental data: secret and confidential data
- Types of sensitive data
 - Restricted Data 
 - Private Data or Data Privacy 
 - Public Data 

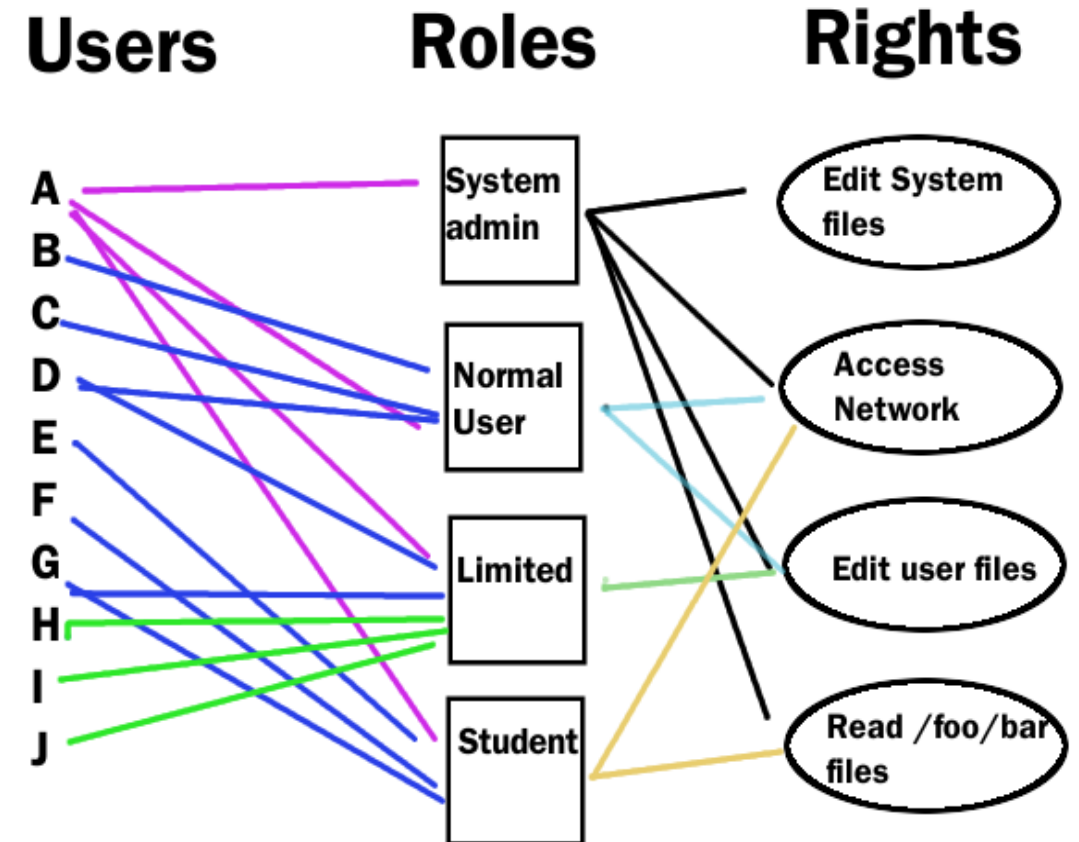
TYPES OF ACCESS CONTROL

3 types of access control that manage people to gain access to the physical access control system

a) The Role-Based Access Control (RBAC)

The Role-Based Access Control

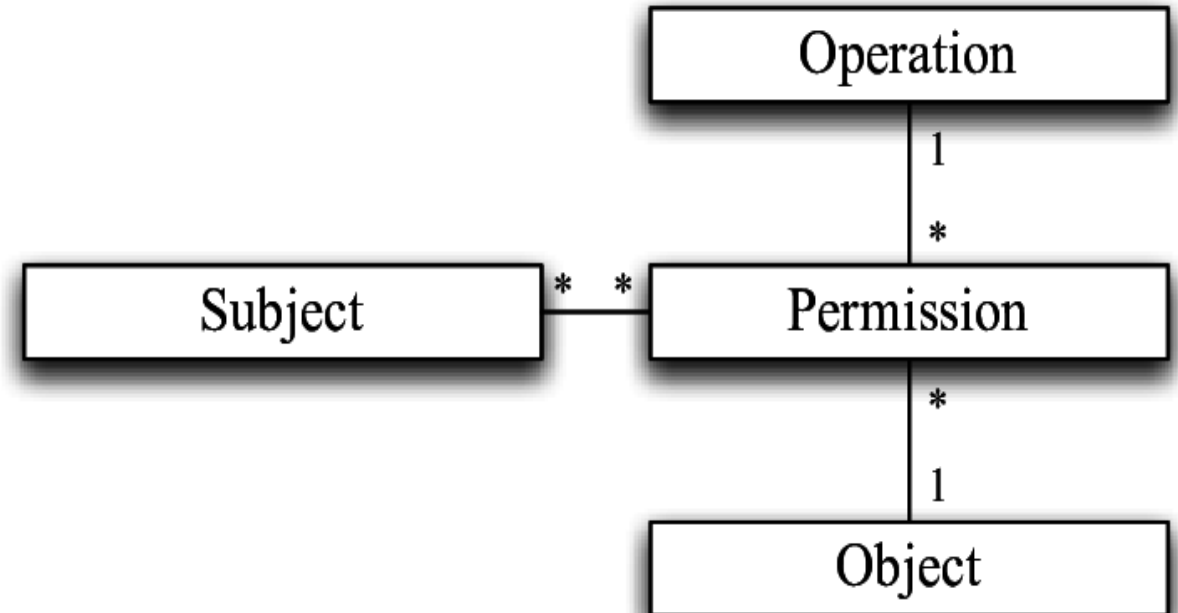
- RBAC is an approach to restricts the network access based on the roles of individual user within an organization.
- Example, employee has only access rights to information that related to the work and prevent from accessing other not related information.
- Permissions and privileges settings are setup to enable access to authorized users.



b) The Discretionary Access Control (DAC)

The Discretionary Access Control (DAC)

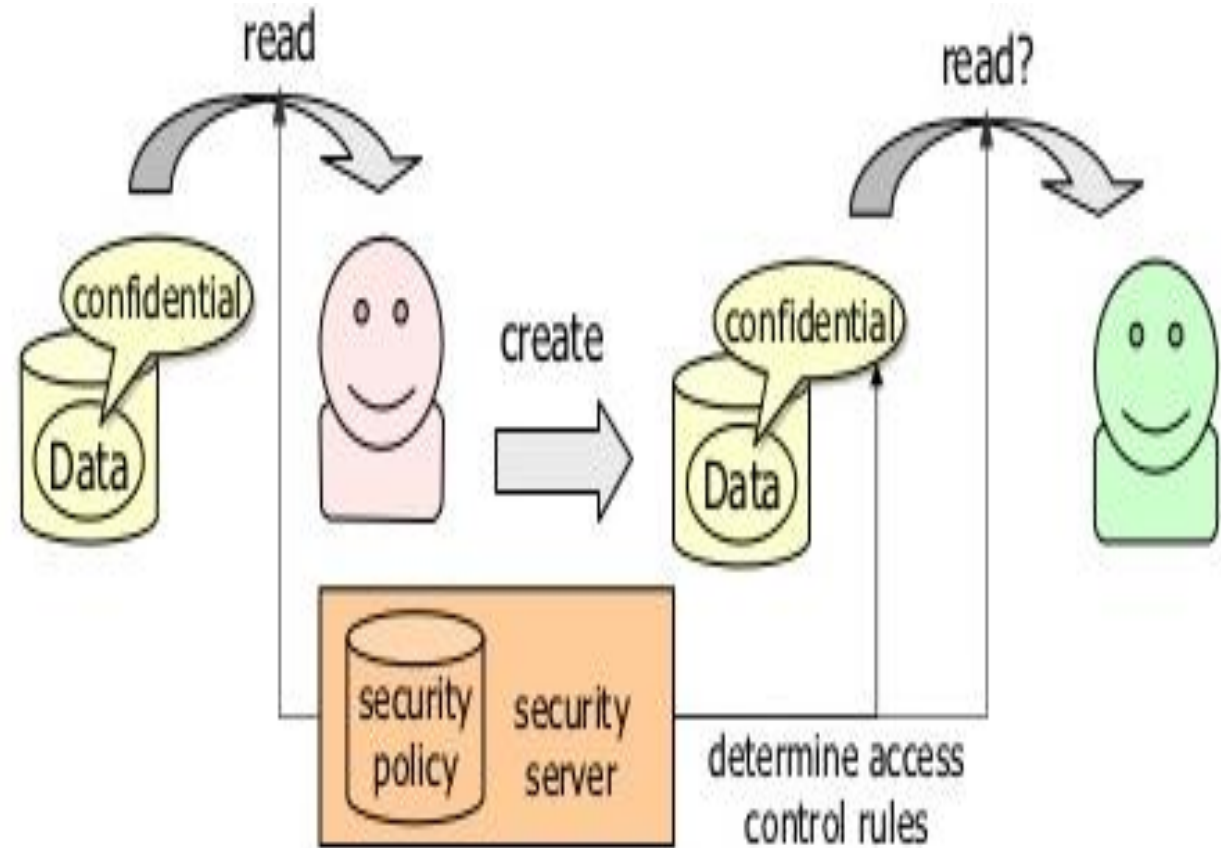
- DAC permits access for one operation to one object but an operation or an object can be used in multiple permissions.
- For instance, a programmer develops software codes and owned the source codes. The programmer decides how to share the codes and select the permission (read/write/both) to other users to further perform the development.



c) The Mandatory Access Control (MAC)

The Mandatory Access Control

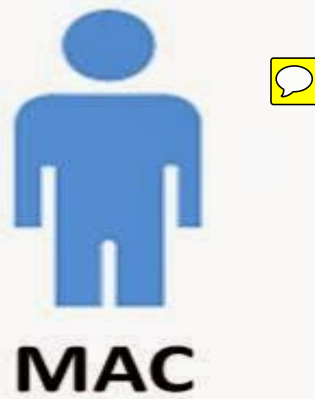
- MAC restricts the access to resources using hierarchical approach, which all access to resource objects are controlled by the operating system based on administrator's settings.
- Example 1: user works in an organization but the data is controlled by the organization.
- Example 2: The patient records are owned by the hospital and limit the sharing.



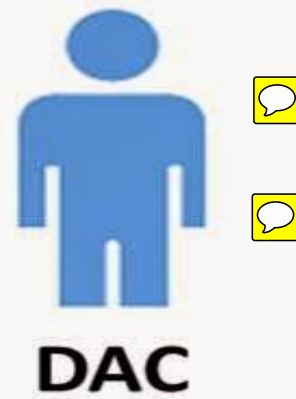
Summary of Access Control

RBAC	DAC	MAC
<ul style="list-style-type: none"> Provides access based on the position of an individual own in the organization Dynamically assign roles to users based on criteria or level defined by system administrator 	<ul style="list-style-type: none"> Least restrictive model Allows an individual a complete control over any objects they own 	<ul style="list-style-type: none"> Only system owner manages access control End user has no control over any privileges

SUBJECTS



Authorizations based on (user or group) permissions and object labels.



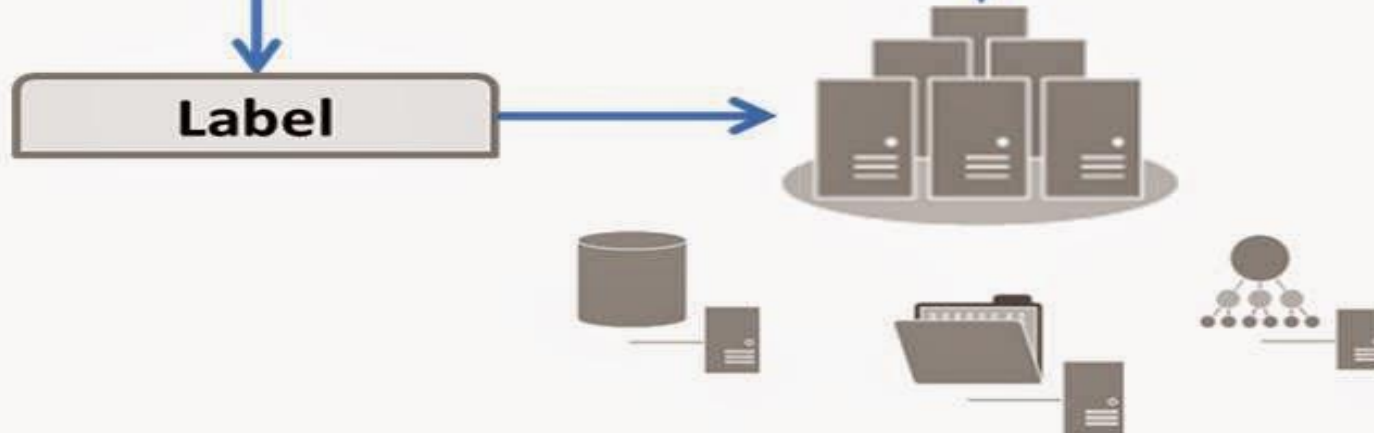
Authorizations based on (user or group) permissions. Zero knowledge of object sensitivity.



Authorizations based on group permissions. User is part of a group.

Reference Monitor

Label

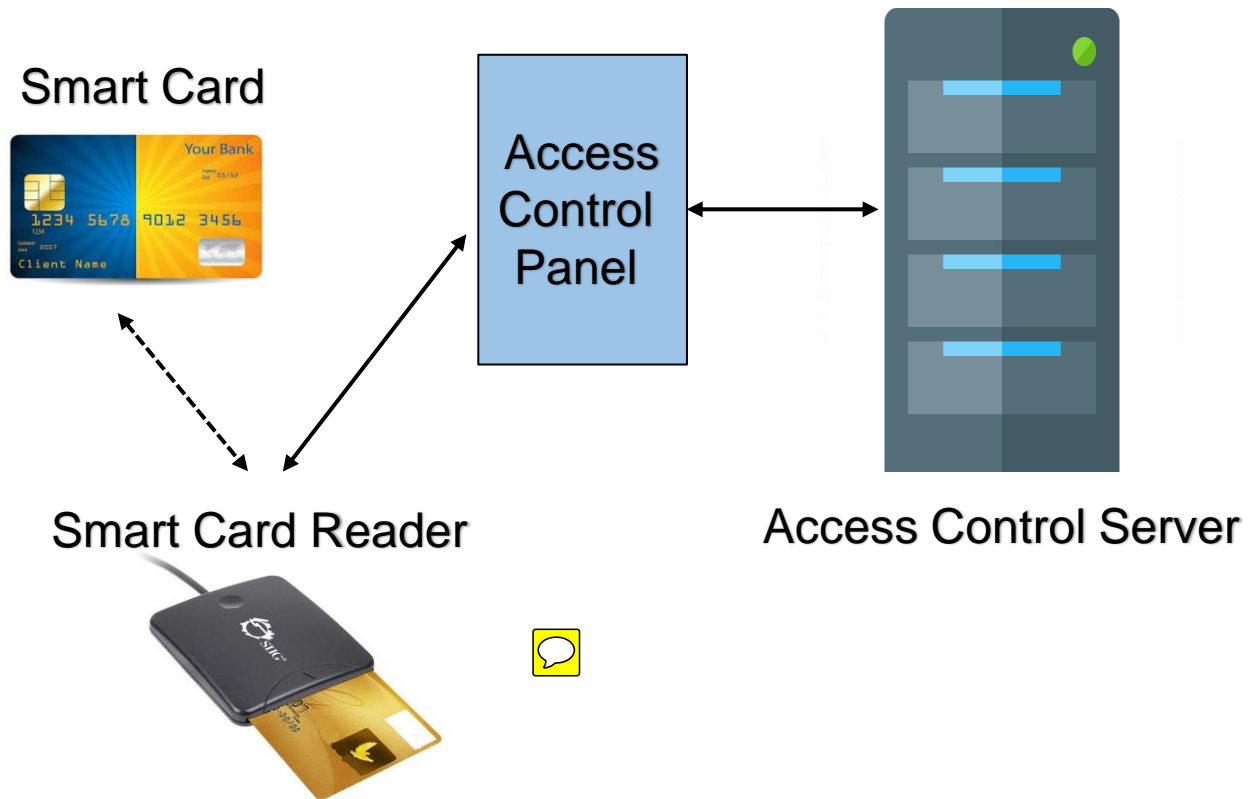


OBJECTS

TECHNIQUES / TECHNOLOGY OF PHYSICAL ACCESS CONTROL

Smartcard, Biometric, RFID

Smartcard based Physical Access Ctrl System



- Smart card is a plastic card with an embedded computer chip. The chip is programmed with information for storing, processing data receiving and data transmitting.
- Smart card is useful for access control solutions with other authentication mechanism.

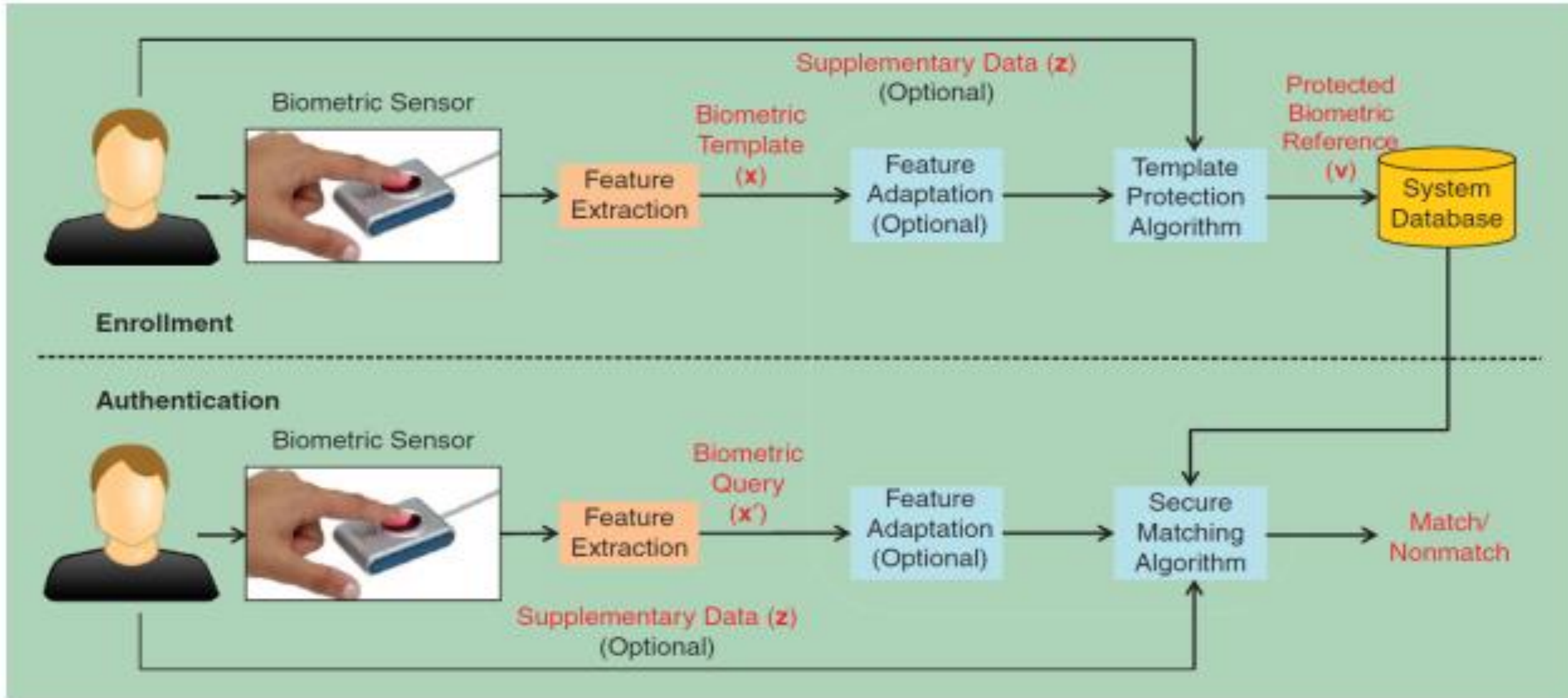
Smartcard based Physical Access Ctrl System

- The traditional card is the magstripe card with no security protection and uses ISO standard. Moreover, the card has low frequency (125 kHz) called as Prox Card that provides efficient and effective access control.
- However, smart card can be cloned or duplicated for gaining access to assets.
- Therefore, the smartcard has evolved when smart card combines with other technology such as password, biometrics, rfid and cloud for better security solution.
- Example: Smart card used for attendance system and credit card owned by the user to make payments either online or traditional way.

Biometric based Physical Access Ctrl System

- Biometric system is an automated technique that verify or identify people based on physical or behavioral characteristics.
- The physical access control and security applications use human characteristics as a biometric key to access to building, verify the attendance records and system approval.
- Example: An employee uses his fingerprint to access to the main server, face recognition to enter the door and iris scan in order to perform authentication in network environment.

Biometrics Framework / Methodology



Biometric based Physical Access Ctrl System

- Biometrics are used to prevent data theft and hacking activity. The combination of biometrics into the physical access control generates a secured digital features and protection in accessing the physical assets.
- Biometrics focuses on something the user has or knows instead of identity associated to the possession of an ID card. Thus, biometrics prevent from someone else card to get access to privileged resources.

Radio Frequency Identification (RFID)

- RFID is a technology that electronically identify object or human and validate the identity, status and authenticity of the data.
- Transmits the identified of an object using radio-frequency waves
- RFID is fast, reliable and does not require physical contact between RFID reader/scanner and RFID tagged item

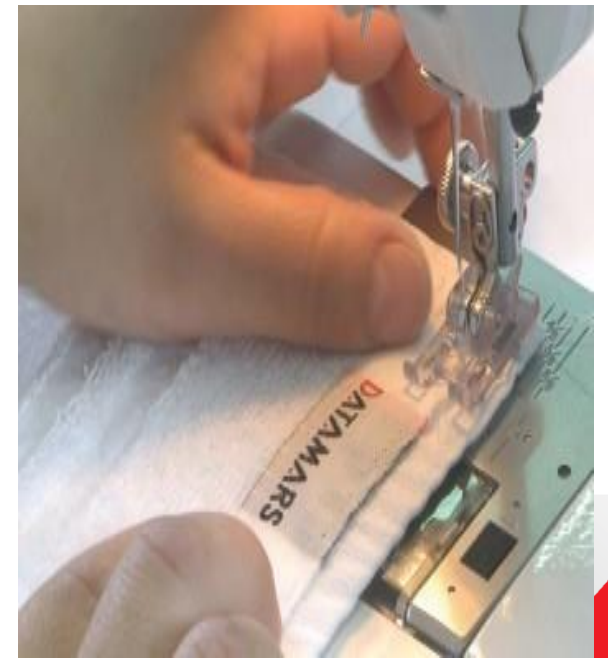
"I'm a Cow"



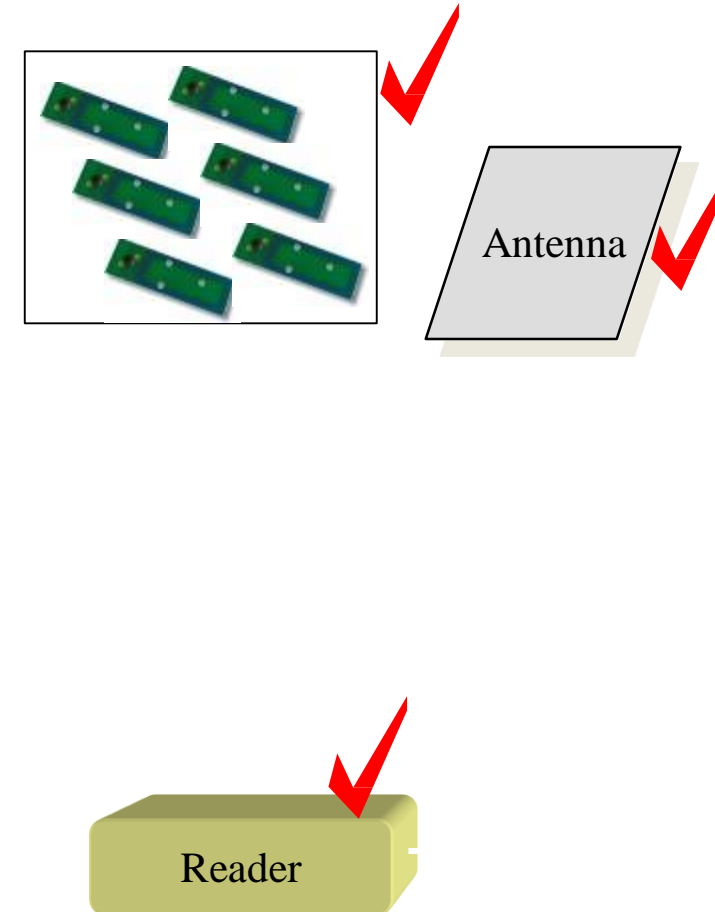
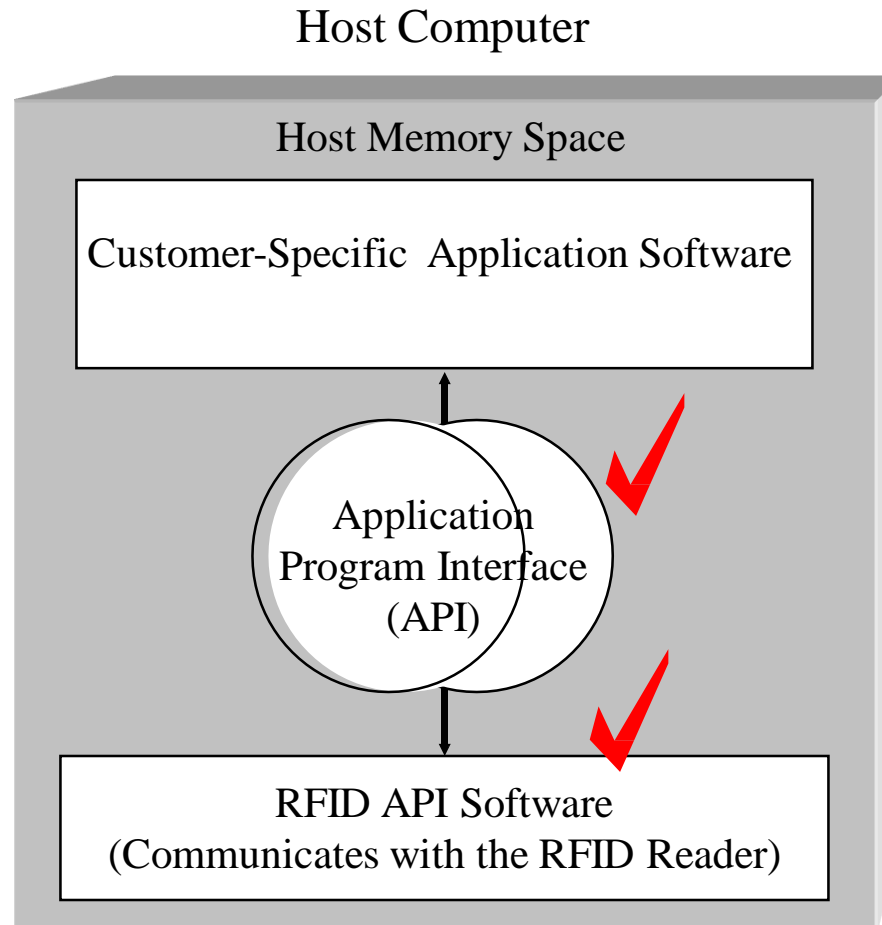
"I'm a Toaster"



"I'm a Baby"



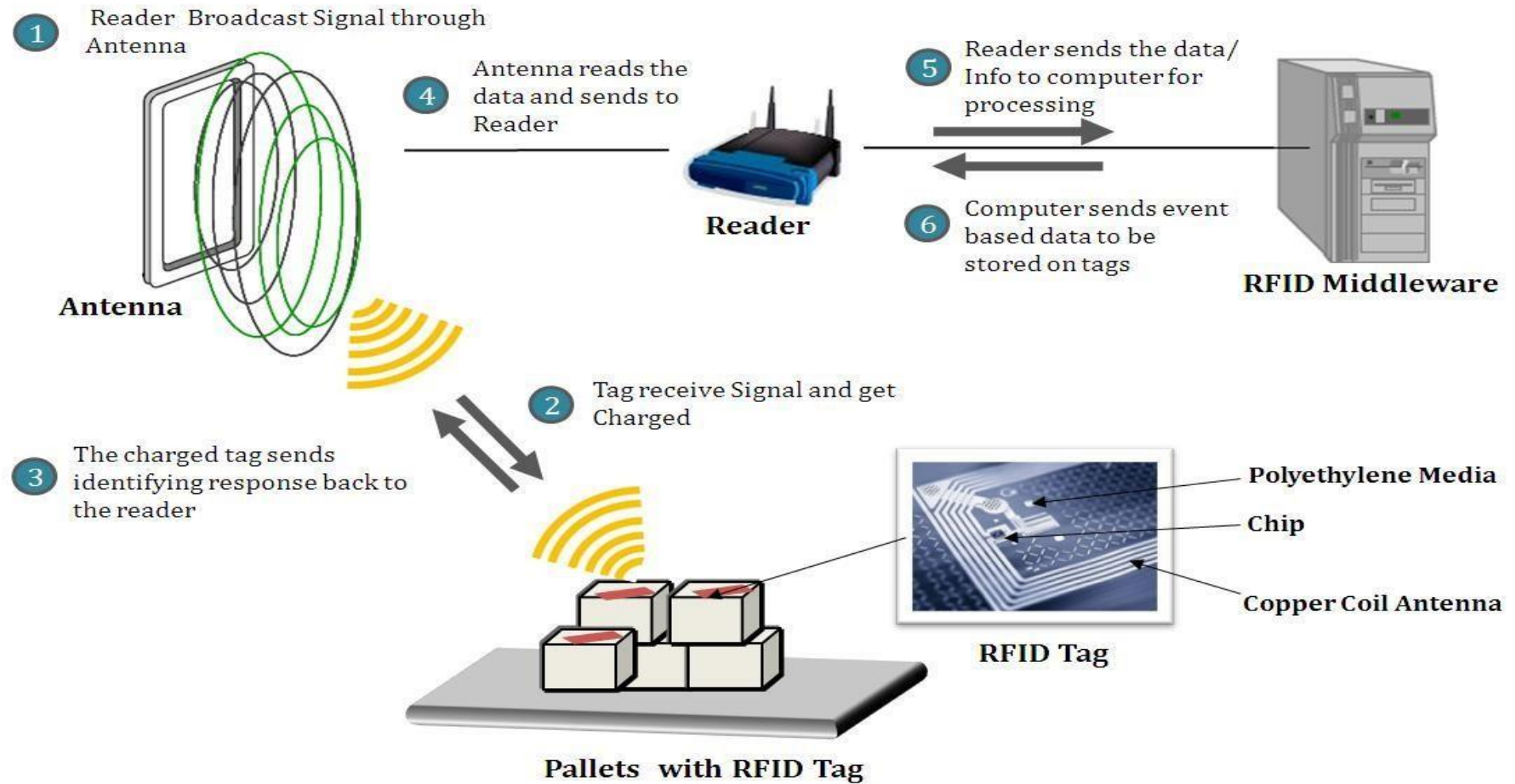
RFID System Components



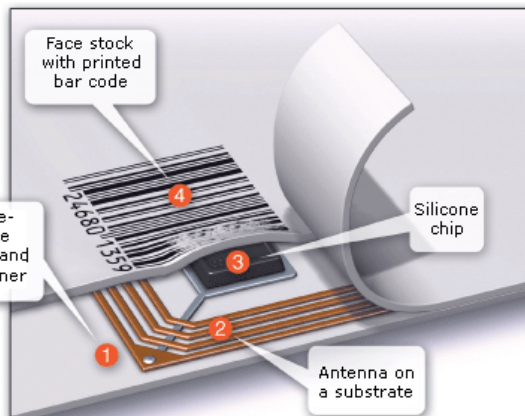
Parts of RFID System

- There are three parts to a RFID system:
- Antenna
 - Provides a means of communication and energy to communicate with RFID tag
 - RFID tag passes through field of the antenna and the RFID tag detects the activation signal from the antenna causing the RFID tag to transmit the information on the microchip to the transceiver.
 - Permanently affixed to a surface or handheld
- Transceiver
 - Has a decoder to interpret the data
- RFID Tag (Transporter)
 - Programmed with information

■ How it Work?



■ Examples



How RFID Works

- Basic components of RFID system combine in the same manner
- All objects are physically tagged with transponders
- Type of tag used varies from application to application
- Passive tags are most promising
- Transceivers are strategically placed for given application
- Access Control has readers near entrance
- Sporting events have readers at the start and finish lines

Advantages of RFID systems

- Ability to read data without visual access
- Ability to read data from moving objects
- Ability to read data at distance, from 3cm to 100 metres
- Ability to secure the tag data
- Ability to update data in the tag (write)
- Ability to have automated read of tags.
- Ability to have the tag form to suit the application

Benefits and Threats

Always A Pioneer, Always Ahead

- Airline passenger and baggage tracking made practical and less intrusive
- Authentication systems already in use (key-less car entry)
- Non-contact and non-line-of-sight
- Promiscuity of tags

History of RFID

- 1940-1950
 - First work exploring RFID by Harry Stockman
 - Followed advances in radio & radar
- 1950-1960
 - Era of exploration, laboratory experiments
- 1960-1970
 - First and most widespread commercial use
 - Electronic article surveillance, Sensormatic
- 1970-1980
 - Explosion of RFID development work
 - Animal and vehicle tracking, factory automation

History of RFID

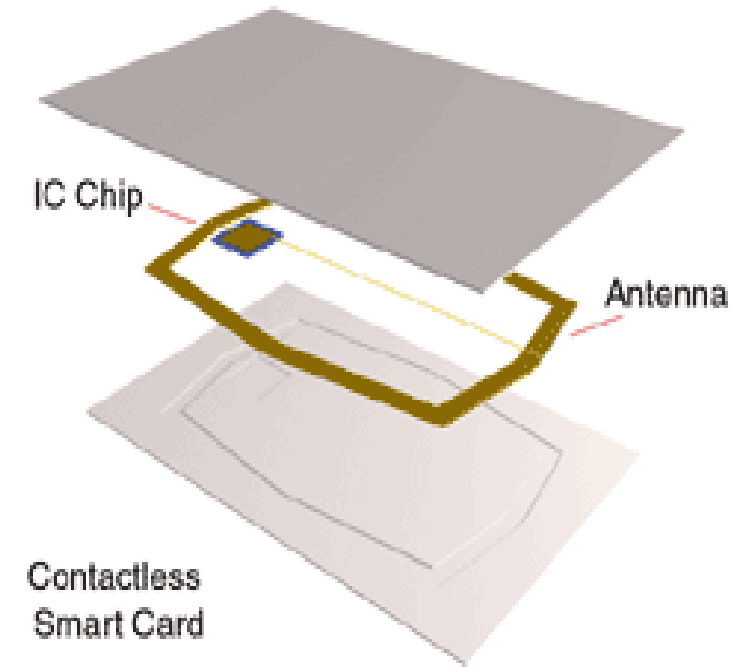
Always A Pioneer, Always Ahead

- 1980-1990
 - Commercial implementation enters mainstream
 - Transportation, personnel access, & animals
- 1990-2000
 - Emergence of Standards
 - Becomes part of everyday life
 - Electronic highway tolling system
- 2000-now
 - Exciting times await in the advancement of RFID

Access Control & Identification

Always A Pioneer, Always Ahead

- Cards for access to secure areas. Not only verifies identity but checks if certain requirements to enter have been met.
- Wristbands to provide access to unattended buildings.
- Wristbands at hotels and resorts acting as a key and as coupons to access services



RFID in Applications

- Health Care and pharmaceutical industry
 - Surgical equipment, Drug Pedigree, Blood banks, Patient tracking
- Animal Identification
 - Livestock tracking, Data critical for the safety of food supply, Ear tags, injectable tags, RFID tattoos
- Vehicle Identification
 - Fleet management, Access to parking lots, Railway industry
- Sports and Health
 - Racecar tracking, “Champion Chip” for time tracking
- Tracking people and objects
 - Children in theme parks, Protection of expensive objects
- Libraries
 - From barcodes to RFID tags.
- Production Line Control and Monitoring
 - Identify vehicles through assembly line prior to the execution of a given assembly task.
- Distribution and transportation
 - Order Filling, Shipping, Product and asset tracking

Technical problem with RFID

- RFID systems can be easily disrupted
 - Since RFID systems make use of the electromagnetic spectrum, they are relatively easy to jam using energy at the right frequency. This problem could be disastrous in business where RFID is increasingly used, like hospitals or in the military in the field.
- RFID reader collision
 - Reader collision occurs when the signals from two or more reader overlap. The tag is unable to respond to simultaneous queries.
- RFID tag collision
 - Tag collision occurs when many tags are present in a small area; but since the read time is very fast, it is easier for vendors to develop systems that ensure that tags respond one at a time.

Security and privacy problems with RFID

■ Loss of privacy

- Tag can be read at a distance, it become possible to gather sensitive data about individual without consent.

■ RFID tags with unique serial numbers could be linked to an individual credit card number.

- At present, each individual item has its own number. When the item is scanned for purchase and is paid for, the RFID tag number for a particular item can be associated with a credit card number.

Future with RFID

Always A Pioneer, Always Ahead

- RFID will replace barcode.
 - RFID is a great tool for the supply chain and companies wishing to better track their products and inventory. As a result, it will definitely become a requirement for all suppliers to use RFID tags when the tag become affordable.
- RFID's price will reduces
 - With mass production, their price eventually reduces to perhaps a cent.
- RFID chips are no bigger than grains of sand.

Future with RFID

Always A Pioneer, Always Ahead

- Every item in house will eventually come from the store with a tiny, almost invisible RFID tag attached.
- Most of the retailers and restaurants will use RFID to track condition of goods.



LONG RANGE HIGH FREQUENCY RFID



CONCLUSION

Conclusion

- Physical access control is an important system that need to be implemented by 24x7 monitoring, the security analysts and higher level authority at every point of the organization.
- Physical access control system controls people or assets at the entrance and exit point through the secure perimeter based on the authorization rules.
- Physical access control system combines and integrates various technology from smartcard, biometrics and RFID more secured system and better performance solutions.

Thank You



www.utem.edu.my