



# Cyber Security Unit – IV

**Dr. R. A. ROSELINE** M.Sc., M.Phil., Ph.D.,  
Associate Professor and Head,  
Post Graduate Department Of Computer Applications,  
Government Arts College, Coimbatore – 18.



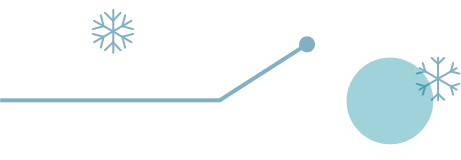
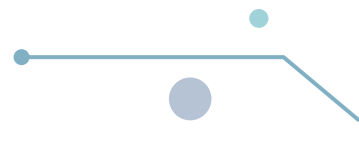
# Contents

- **Access Control**
    - Business Requirements for Access Control
    - User Access Management
    - System and Network Access Control
    - Operating System Access Control
    - Monitoring Access Control
    - Cryptography
  - **Physical Security**
    - Data Centre Requirement
    - Physical Access Control
    - Fire Prevention and Detection
    - Verified Disposal of Documents
    - Agreements
    - Intrusion Detection Systems
- 





# Access control

- Access control is the technical mechanism that restricts unauthorized users from the system, grants access to authorized users, and limits what authorized users can do on the system.
  - Access controls in addition to security policy are the key components of information security.
  - There are several ways in which an organization can implement access control.
  - There are two popular models to follow when it comes to access control: mandatory and discretionary.
- 
- 



# Business Requirements for Access Control

- **Access Control Policy**
  - In mandatory access control, the permission granted on the system is defined by policy. This is often used in highly secure and government installations. This policy requires a process known as labeling, where each user, file, and system is grouped in security categories.
- 
- 



# Discretionary access control

- Another popular access control system is discretionary access control. With discretionary access, permissions are not granted by policy but rather granted by the data or system owner. The reduced overhead of discretionary access control makes it more applicable to most private-sector companies.





# User Access Management

- Account Authorization
- Access Privilege Management
- Account Authentication Management







# Account Authorization

- Account authorization is also known as user registration. Whatever you call this process, the function of it will remain the same. This process allows for authorized users to establish initial access to the system and, moreover, what access on the system they will have.



- 
- This process takes place in most types of access control technologies but has an increased role in access control that uses digital certificates.
  - This is due to the fact that the digital certificate must be generated and distributed to the end user; the process can be somewhat automated using a technology known as a **registration authority**.
- 





# Access Privilege Management

- After a user has been with a company for a long period of time, access permissions may no longer align with current job responsibilities.
- The information security manager should have a procedure in place to review access permissions on a regular basis and make sure that the permissions are appropriate based on the job function of the user.


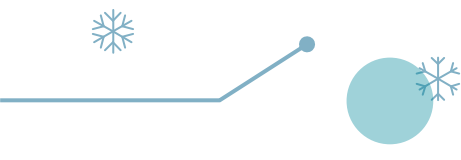
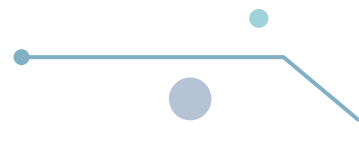




# Account Authentication Management

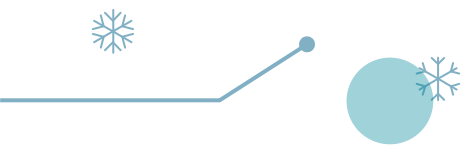
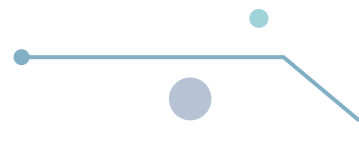
- Passwords should be changed on a regular basis; the current industry standard is around 30 days. However, the time to change passwords should reflect the security necessary to protect the information on the system.



- 
- There are two primary approaches to **single sign-on: script-based single sign-on and host-based single sign-on.**
  - With script-based single sign-on, the user logs in to the primary network operating system and when this happens, the operating system runs a log-in program, often called a login script, that will authenticate the user to other systems on the network.
- 
- 



# Disadvantage


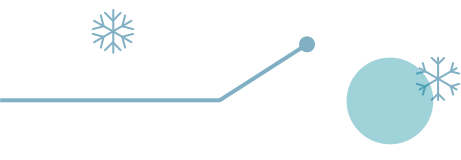
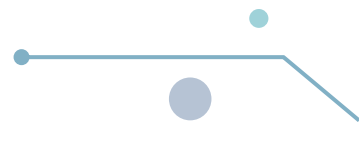
- The disadvantage to using this type of single sign-on is that the password stored in the log-in script is often stored in plaintext, which means that no encryption is used to protect the password in the file.
  - Any entity that reads this file will be able to recover the username and password for that user. Also, these username and password combinations are often transmitted on the network in plaintext.
  - This allows any malicious user with a network sniffer to capture the username and password.
- 
- 



# Network sniffer

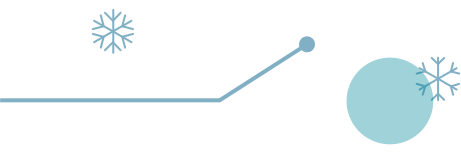
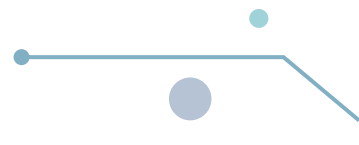
- A network sniffer is a utility available for free on the Internet that is used to read all the network packets on a network segment. This utility can be used for troubleshooting, but can also be used maliciously to record log-in attempts.
  - The second type of single sign-on implementation is much more commonly used than the script-based method mentioned previously.
  - This second type is known as host-based single sign-on because it uses a centralized authentication server or host.

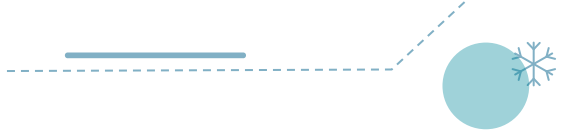
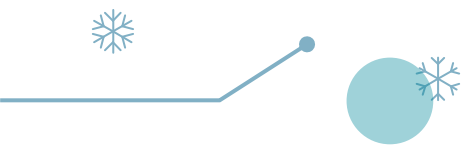
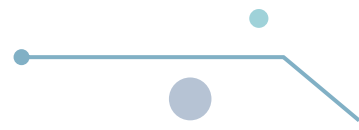


- 
- There are a large number of protocols that can be used for this type of single sign-on. Some of the more common include Kerberos and **RADIUS**.
  - There are a large number of secondary authentication protocols that are not used as often; these include protocols such as **SESAME** and **RADIUS**' successor, **DIAMETER**.
  - Many of these authentication protocols can be configured to send the username and password encrypted, and this can stop malicious users from intercepting the username and password with a network sniffer
- 
- 



# System and Network Access Control

- Protecting networking resources is one of the areas of information security that currently receives the most focus. When thinking of security, senior management often envisions firewalls, intrusion detection systems, and other technological solutions, but often overlooks the importance of integrating these with the existing user community.
  - A user with the appropriate access control is able to use any PC or workstation on the local area network to run an application or access certain data.
- 
- 

- 
- However, where such data or system is classified as sensitive or requires restricted physical access, an enforced path may be applied.
  - This is a straightforward configuration setting, performed by the information security manager, whereby access is restricted to a specific workstation or range of workstations.
  - Enforcing the path will provide added security because it reduces the risk of unauthorized access, especially where such a workstation is itself within a secure zone, requiring physical access codes or other physical security mechanisms.
- 
- 

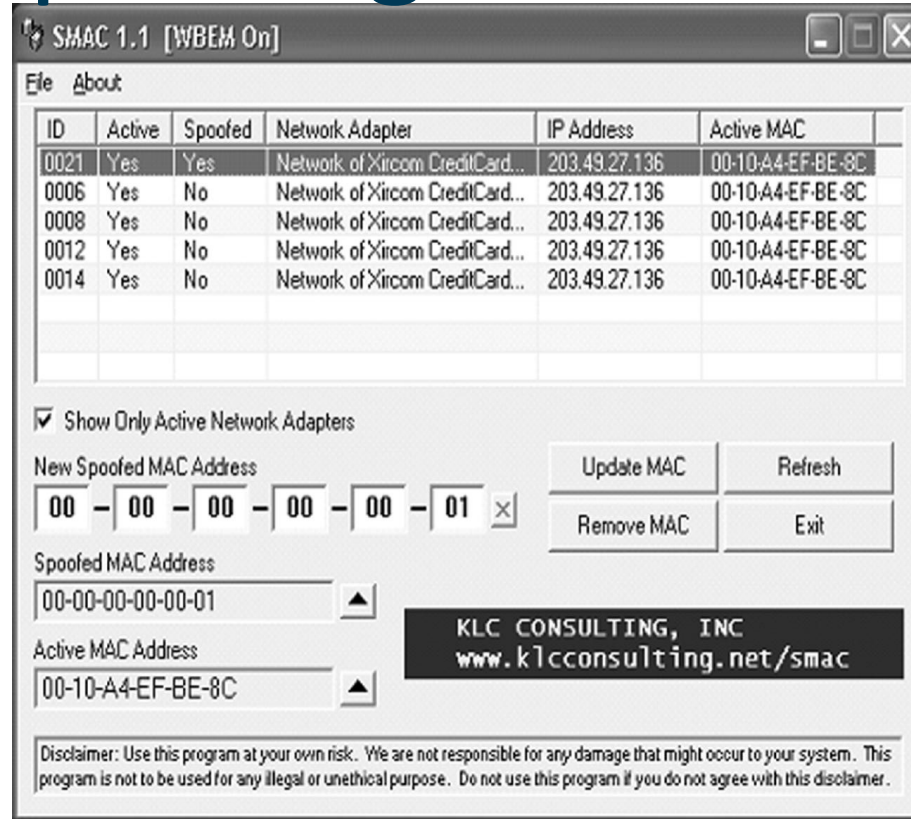




- The typical network uses user authentication, wherein a user provides a username for identification and a password for authentication.
- In some networks the authentication requires not just user authentication but node authentication as well.
- There are many different ways to get node authentication; it can be from a digital certificate issued to the machine, based on the system's IP address, or from the systems hardware address itself. Using any of these authentication components with the user authentication component is not a good idea.
- With the exception of the digital certificate, it is very easy to change an IP address or hardware address to “spoof” an address of an authorized machine.



# Spoofing Hardware



SMAC 1.1 [WBEM On]

File About

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0021	Yes	Yes	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0006	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0008	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0012	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C
0014	Yes	No	Network of Xircom CreditCard...	203.49.27.136	00-10-A4-EF-BE-8C

Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 00 - 00 - 00 - 00 - 01

Update MAC Refresh

Remove MAC Exit

Spoofed MAC Address: 00-00-00-00-00-01

Active MAC Address: 00-10-A4-EF-BE-8C

**KLC CONSULTING, INC**  
[www.klcconsulting.net/smac](http://www.klcconsulting.net/smac)

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.



- Spoofing the user on the rogue machine changes the system or IP address of the system to be that of another system that is trusted or permitted on network.
- The task of using hardware address node authentication was offered as a security solution to the problems with wireless networks.
- This authentication was easily bypassed with spoofing, leading to the same security problems that existed previously.
- Another key component of network security is to have network monitoring in place. One of the easiest ways to have the security of monitoring the network is to implement remote port protection.





- “Port” is the term for one of the hardware interfaces on a hub or switch. Most hubs or switches are classified by the number of ports on them. You will often hear of 24 port switches, which means that there are 24 slots for network cables to be connected to the switch. In most environments, there are ports that are not used and left open.
- If an attacker is able to get physical access to the switch, he can plug a new network device into the open port in the switch. Because this might lead to a security breach, the information security manager should be notified if one of these switch ports that is left open suddenly becomes active. This is where having remote port detection can provide security.





# Drawback

- The only real drawback to using this type of method for network segregation is if your organization is using Dynamic Host Configuration Protocol (DHCP).
- If your network uses DHCP, a server will automatically assign an IP address for all devices plugged into that network segment. A user can bypass the security of network address translation and routing by plugging the device into a new location and receiving a new IP address.





# System Standards

- There is difficulty in supporting multiple systems for the information security manager and the support staff. To minimize the differences between systems, it might be in the best interests of your organization to create a standard.
- This standard would then be a recommended guideline for how the systems should be configured and what software packages should be installed on the systems. This will also help minimize the amount of non-standard applications that will be installed but can have a dangerous security impact on the network.


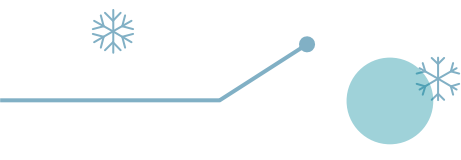
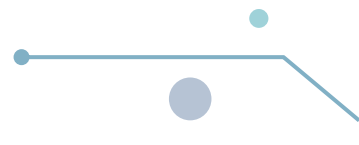





# Remote Access

- Remote access is a favorite target of hackers because they are trying to gain remote access to your organization's network. As such, additional security controls must be deployed to protect remote access and remote access services. Some of the more commonly deployed technologies include virtual private networking (VPN) and two-factor authentication.
- Virtual private networking takes advantage of encryption technologies to help minimize the exposure of allowing outside users to have access to the network.



- 
- Two-factor authentication is another technology that can help protect remote access. It uses multiple types of authentication technologies to provide for stronger authentication. Authentication can often be broken down into three categories:
    - Passwords
    - PINs
    - Passphrases
  - From the “something the user has” category, we would be looking at authentication components such as:
    - Smart cards
    - Magnetic cards
    - Hardware tokens
    - Software tokens
- 
- 

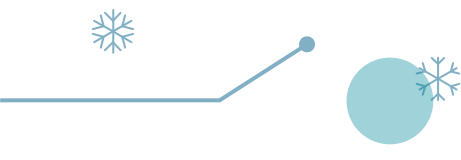
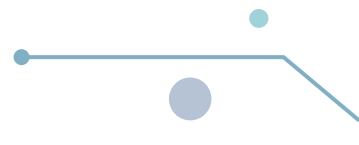


- 
- And from the “something the user is” category, we would be looking at biometrics and other behavior-based authentication systems. Biometric devices use unique characteristics of each person, including:
    - Fingerprints
    - Retina patterns
    - Hand geometry
    - Palm prints
  - Two-factor authentication takes an authentication component from two of the groups mentioned above. This requires more than just a username and password to get access. Because remote access connections to the network originate from outside the network, it is a prime location for stronger authentication controls.



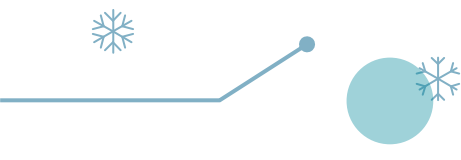
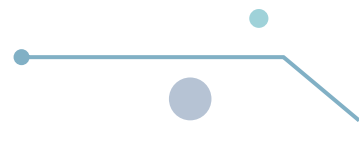


# Operating System Access Controls

- 1. Operating Systems Standards
  - Standards can minimize the amount of customization of employee workstations and this can minimize the difficulty in performing system and network maintenance. This can be extended further through the use of operating system standards.
  - These standards are provided by a number of sources, including the manufacturer, third-party security organizations, and the government. One of the most common sources of operating system standards is the National Institute of Standards and Technology (NIST).
- 
- 



## 2. Change Control Management

- One of the most unglamorous areas of information security is the change control process. In many small organizations, change control is omitted altogether and administration changes are made through an ad hoc process. While not having a change control process reduces administrative overhead, the resulting drawbacks are pretty severe.
  - Each organization is unique and the change control process should be modified to fit the organization. The most important steps are there to ensure that all changes are submitted, approved, tested, and recorded.
- 
- 



# Monitoring System Access

- Most current systems allow for enabling audit logs, and more and more systems are enabling logging by default. As an information security manager, you need to verify that event logging is enabled and is adequate for the relative security level of the system.
- These systems can also manage one of the more difficult components of log analysis: time synchronization. Many system clocks lose or gain time as the system stays in an operating production environment. A central log reporting system can also function as a network time server to help all system clocks stay synchronized.





# Monitoring Standards

- In organizations that wish to use information security monitoring, it is a good practice to include a warning banner on the systems before a user is authenticated. These warning banners should have three components:
  - This system is for authorized users only.
  - All activities on this system are monitored
  - By completing the log-on process, you are agreeing to the monitoring.

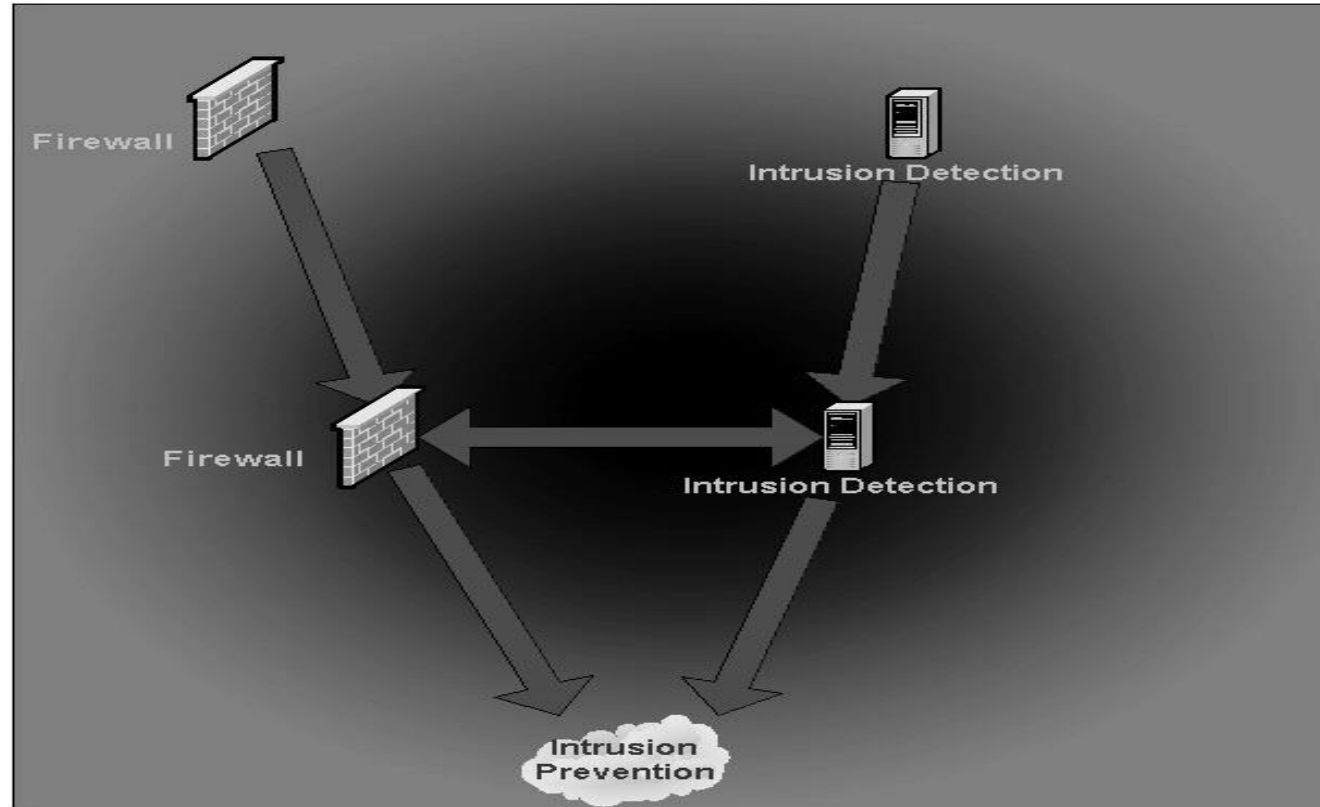




# Intrusion Detection Systems

- Intrusion detection systems (IDS) are designed to function like a burglar alarm on your house — from a technical standpoint, of course.
- These systems should record suspicious activity against the target system or network, and should alert the information security manager or support staff when an electronic break-in is underway.
- network-based intrusion detection system (NIDS) works by monitoring a network segment to determine if the network traffic matches the pattern of a well-known network attack.

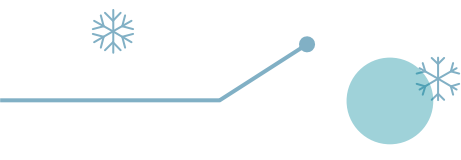
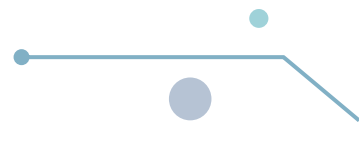




**IDS to IPS Migration**



# CRYPTOGRAPHY

- It is the study of secure communications techniques that allows only the sender and intended recipient of a message to view contents.
  - The Encryption and Decryption of email and other plain messages.
  - Example: Proton mail
  - The amount of time, effort and resources required to defeat the cryptosystem is known as the WORK FACTOR.
- 
- 





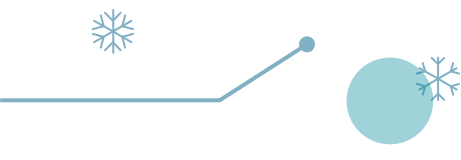
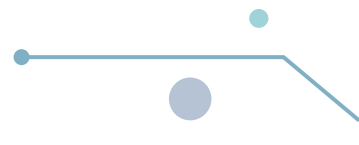
# Types of Encryption Algorithm

- Classical Substitution Cipher ( Caesar cipher).
- Poly-Alphabetic cipher.
  - There are also encryption machines.
  - Some are Enigma machines.
  - It had numerous rotors and switches that were attached to a typewriter keyboard.



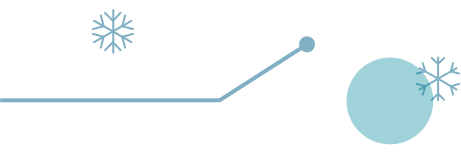
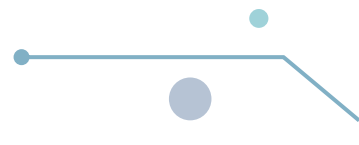


# Private Key

- These are easier to set up for a small number of users.
  - All of the secrecy from private key algorithms comes from keeping the key secure.
  - Private key cryptography is also known as symmetric cryptography because whatever process is done to encrypt the message, the reverse process is done to decrypt the message.
- 
- 

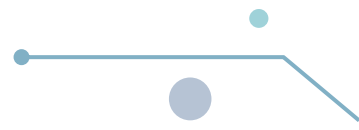


# Public key

- There are two keys that are related .
  - The two keys in public key cryptography are known as the private key and the public key.
  - These keys are related so the anything encrypted with the public key can be decrypted with the private key. It is called as public key because anyone can have the access to it.
  - The public key cryptography is also known as the asymmetric cryptography. The technical structures necessary to implement public key cryptography are collectively known as public key infrastructure (PKI).
- 
- 



# PKI Components

- Certification Authority
  - Registration Authority
  - Certificate Repository
  - Certificate Revocation list
- 
- 

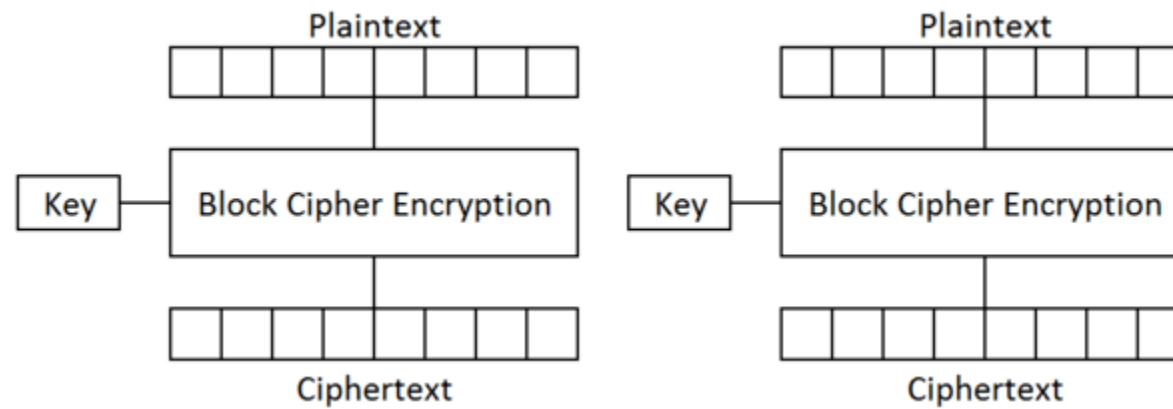


# BLOCK CHIPHER

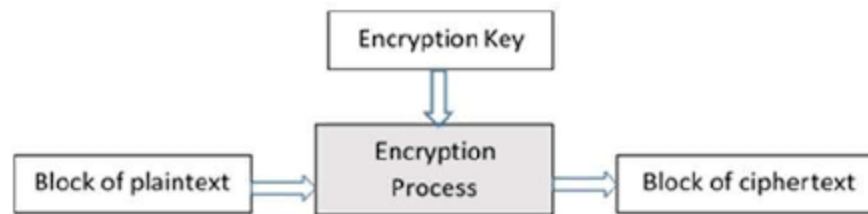
- In cryptography, a block cipher mode of operation is an algorithm that uses a block cipher to provide information security such as confidentiality or authenticity. A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.



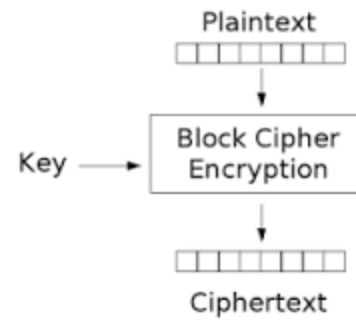
# Block mode



# Cipher block

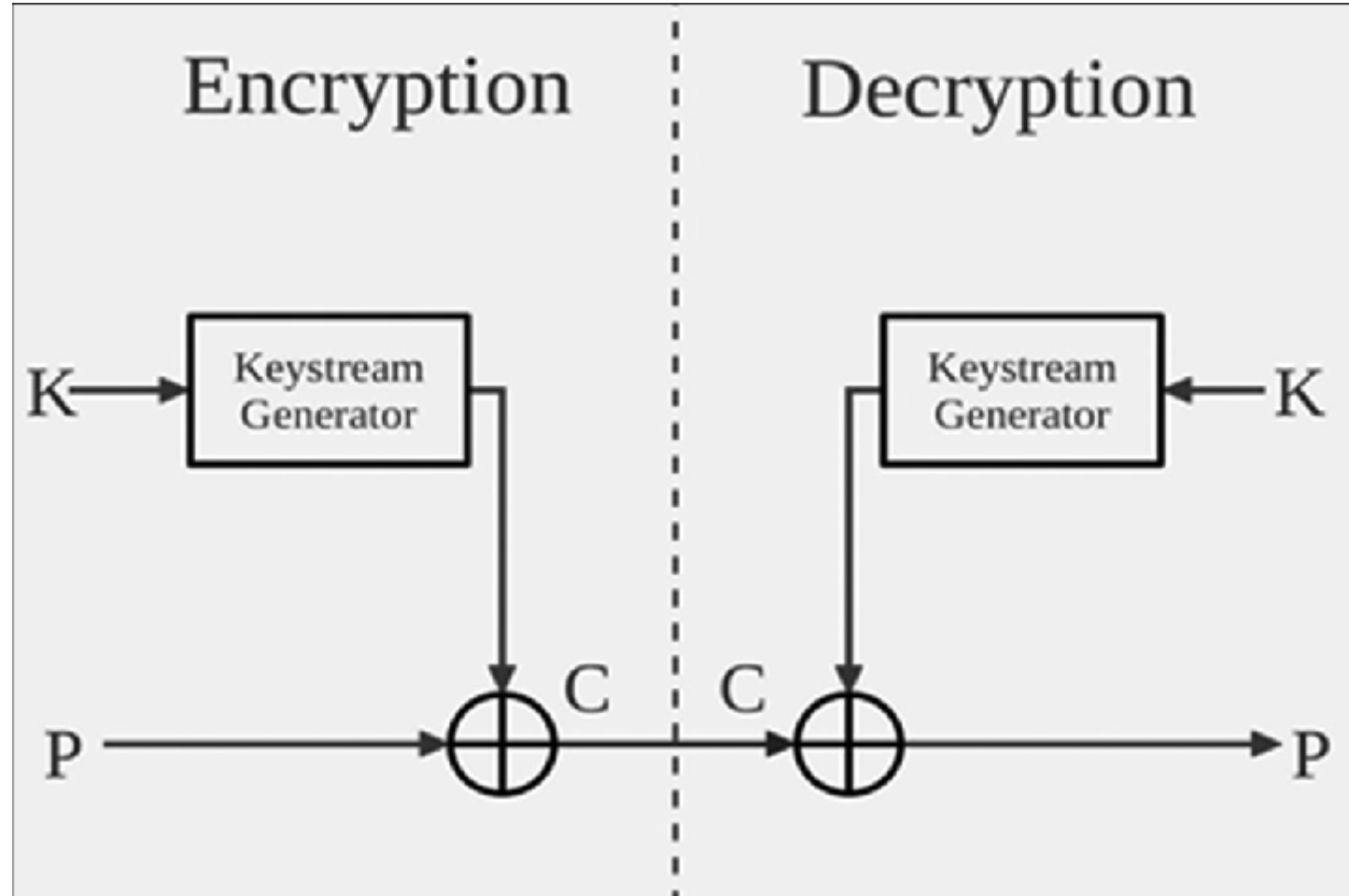


# Cipher Block



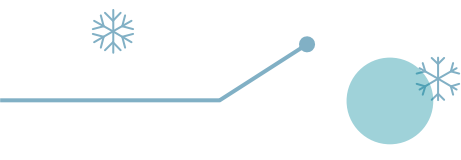
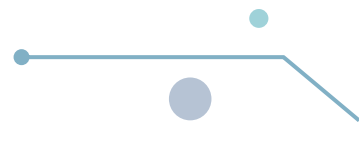


# Stream cipher





# Physical Security

- 1.Data Center Requirements
  - The nature of physical security for a data center should be one of concentric rings of defense — with requirements for entry getting more difficult the closer we get to the center of the rings.
  - While company employees, authorized visitors, and vendors might be allowed inside the outermost ring, for example, only data center employees and accompanied vendors might be allowed within the innermost ring
- 
- 



Concentric Rings of Protection

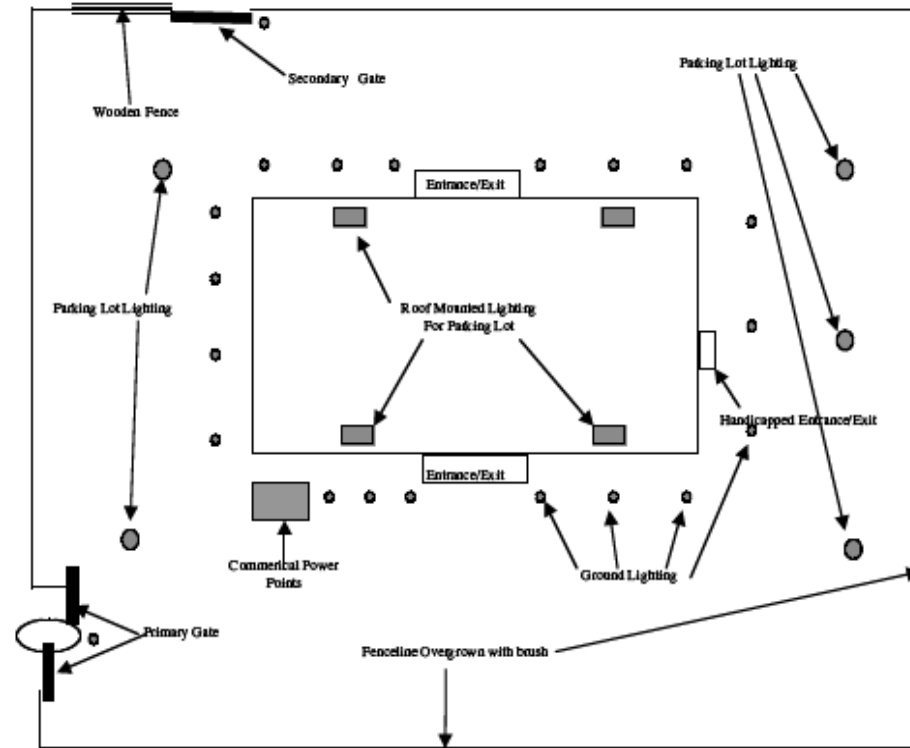


FIGURE 7.2 Outer Ring of Protection



## 2.Potential Threats

- When assessing potential threats, a large dose of common sense is often the best tool. The threats that exist for high-profile commercial or politically sensitive operations differ very much from those faced by, say, a biscuit manufacturer. Likewise, an operations center located in the middle of a turbulent city will face a much greater threat than one sited in an industry park in a semirural setting. We must also take into account the nature and recent history of the organization itself.





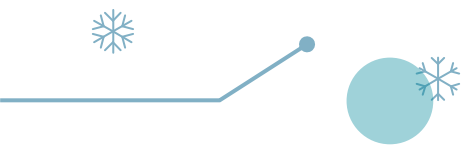
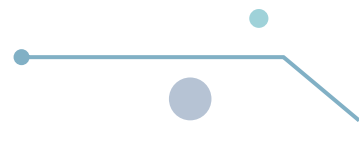
# 3. Attitude toward Risk

- Perhaps the most common complaint among information security professionals is that “they” do not understand the need for protective controls — “they” most often being management and senior management of the organization.
- It is also a fact of life that individual managers have equally variable attitudes toward risk. These constitute the third set of variations to consider when choosing physical access controls.



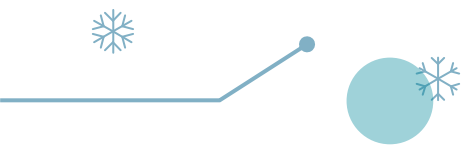
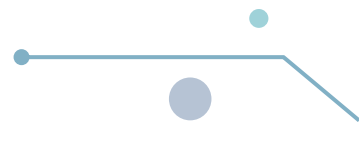


# Fire Prevention and Detection

- Fire prevention and detection standards vary according to the premises — whether or not the premises also house materials or processes that increase the risk of fire and whether or not the premises themselves are located in an area where fire risk is higher or lower.
  - Generally, the local fire authority (Fire Marshall in the United States) can be consulted for advice on fire prevention and detection measures, and architects and vendors of data center equipment are also ready to give advice.
- 
- 

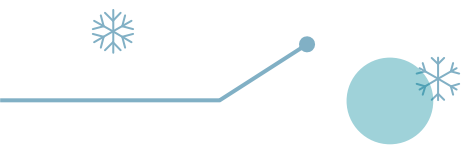
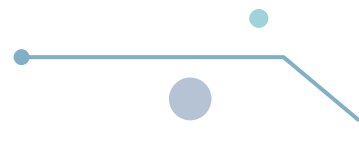


# 1. Fire Prevention

- No smoking is the first rule. Although this is a common requirement throughout the United States at the time of writing, it is neither a federal law nor a universally implemented state law. However, the use of smoking materials anywhere within a building that houses or processes critical information must be prohibited.
  - All flammable material — such as printer paper, plastic wrapping, and tapes — should be stored in an area separated from the main server or computer room by a fire-rated wall. Supplies for one day's processing can be kept in the server or computer room, but larger supplies must be stored separately.
- 
- 



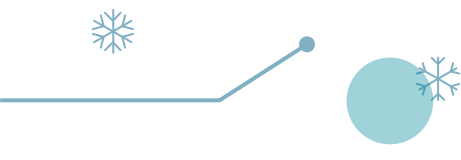
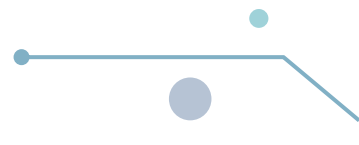
## 2.Fire Detection



- The most common sources of fires in data centers include the electrical system and the hardware. Breakdowns in insulation and the resultant short-circuiting can lead to intense heat that can melt materials or cause a fire.
  - Data center fires are often small or smoldering, with little effect on the temperature in the room. Because the smoke itself can impact the computer hardware, it is necessary to employ a detection system that is sensitive to smoke and other products of combustion rather than the temperature.
- 
- 





# 3. Fire Fighting

- In data centers, as much damage can be done by the fire suppression equipment as by the fire itself. Nonetheless, effective fire suppression systems must be installed in data centers.
  - A passive system reacts to smoke and fire without manual intervention.
  - The most common forms of passive suppression are sprinkler systems or chemical suppression systems. Sprinkler systems can be flooded (wet pipe) or pre-action (dry pipe).
- 
- 

- 
- A flooded system means that the pipes are full at all times, which allows the system to discharge immediately upon detection.
  - A pre-action system will fill the sprinkler pipes upon an initial detection, but will delay discharging until a second detection criteria has been met. Chemical total flooding systems work by suffocating the fire within the controlled zone.
- 



# Verified Disposal of Documents

- While security precautions and fire prevention and suppression systems can ensure the safety of information within data centers, often little is done to protect information when it leaves the data center. Printed documents and documents on electronic media all leave the data center and, hopefully, fall under policies and standards for the protection of data throughout the workplace. But when documents are disposed of, all too often the commonsense rules for protecting information are left behind.

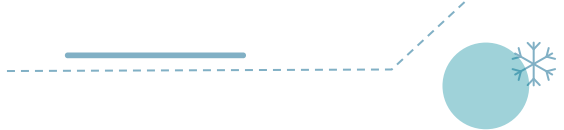
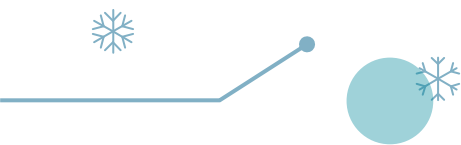
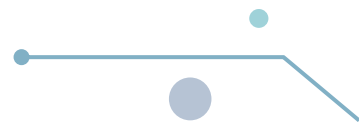




# 1. Collection of Documents

- The procedures for the collection of documents prior to their disposal should be documented and taught to all employees — and should avoid using large receptacles clearly marked “Confidential Documents Only.”
- Where documents are collected in bins, we have to make a decision on whether or not to lock the bins.



- 
- the advantages are that paper is secure (relatively) once deposited in the bin and we can demonstrate — to clients and auditors — that our information security circle of protection encompasses documents ready for disposal.
  - Disadvantages include the procedures necessary to track keys, the extra expense, and the added attraction (for wrong-doers) of a locked (versus unlocked) document bin.
- 
- 



## 2. Document Destruction Options

- There are three basic options for destruction of documents: recycling (commonly called pulping), shredding, and burning; some organizations use a combination of one or more of these.
- Shredding paper increases its volume and sometimes produces a false sense of security. Less expensive shredders, in fact, only cut paper into ribbons that can be easily pieced together again and read.





# 3.Choosing Services

- Document disposal and recycling functions are most often contracted services. However, the organization's responsibility for security of the documents does not end when they are removed from the facility. Making sure that the documents are subject to secure and reasonable processes until the information is destroyed is still the organization's facility's responsibility.



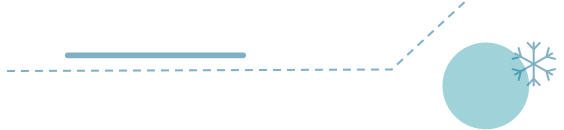
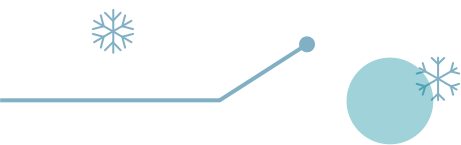
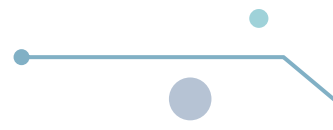


# Agreements

- The agreement must limit the vendor to use and disclosure of documents and the information contained in the documents to those uses stated in a contract.





- 
- Contractual language protecting the confidentiality of the waste should be built into all contracts with solid waste and recycling haulers and include the following elements:
  - Specify the method of destruction or disposal.
  - Specify the time that will elapse between acquisition and destruction or disposal of documents (or electronic media, if that is also to be disposed of).
  - Establish safeguards against breaches in confidentiality.
  - Indemnify the organization from loss due to unauthorized disclosure.
  - Require that the vendor maintain liability insurance in specified amounts at all times the contract is in effect.
  - Provide proof of destruction or disposal.
- 
- 



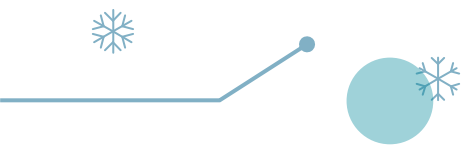
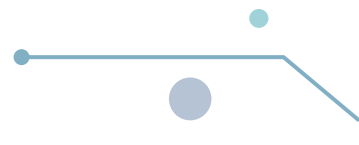
# Intrusion Detection Systems

- Intrusion detection systems mean tools used to detect activity on the boundaries of a protected facility.
- The simplest IDS is a guard patrol. Guards who walk the corridors and perimeter of a facility are very effective at identifying attempts to break into the facility and either raising the alarm or ending the attempt by challenging the intruder.





# 1. Purpose

- Our first task in defining the requirements of an IDS is to define what is to be protected and what is the level and nature of the threat.
  - the purpose of the IDS relate to the history of the facility. For example, has there been a specific parking lot incident, grounds incident, or a property/facility trespassing incident? Are there general vulnerability concerns that may include trespass, assault, or intimidation? When was the last occurrence, and what were the circumstances? Are the authorities aware and involved? Is there documentation available for review?
  - Answering these questions will help define the purpose of the IDS.
- 
- 

# 2.Planning

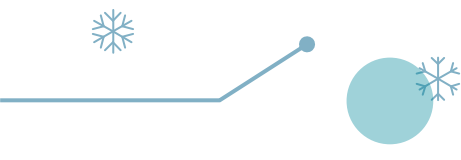
- The planning should have been carried out with an objective to provide a solution that addresses:
  - Surveillance
  - Control
  - Maintenance
  - Training
- During the planning, the nature of the facility and the contents of the facility themselves should be taken into account.

# 3.Elements

- The planning should produce a draft design that addresses the requirements of the premises.
  - Elements to consider when installing an IDS include:
    - Video surveillance
    - Illumination
    - Motion detection sensors
    - Heat sensors
    - Alarm systems for windows and doors
    - “Break-glass” sensors (noise sensors that can detect the sound made by broken glass)
    - Pressure sensors for floors and stairs



# 4.Procedures

- Whatever tools or technologies are used in the IDS, the system will fail to provide security unless adequate procedures are put in place and training on those procedures is given to staff expected to monitor and react to alarms created by the IDS.
  - Procedures should also include logging procedures that allow for all events — not just events requiring responses — to be logged for audit purposes or for purposes of follow-up.
- 
- 