Table of Contents

Table of Contents 1
C1: Introduction to Internet Security 3
//Key Security Concepts 3
-> CIA… 3
//Security Attacks 3
C2: Symmetric Encryption & Message Confidentiality 4
...Create-> Cryptography 4
//symmetric encryption 4
//Advanced Encryption Standard 4
//Feistel Cipher 4
//asymmetric encryption 4
...Attack-> Cryptanalysis 5
C3: Public Key Cryptography & Message Authentication 6
//Approaches to Message Authentication(3) 6
C4: Key Distribution & User Authentication 8
C5: Electronic Mail Security 9
//PGP Operation 9
C6: Transport level Security 10
SSL Session: 10
SSL Connection: 10
SSL exchanges 10
//SSL/TLS Record Protocol 11
C7: IP Security 12
//Application of IPSEC 12
General IP Security mechanisms provide: 12
1. Authentication AH 12
2. Confidentiality ESP 12
3. Key Management IKE 12
Security Association SA 12
1. Transport Mode 12
2. Tunnel Mode 12
C8: Intruder 13
//Intruder 入侵者 (hackers or crackers) 13
Masquerader (Outsider) 13
Clandestine (Outsider/Insider) 13
Misfeasor (Insider) 13
Countermeasure: 13
C9: Firewalls 15
//Firewalls Characteristics 15
● Four techniques: 15
Firewall types: 15
Packet filtering 15
Stateful Inspection 15
Application Proxy 15
Circuit-level Proxy 15

C10: Malicious Software 17

C11: Risk Management 18

//Risk Management 18

Compliance 18

Risk Analysis 18

Risk Types 18

Risk Assessment 18

Risk Strategy 18

Risk Control 19

C1: Introduction to Internet Security

Computer Security Concepts

1. Computer security: generic name for the tools designed to protect data and thwart阻止hackers
2. Network security: measures to protect data during transmission
3. Internet security: measures to protect data during transmission over a collection of interconnected networks
    a. Focused. to deter, prevent, detect, and correct security violations that involve the transmission of information

//Key Security Concepts

- Information Security
- Hardware
- Software
- Data
- Networks
- Systems

-> CIA...

Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes - Passive attack: Release of message content, Traffic analysis
Integrity	The property that data has not been altered or destroyed in an unauthorized manner - Active attack: Masquerade, Modification of messages, Replay
Availability	The property of being accessible and useable upon demand by an authorized entity - Active attack: Denial of service

//Security Attacks

Passive attack	• Learn or make use of information from the system but does not affect system resources • gather information covertly隐蔽 • Eg.: eavesdropping, traffic analysis, and data interception
Active attack	• Attempts to alter system resources or affect their operation • Difficult prevent because of the wide variety of potential vulnerability (physical,software, network) • data modification, unauthorized access, denial of service (DoS), spoofing, or injection of malicious code

C2: Symmetric Encryption & Message Confidentiality

//Symmetric & Asymmetric Encryption
//Advanced Encryption Standard
//Feistel Cipher
//Cryptanalysis

Cryptology...

...Create-> Cryptography

//symmetric encryption

- 1key: Secret key
- plaintext processed by
  - **1. Block**
    operation types: Substitution, Transposition/permutation
    - DES, 3DES, AES

	DES	3DES	//Advanced Encryption Standard AES
Block size	64 bits	64 bits	128 bits
Key size	56 bits	112 / 168 bits	128 / 192 / 256 bits
Round	16	16 x 3	10 / 12 / 24
Operation	Permutation /Substitution	Permutation /Substitution	Substitute bytes /Shift rows/ Mix columns /Add round key
Algorithm	DEA (Feistel)	Triple DEA	Rijndael / Substitution-permutation network

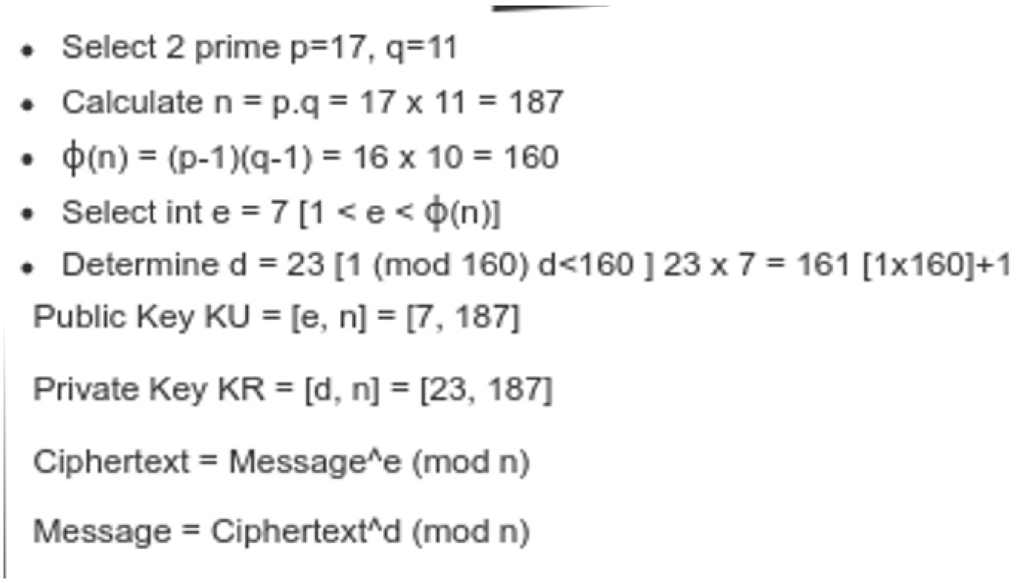
  - **2. Stream**
    operation type: Substitution
    - RC4

//Feistel Cipher

A substitution is performed on the left half
Apply round function F with subkey Ki to right half
Take the result to XOR with left half
Permutation is performed that consists interchange of two halves

//asymmetric encryption

- 2keys: Public and Private key
  - 1. Integer factoring
    **RSA



- Select 2 prime p=17, q=11
- Calculate n = p.q = 17 x 11 = 187
- ϕ(n) = (p-1)(q-1) = 16 x 10 = 160
- Select int e = 7 [1 < e < ϕ(n)]
- Determine d = 23 [1 (mod 160) d<160] 23 x 7 = 161 [1x160]+1

Public Key KU = [e, n] = [7, 187]

Private Key KR = [d, n] = [23, 187]

Ciphertext = Message^e (mod n)

Message = Ciphertext^d (mod n)

**

- 2. Discrete Logarithm
  - Diffie-Hellman (DH)
  - Digital Signature Standard (DSS)
  - Elliptic Curve (EC)
  - ElGamal

...Attack-> Cryptanalysis

(Process of attacking to discover the plaintext or key)

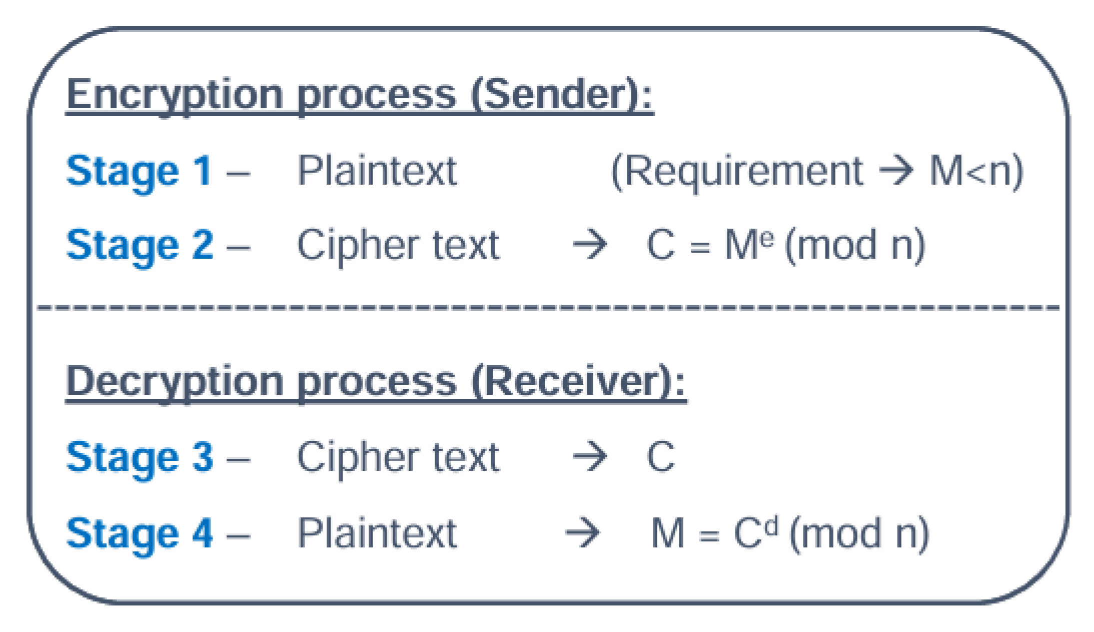
Brute force attack	• Trying and testing all possible keys in order to recover the plaintext from ciphertext • all possibilities are searched exhaustively
Dictionary attack	• Defeating a cipher text by trying to determine decryption key searching a large number of possibilities • only tries possibilities that are most likely to succeed
Probable word attack	• Make guess to word that may occur in the text like encrypted document

C3: Public Key Cryptography & Message Authentication

//RSA Encryption Algorithm (No calculation)

RSA is a block cipher

- The most widely implemented



Encryption process (Sender):

Stage 1 – Plaintext (Requirement → $M<n$)

Stage 2 – Cipher text → $C = M^e \pmod n$

Decryption process (Receiver):

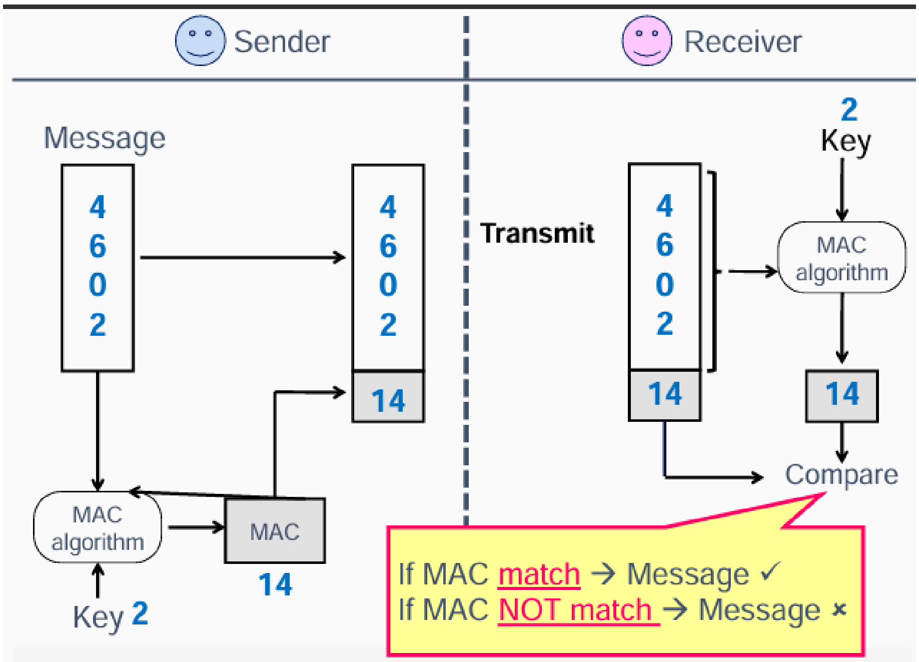
Stage 3 – Cipher text → C

Stage 4 – Plaintext → $M = C^d \pmod n$

//Approaches to Message Authentication(3)

1. Authentication using conventional(normal) encryption
   a. Only sender and receiver shared a key
2. Message authentication without message encryption
   a. Not rely on encryption
   b. Confidentiality is not provided
   c. An authentication tag is generated and appended to each message
3. Authentication code
   a. Use secret key instead of encryption

b. A secret key used to generate a small block of data(message authentication code MAC)



If MAC match → Message ✓
If MAC NOT match → Message ×

Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

. MAC/ One-way hash/ Secure Hash/ HMAC

One-way hash	● Accepts a variable size message M as input ● Produce a fixed size message digest H(M) as output
Secure Hash	● Intended to provide proof of data integrity by providing verifiable fingerprint
HMAC	● Use specific algorithm that combine cryptographic hash function and a secret key

C4: Key Distribution & User Authentication

//Kerberos Server

Kerberos authentication server (AS):	A centralized trusted authentication server for the whole system, who issues long lifetime tickets.
Ticket-granting servers (TGS):	Issue short lifetime tickets
Service server (S):	Provide different services.

Kerberos

Threats(3?)

- User impersonation
- Eavesdropping, Replay, DOS
- Network address impersonation

Version4

C= User logs on and requests service

C->AS=Request TGS ticket

AS ->C=TGS ticket +session key

C->TGS=TGS ticket+Authenticator

TGS->C=Service ticket+session key

C->V=Service ticket +Authenticator

V->C= Provide service

C5: Electronic Mail Security

PGP consist of 5 services:
Authentication
Confidentiality
Compression (ZIP)
E-mail compatibility (RADIX-64)
Segmentation & Reassembly

PGP	S/MIME
//PGP Operation 1-Authentication 1. Sender creates a message. 2. Make SHA-1160-bit hash of the message. 3. Attached RSA signed hash to the message. 4. Receiver decrypts & and recovers hash code. 5. Receiver verifies received message hash. 2-Confidentiality 1. Sender forms 128-bit random session key. 2. Encrypts message with session key. 3. Attaches session key encrypted with RSA. 4. Receiver decrypts & recovers session key. 5. Session key is used to decrypt message. 3- Confidentiality & Authentication 1. Create a signature & and attach it to the message. 2. encrypt both message & signature. 3. attach RSA/ElGamal encrypted session key.	Certificate (X.509) Address SMTP limitations -Enveloped data -Signed data -Signed and enveloped data -Clear-Signed data

C6: Transport level Security

Two important concepts of SSL:

SSL Session:

- An association between a client and a server.
- Sessions are created by the Handshake Protocol.
- A session defines a set of cryptographic security parameters, which can be shared among multiple connections.

SSL Connection:

- A transport that provides a suitable type of service,

e.g., a peer-to-peer relationship. Every connection is associated with one session.

SSL exchanges

SSL Handshake Protocol	The most complex part of SSL. Used before any application data is transmitted. Allows the server and client to authenticate each other. Negotiates: ● Encryption algorithm ● MAC (Message Authentication Code) algorithm ● Cryptographic keys Consists of a series of messages exchanged by the client and server. **Operations**: Phase 1: Establish Security Capabilities ● Client sends client_hello ● Begins logical connection and sets security capabilities Phase 2: Server Authentication and Key Exchange ● Server sends certificate (X.509 chain) if authentication is needed ● Certificate required for all key exchange methods except anonymous Diffie–Hellman ● For fixed Diffie–Hellman, certificate includes server's public DH parameters Phase 3: Client Authentication and Key Exchange ● Client verifies server certificate (if present) ● Checks server_hello parameters ● If valid, client sends key exchange message and optional client certificate Phase 4: Finish ● Client sends change_cipher_spec to apply new CipherSpec ● (not part of Handshake Protocol, but required for transition) ● Immediately sends finished message encrypted with new keys and algorithms

SSL Change Cipher Spec Protocol	Structure: 1-byte message, value = 1 Purpose: Instructs switch from current to pending cryptographic state Process: Activates new cipher suite for future communication
SSL Alert Protocol	Structure: 2-byte message Byte 1: level ; Byte 2: alert Purpose: Notifies peer of SSL/TLS alerts Process: Alerts are compressed and encrypted using current session settings

//SSL/TLS Record Protocol

Services SSL/TLS connections (2)

Confidentiality

- Handshake Protocol defines a shared secret key that use for encryption of SSL Payloads

Message integrity

- Handshake Protocol defines a shared key that use to form a message authentication code (MAC)

SSL/TLS Record Protocol Operations

1. Application Data
   - The Record Protocol takes an application SEND messages to be transmitted...
   - raw data generated by the application layer (e.g., HTTP requests).
2. Fragment
   - The data is broken into chunks that are suitable for transmission, as SSL/TLS has a maximum record size limit.
3. Compress (optional)
   - The fragmented blocks may be compressed to reduce size, although compression is often disabled due to security concerns.
4. Encrypt (Compress + MAC)
   - First, a Message Authentication Code (MAC) is added to ensure integrity.
   - Then the resulting data (compressed + MAC) is encrypted for confidentiality.
5. Append SSL Header
   - A record header is added, specifying the content type, SSL version, and length.

C7: IP Security

//Application of IPSEC

- **Secure branch office connectivity over the Internet (VPN)**
  - *A company can build a secure virtual private network over the Internet or a public WAN, reducing private network costs and management overhead.*
- **Secure remote access over the Internet (VPN client)**
  - *Remote users can securely access the company network via IPsec, reducing toll charges and enabling telecommuting.*
- **Establishing extranet and intranet connectivity with partners**
  - *IPsec ensures secure communication between organizations with authentication, confidentiality, and key exchange.*
- **Enhancing electronic commerce security**
  - *IPsec ensures designated traffic is encrypted and authenticated, adding a security layer beyond the application level.*

General IP Security mechanisms provide:

1. Authentication AH	ensures data integrity and authenticity.
2. Confidentiality ESP	Encapsulating Security Payload (ESP) provides encryption for secure communication.
3. Key Management IKE ● Manual ● Automated OAKLEY ISAKMP	Key distribution and agreement can be manual or automated using protocols like Oakley and ISAKMP.

Security Association SA

- SA is a one-way logical connection, providing security services between sender and receiver.

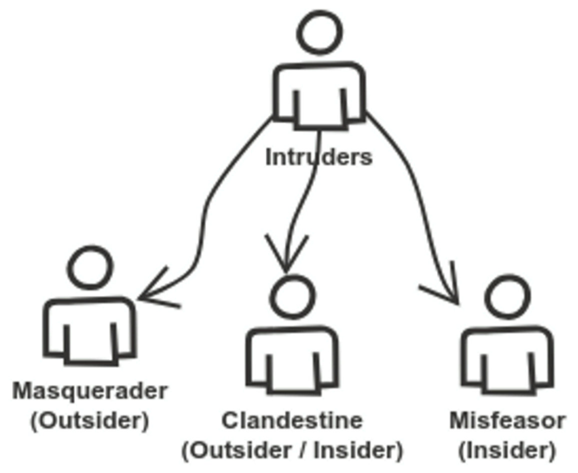
(Each SA is uniquely identified by) 3 parameters:

1. Security Parameter Index (SPI)
2. IP Destination address
3. Security Protocol Identifier

1. Transport Mode	protects upper-layer protocols by applying security to the payload of an IP packet.
2. Tunnel Mode	protects the entire IP packet by encapsulating it with security headers and treating it as the payload of a new IP packet, commonly used in VPNs.

C8: Intruder

//Intruder 入侵者 (hackers or crackers)

 Intruders Masquerader (Outsider) Clandestine (Outsider / Insider) Misfeasor (Insider)	**Masquerader (Outsider)** unauthorized individual who exploits legitimate user's account
	Clandestine (Outsider/Insider) Individual who seizes supervisory control掌握监管控制权 and uses it to evade规避 auditing or access controls
	Misfeasor (Insider) Legitimate user, who misuses their privileges

Countermeasure:

Detection - detect/ report	Statistical anomaly: ✅masqueraders-unlikely mimic behavior ❌misfeasor define normal, expected behavior ● Threshold (define limit, check event frequency) ● Profile (check change in user activity, their behavior) Rule-based: ✅misfeasor define proper behavior define set of rules, decide what behavior is intruder ● anomaly (rules to detect deviation from previous usage) ● penetration identification (search suspicious behavior)
Prevention - detect/drop	Attempts to thwart阻挠 all possible attacks (a very challenging task) will work but in real life, it might fail.
Password management	● Most multi-user systems require a user ID and password ● Password authenticates the user's identity ● User ID defines access privileges **Salt** Used in password hashing to: • Prevent duplicate passwords • Increase password complexity • Prevent hardware brute-force attacks **Verifying Password File** Ensures password file integrity and prevents unauthorized access.

	Password Selection Strategies • User education – Teach users to choose strong passwords • Computer-generated passwords – System provides secure passwords • Reactive checking – System tests existing passwords and removes weak ones • Proactive checking – System checks password strength during creation and rejects weak ones **Criteria for Better Passwords** • Use letters, numbers, and symbols • Minimum 8 characters • Avoid easy-to-guess passwords like “admin” or “abc123”
Honeypot	● Divert转移 an attacker from accessing critical systems. ● Collect information about attacker activity. ● Encourage the attacker to stay on the system long enough for administrators to respond
Audit record	record of ongoing activity of users must be maintained as input to an intrusion detection system Two plans: Native audit records ● Collect user activity by os software ‘accounting software’ Detection-specific audits records ● Generate audit records only required by intrusion detection system

C9: Firewalls

//Firewalls Characteristics

Firewall Design Goals

- All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall).
- Only authorized traffic (defined by the local security policy) will be allowed to pass.
- The firewall itself is immune to penetration. Trusted computer systems are suitable for hosting a firewall and are often required in government applications.
- **Four techniques:**
    - Service Control:
        - Determines services can accessed, inbound or outbound
        - Filters traffic based on ip, protocol, port num
        - Provides proxy software or host itself that receives and interprets each service request
    - Direction Control:
        - Determines direction in which particular service requests may be initiated and allowed to flow through the firewall
    - User Control:
        - Controls access to a service according to which user is attempting to access
        - Typically applied to local users, also for incoming traffic from external users
    - Behavior Control:
        - Controls how particular services are used
        - Eg.: filter email to eliminate spam

Firewall types:

Packet filtering	• Filters based on IP, port, protocol. • Pros: Fast, simple. • Cons: No deep inspection, no authentication.
Stateful Inspection	• Tracks connection state and context. • Detects session-related attacks and sequence issues.
Application Proxy	• Intercepts application traffic (e.g., FTP, Telnet). • Pros: High security, audit-ready. • Cons: Slower, higher processing load.
Circuit-level Proxy	• Relays TCP segments without inspecting content. • Controls which connections are allowed. • Often used for outbound trusted traffic.

C10: Malicious Software

Virus	● A malicious code embedded within a program that replicates by inserting copies of itself into other programs and performs unwanted functions.
Worm	● A self-replicating program that spreads across network connections, often via email or file sharing, without needing a host program.
Trojan Horse	● A seemingly useful program that contains hidden malicious functions, such as sending sensitive data to an attacker when executed.
Ransomware	● (Not explicitly in the text but related) Malware that encrypts a user’s data and demands payment for decryption.
Social Engineering - Phishing	● Using crafted emails or websites to trick users into revealing sensitive personal information.
Logic Bomb	● Malicious code embedded in a program that triggers harmful actions when specific conditions, such as a date, are met.
DDoS (Distributed Denial of Service)	● An attack that overwhelms a target system with excessive traffic from multiple compromised hosts (zombies), making it unavailable to legitimate users.
Bots/Zombies → Botnet	● Compromised computers controlled remotely (zombies) that form a network (botnet) used to launch coordinated attacks like DDoS.

C11: Risk Management

//Risk Management

Compliance

Regulations: Rules set by governing bodies to ensure organizational adherence.
Legislation: Laws enacted by authorities that organizations must follow.
Policy: Internal guidelines and standards to maintain compliance and manage risks.

Risk Analysis

Risk Types	i. Internal and external • An internal risk comes from within an organization (such as employee theft) • An external risk is from the outside (like the actions of a hacktivist) ii. Legacy systems • Pose risks due to outdated hardware or software iii. Multiparty • Impact that vulnerabilities of one organization can have on other organizations that are connected to it iv. Intellectual property (IP) • Theft involves stealing creative works or inventions v. Software compliance and licensing • Risks arise from violating licensing agreements for specialised software
Risk Assessment	Qualitative ● Assign value or label Quantitative ● Calculate likelihood and impact ● Single Loss Expectancy (SLE) = Asset Value (AV) x Exposure Factor (EF) ● Annualised Loss Expectancy (ALE) = SLE x Annualised Rate of Occurrence (ARO)

Risk Strategy

Acceptance: Simply means that the risk is acknowledged but no steps are taken to address it (eg. Loss of car due to Flood)
Transference: transfer the risk to a third party (eg. Insurance Company)
Avoidance: Involves identifying the risk but making the decision to not engage in the activity(eg. Park at higher or other area/Not purchase it)
Mitigation: Risk mitigation is the attempt to address risk by making it less serious. (eg. Weather Forecasts, Early Flood Warning Systems, Flood Barriers

Risk Control

Deterrent: discourage security violations before they occur.
Preventative: prevent the threat from coming in contact with the vulnerability
Physical: implements security in a defined structure and location.
Detective: A detective control is designed to identify any threat that has reached the system
Compensating: provides an alternative to normal controls that for some reason cannot be used.
Corrective: mitigate or lessen the damage caused by the incident is called a corrective control.