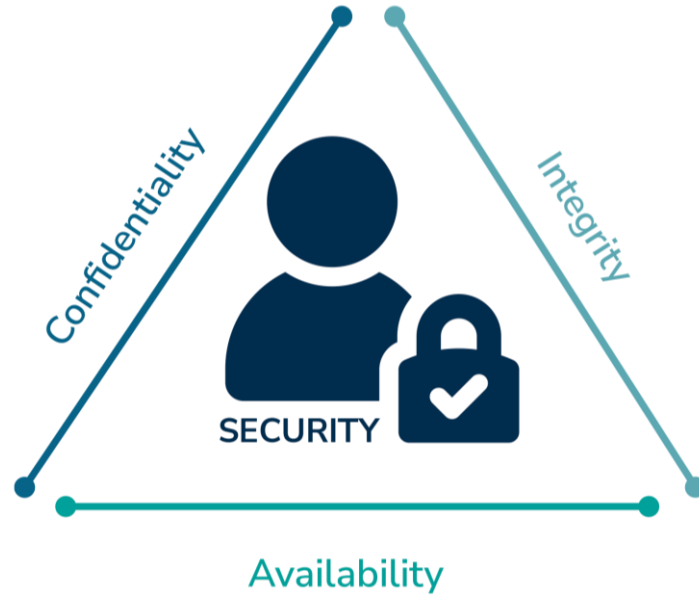




آموزش نتورک پلاس

Network Security

CIA triad

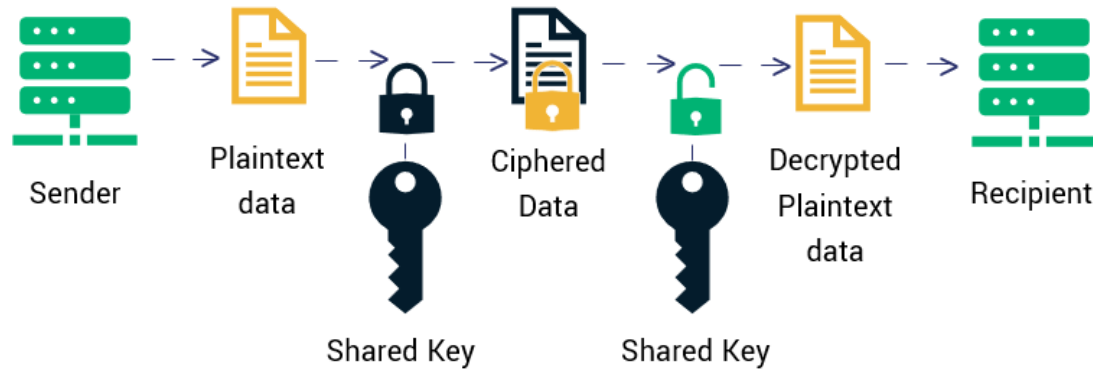


Confidentiality

- Symmetric and Asymmetric Encryption



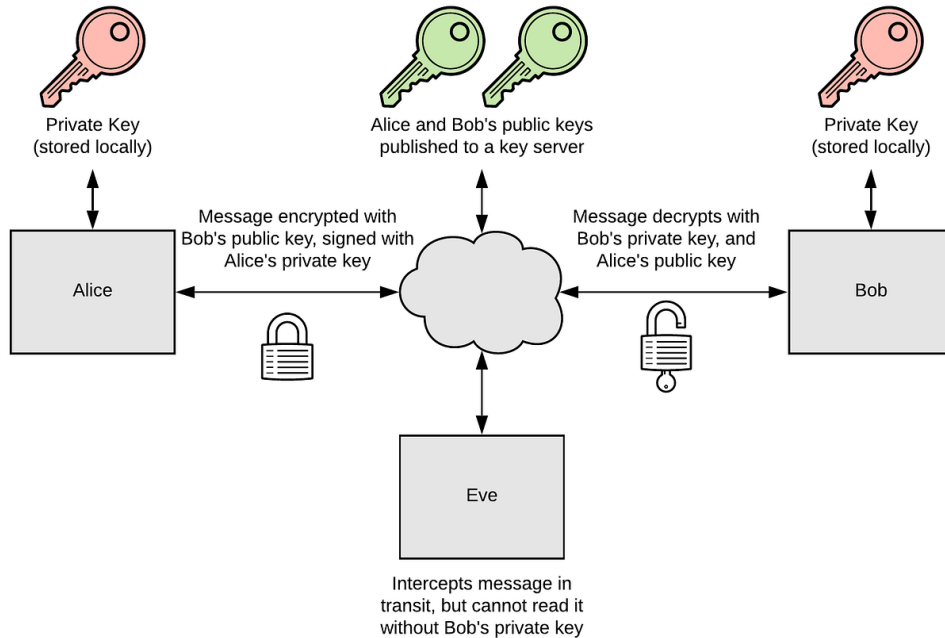
Symmetric Encryption



Symmetric Encryption

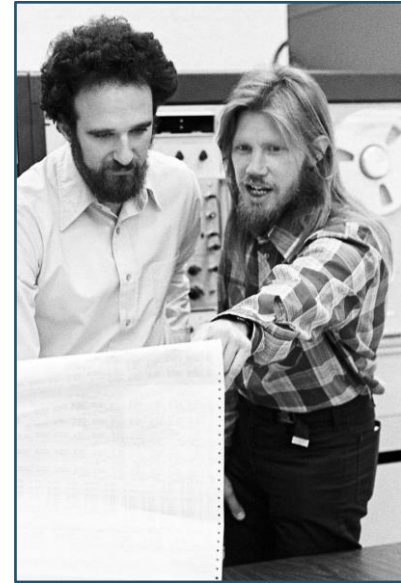
- Data Encryption Standard (DES – 56bit)
- Triple DES (112 or 168 bits)
- Advanced Encryption Standard (128-bit, 192-bit, 256-bit)
- Symmetric encryption is almost 1000X faster than Asymmetric encryption.

Asymmetric Encryption



Asymmetric Encryption

- RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC)



Integrity

- Hashing

Encryption

(used to protect sensitive information)



Hashing

(used to validate information)



Integrity

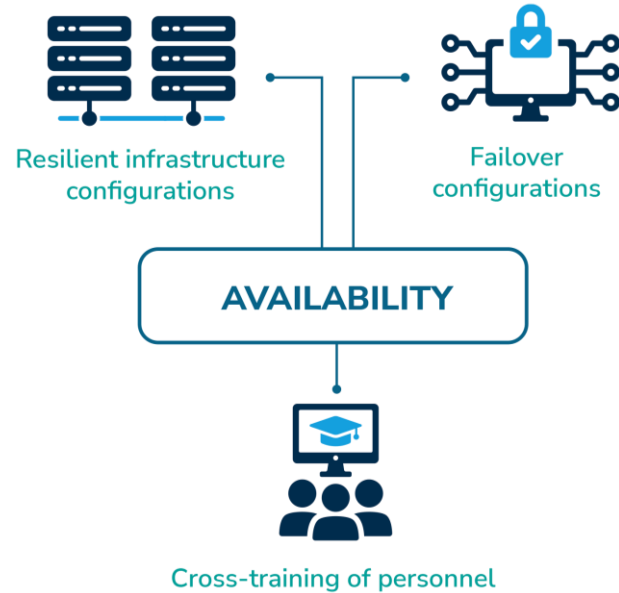
- MD5 (Message Digest Method 5 – 128bit)
- SHA-1 (Secure Hash Algorithm 1 – 160bit)
- SHA256
- SHA512
 -
 -
 -

Integrity

Certutil -hashfile <file> MD5



Availability



Threats and Vulnerabilities



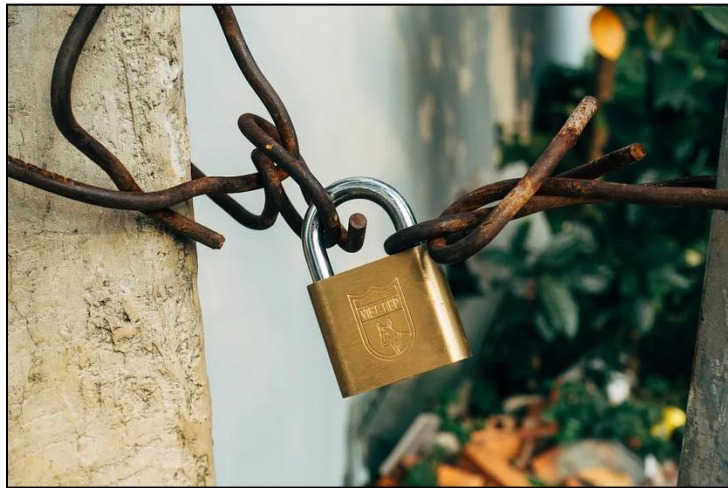
Threat

- A person or event that has the potential for negatively impacting a valuable resource.
- Internal (insider) Threat vs External Threat



Security Principles

- Least privilege
- Access controls
- Zero-trust
- Separation of Duties
 - E.g. Backup and Restore
 - Split Knowledge



Vulnerabilities

- Environmental
- Physical
- Operational
- Technical (CVE, Zero-day)



Common Vulnerabilities and Exposures

- <https://cve.mitre.org>



Zero-Day Vulnerability

- CVE (known vulnerabilities)
- Zero-Day (Brand new vulnerability)

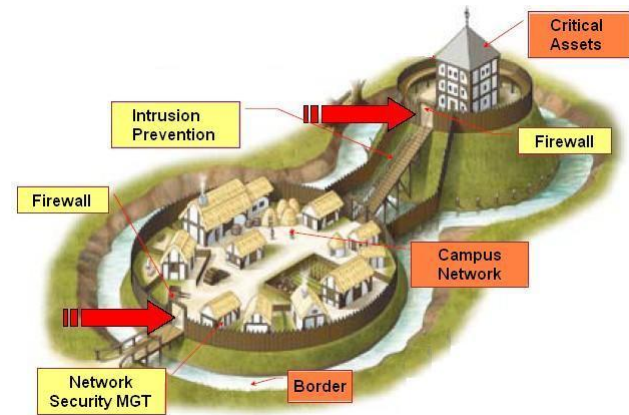


Exploit

- piece of software code that takes advantage of a security flaw or vulnerability within a system or network.
- <https://www.exploit-db.com>

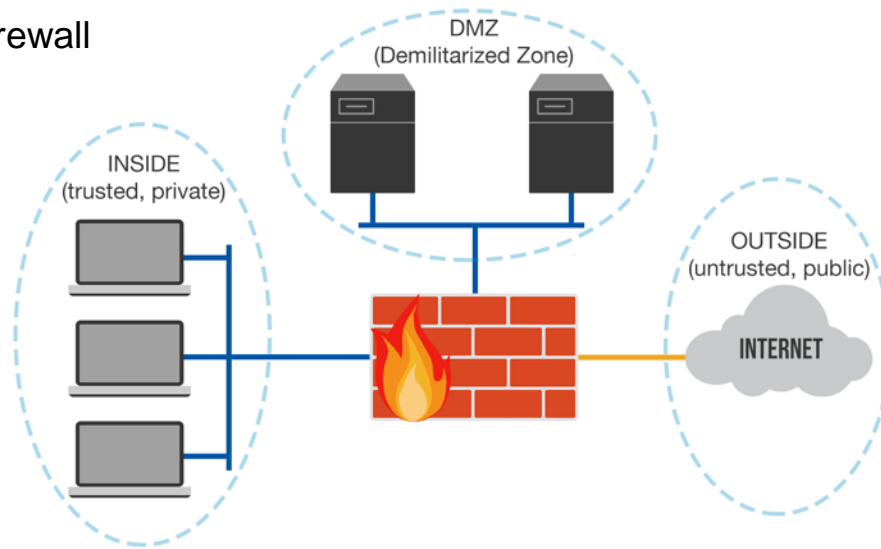


Defense in Depth



Network Security Zones

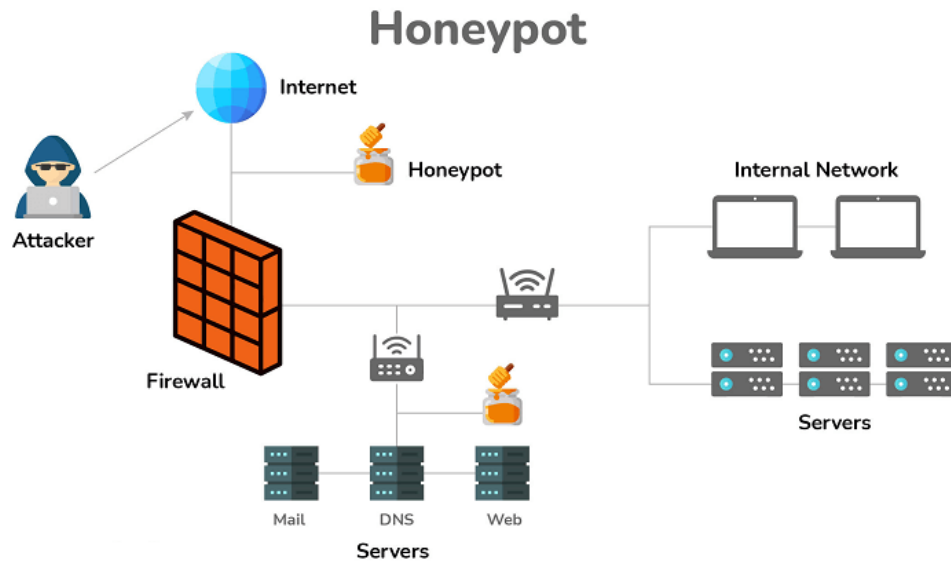
Triple-homed firewall



Network Security Zones



Honeynet



Multifactor Authentication

- Something you **know**
- Something you **have**
- Something you **are**
- Something you **do**
- **Somewhere** you are

Authentication	AKA	Examples
Something you know	Knowledge	<ul style="list-style-type: none">• Usernames• Passwords• PINs• Personal question answers
Something you have	Possession	<ul style="list-style-type: none">• Smartcards• RSA key fobs• RFID tags
Something you are	Inherence	<ul style="list-style-type: none">• Fingerprints• Retina scans• Voice prints
Something you do	Action	<ul style="list-style-type: none">• How you sign your name• How you draw a pattern• How you say a catchphrase
Somewhere you are	Location	<ul style="list-style-type: none">• Geotagging• Geofencing

Multifactor Authentication

- Something you **know**
 - Default credentials
 - Common passwords
 - Weak/short password
- Dictionary Attack
- Brute Force Attack
 - Use a longer and more complicated password
- Hybrid Attack

Authentication Methods

- Local authentication
- Lightweight Directory Access Protocol (port 389, 636)
 - Active Directory
- Kerberos
Provides secure authentication over an insecure network
- SSO : Single sign-on



Network Access Protocols

- Authentication, Authorization, Accounting
- RADIUS : Remote Authentication Dial-In Service
- TACACS+ : Terminal Access Controller Access Control System Plus
- 802.1X : port-based authentication on both wired and wireless networks
- EAP : Allows for numerous different mechanisms of authentication

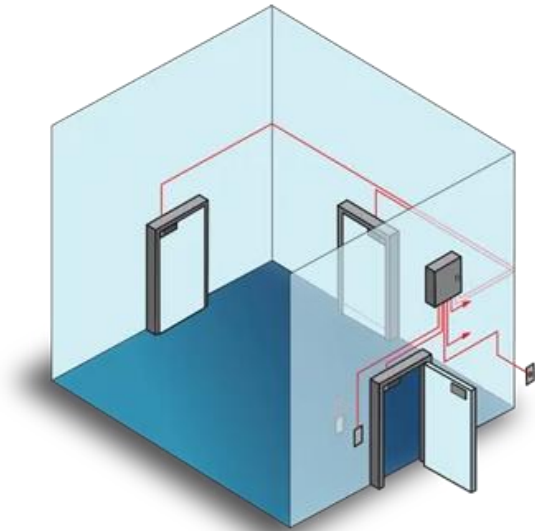
Network Access Control (NAC)

- Ensures a device is scanned to determine its current state of security prior to being allowed network access.
- Persistent vs Non-Persistent Agent
- IEEE 802.1x used in port-based Network Access Control
Time-based, Location-based, Role-based, Rule-based



Physical Security

- User awareness
- Rack Security
- Indoor vs Outdoor camera
- Asset Tag
- Mantrap



Asset Disposal



dumpster diving





عباس ولی زاده

مدرس دوره های شبکه و امنیت