
Lesson 1:
Introduction
to
Cybersecurity
Sign in
Password
L6Rm8TY9PqZ4W
Forgot password

Who Am I

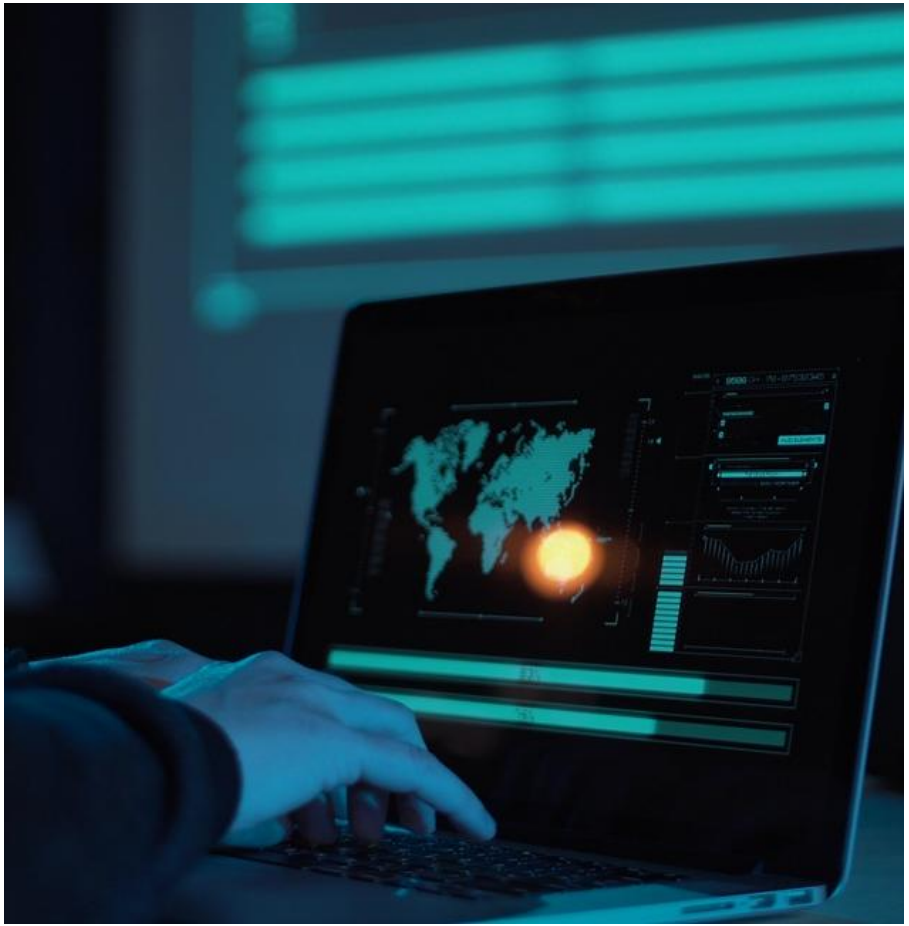
- Ph.D. Computer Science,
- Ph.D. Nanotechnology
- D.Sc. Cybersecurity
- Four masters (systems engineering, education, applied computer science, strategic and defense studies)
- 45 books
- 27 patents
- 80+ Computer Industry/Cybersecurity certifications
- 30+ years of experience
- **Chuck Easttom, M.Ed., MBA, MSDS, MSSE, Ph.D., D.Sc.**
- **www.ChuckEasttom.com**
- **chuck@chuckeasttom.com**

Cybersecurity and the DoD

- The Department of Defense and related organizations have a deeper requirement for cybersecurity. Not only do you face the same issues of any organization today, but cyber warfare is a substantial issue.

Lesson 1

This first lesson is about providing students with a general understanding of cybersecurity concepts/terms/ and technologies. This will provide the basis for later lessons.



The Cyber Paradigm

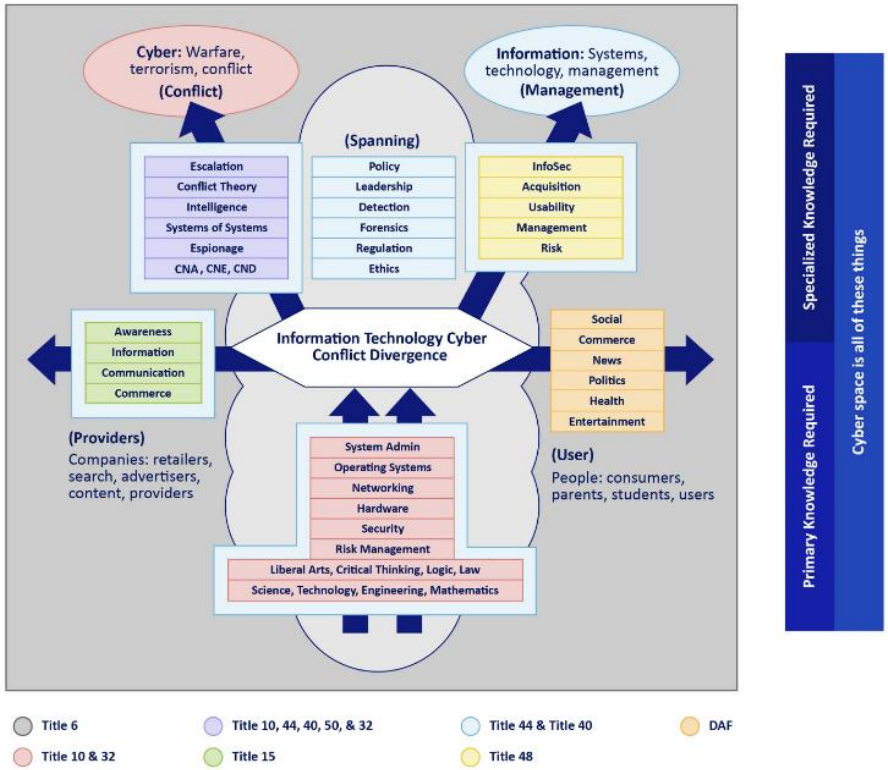
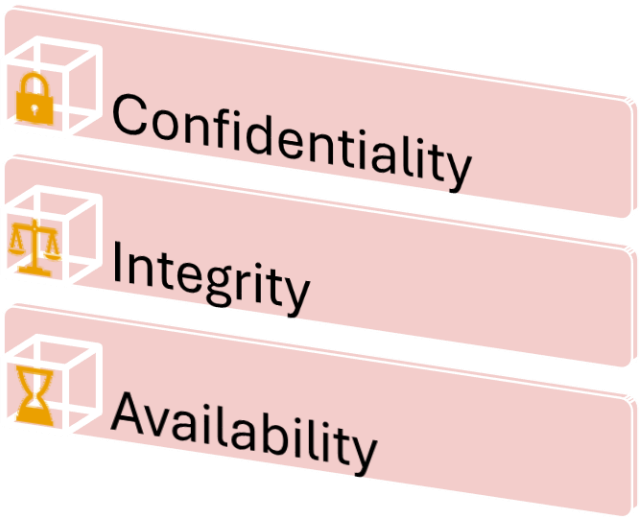


Figure 2: The Cyber Paradigm

https://www.dafcio.af.mil/Portals/64/The%20Cyber%20Cake.pdf

The CIA Triangle



The CIA triad may also be described by its opposite: Disclosure, Alteration, and Destruction (DAD).

The McCumber Cube

The McCumber cube is a way of evaluating security of a network, looking at all aspects. It was described in detail in 2004 in the book *Assessing and managing security risk in IT systems: A structured methodology*. It looks at security as a three-dimensional cube. The dimensions are goals, information states, and safeguards.

McCumber Cube Dimensions

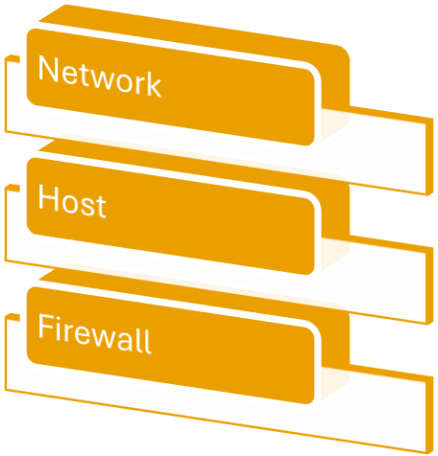
Goals
- Confidentiality
- Integrity.
- Availability

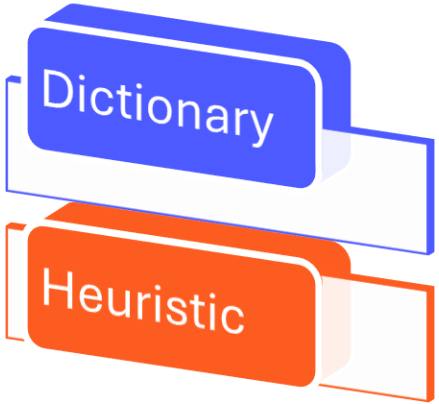
Information states
- Storage
- Transmission
- Processing

Safeguards
- Policy and practices
- Human factors
- Technology

Other Security Concepts/Terms

Antivirus





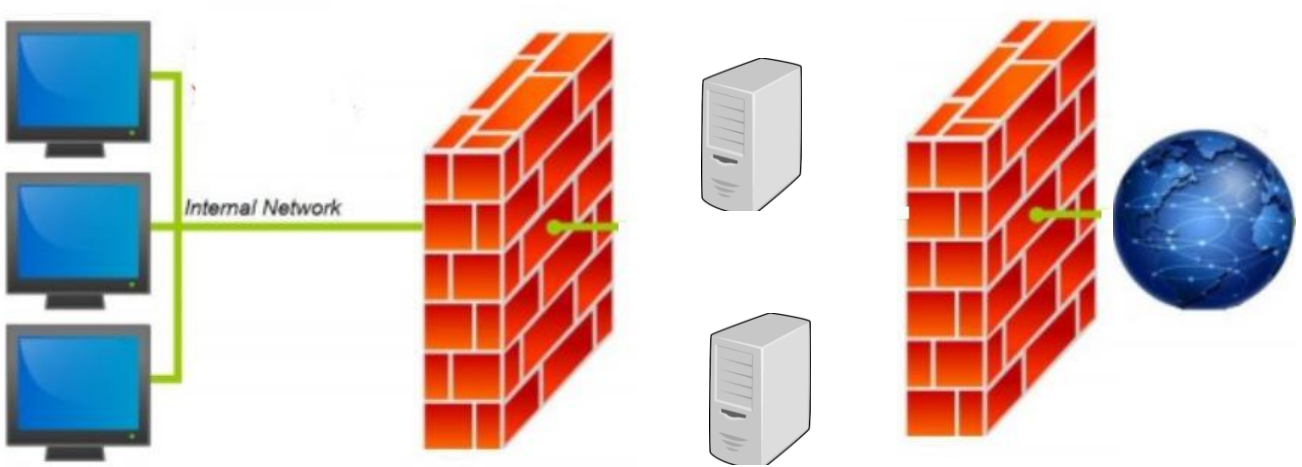
Major vendors

- Norton
- McAffee
- AVG
- Kaspersky
- Bit Defender
- Malware Bytes
- Panda

Types of firewalls

- Packet Filter/Stateless
- Stateful Packet Inspection
- Application Gateway
- Circuit Gateway
- Web Application Firewall
- NGFW

DMZ



Circuit Level Gateway

- Circuit level gateway: operates at the Transport layer of the OSI or as a shim between the application and transport layer of the TCP/IP model. Information passed through a circuit level gateway appears to come from the gateway.

Firewall Terms

- Network address translation (NAT)
- DMZ - De-Militarized Zone
- ACL - Access Control List
- Choke, Choke router
  - A router with packet filtering rules (ACLs) enabled
- Gate, Bastion host, Dual Homed Host
  - A server that provides packet filtering and/or proxy services
- proxy server
  - A server that provides application proxies

IDS/IPS

Components of an IDS

- An *activity* is an element of a data source that is of interest to the operator.
- The *administrator* is the person responsible for organizational security.
- A *sensor* is the IDS component that collects data and passes it to the analyzer for analysis.
- The *analyzer* is the component or process that analyzes the data collected by the sensor.
- An *alert* is a message from the analyzer indicating that an event of interest has occurred.

Components of an IDS (continued)

Manager: the part of the IDS used to manage, for example a console.

Notification is the process or method by which the IDS manager makes the operator aware of an alert.

The *operator* is the person primarily responsible for the IDS. This is often the administrator.

An *event* is an occurrence indicates that a suspicious activity may have occurred.

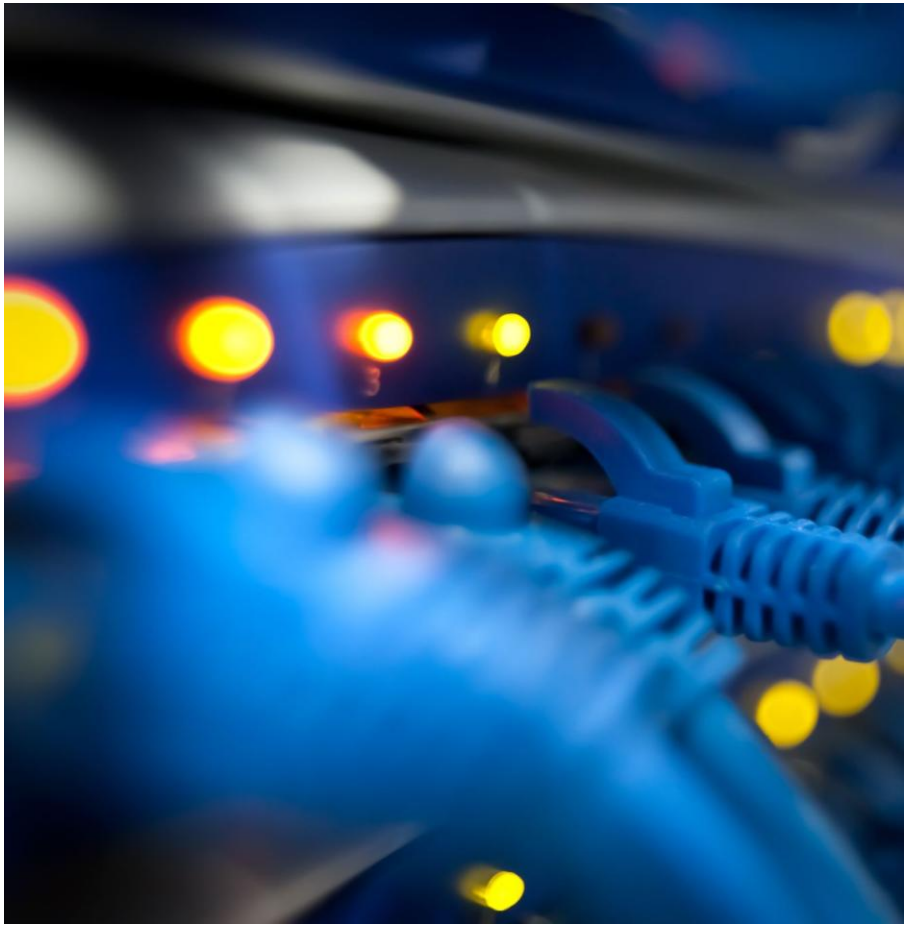
The *data source* is the raw information that the IDS uses to detect suspicious activity.

IDS Types

- Signature Based vs. Anomaly Based
  - Signature compares activity against known attacks.
  - Anomaly looks for any deviation from normal range of activity
  - Behavior looks for any behavior that can be considered possibly an attack.

IDS Examples

- Snort
- SilverSky
- Cisco IPS
- SNARE
- Vangaurd
- Peek & Spy
- IDP8200
- Mobile
    - Wi-Fi IDS
    - Wi-Fi Intruder Detector Pro
    - Wi-Fi Inspector



NAC

Network Access Control

- Network Access Control allows the network to scan a device before allowing it to connect.
- They can be agent based or agentless.
- With agent NAC, a software agent is installed on any device that wishes to connect to the network. That agent can do a much more thorough systems health check of the BYOD.
- The agent can be permanent or dissolvable.

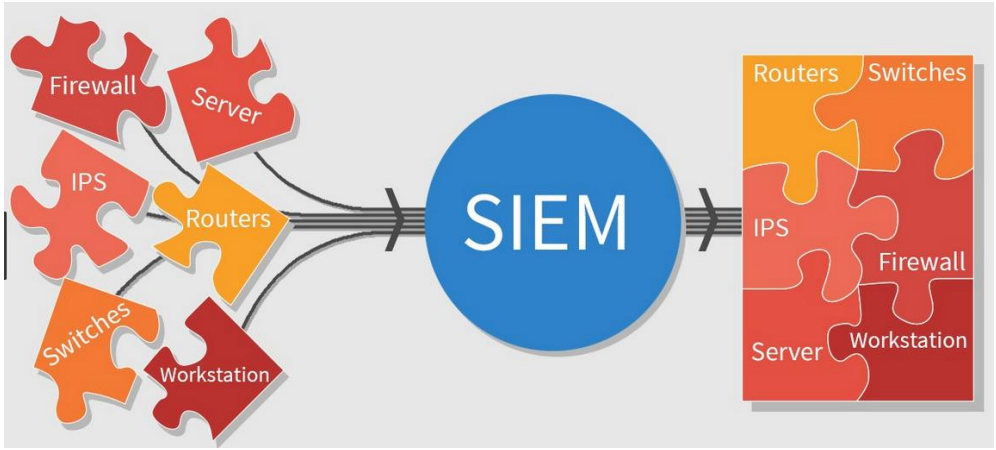
DAM

- Database Activity Monitoring
- It is monitoring and analyzing database activity that operates independently of the database management system (DBMS) and does not rely on any form of native (DBMS-resident) auditing or native logs such as trace or transaction logs. DAM is typically performed continuously and in real-time.
- Database activity monitoring and prevention (DAMP) is an extension to DAM that goes beyond monitoring and alerting to also block unauthorized activities

Honey pot

- What they are
- Where to put them

SIEM



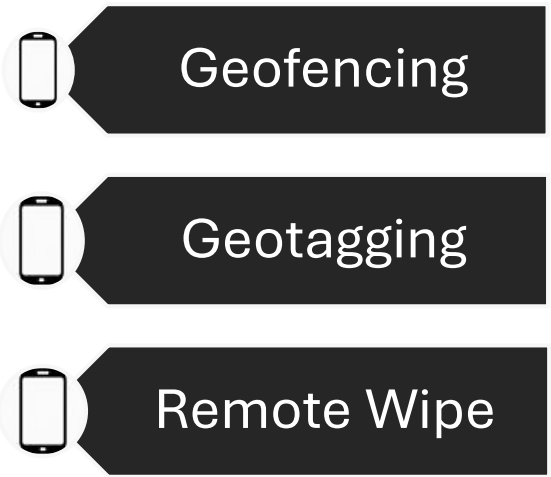
- security information and event management (SIEM)
  - Data aggregation
  - Correlation
  - Alerting
  - Retention
  - Compliance
  - Forensic analysis
  - Dashboards/Interfaces

SYSLOG

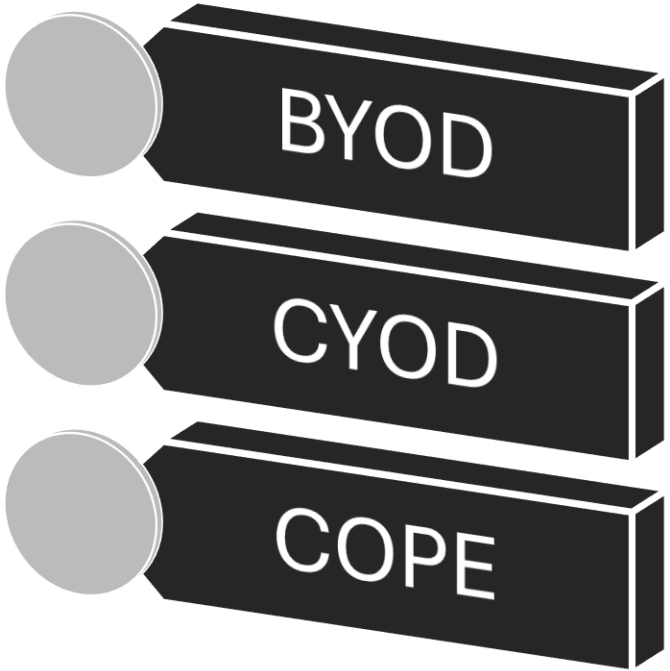
Level	Description	System Status
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical condition
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages
7	debugging	Debugging messages

- syslog is a standard for message logging
- Severity levels

Portable Device Security



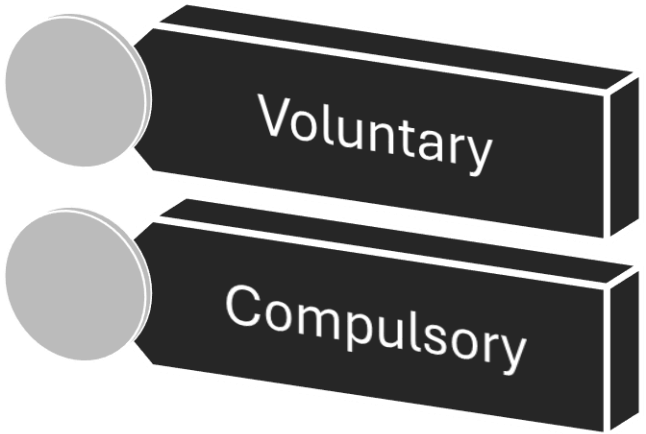
Portable Issues



VPN

- In order to accomplish its purpose, the VPN must emulate a direct network connection. This means it must provide the same level of access, and the same level of security. In order to emulate a dedicated point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it transmit across the internet to reach its destination. This creates a virtual network connection between the two points. The data being sent is also encrypted thus making that virtual network private.
- Internet Week (Salmone, 1998), gives an excellent definition of a VPN:
- “a combination of tunneling, encryption, authentication, and access control technologies and services used to carry traffic over the Internet, a managed IP network or a provider's backbone.”
- The first thing you must realize is that a VPN does not require separate technology, leased lines, or direct cabling. It is a *virtual* private network. The key term to consider here is virtual. It is not an actual physical private network, but rather a virtual one. This means it can use existing connections to provide a secure connection. In most cases it is used over normal Internet connections. Basically the VPN is a way to ‘piggy back’ over the internet to create secure connections.

VPN (continued)



VPN Gateways

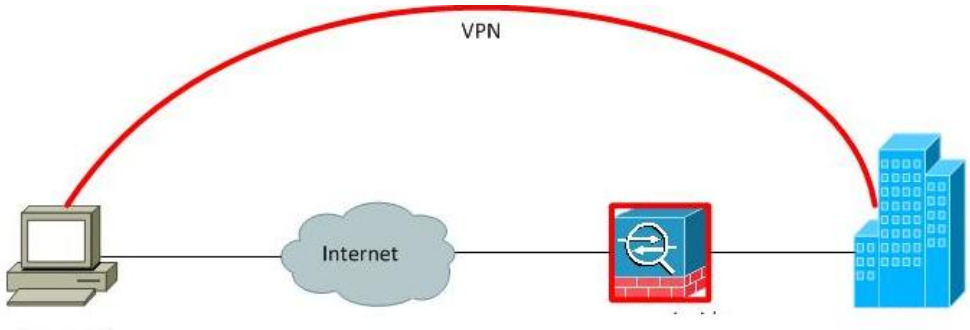
- VPN gateways can be categorized as Standalone or Integrated.
- Standalone VPNs incorporate purpose-built devices between - the source of data and WAN link or between the modem and a data source in a remote office.
- Integrated implementations add VPN functionality to existing devices such as routers, firewalls.

VPN Concentrator

- A VPN concentrator is a type of networking device that provides secure creation of VPN connections and delivery of messages between VPN nodes.

- It is a type of router device, built specifically for creating and managing VPN communication infrastructures.

Split Tunneling



- Split tunneling allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN or WAN at the same time

Types of VPN

PPTP

L2TP

IPSEC

SSL/TLS

IPSec

- IP Security – Internet Protocol Security
- IPSec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream
- Used to create VPN’s
- Also handles key exchange and mutual authentication
- Provides two modes: 1 Transport mode, only the payload is encrypted, 2 Tunnel mode, both data and IP headers are encrypted

AH v ESP

- Authentication Header- The AH protocol provides a mechanism for authentication only. AH provides data integrity, data origin authentication, and an optional replay protection service. Data integrity is ensured by using a message digest that is generated by an algorithm such as HMAC-MD5 or HMAC-SHA. Data origin authentication is ensured by using a shared secret key to create the message digest
- Encapsulating Security Payload- The ESP protocol provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection). ESP can be used with confidentiality only, authentication only, or both confidentiality and authentication.

Either protocol can be used alone to protect an IP packet, or both protocols can be applied together to the same IP packet.

IPSEC basic notes

- Transport mode is the mode wherein IPSEC encrypts the data, but not the packet header.
- Tunneling mode does encrypt the header as well as the packet data.
- IKE or Internet Key Exchange is used in setting up security associations in IPSEC.
- ESP or Encapsulating Security Payload is used for authentication and encryption in IPSEC, whether tunneling or transport mode is used. Encapsulating Security Payload provides both integrity and encryption but only authenticates the data, not the header
- Authentication Header will provide complete packet authentication including the header, but won't provide encryption

IPSEC

Terms

- Authentication Headers (AH) provides connectionless integrity and data origin authentication for IP packets.
- Encapsulating Security Payloads (ESP) provides origin authenticity, integrity and confidentiality protection of packets. It has encryption only and authentication only configurations.
- Security Associations (SA) provide the parameters necessary for AH and/or ESP operations. Security associations are established using the Internet Security Association and Key Management Protocol
- The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange
- Internet key exchange (IKE and IKEv2) is used to set up a security association (SA) by handling negotiation of protocols and algorithms and to generate the encryption and authentication keys to be used.

IPsec Protocol Suite

Internet Key Exchange (IKE) protocol

For negotiating security parameters and establishing authenticated keys

Uses UDP port 500 for ISAKMP

Encapsulating Security Payload (ESP) protocol

For encrypting, authenticating, and securing data

IP protocol 50

Authentication Header (AH) protocol

For authenticating and securing data

IP protocol 51

IPsec Tunnel Creation using IKE

- Negotiate a secure authenticated communication channel using main mode or aggressive mode negotiation, resulting in creation of an IKE Security Association (SA) between the two IPsec peers (IKE phase I)
- Create two IPsec SAs between the two IPsec peers via IKE quick mode negotiation (IKE phase II)
- Send data over encrypted tunnel using ESP and/or AH encapsulation

Main Mode and Aggressive Mode

- **Main Mode:** The first exchange between nodes establishes the basic security policy; the initiator proposes the encryption and authentication algorithms it is willing to use. The responder chooses the appropriate proposal and sends it to the initiator. The next exchange passes Diffie-Hellman public keys and other data. All further negotiation is encrypted within the IKE SA. The third exchange authenticates the ISAKMP session. Once the IKE SA is established, IPSec negotiation (Quick Mode) begins.
- **Aggressive Mode** Aggressive Mode squeezes the IKE SA negotiation into three packets, with all data required for the SA passed by the initiator. The responder sends the proposal, key material and ID, and authenticates the session in the next packet. The initiator replies by authenticating the session. Negotiation is quicker, and the initiator and responder ID pass in the clear.
- **Quick Mode** IPSec negotiation, or Quick Mode, is similar to an Aggressive Mode IKE negotiation, except negotiation must be protected within an IKE SA. Quick Mode negotiates the SA for the data encryption and manages the key exchange for that IPSec SA.

Goals of Main Mode and Aggressive Mode

- Agreeing on a set of parameters that are to be used to authenticate the two peers
- Agreeing on parameters used to encrypt a portion of the main mode and all of the quick mode messages
- None of the aggressive mode messages are encrypted
- Authenticate the two peers to each other
- Generate keys used to generate keying material for subsequent encryption of data
- All of the parameters negotiated and the keys used to generate keys for encryption are stored as IKE or ISAKMP security association (SA)

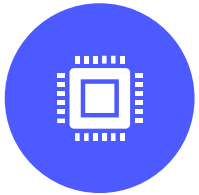
SSL/TLS vpn

- The user logs into a website but the website configures SSL/TLS rather than simply access to a secure web page.

Remote Access Security- SSL

SSL, OR SECURE SOCKETS LAYER, IS A TECHNOLOGY EMPLOYED TO ALLOW FOR TRANSPORT-LAYER SECURITY VIA PUBLIC-KEY ENCRYPTION.

A PROTOCOL DEVELOPED BY NETSCAPE FOR TRANSMITTING PRIVATE DOCUMENTS VIA THE INTERNET



BY CONVENTION, URLS THAT REQUIRE AN SSL CONNECTION START WITH *HTTPS:* INSTEAD OF *HTTP*:.

History of SSL

- Unreleased v1 (Netscape)
- Version 2 released in 1995 but had many flaws
- Version 3 released in 1996 RFC 6101
- Standard TLS1.0 RFC 2246 released in 1999
- TLS 1.1 was defined in RFC 4346 in April 2006
- TLS 1.2 was defined in RFC 5246 in August 2008. It is based on the earlier TLS 1.1 spec
- TLS 1.3 was defined in RFC 8446 in August 2018.

TLS v 1.3

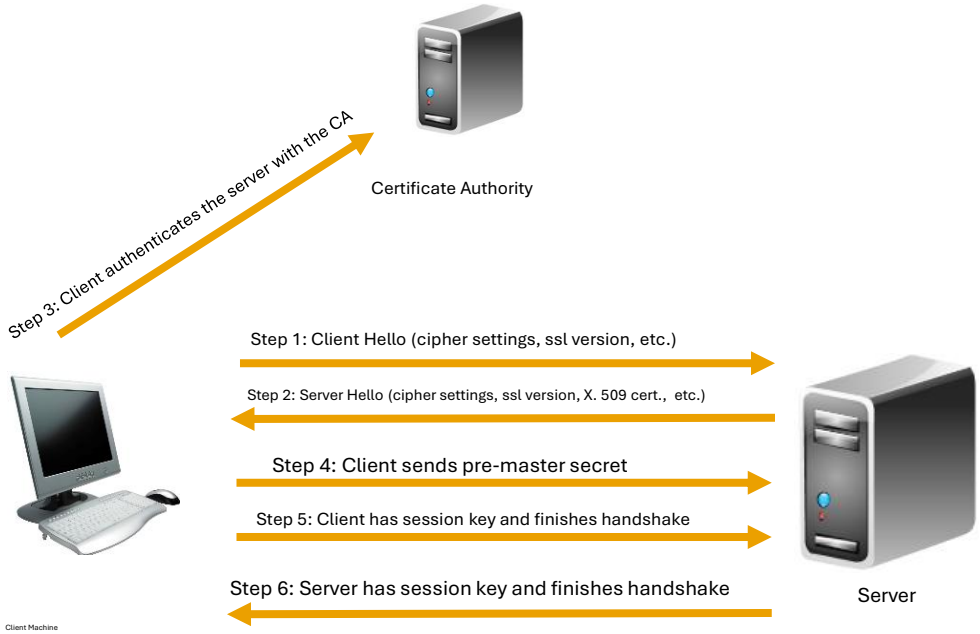
- Separating key agreement and authentication algorithms from the cipher suites
- Removing support for weak and lesser-used named elliptic curves
- Removing support for MD5 and SHA-224 cryptographic hash functions
- Requiring digital signatures even when a previous configuration is used
- Integrating HKDF and the semi-ephemeral DH proposal
- Replacing resumption with PSK and tickets
- Supporting 1-RTT handshakes and initial support for 0-RTT
- Mandating perfect forward secrecy, by means of using ephemeral keys during the (EC)DH key agreement
- Dropping support for many insecure or obsolete features including compression, renegotiation, non-AEAD ciphers, non-PFS key exchange (among which static RSA and static DH key exchanges), custom DHE groups, EC point format negotiation, Change Cipher Spec protocol, Hello message UNIX time, and the length field AD input to AEAD ciphers
- Prohibiting SSL or RC4 negotiation for backwards compatibility
- Integrating use of session hash
- Deprecating use of the record layer version number and freezing the number for improved backwards compatibility
- Moving some security-related algorithm details from an appendix to the specification and relegating ClientKeyShare to an appendix
- Adding the ChaCha20 stream cipher with the Poly1305 message authentication code
- Adding the Ed25519 and Ed448 digital signature algorithms
- Adding the x25519 and x448 key exchange protocols.

Remote Access Security - TLS

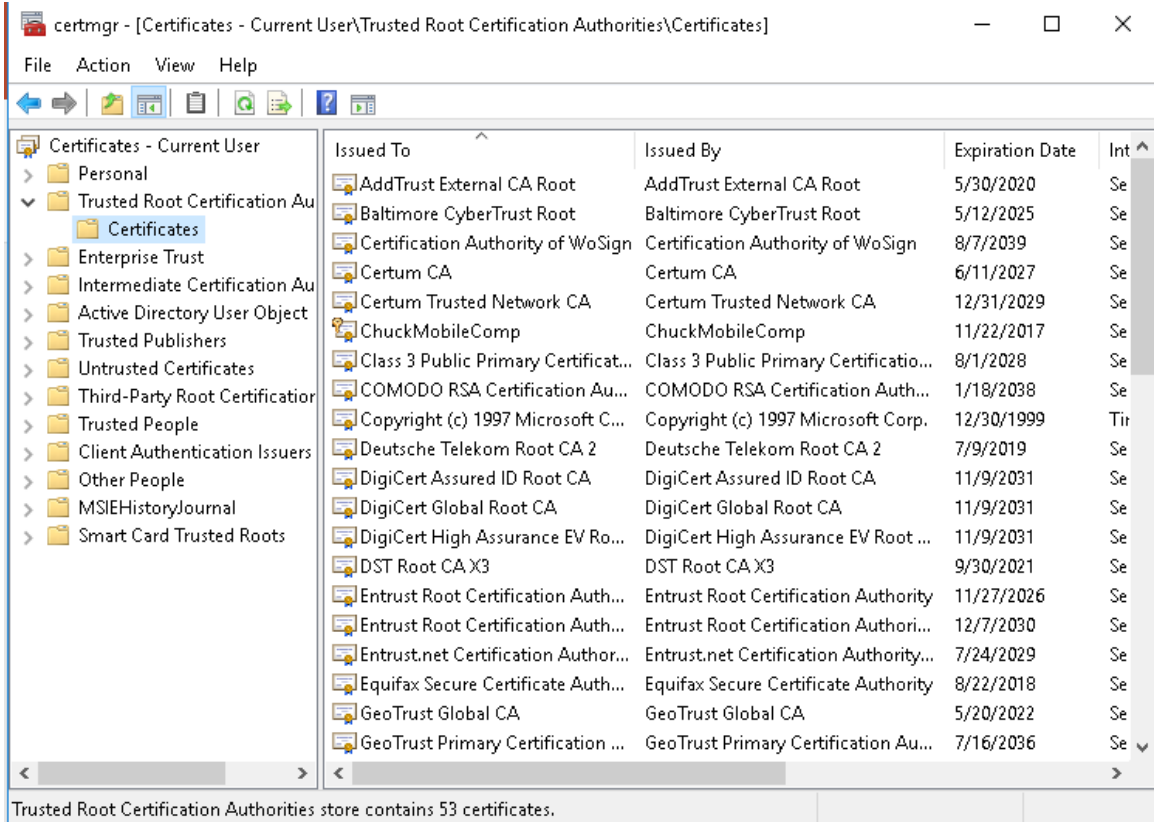
Transport Layer Security provides RSA encryption It is the successor to SSL

TLS also supports the more secure *bilateral* connection mode (i.e. mutual authentications), in which both ends of the communication session can verify each other.

Typically, the key information and certificates necessary for TLS are handled in the form of X.509 certificates, which define required fields and data formats.


Certificate Authority
Step 3: Client authenticates the server with the CA
Step 1: Client Hello (cipher settings, ssl version, etc.)
Step 2: Server Hello (cipher settings, ssl version, X. 509 cert., etc.)
Step 4: Client sends pre-master secret
Step 5: Client has session key and finishes handshake
Step 6: Server has session key and finishes handshake
Server
Client Machine

Certificate Store



Handshake step by step

1.The client sends the server the client's SSL version number, cipher settings, session-specific data, and other information that the server needs to communicate with the client using SSL.

2.The server sends the client the server's SSL version number, cipher settings, session-specific data, and other information that the client needs to communicate with the server over SSL. The server also sends its own certificate, and if the client is requesting a server resource that requires client authentication, the server requests the client's certificate.

3.The client uses the information sent by the server to authenticate the server—e.g., in the case of a web browser connecting to a web server, the browser checks whether the received certificate's subject name actually matches the name of the server being contacted, whether the issuer of the certificate is a trusted certificate authority, whether the certificate has expired, and, ideally, whether the certificate has been revoked.[7] If the server cannot be authenticated, the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established. If the server can be successfully authenticated, the client proceeds to the next step.

4.Using all data generated in the handshake thus far, the client (with the cooperation of the server, depending on the cipher in use) creates the pre-master secret for the session, encrypts it with the server's public key (obtained from the server's certificate, sent in step 2), and then sends the encrypted pre-master secret to the server.

Handshake step by step continued

5.If the server has requested client authentication (an optional step in the handshake), the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case, the client sends both the signed data and the client's own certificate to the server along with the encrypted pre-master secret.

6.If the server has requested client authentication, the server attempts to authenticate the client. If the client cannot be authenticated, the session ends. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret, and then performs a series of steps (which the client also performs, starting from the same pre-master secret) to generate the master secret.

7.Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity (that is, to detect any changes in the data between the time it was sent and the time it is received over the SSL connection).

8.The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.

9.The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.

WEP

Wired Equivalent Privacy uses the stream cipher RC4 to secure the data and a CRC-32 checksum for error checking. Standard WEP uses a 40-bit key (known as WEP-40) with a 24-bit initialization vector, to effectively form 64-bit encryption. 128 bit WEP uses a 104 bit key with a 24 bit IV.

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

WPA

Wi-Fi Protected Access. WPA uses Temporal Key Integrity Protocol. TKIP is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.

WPA2

WPA2 is based on the IEEE 802.11i standard. It provides the following:

- The Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP) that provides data confidentiality, data origin authentication, and data integrity for wireless frames.
- WPA Enterprise provides RADIUS based authentication using 802.1X. WPA Personal uses a pre-shared Shared Key (PSK) to establish the security using an 8 to 63 character passphrase. The PSK may also be entered as a 64 character hexadecimal string. It also uses EAP variations for authentication.

- NOTE: For the test you must be able to describe WEP, WPA, and WPA 2

WPA3

- WPA3, on the other hand, requires attackers to interact with your Wi-Fi for every password guess they make, making it much harder and time-consuming to crack.
- WPA3's new "Wi-Fi Easy Connect," though, you'll be able to connect a device by merely scanning a QR code on your phone.
- WPA3, even open networks will encrypt your individual t

Wireless configuration

- Thin vs Fat WAP refers to the functionality in the WAP
- A fat Wireless Access Point is one that has all the functionality needed, and no other servers or devices are required. Stand alone is synonymous for fat WAP.
- Thin WAPs require some server or device to offload some functionality to.

Other Wi-Fi security Measures

- Disable SSID broadcast
- Lock down admin
- No Default Passwords
- MAC Filtering

Other Wireless Security Measures

- Black holing is one possible way of stopping a DoS attack. This is a situation where we drop all IP packets from an attacker.
- Validating the handshake involves creating false opens, and not setting aside resources until the sender acknowledges. Some firewalls address SYN floods by pre-validating the TCP handshake. This is done by creating false opens. Whenever a SYN segment arrives, the firewall sends back a SYN/ACK segment, without passing the SYN segment on to the target server.

Bluetooth

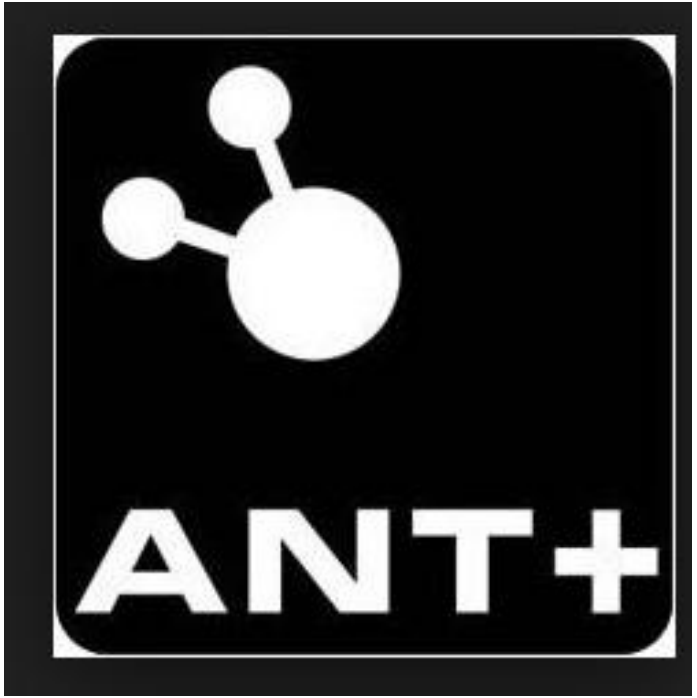
- Short-distance radio (10 to 240 meters)
- UHF 2.4 to 2.485 GHz
- Developed by the Bluetooth Special Interest Group
  - Includes over 1,000 companies
  - Siemens, Intel, Toshiba, Motorola, and Ericsson
- The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard.
- Enables devices to discover other Bluetooth devices within range
- Devices self-configure and begin communicating
- The name comes from king Harald Bluetooth 10th century Danish king. He united the tribes of Denmark, thus the implication is that bluetooth unites communication protocols. There have been different explanations for his name. One being that he had a bad tooth that was blue (i.e. rotted). Another explanation is that he was often clothed in blue.

Bluetooth

Version	Bandwidth & Range	
3.0	25 Mbit/s (33 ft)	10 meters
4.0	25 Mbit/s (200 ft)	60 meters
5.0	50 Mbit/s (800 ft)	240 meters

ANT+ and NFC

- ANT+ is a wireless protocol often used with sensor data such as in bio sensors or exercise applications
- NFC or Near Field communication works if the two devices are within 4 cm (1.6 inches) of each other. Operates on globally available unlicensed radio frequency ISM band of 13.56 MHz on ISO/IEC 18000-3 air interface at rates ranging from 106 to 424 Kbit/s. NFC is standardized in ECMA-340 and ISO/IEC 18092.



RFID

- Radio Frequency Identifiers are used to identify specific items based on a radio frequency. An RFID chip is encoded with the identifying information. This is often used in NFC

ZigBee

ZigBee is a standard developed by a consortium of electronic manufacturers for mainly residential applications of wireless devices as related to appliances and security and such. It is based on the 802.15.4 standard. What appears to be confusing is that the standard is represented by the name “ZigBee” rather than a number. The term *ZigBee* is used similar to the way the term *Wi-Fi* is used.

Z Wave

- Z-Wave is a wireless communications protocol used primarily for home automation. It uses a low energy radio for appliance to appliance communication using a mesh network.

Wireless

- Thin vs Fat WAP refers to the functionality in the WAP. A fat (or thick) Wireless Access Point is one that has all the functionality needed, and no other servers or devices are required. In this case, since each WAP might have completely different needs, a fat WAP is preferred.

DLP

- Data Loss Prevention
  - USB Blocking
  - Email monitoring

NAC

- Network Access Control allows the network to scan a device before allowing it to connect.
- They can be **agent based** or **agentless**.
- With agent NAC, a software agent is installed on any device that wishes to connect to the network. That agent can do a much more thorough systems health check of the BYOD.
- The agent can be **permanent** or **dissolvable**.

Mobile Device Issues

BYOD/CYOD

COPE

Geofencing/Geotagging

Mobile Measures

- Custom firmware
- Carrier unlocking
- Camera use
- Firmware OTA (over the air) updates
- Camera use
- USB OTG (On The Go)
- GPS tagging
- Tethering

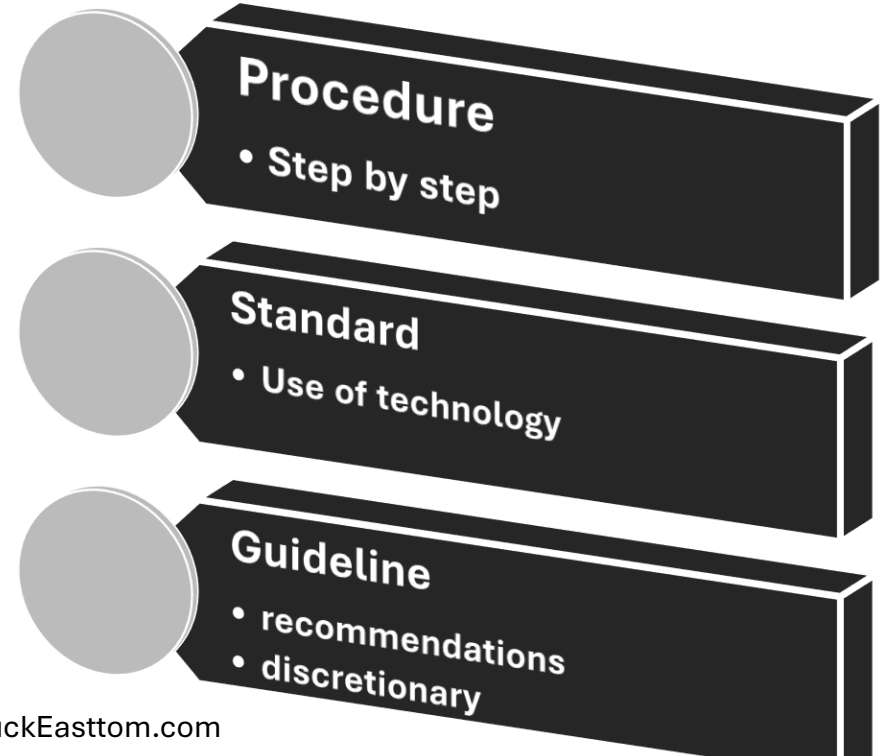
Policies

- Policies: are high-level management directives.
- All policies should contain these basic components:
  - Purpose
  - Scope
  - Responsibilities
  - Compliance

ISO 17799

- How to develop security policies. Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
- ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:
    - security policy;
    - organization of information security;
    - asset management;
    - human resources security;
    - physical and environmental security;
    - communications and operations management;
    - access control;
    - information systems acquisition, development and maintenance;
    - information security incident management;
    - business continuity management;
    - compliance.

Procedures , Standards, and Guidelines



Policy Types

- Planning policies
- Security policy
- Remote access policy
- Wireless security policy
- Password/authentication policy
- Physical security policy
- Network policy
- Audit policy
- Change management policy

Items policies must address

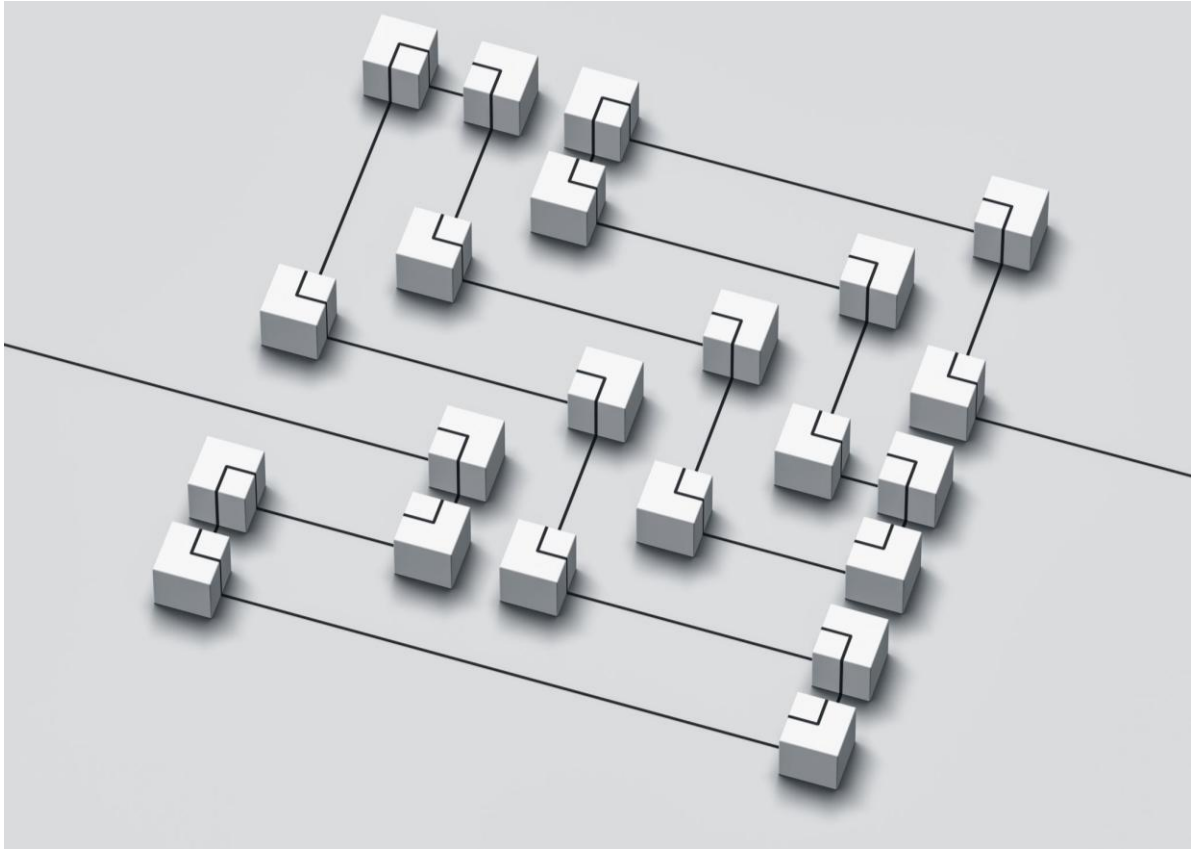
- Exiting employees
- What is appropriate use
- What will happen to violators
- How often and what method will you use for auditing
- What is the response process to an incident
- How to handle outside contractors
- What to do about new software releases
- How to handle updates/patches
- Disaster recovery
- Who is responsible for what

Document and Media Handling

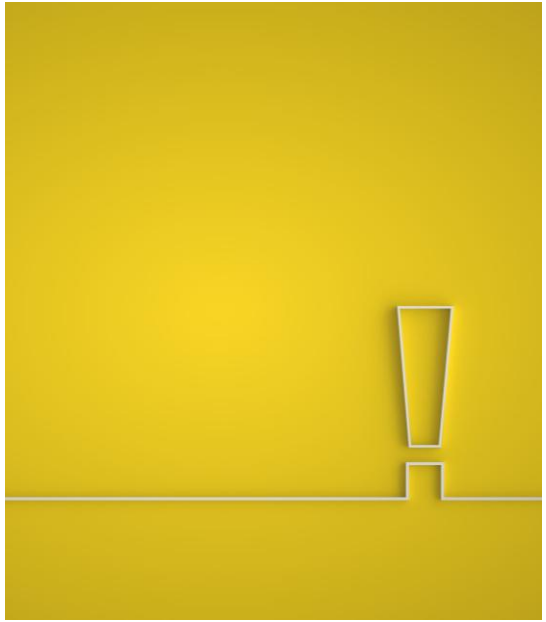
- Classification
- Storage
- Disposing

Change management

- Change management activities are frequently managed through a change control board (CCB) process,
- Change management is an enterprise -level process designed to control changes. It should be governed by a change management policy and implemented via a series of change management procedures.



Change management



- Procedures for network changes
- Initiated with RFC document(Request for Comments or Request for Change)
- RFC sent for approval
  - Priority is set
  - Assigned to whoever makes the change
  - Document decisions
- Evaluate by CAB (Change Advisory Board or Change Approval Board)
- RFC scheduled
- Complete when change owner and requester verify successful implementation
- Review of RFC

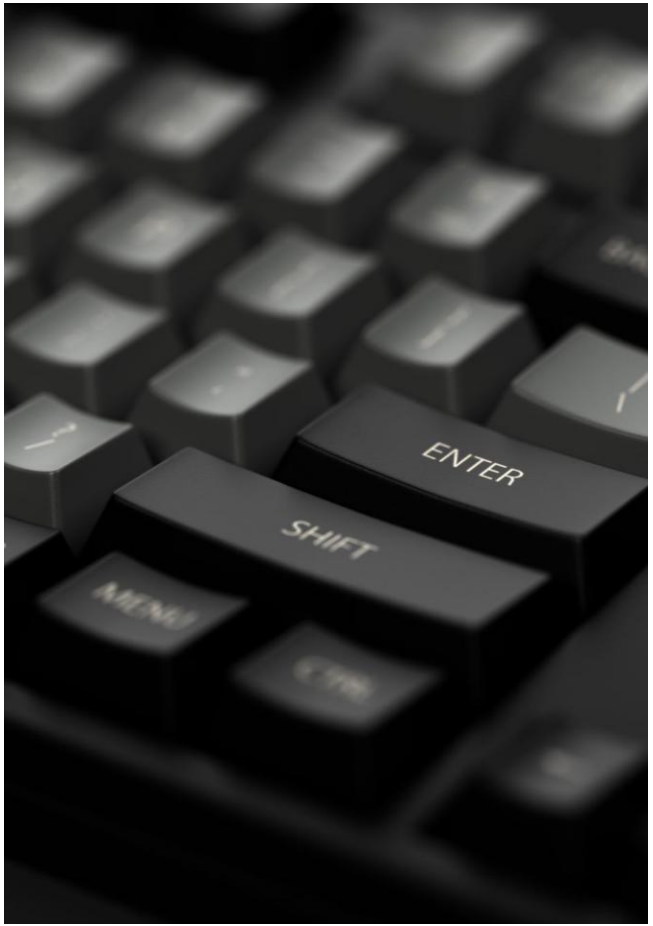
.

Change documentation

- Describes initial state and all changes
  - Configuration information
  - Patches applied
  - Backup records
  - Details about suspected breaches
  - Rollback method/plan
- Smooths system maintenance

Operating System Hardening

- Close ports
- Shut down services
- Keep patched
- Shut down shares
- Shut down un-needed accounts
- Password policies
    - Lockout
    - Password complexity
    - Password age



Operating System Hardening

- Windows SYSKEY-a utility that encrypts the hashed password information in a SAM database in a Windows system using a 128-bit RC4 encryption key that, by default, is stored in the Windows registry.

FIPS 200

FIPS 200, formally titled "Minimum Security Requirements for Federal Information and Information Systems," is a U.S. federal standard issued by NIST (National Institute of Standards and Technology) under the Federal Information Security Management Act (FISMA) of 2002. It establishes the baseline security requirements that all federal agencies must meet to protect their information systems.

- Provides a mandatory framework for federal agencies to ensure adequate protection of their information and systems.
- Defines the minimum security requirements that must be satisfied through the implementation of security controls.

FIPS 200

- FIPS 200 specifies 17 security-related areas, which align with the NIST Special Publication 800-53 control families. Agencies must implement controls to meet the minimum requirements in each of these areas:
- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Certification, Accreditation, and Security Assessments (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- Systems and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Risk Based Approach

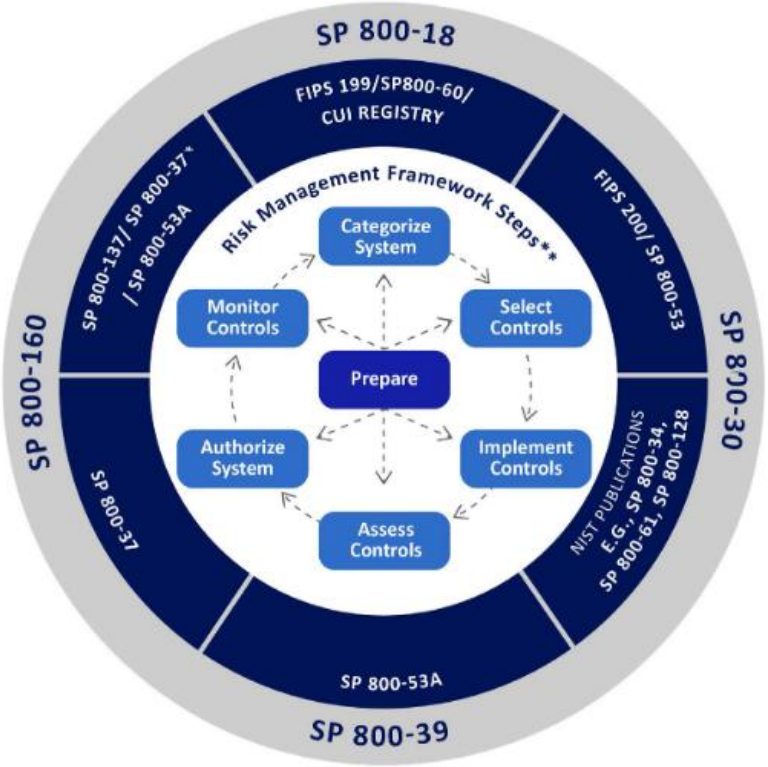


Figure 3: Risk-Based Approach

https://www.dafcio.af.mil/Portals/64/The%20Cyber%20Cake.pdf

STIGS

Security Technical Implementation Guides (STIGs) provide guidance on implementing various technologies
https://www.cyber.mil/stigs/downloads

Kubernetes STIG SCAP Benchmark - Ver 2, Rel 3	Unclassified	2025-04-08	STIGs	Download
Layer 2 Switch SRG - Ver 3, Rel 2	Unclassified	2025-04-07	STIGs	Download
Mainframe Product SRG - Ver 3, Rel 3	Unclassified	2025-01-28	STIGs	Download
MariaDB Enterprise 10.x STIG - Ver 2, Rel 3	Unclassified	2025-01-28	STIGs	Download
MarkLogic Server v9 STIG - Ver 3, Rel 2	Unclassified	2024-10-23	STIGs	Download