

CSX – Cybersecurity Fundamentals

Section 3 : Security architecture principles



Course Plan

Module Titles

Section 1 – Cybersecurity Introduction and Overview

Section 2 – Domain 1: Cybersecurity Concepts

Section 3 – Domain 2: Security Architecture Principles

Section 4 – Domain 3: Security of Networks, Systems, Applications and Data

Section 5 – Domain 4: Incident Response

Section 6 – Domain 5: Security Implications and Adoption of Evolving Technology

Section 7 – Course Review

Section 8 – Practice Exam



Learning Outcomes for this Module

- Knowledge of network design processes, to include understanding of security objectives, operational objectives and trade-offs
- Knowledge of security system design methods, tools and techniques
- Knowledge of network access, identity and access management
- Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)
- Knowledge of network security architecture concepts, including topology, protocols, components and principles (e.g., application of defense in depth)
- Knowledge of malware analysis concepts and methodology



Learning Outcomes for this Module

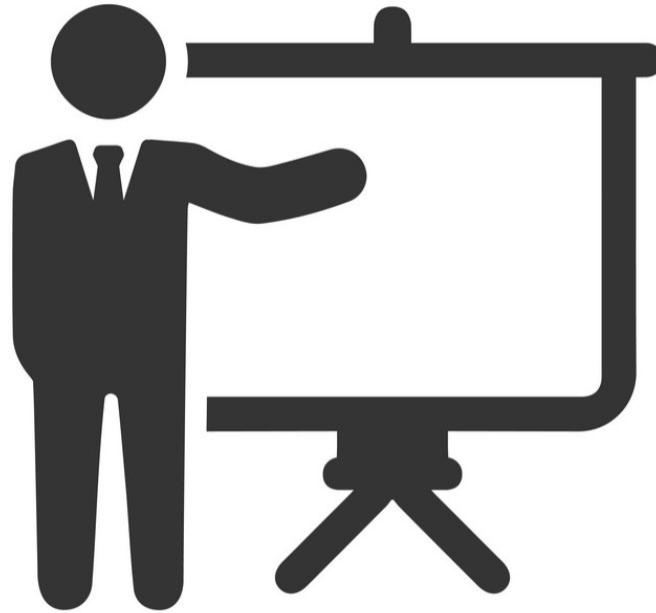
- Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies
- Knowledge of defense in depth principles and network security architecture
- Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE])
- Knowledge of cryptography
- Knowledge of encryption methodologies
- Knowledge of how traffic flows across the network (i.e., transmission and encapsulation)
- Knowledge of network protocols



Topics for this Module

- **3.1** Overview of security architecture
- **3.2** The OSI model
- **3.3** Defense in depth
- **3.4** Information flow control
- **3.5** Isolation and segmentation
- **3.6** Logging, monitoring and detection
- **3.7** Encryption fundamentals, techniques and applications

Current Events



Section 3.1

Overview of security architecture



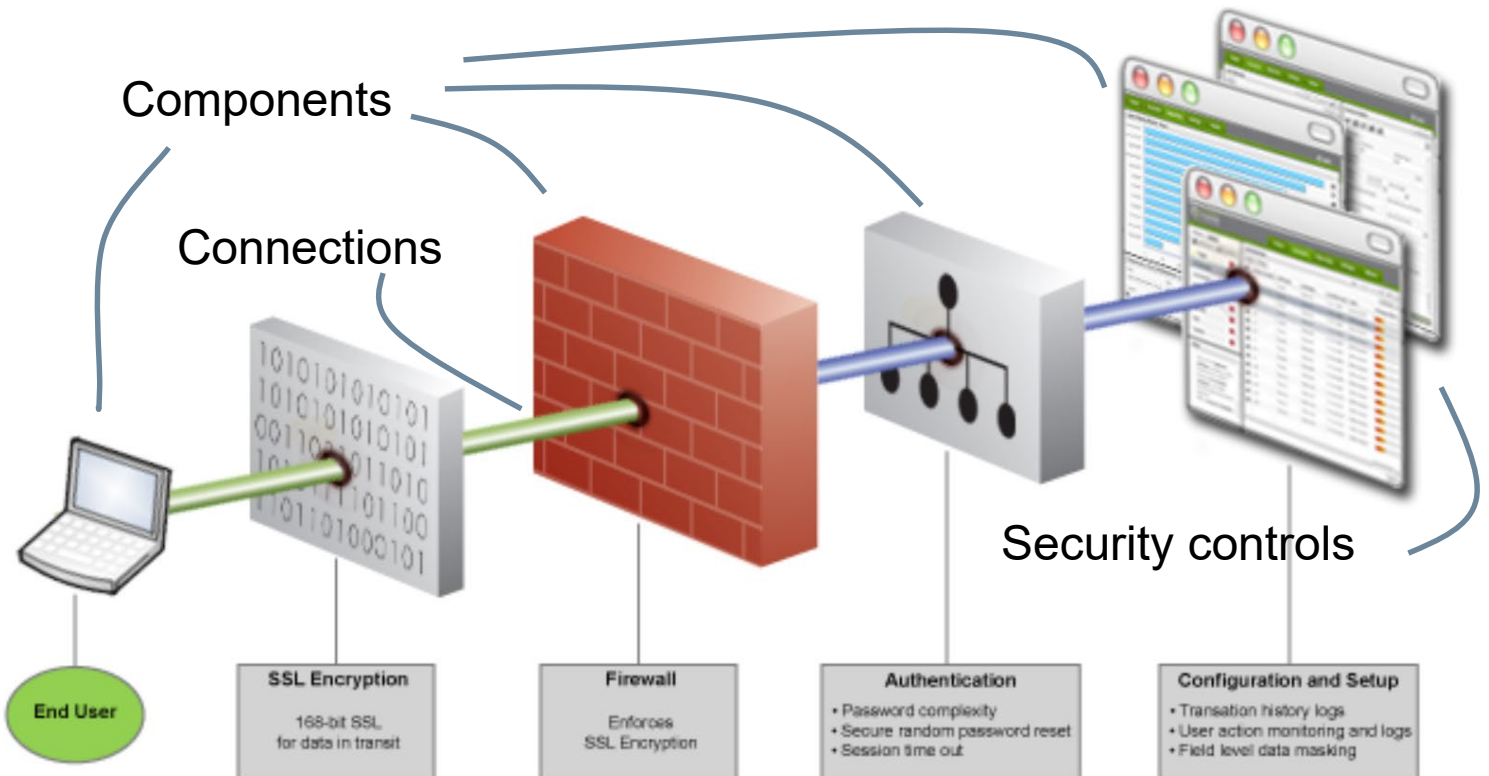
Question

What is security architecture?



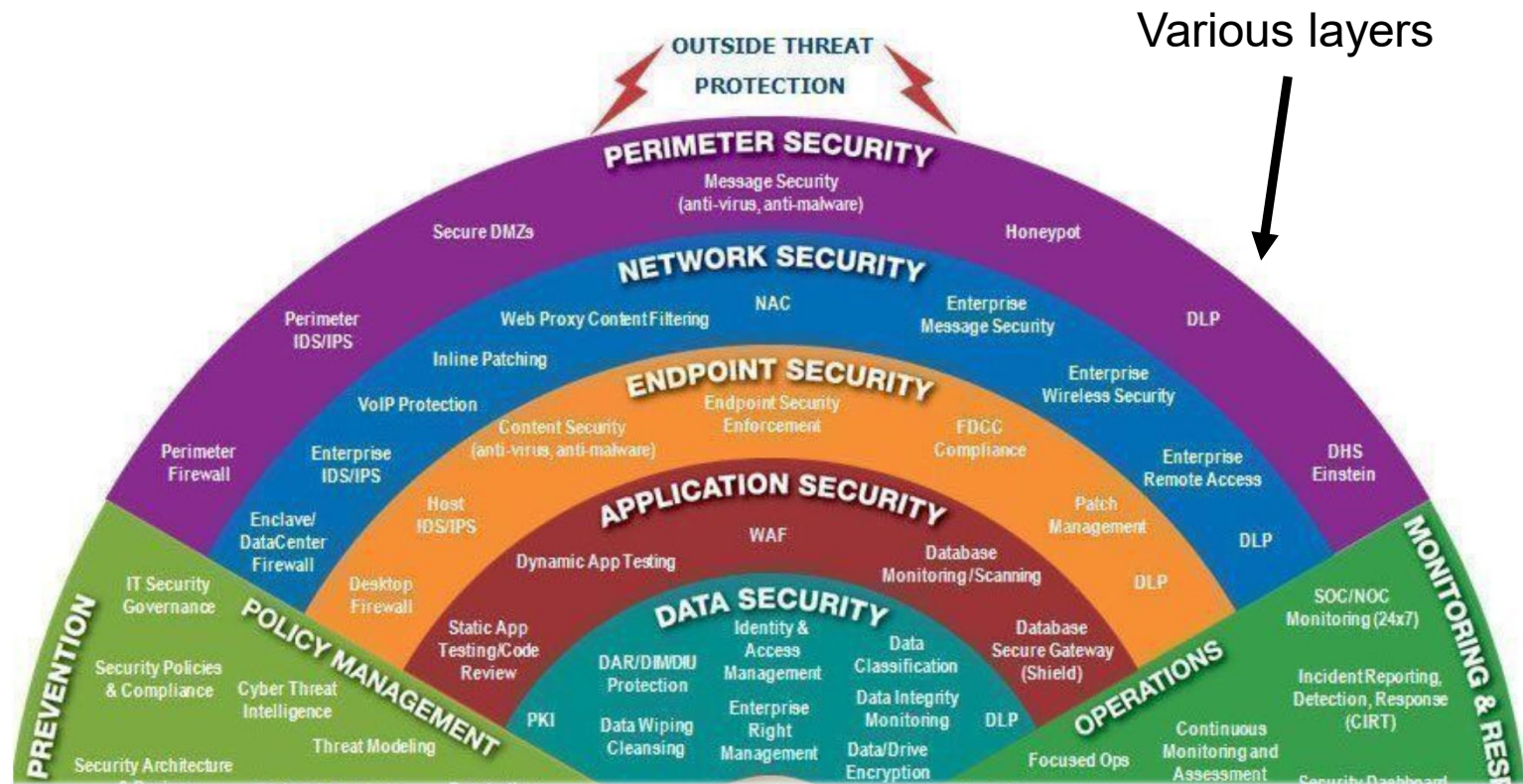
What is security architecture?

Structure

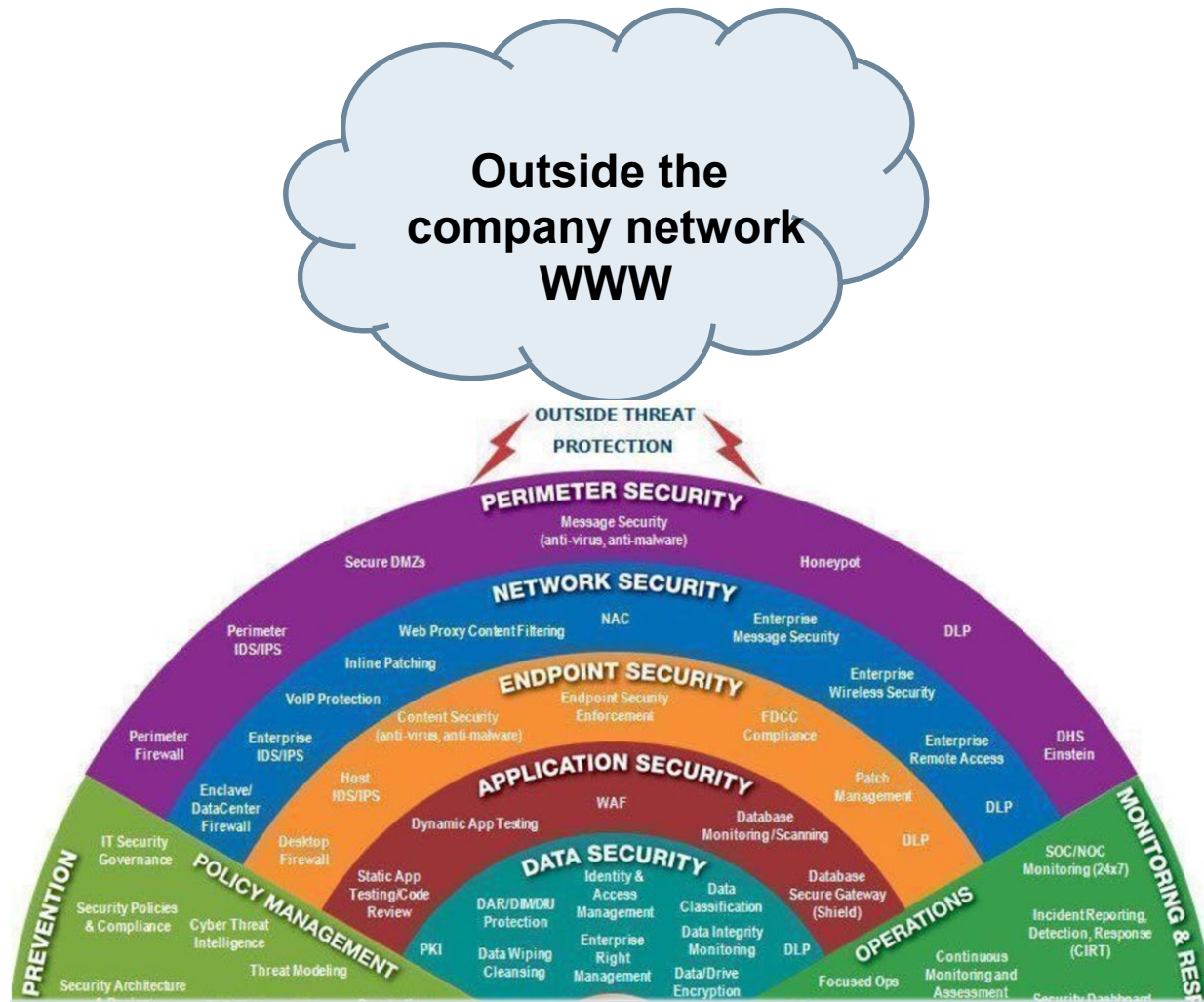


Security architecture

Term: Defense in depth



The security perimeter



The security perimeter

Controls:

- Network or System-centric
 - Places the emphasis on controls at the network and system level to protect information (i.e. firewalls, IDS, honeypots)
- Data-centric:
 - Is an approach to security that emphasizes the security of the data itself rather than the security of networks, servers, or applications (i.e. Big data)

Internet perimeter is an important component of “Security Perimeter”

The security perimeter

In order to provide security of email, front-end mobile and web apps, domain name system (DNS), etc., the Internet perimeter should:

- **Route traffic** between the enterprise and the Internet
- Prevent executable files from being transferred through email attachments or web browsing
- **Monitor internal and external** network ports for rogue activity
- **Detect and block traffic** from infected internal end point
- **Control user traffic** bound toward the Internet (**access lists**)
- Identify and block anomalous traffic and malicious packets recognized as potential attacks
- Eliminate **threats such as email spam**, viruses and worms
- Enforce filtering policies to block access to websites containing malware or questionable content

Interdependencies

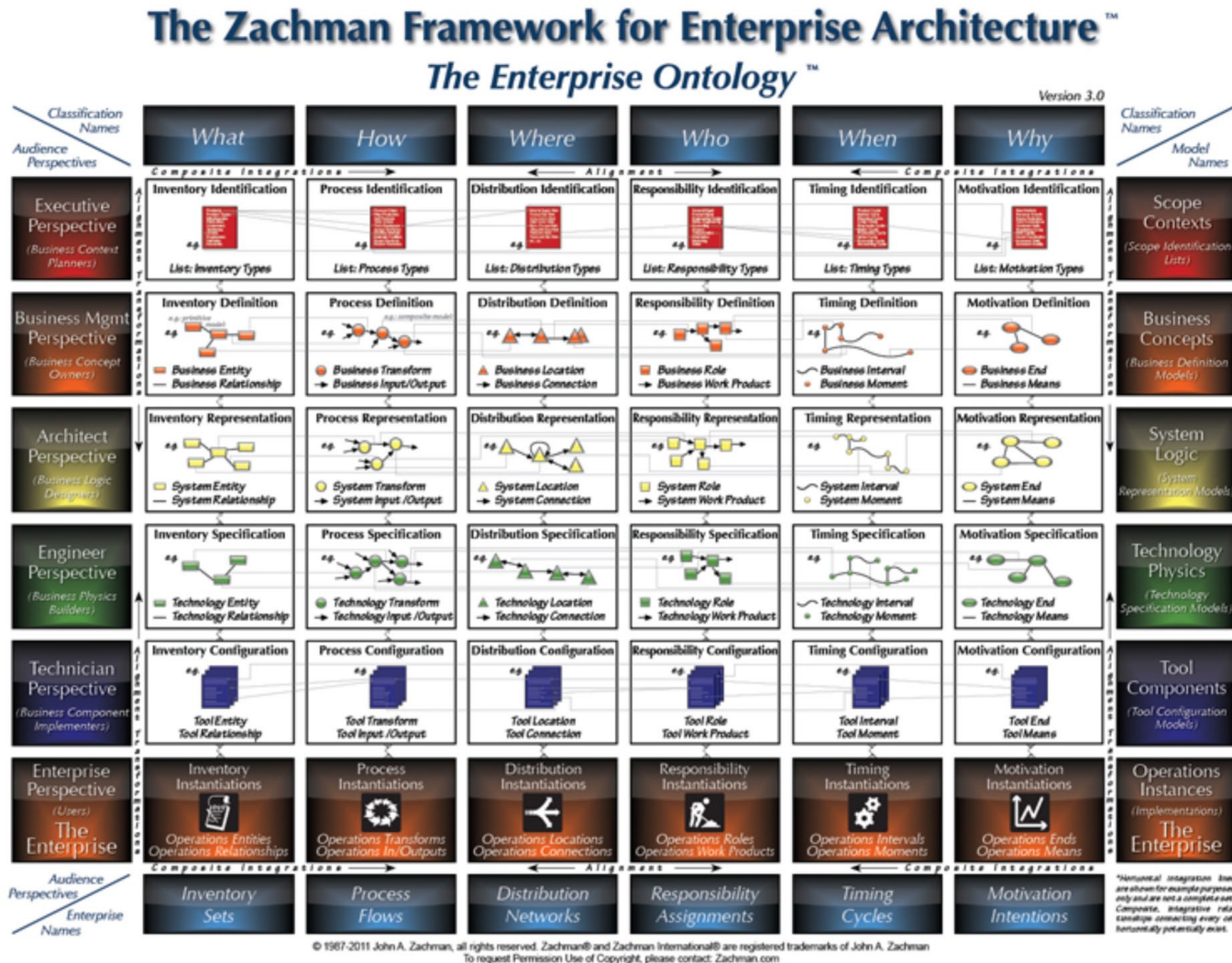
There are a lot of interdependencies to consider because the landscape has changed drastically and evolved:

- Cloud services (PaaS, IaaS, SaaS, etc.)
- BYOD
- Increase in mobile phones
- Tablets
- VPN
- Increase in data repositories in the cloud

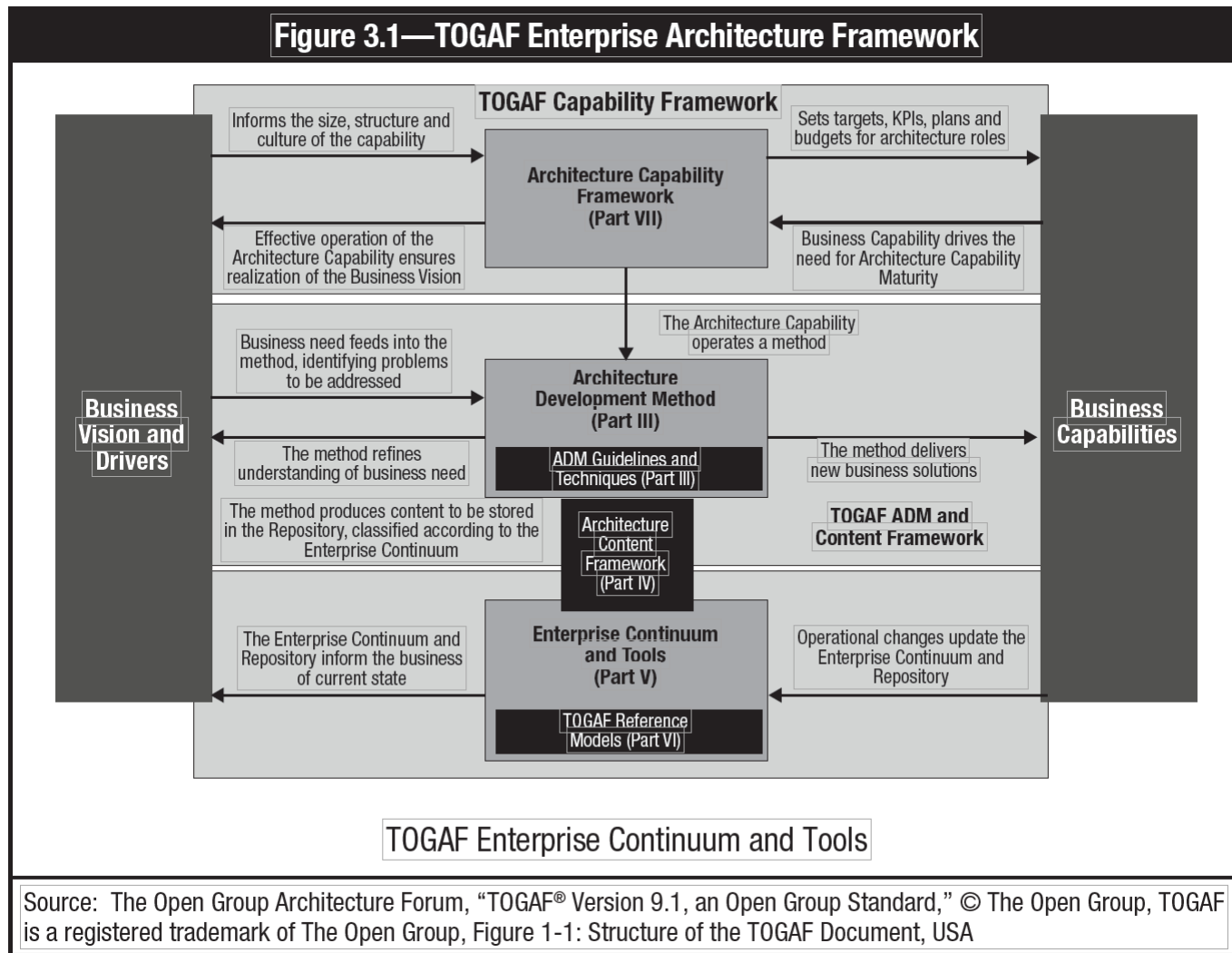
Frameworks - SABSA

- SABSA is a proven methodology for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives.
- Used for Information Assurance Architectures, Risk Management Frameworks, and to align and seamlessly integrate security and risk management into IT Architecture methods and frameworks.

Frameworks - ZACHMAN



Frameworks - TOGAF

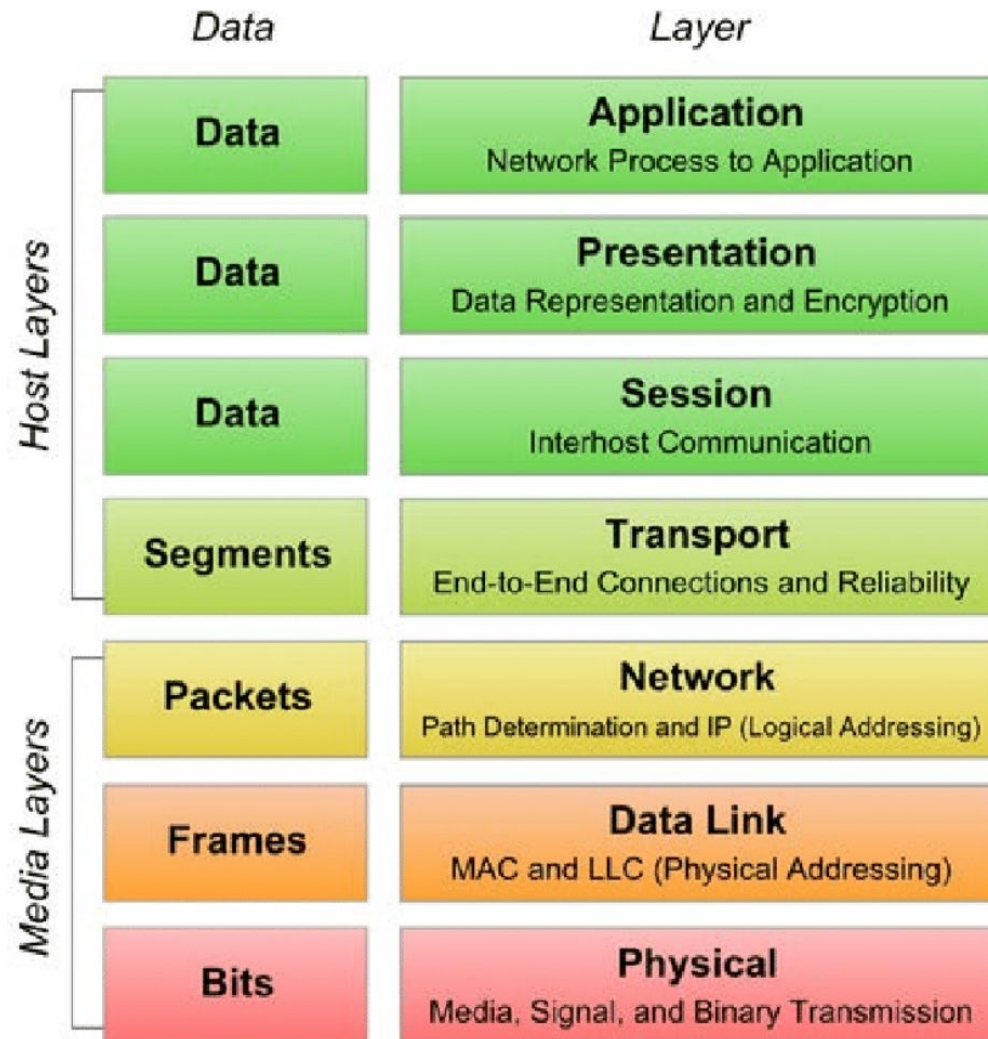


Any questions?

Section 3.2

The OSI model

The OSI Model



The OSI / TCP/IP Model

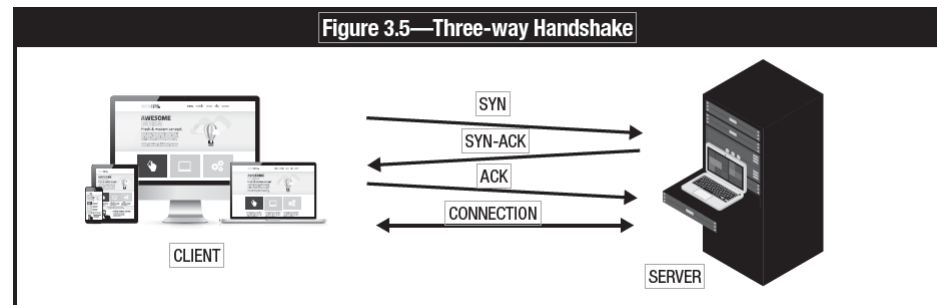
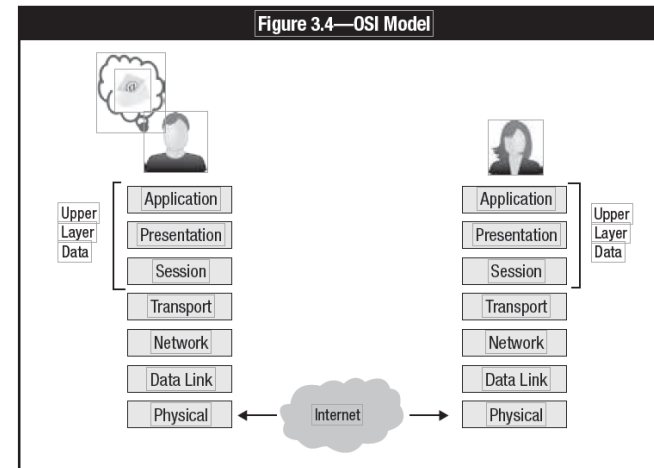
Review OSI video:

<https://www.youtube.com/watch?v=i9RL5jD9cTI>

Figure 3.3—OSI Association With the TCP/IP Suite

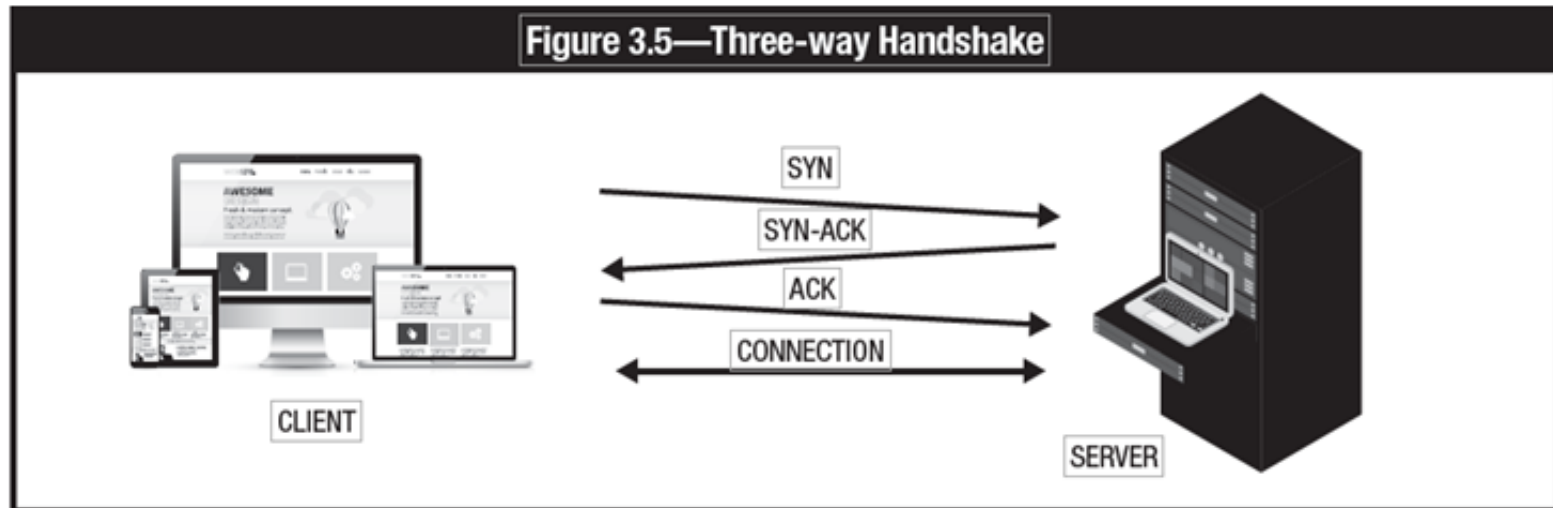
OSI Model	TCP/IP Conceptual Layers	Protocol Data Unit (PDU)	TCP/IP Protocols	Equipment	Layer Functions	Layer Functions
7	Application	Data	HTTP File Transfer Protocol (FTP) Simple Mail Transport Protocol (SMTP) TFTP NFS Name Server Protocol (NSP) Simple Network Management Protocol (SNMP) Remote Terminal Control Protocol (Telnet) LPD X Windows DNS DHCP/BootP	Gateway	Provides user interface	File, print, message, database, and application services
6	Presentation				Presents data	Data encryption, compression and translation services
5	Session				Handles processing such as encryption	Dialog control
4	Transport	Segment	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)	Layer 4 switch	Keeps separate the data of different applications	End-to-end connection
3	Network	Packet	ICMP ARP RARP Internet Protocol (IP)	Router Layer 3 switch	Provides logical addressing which routers use for path determination	Routing
2	Data link	Frame	Ethernet Fast Ethernet FDDI Token Ring Point-to-point Protocol (PPP)	Layer 2 switch Bridge Wireless AP	Combines packets into bytes and bytes into frames	Framing
1	Physical	Bits		NIC Hub Repeater NIC	Provides access to media using MAC address Performs error detection, not error correction Moves bits between devices Specifies voltage, wire speed and pin-out of cables	Physical topology

Source: ISACA, CISA Review Manual 28th Edition, USA, 2015, figure 4.23



Encapsulation

Review video: <https://www.youtube.com/watch?v=xaKvGnnuYmk>



Any questions?

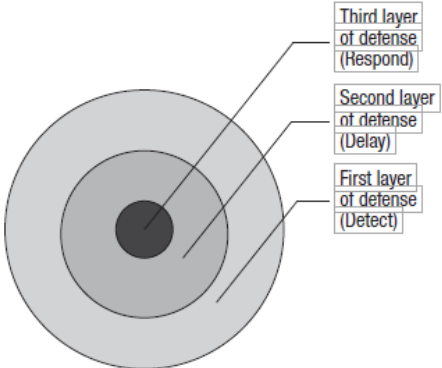
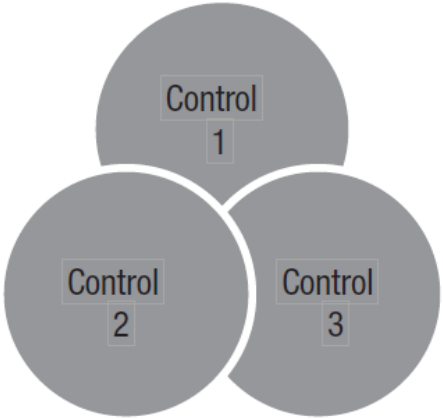
Section 3.3

Defense in depth

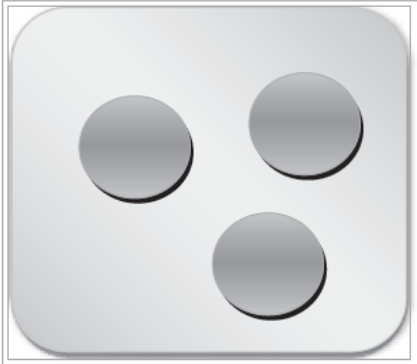
Defense in depth

- Defense in depth is the process of layering defenses
- The number of layers depends on the assets:
 - Criticality
 - Reliability
 - Value
- Two layer example:
 - Firewall – protects network intrusion
 - Training / awareness – adds protection at the human layer

Types of defense

Figure 3.6—Types of Defense in Depth Implementations		
Type of Defense	Graphical Representation	Description
Concentric Rings (or nested layering)	 <p>The diagram shows three concentric circles. The innermost circle is labeled 'First layer of defense (Detect)'. The middle ring is labeled 'Second layer of defense (Delay)'. The outermost ring is labeled 'Third layer of defense (Respond)'.</p>	<p>Creates a series of nested layers that must be bypassed in order to complete an attack.</p> <p>Each layer delays the attacker and provides opportunities to detect the attack.</p>
Overlapping redundancy	 <p>The diagram shows three overlapping circles labeled 'Control 1', 'Control 2', and 'Control 3'. The circles overlap in various combinations, creating a central area where all three controls overlap.</p>	<p>Two or more controls that work in parallel to protect an asset.</p> <p>Provides multiple, overlapping points of detection. This is most effective when each control is different.</p>

Types of defense

Figure 3.6—Types of Defense in Depth Implementations (cont.)		
Type of Defense	Graphical Representation	Description
Segregation or compartmentalization		<p>Compartmentalizes access to an asset, requiring two or more processes, controls or individuals to access or use the asset.</p> <p>This is effective in protecting very high value assets or in environments where trust is an issue.</p>
Source: Encurve, LLC.		

Any questions?

Section 3.4

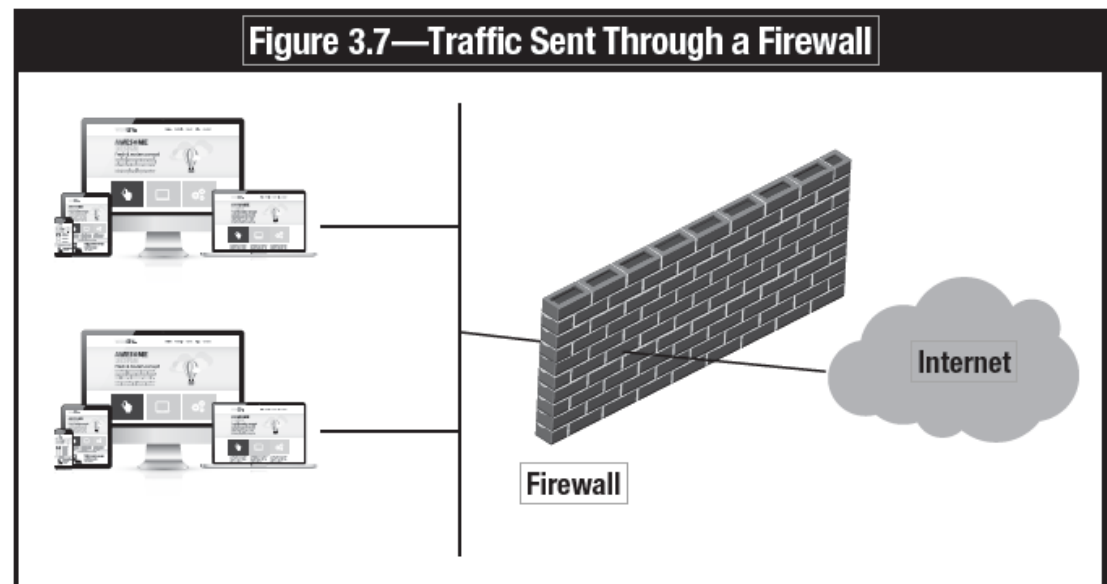
Information flow control

Information flow control

- Information flow protection is needed
- All network touch Public Network – “Internet”
- Firewalls are need

Firewall role:

- Block
- Limit
- Prevent
- Monitor
- Encrypt
(VPN traffic)



Types of firewalls

Figure 3.8—Firewall Types

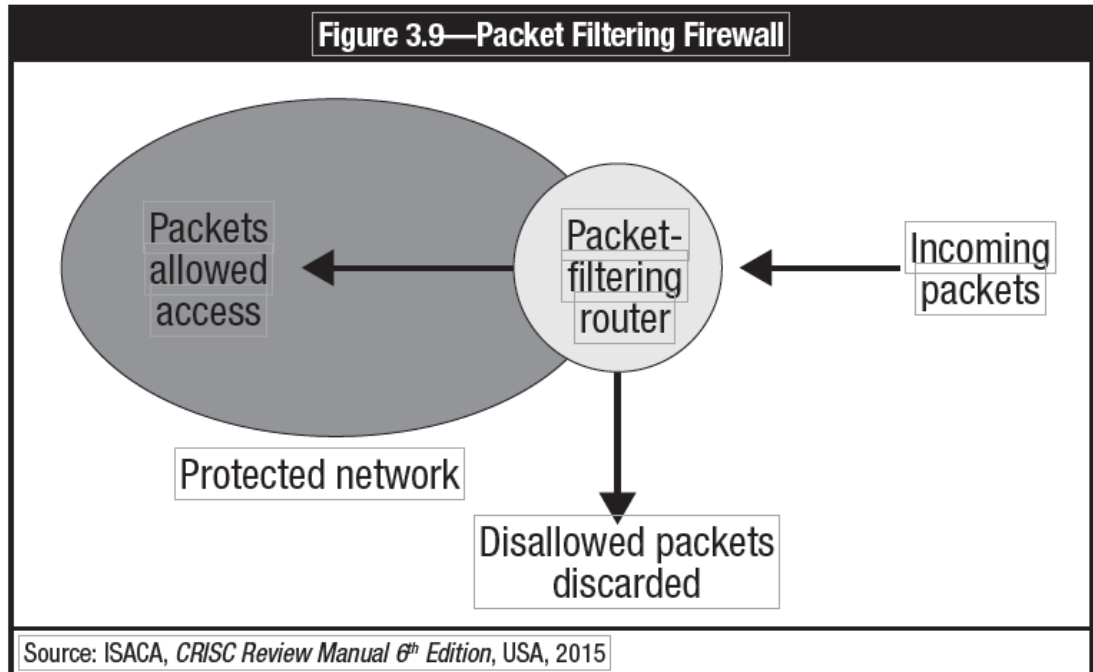
First Generation	A simple packet-filtering router that examines individual packets and enforces rules based on addresses, protocols and ports.
Second Generation	Keeps track of all connections in a state table. This allows it to enforce rules based on packets in the context of the communications session.
Third Generation	Operates at layer seven (the application layer) and is able to examine the actual protocol being used for communications, such as Hypertext Transfer Protocol (HTTP). These firewalls are much more sensitive to suspicious activity related to the content of the message itself, not just the address information.
Next Generation	Sometimes called deep packet inspection—is an enhancement to third generation firewalls and brings in the functionality of an intrusion prevention system (IPS) and will often inspect Secure Sockets Layer (SSL) or Secure Shell (SSH) connections.

Source: ISACA, *CRISC Review Manual 6th Edition*, USA, 2015

Packet Filter concept

1st Gen FW - In packet filtering, a screening router examines the header of every packet of data traveling between the Internet and the corporate network.

2nd, 3rd, Next Gen FW – Deeper inspection



Types of network attacks

IP spoofing:

- Is a technique used to gain unauthorized access to machines, whereby an attacker illicitly impersonates another machine by manipulating IP packets. **IP Spoofing involves modifying the packet header with a forged (spoofed) source IP address**, a checksum, and the order value.

Source routing specification:

- This type of attack centers around the routing that an IP packet must take when it traverses the Internet from the source host to the destination host. In this process, it is possible to **define the route so it bypasses the firewall.**

Miniature fragment attack:

- IP fragmentation attacks are a common form of **denial of service** attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms.

Application firewall systems

Application-level gateway:

- Application-level gateways are systems that analyze packets through a set of proxies—one for each service (e.g., Hypertext Transmission Protocol [HTTP] proxy for web traffic, FTP proxy)

Circuit-level gateway:

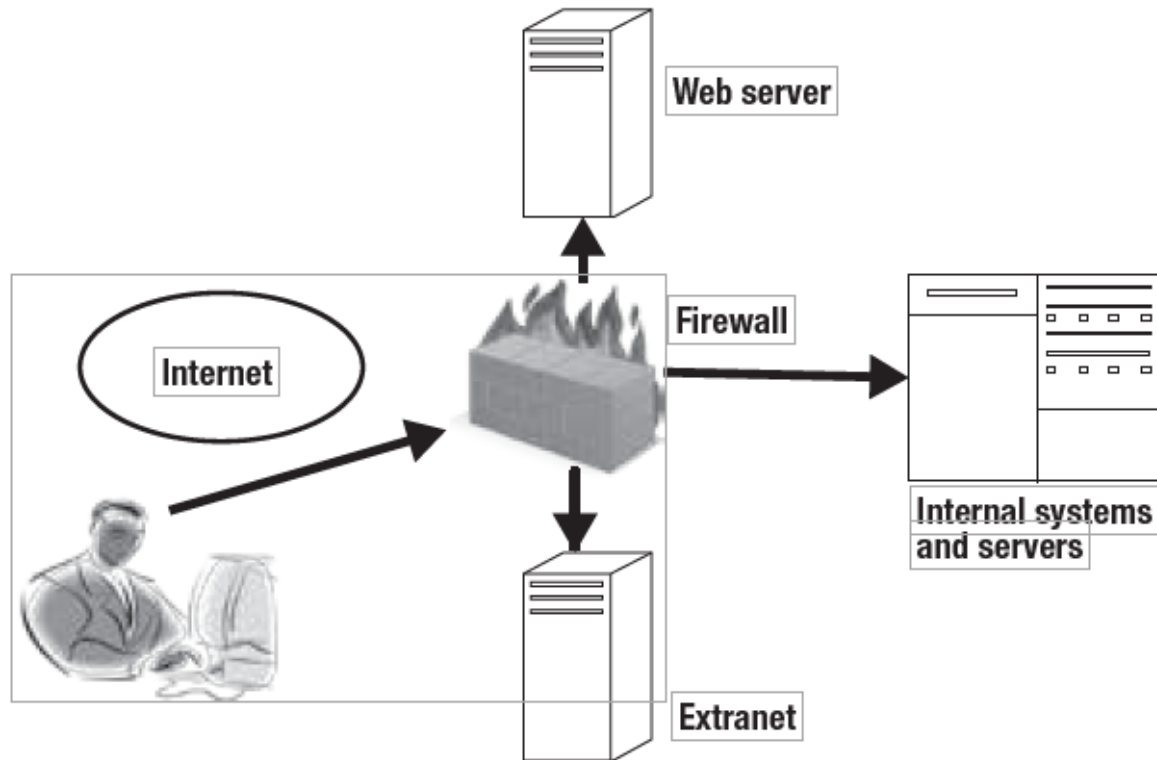
- A circuit-level gateway is a type of firewall. Circuit-level gateways work at the session layer of the OSI model, or as a "shim-layer" between the application layer and the transport layer of the TCP/IP stack.

Stateless vs. Stateful firewalls

- Stateless filtering **does not keep the state of ongoing TCP connection sessions.** In other words, it has no memory of what source port numbers the sessions' client selected.
- Stateful firewalls keep track of TCP connections. **The firewall keeps an entry in a cache for each open TCP connection.** Stateless firewalls perform more quickly than stateful firewalls, but they are not as sophisticated.
- Review video:
<https://www.youtube.com/watch?v=gMvXruavqDI>

Firewall topology

Figure 3.13—The Demilitarized Zone



Source: ISACA, *CRISC Review Manual 6th Edition*, USA, 2015

Firewall risks

Configuration errors:

- Misconfigured firewalls may allow unknown and dangerous services to pass through freely.

Monitoring demands:

- monitoring activities may not always occur on a regular basis.

Policy maintenance:

- Firewall policies may not be maintained regularly.

Vulnerability to application- and input-based attacks:

- Most firewalls operate at the network layer; therefore, **they do not stop any application-based or input-based attacks, such as SQL injection and buffer-overflow attacks**. Newer generation firewalls are able to inspect traffic at the application layer and stop some of these attacks.

Firewall platforms

- Firewalls come in many flavours:
 - Hardware
 - Software
 - Virtual
- Hardware based firewalls perform better than software. Software firewalls have more overhead to deal with and process

Next Generation Firewalls (NGFW)

- Benefits:
 - 1) the **inability to inspect packet payload** and
 - 2) the inability to distinguish between types of web traffic.
 - 3) Deep packet inspection (DPI)
 - 4) Intrusion prevention system (IDS)
 - 5) Secure Socket Layer (SSL) inspection
 - 6) Web filtering
 - 7) Secure Shell (SSH) inspection
- An NGFW is an adaptive network security system capable of **detecting and blocking sophisticated attacks**.

Next Generation Firewalls (NGFW)

- Benefits:
 - 1) the **inability to inspect packet payload** and
 - 2) the inability to distinguish between types of web traffic.
 - 3) Deep packet inspection (DPI)
 - 4) Intrusion prevention system (IDS)
 - 5) Secure Socket Layer (SSL) inspection
 - 6) Web filtering
 - 7) Secure Shell (SH) inspection
- An NGFW is an adaptive network security system capable of **detecting and blocking sophisticated attacks**.

Any questions?

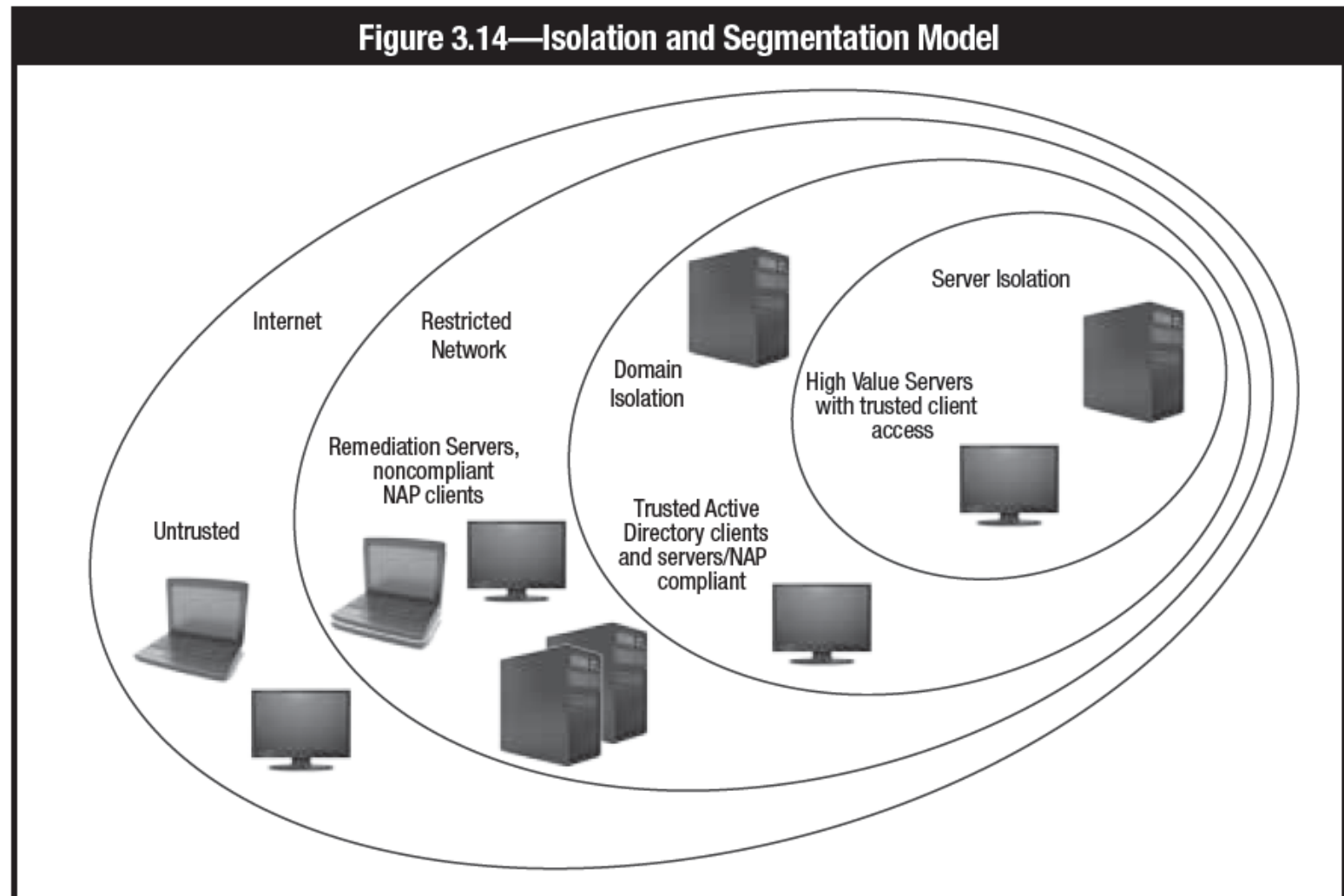
Section 3.5

Isolation and segmentation

Isolation and segmentation

- Virtual Local Area Network (VLANs):
 - 1) Network that are segmented logically (not physical)
 - 2) Configure ports on switch with VLANs
 - 3) Devices connected to those ports communicate through VLANs
 - 4) VLANs allow for flexibility
- Virtual Local Area Network (VLANs):
 - Layer 4 switching uses Transport Layer
 - Application layer information carried with Layer 3 addresses
 - Layer 3 more resource intensive, carry more protocol information

Security zones and demilitarized zones (DMZ)



Any questions?

Section 3.6

Logging, monitoring and detection

Logging, monitoring and detection

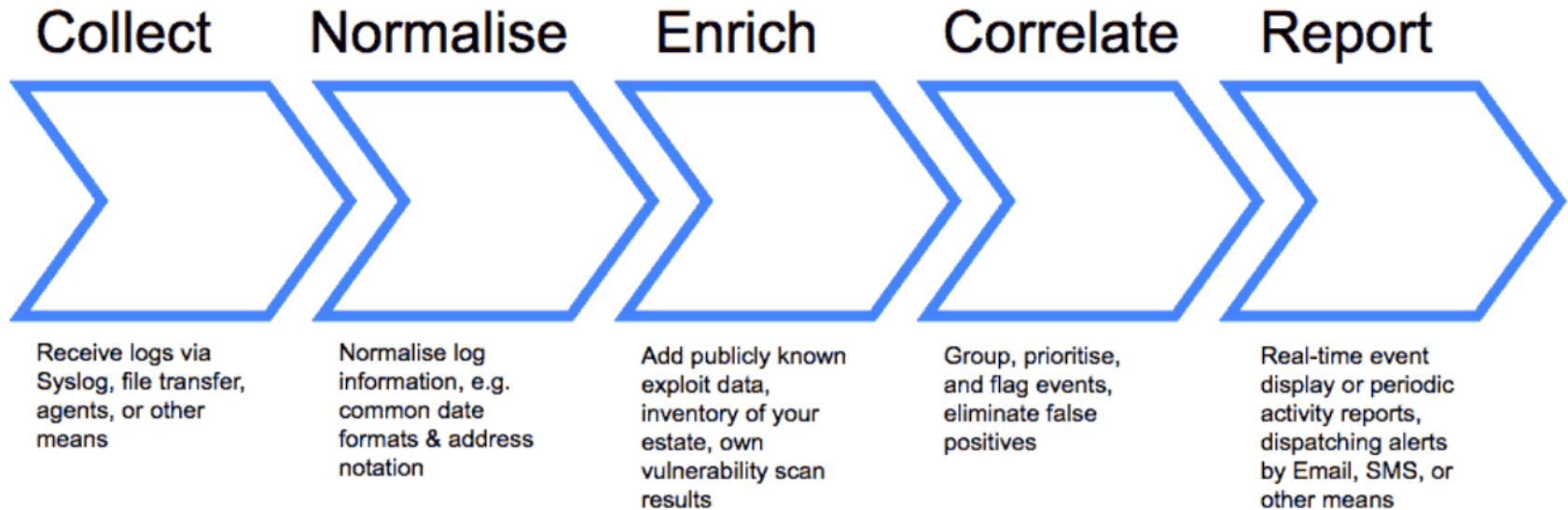
- Monitoring, detection and logging are integral parts of cybersecurity
- Monitoring what information (flow) comes in and out is essential to prevent data loss
- What to log?
 - Time of the event
 - Changes to permission
 - System start-up or shutdown
 - Login or logout
 - Change to data
 - Errors or violations
 - Job failures

Logging, monitoring and detection

- **Logs can reveal:**
 - Risk relevant events
 - Compliance violations
 - Suspicious behaviour
 - Errors, abnormal behaviour
- **Segregation of duties (SoD) is important:**
 - Ability to change system configuration segregated from ability to review, modify or delete logs
- **Challenges:**
 - Having too much data
 - Difficult searching
 - Improper configuration
 - Modifying or deleting of data before read (i.e. too little storage space)

Security information and event management

Security Event Management Systems (SEM)
System flow:

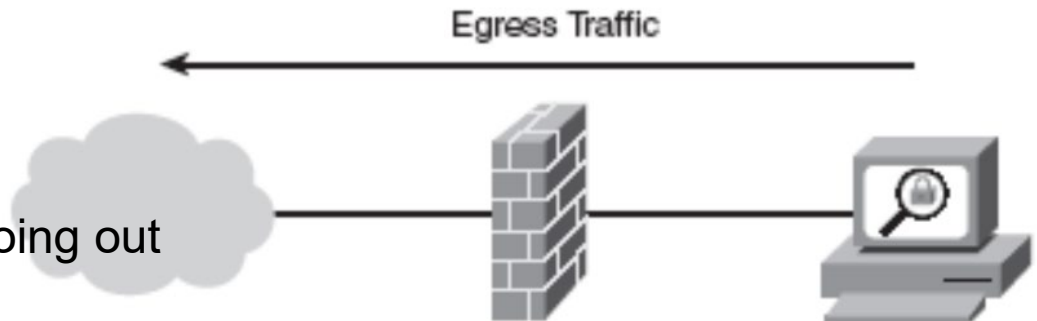


Ingress, egress and data loss prevention (DLP)

Ingress:
networking communication coming in



Egress:
networking communication going out



Ingress, egress and data loss prevention (DLP)

- **Data at rest** is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way
- **Data in transit**, or data in motion, is data actively moving from one location to another such as across the internet or through a private network
- **Data in use** is an information technology term referring to active data which is stored in a non-persistent digital state typically in computer random-access memory (RAM), CPU caches, or CPU registers.



Antivirus and anti-malware

What is a virus?

What is malware?

- Answer = Malicious code. Most common threat vector to compromise systems
- Virus signatures will help to certain extend, not effective with unknown viruses or malware

Controls needed:

Heuristic-based methods of detecting unknown malware

- Restriction outbound traffic
- Policies and awareness that trains users (suspicious emails)
- Multi-layers of anti-malware (no one solution is the silver bullet)

Intrusion detection system (IDS)

IDS works in conjunction with routers and firewalls:

Two types:

- **Network-based IDSs**—These identify attacks within the monitored network and issue a warning to the operator
- **Host-based IDSs**—These are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. **They can detect the modification or execution of files** and issue a warning when an attempt is made to run a privileged command.

Intrusion detection systems (IDS)

Types of IDS:

- **Signature-based**—These IDS systems protect against **detected intrusion patterns**. The intrusive patterns they can identify are stored in the form of signatures.
- **Statistical-based**—These systems need **a comprehensive definition of the known** and expected behavior of systems
- **Neural networks**—An IDS with this feature **monitors the general patterns of activity** and traffic on the network and **creates a database**. It is similar to the statistical model but with added self-learning functionality.

Intrusion detection systems (IDS)

IDS Features	IDS Limitations
Intrusion detection	Weakness in the policy definition
Ability to gather evidence on intrusive activity	Application-level (programming) vulnerabilities
Automated response	Back door into applications
Security policy	Weaknesses in identification and authentication schemes
Interface with system tools	
Security policy management	

Intrusion prevention systems (IDS)

- An intrusion prevention system (IPS) is a system that monitors a network for malicious activities such as security threats or policy violations
- The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it

Any questions?

Section 3.7

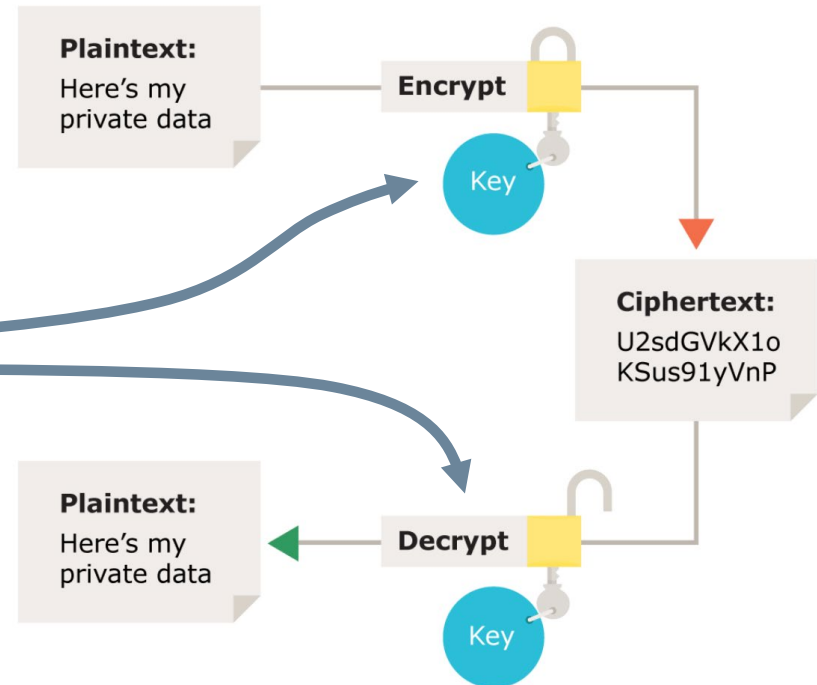
**Encryption fundamentals,
techniques and applications**

Encryption fundamentals, techniques and applications

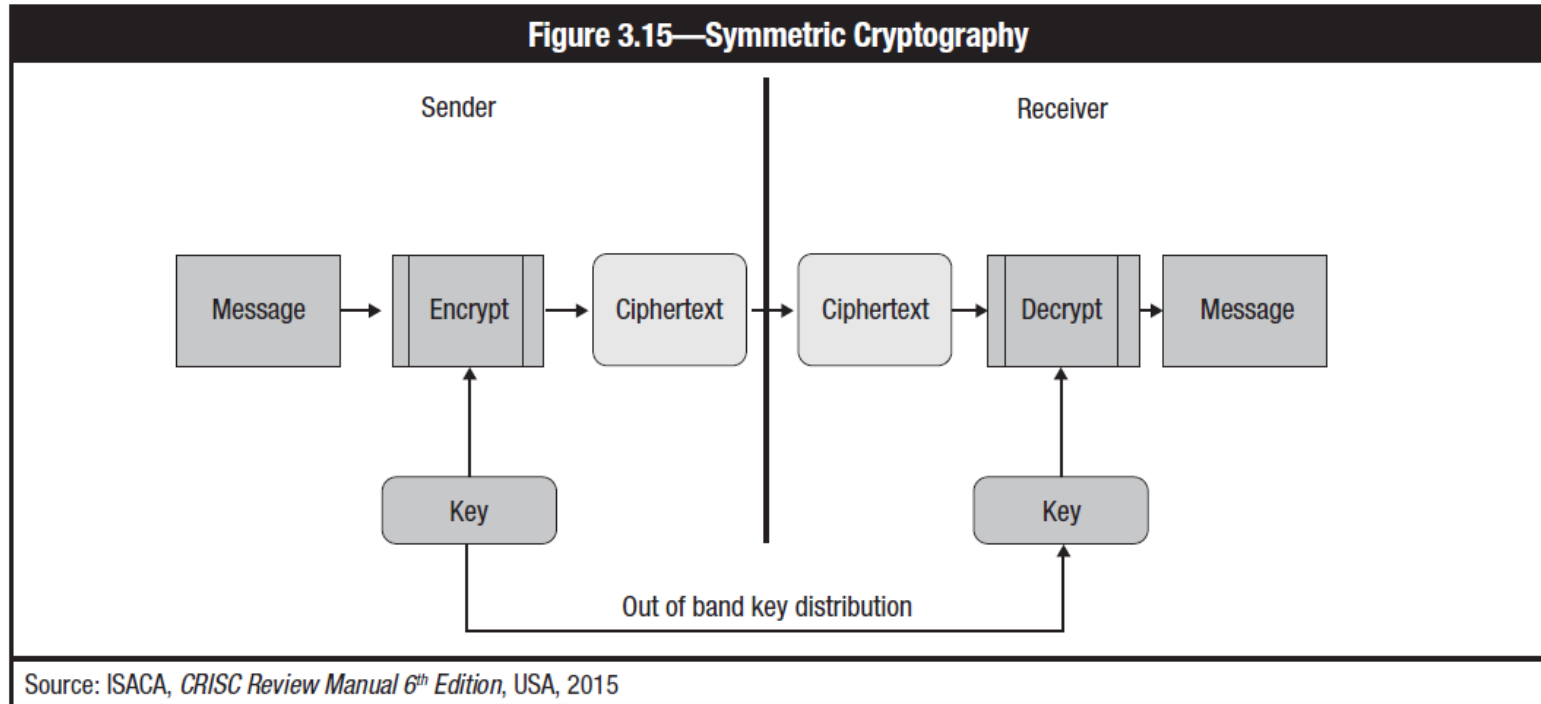
What is encryption?:

- Is the process of converting plaintext message into a secure form of text
- This is a science called, **“Cryptography”**

Mathematical algorithms
Used to encrypt / decrypt



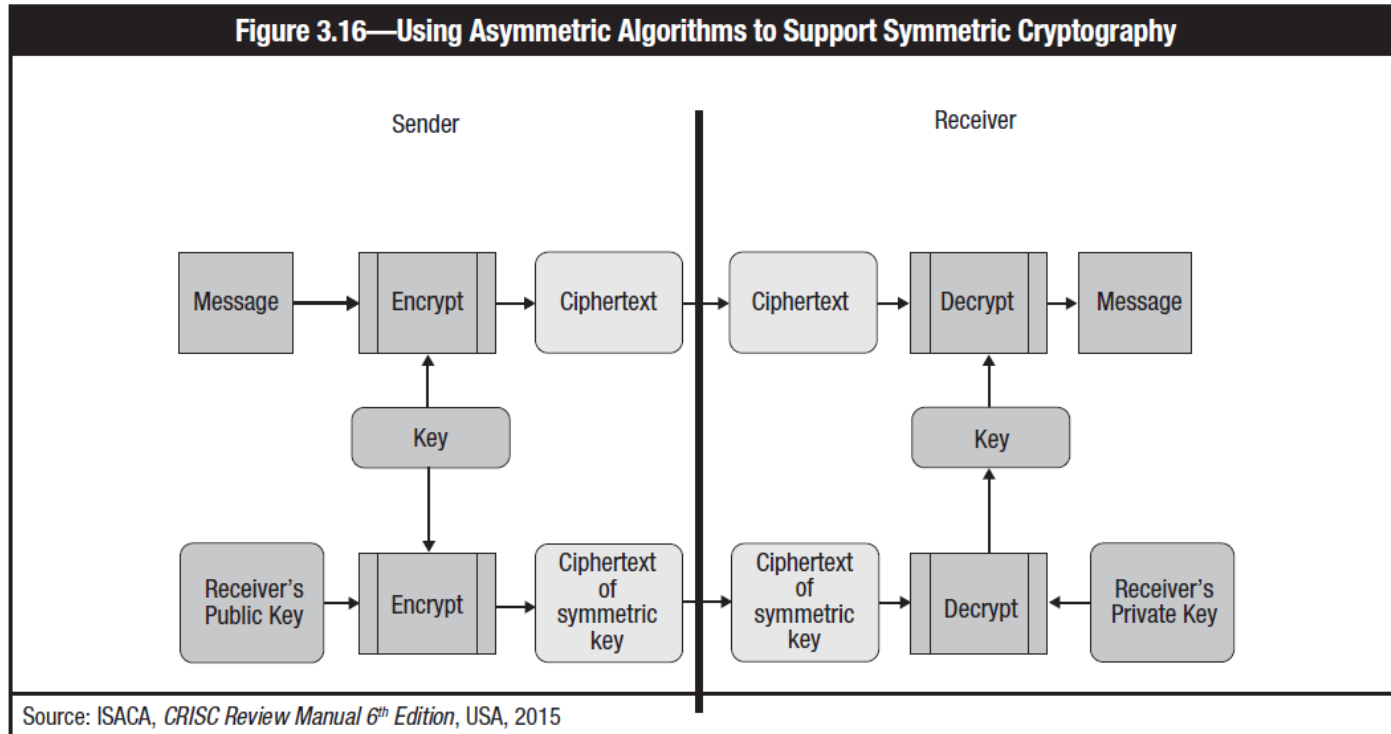
Symmetric (private) key encryption



Uses the same key to encrypt / decrypt plaintext to ciphertext

Examples: DES, 3DES, AES

Asymmetric (private) key encryption



Uses two keys that work as a pair to encrypt / decrypt plaintext to ciphertext. Sender key is the **private key**, receiver key is **public key**

Other cryptography's

Elliptic-curve cryptography (ECC):

- Is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security - Wikipedia

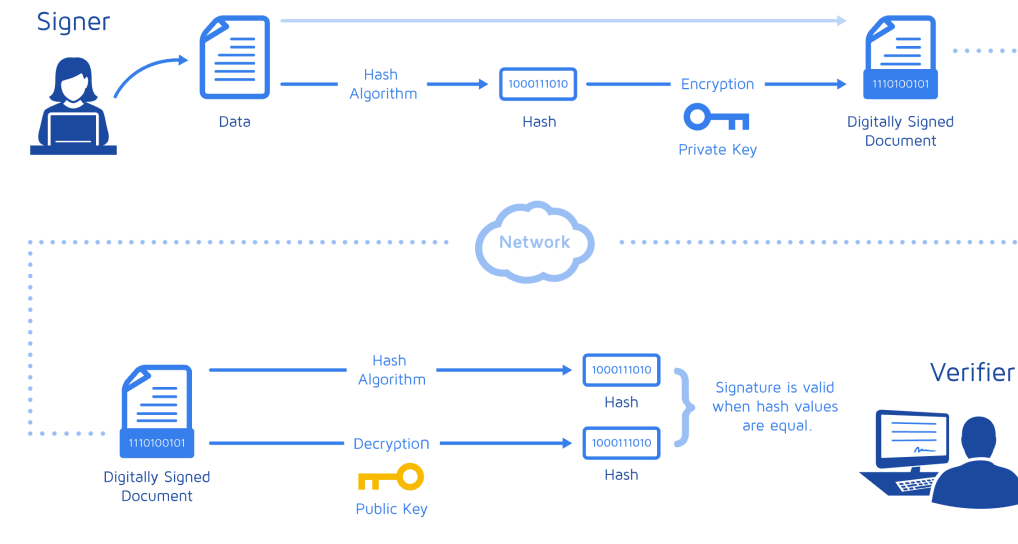
Quantum cryptography:

- Is the next generation of cryptography that may solve some of the existing problems associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys.

Other cryptography's

Digital signatures:

- A **digital signature** is an electronic identification of a person or entity created by using a public key algorithm. It serves as a way for the recipient to verify the integrity of the data and the identity of the sender.



<https://www.docusign.ca/how-it-works/electronic-signature/digital-signature/digital-signature-faq>

Application of cryptographic systems

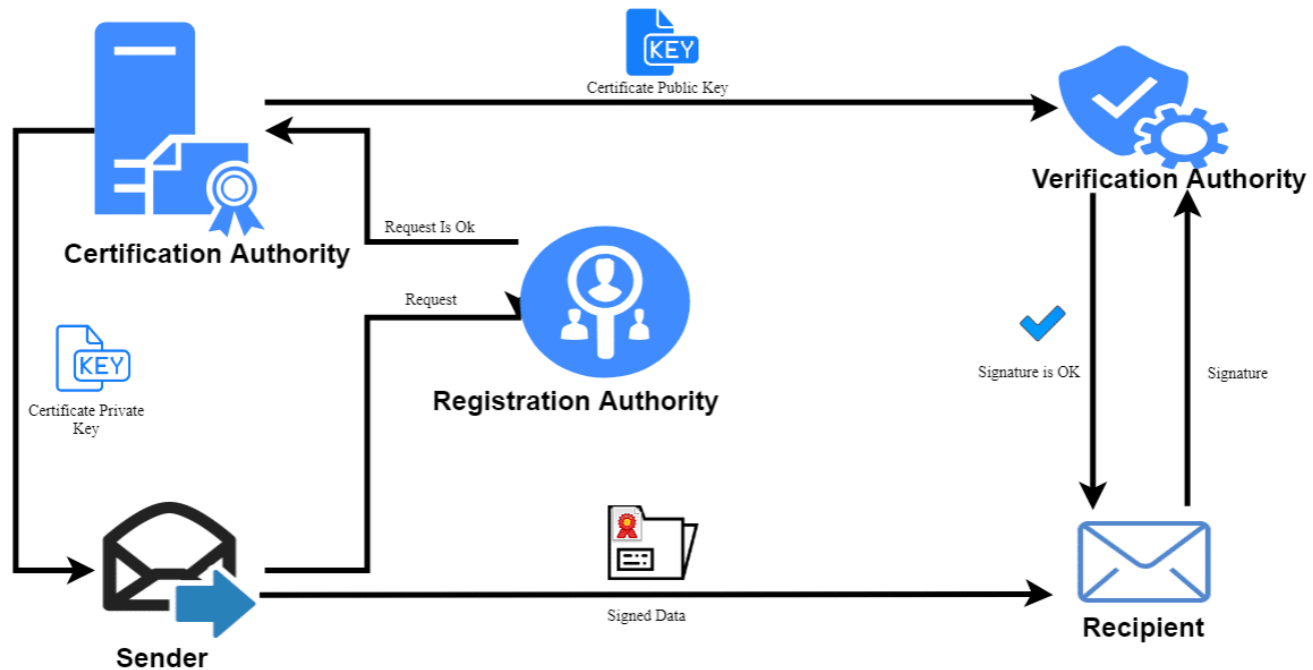
- **Transport Layer Security (TLS):** TLS is a cryptographic protocol that provides secure communications on the Internet. TLS is a session- or connection-layered protocol widely used for communication between browsers and web servers
- **Secure Hypertext Transfer Protocol (HTTPS):** As an application layer protocol, HTTPS transmits individual messages or pages securely between a web client and server by establishing a TLS-type connection
- **Virtual Private Network (VPN)**—A VPN is a secure private network that uses the public telecommunications infrastructure to transmit data

Application of cryptographic systems

- **IPSec:** IPSec is used for communication among two or more hosts, two or more subnets, or hosts and subnets
- **SSH:** SSH is a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon
- **Secure Multipurpose Internet Mail Extensions (S/MIME):** S/MIME is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of a message's contents, including attachments
- **Secure Electronic Transactions (SET)**—SET is a protocol developed jointly by VISA and MasterCard to secure payment transactions among all parties involved in credit card transactions.

Private key infrastructure

Public Key Infrastructure Explained



PKI explained:

- <https://www.youtube.com/watch?v=t0F7fe5Alwg>



Encryption vector

- **Data encryption is not fail safe:**
- **Cybercriminals are increasingly using encryption to conceal and launch attacks**
- **Podcast:**
 - <https://soundcloud.com/helpnetsecurity/cybercriminals-are-increasingly-using-encryption-to-conceal-and-launch-attacks>

Any questions?

Thank You