COMPTIA SECURITY+ SY0-701

Security Architecture

Cloud Computing, Network Architecture & Data Protection

Based on Professor Messer's Course Notes

2024 Edition

Navigation

Course Overview

01 **Cloud Infrastructure Models**
IaaS, PaaS, SaaS, and shared responsibility

02 **Network Infrastructure & Segmentation**
Physical and logical isolation strategies

03 **Infrastructure Security**
Securing networks, devices, and communication

04 **Data Protection & Classification**
Understanding and protecting organizational data

05 **Resiliency & Business Continuity**
Building resilient systems and disaster recovery planning

CHAPTER 01

Cloud Infrastructure Models

IaaS, PaaS, SaaS, and the shared responsibility model

Cloud Fundamentals

Cloud Service Models & Responsibility Matrix

Understanding who is responsible for security across cloud deployment models

IaaS

Infrastructure

Infrastructure as a Service provides virtualized computing resources over the internet.

Provider Manages:
Physical hosts, network, data center

Customer Manages:
OS, applications, data, identities

Examples: AWS EC2, Azure VMs, Google Compute

PaaS

Platform

Platform as a Service provides a development and deployment environment.

Provider Manages:
OS, middleware, runtime, infrastructure

Customer Manages:
Applications, data, access control

Examples: Heroku, AWS Elastic Beanstalk

SaaS

Software

Software as a Service delivers applications over the internet, on-demand.

Provider Manages:
Everything - app to infrastructure

Customer Manages:
Data, user access, identities

Examples: Office 365, Salesforce, Gmail

Shared Responsibility

Security is Well Documented

Most cloud providers provide a clear matrix of responsibilities so everyone knows their role upfront.

Responsibilities Vary

Different cloud providers and contractual agreements can shift responsibilities between provider and customer.

Third-Party Vendors

You, the cloud provider, and third-party vendors all share responsibility. Ongoing vendor risk assessments are critical.

Hybrid Considerations

Hybrid clouds add complexity: mismatched network protection, diverse authentication, different monitoring tools, and data leakage risks.

Modern Architectures

Cloud Architecture Patterns

Serverless, microservices, and infrastructure automation

Serverless Architecture

Function as a Service (FaaS) removes the operating system from the equation. Apps are separated into individual, autonomous functions.

Key Characteristics

- Event-triggered and ephemeral
- Runs in stateless compute containers
- Managed by third-party provider

Security Note: Watch for changes and unusual activity. All OS security concerns are at the third-party.

Infrastructure as Code

Describe infrastructure—servers, network, and applications—as code for consistent, repeatable deployments.

Benefits

- Version control infrastructure changes
- Build identical environments every time
- Critical for cloud computing

Challenge: Large codebase and change control complexity

Microservices vs Monolithic

Monolithic

One big application that does everything—UI, business logic, data I/O combined.

- Large codebase
- Change control challenges

Microservices

Small, independent services that work together via APIs.

- Scalable
- Resilient
- Built-in containment

APIs as Glue

Application Programming Interfaces connect microservices, allowing them to work together as a unified application.

API Security Considerations

- Authentication and authorization
- Rate limiting and throttling
- Input validation

Best Practice: API gateways provide centralized security, monitoring, and rate limiting.

CHAPTER 02

Network Infrastructure & Segmentation

Physical and logical network isolation strategies

Network Security

Network Segmentation Strategies

Creating security boundaries through physical and logical isolation

Physical Isolation

Devices are physically separate with an air gap between them.

Implementation

Separate switches, different racks, no physical connection

Use Cases

- ✓ Web servers in one rack, databases in another
- ✓ Customer A on Switch A, Customer B on Switch B

No opportunity for mixing data

Physical Segmentation

Multiple physical infrastructure units with separate hardware.

Characteristics

- ✓ Separate switches, routers, firewalls
- ✓ Dedicated infrastructure per segment

Considerations

- + High security
- − Expensive
- − Complex to manage

VLANs

Virtual Local Area Networks—logical separation on shared hardware.

How VLANs Work

Separated logically instead of physically. VLANs cannot communicate without a Layer 3 device (router).

Benefits

- ✓ Cost-effective
- ✓ Flexible and scalable
- ✓ Easy to reconfigure

Best Practice: Use VLANs to isolate departments, guest networks, and IoT devices.

Defense in Depth: Combine multiple segmentation strategies. Use VLANs for departmental separation and physical segmentation for high-security zones.

Infrastructure Technologies

Modern Infrastructure Technologies

SDN, virtualization, containerization, and specialized systems

Software Defined Networking (SDN)

Separates networking functions into logical planes of operation.

Data Plane (Infrastructure)

Processes frames and packets—forwarding, trunking, encrypting, NAT.

Control Plane

Manages data plane actions—routing tables, session tables, dynamic updates.

Management Plane (Application)

Configures and manages the device—SSH, browser, API access.

Virtualization vs Containerization

Virtualization (VMs)

Run many OS instances on same hardware. Each app has its own OS—adds overhead and complexity.

Containerization (Docker)

Containers include code and dependencies. Isolated processes in sandboxes—lightweight, uses host kernel.

IoT & Embedded Systems

IoT Devices

Sensors, smart devices, wearables, facility automation. Weak defaults are a major security concern.

SCADA / ICS

Industrial Control Systems for power, refining, manufacturing. Requires extensive segmentation—no outside access.

RTOS

Real-Time Operating Systems with deterministic processing—industrial equipment, automobiles, medical systems.

High Availability

Redundancy doesn't always mean always available. HA means always on, always available.

HA Components

- ✓ Active/Active configurations
- ✓ Multiple redundant systems

$ **Trade-off:** Higher availability = higher costs

Design Factors

Infrastructure Design Considerations

Key factors when designing and deploying infrastructure

Availability

System uptime for data access and transactions. Balance availability with security.

Resilience

Ability to maintain availability and recover. Measured as MTTR (Mean Time to Repair).

Cost

Initial installation, ongoing maintenance, replacement costs. Consider tax implications (OpEx vs CapEx).

Recovery

How easily can you recover from failures? Malware infection recovery time varies by platform.

Responsiveness

Speed is critical for interactive applications. All components contribute—there's always a weakest link.

Scalability

Ability to increase/decrease capacity quickly (elasticity). Include security monitoring in scaling.

Deployment

Applications have many moving parts. Orchestration and automation simplify deployment.

Risk Transfer

Cybersecurity insurance covers attacks, downtime, and legal issues. Popular with rise in ransomware.

Patching

Regular updates are critical. Some systems (embedded) can't be patched—need additional controls.

Power

Foundational element requiring engineering. Consider UPS and generators for outages.

Compute

More options available in the cloud. Use multiple CPUs across clouds for enhanced scalability with added complexity.

Centralized vs Decentralized: Most organizations are physically decentralized. Centralize security management for correlated alerts, consolidated logs, and comprehensive patching.

CHAPTER 03

Infrastructure Security

Securing networks, devices,
and communication channels

Security Fundamentals

Secure Infrastructure Design

Fundamental principles for designing secure infrastructure

Device Placement

Every network is different, but there are common patterns for secure device placement.

Firewall Placement

Separate trusted from untrusted networks. Provide additional security checks at network boundaries.

Additional Security Technologies

- ✓ Honeypots for intrusion detection
- ✓ Jump servers for secure access
- ✓ Load balancers for distribution
- ✓ Sensors for monitoring

Attack Surface

How many ways into your network? Everything can be a vulnerability.

Attack Vectors

- ⚠ Application code vulnerabilities
- ⚠ Open ports on servers
- ⚠ Authentication processes
- ⚠ Human error

Minimization Strategies

- ✓ Audit and secure code
- ✓ Block unnecessary ports
- ✓ Monitor network traffic

Security Zones

Zone-based security is more flexible and secure than IP address ranges.

Common Zone Types

Trusted	Untrusted
Internal	External
Inside	Internet
Servers	Databases

Simplified Policies

Define traffic flow between zones: Trusted → Untrusted, Untrusted → Screened, etc.

Secure Connectivity

Physical Layer

Secure network cabling and protect physical drops from tampering.

Application Layer

Application-level encryption (HTTPS, TLS) protects data in transit.

Network Layer

Network-level encryption through IPsec tunnels and VPN connections.

Threat Detection

Intrusion Detection & Prevention Systems

IDS/IPS technologies and monitoring approaches

Failure Modes

When security systems fail, how should they behave?

Fail-Open

When a system fails, data continues to flow. Prioritizes availability over security.

Fail-Closed

When a system fails, data does not flow. Prioritizes security over availability.

IDS vs IPS

Intrusion Detection System (IDS)

Monitors network traffic for suspicious activity and generates alerts.

- ✓ Passive monitoring only
- ✓ Alarm or alert when intrusion detected
- ✓ Cannot block traffic in real-time

Intrusion Prevention System (IPS)

Actively monitors and can block malicious traffic in real-time.

- ✓ Active monitoring (inline)
- ✓ Can block traffic in real-time
- ✓ Stops intrusions before they enter

Monitoring Types

Active Monitoring

System is connected inline with the network traffic.

- ✓ Data passes through the device
- ✓ Can block traffic in real-time
- ✓ IPS commonly uses active monitoring

Passive Monitoring

A copy of network traffic is examined using taps or port mirrors.

- ✓ Original traffic flows normally
- ✓ Cannot block traffic in real-time
- ✓ IDS commonly uses passive monitoring

Intrusion Types

- OS exploits
- Application vulnerabilities
- Buffer overflows
- Cross-site scripting (XSS)

Security Infrastructure

Network Security Appliances

Jump servers, proxies, and load balancers

Jump Server

A highly-secured device that provides access to secure network zones.

Purpose

Access mechanism to protected networks. All administrative access flows through this controlled point.

Characteristics

- ✓ Hardened and monitored
- ✓ SSH/Tunnel/VPN access
- ✓ RDP/SSH from jump server

Critical: Jump server compromise is a significant breach

Proxy Servers

Sits between users and external networks, forwarding requests on behalf of users.

Forward Proxy

Internal proxy protecting user access to the Internet. Used for caching, access control, URL filtering.

Reverse Proxy

Handles inbound traffic from Internet to internal services. Provides load balancing and SSL termination.

Open Proxy

Third-party, uncontrolled proxy. Significant security concern—often used to circumvent controls.

Load Balancers

Distributes load across multiple servers, invisible to end-users.

Active/Active

All servers handle traffic simultaneously. Provides scalability and fault tolerance.

Active/Passive

Some servers active, others on standby. Passive servers take over if active fails.

Advanced Features

- ✓ TCP/SSL offload
- ✓ Caching
- ✓ QoS prioritization
- ✓ Content switching

Sensors and Collectors: Aggregate information from network devices (IPS logs, firewall logs, authentication logs). SIEMs correlate diverse sensor data for comprehensive security monitoring.

Access Control

Port Security & Firewall Technologies

Network access control and firewall types

Port Security (802.1X)

IEEE 802.1X provides port-based Network Access Control—you don't get network access until you authenticate.

EAP Framework

Extensible Authentication Protocol—many authentication methods based on RFC standards. Manufacturers can build custom EAP methods.

802.1X Components

- **Supplicant:** The client device
- **Authenticator:** Device providing access (switch)
- **Auth Server:** Validates credentials (RADIUS, LDAP)

Next-Gen Firewall (NGFW)

Operates at OSI Application Layer (Layer 7) with deep packet inspection.

Capabilities

- ✓ Application-aware filtering
- ✓ Identify applications (SQL, Twitter, YouTube)
- ✓ Apply app-specific vulnerability signatures
- ✓ Content filtering and URL filtering

Also Known As

Application layer gateway, stateful multilayer inspection, deep packet inspection

Firewall Types

Network-Based Firewalls

Filter traffic by port (Layer 4) or application (Layer 7). Often Layer 3 devices with NAT functionality at network ingress/egress.

UTM / All-in-One

Unified Threat Management combines firewall, IDS/IPS, VPN, URL filtering, malware inspection, spam filter in one appliance.

Web Application Firewall (WAF)

Not like a normal firewall—applies rules to HTTP/HTTPS conversations.

How It Works

Allows or denies based on expected input. Unexpected input is a common exploit method.

Protects Against

- SQL injection attacks
- Cross-site scripting (XSS)
- Application-layer attacks

PCI DSS: WAF is a major focus of Payment Card Industry compliance

Secure Communication Technologies

VPNs, SD-WAN, and SASE solutions

VPN Technologies

Virtual Private Networks—encrypted data traversing public networks.

SSL/TLS VPN

Uses common SSL/TLS protocol (TCP/443)—almost no firewall issues.

- ✓ No heavy VPN clients needed
- ✓ Usually for remote access
- ✓ User authentication required

Site-to-Site IPsec VPN

Always-on (or almost always) connection between sites.

- ✓ Firewalls often act as VPN concentrators
- ✓ Transparent to users
- ✓ Encrypts all inter-site traffic

SD-WAN

Software Defined Networking in a Wide Area Network—a WAN built for the cloud.

Why SD-WAN?

Cloud has changed everything. Applications communicate directly to the cloud—no need to hop through a central point.

Capabilities

- ✓ Manage network connectivity to cloud
- ✓ Dynamic path selection
- ✓ Application-aware routing

⚠ **Note:** SD-WAN does not adequately address security concerns by itself

SASE (Secure Access Service Edge)

A "next generation" VPN and complete network/security solution delivered from the cloud.

Network as a Service

- ✓ SD-WAN capabilities
- ✓ VPN connectivity
- ✓ QoS and routing
- ✓ SaaS acceleration

Security as a Service

- ✓ Zero Trust Network Access
- ✓ Cloud secure web gateway
- ✓ CASB (Cloud Access Security Broker)
- ✓ Firewall as a Service
- ✓ DLP and DNS security
- ✓ Threat prevention

User Experience

- ✓ SASE client on all devices
- ✓ Automatic connections
- ✓ Consistent process across locations

CHAPTER 04

Data Protection & Classification

Understanding, classifying,
and protecting organizational data

Data Governance

Data Types & Classification Framework

Understanding data types and applying appropriate security controls

Data Types

Regulated Data
Managed by third-parties, government laws and statutes. Subject to compliance requirements.

Trade Secrets
Organization's secret formulas, unique to the organization. Critical competitive advantage.

Intellectual Property
May be publicly visible but protected by copyright and trademark restrictions.

Legal Information
Court records, attorney information, PII. Often stored across many systems.

Financial Information
Internal financials, customer financials, payment records, credit card data.

Data Readability

Human-Readable
Humans can understand the data—very clear and obvious (plain text, documents).

Non-Human Readable
Not easily understood by humans—encoded data, barcodes, images.

Hybrid Formats
CSV, XML, JSON—structured formats readable by both humans and machines.

Data Classification Levels

Critical
Data should always be available. Highest protection required.

Confidential / Restricted
Very sensitive data. Must be approved to view. May require NDA.

Sensitive
Intellectual property, PII, PHI. Restricted access with controls.

Private / Internal
Internal use only. Not for public distribution.

Public / Unclassified
No restrictions on viewing the data. Can be freely shared.

Special Categories

- **PII:** Personally Identifiable Information
- **PHI:** Protected Health Information
- **Proprietary:** Organization's unique data

Data Security

Data States & Protection Strategies

Protecting data at rest, in transit, and in use

Three States of Data

Data at Rest

Data on storage devices (hard drives, SSD, flash).

- Whole disk encryption
- Database encryption
- File/folder encryption
- Access control lists

Data in Transit

Data transmitted over the network (in-motion).

- TLS encryption
- IPsec VPNs
- Network firewalls
- IPS protection

Data in Use

Data actively processing in memory (RAM, CPU cache).

- Almost always decrypted in memory
- Attackers target RAM (Target breach 2013)

Data Sovereignty & Geolocation

Data Sovereignty

Data residing in a country is subject to that country's laws. GDPR requires EU citizen data be stored in the EU.

Geolocation

Determine user location via GPS, 802.11 wireless, or IP address for access control.

Geofencing

Automatically allow or restrict access based on location. Example: Don't allow app to run unless near the office.

Data Protection Techniques

- **Encryption:** Encode to unreadable ciphertext
- **Hashing:** One-way message digest
- **Obfuscation:** Make code difficult to understand
- **Masking:** Hide portions of sensitive data
- **Tokenization:** Replace with non-sensitive placeholder
- **Segmentation:** Separate data into different locations

CHAPTER 05

Resiliency & Business Continuity

Building resilient systems and planning for disaster recovery

Resiliency Planning

High Availability & Site Resiliency

Building systems that withstand and recover from failures

High Availability

Redundancy doesn't always mean always available. HA means always on, always available.

HA Components

- ✓ Multiple components working together
- ✓ Active/Active configurations
- ✓ Automatic failover
- ✓ Scalability advantages

$ **Trade-off:** Higher availability = higher costs

Site Resiliency Options

Hot Site

Exact replica with duplicate everything. Stocked with hardware, constantly updated. You buy two of everything. **Most expensive.**

Warm Site

Somewhere between cold and hot. Big room with rack space—you bring hardware, software, and data. **Moderate cost.**

Cold Site

Empty building with no hardware, no data, no people. You bring everything. **Least expensive.**

Server Clustering

Combine two or more servers that appear and operate as a single large server.

Benefits

- ✓ Easily increase capacity
- ✓ Add more servers to cluster
- ✓ Users see only one device

Configuration

Usually configured in the operating system. All devices commonly use the same OS.

Additional Strategies

Geographic Dispersion

Sites should be physically distant from primary location to avoid regional disasters (hurricanes, floods).

Platform Diversity

Use different OSes to spread risk. Windows vulnerabilities don't affect Linux or macOS.

Multi-Cloud

Data geographically and cloud-service dispersed. A breach with one provider doesn't affect others.

Capacity Planning & Recovery Testing

Matching resources to demand and validating recovery procedures

Capacity Planning

Match supply to demand across three dimensions.

Technology

Pick scalable technologies. Web services can distribute load. Cloud provides on-demand resources.

People

Some services need human intervention (call centers). Balance staffing—too few = poor service, too many = wasted cost.

Infrastructure

Physical devices require purchase and installation. Cloud devices easier to deploy for unexpected changes.

Recovery Testing

Test before an actual event occurs.

Simulation

Test with simulated events—phishing attacks, password requests, data breaches. Use well-defined rules of engagement.

Tabletop Exercises

Get key players together to talk through a simulated disaster without physical drills.

Failover & Parallel Processing

Failover

Create redundant infrastructure. If one component stops working, fail over to the operational unit automatically.

Parallel Processing

Split processes across multiple CPUs. Improves performance and recovery—quickly identify and remove faulty systems.

Backup Strategies

Onsite vs Offsite

Onsite: immediate availability, no Internet needed. Offsite: available after disaster, restore from anywhere. Use both for more options.

Snapshots & Replication

Snapshots: instant backups of entire systems. Replication: ongoing, almost real-time backup keeping data synchronized.

Recovery Testing

Not enough to perform backups—you must be able to restore. Test restored applications and data. Perform periodic audits.

Infrastructure Foundation

Power Resiliency & Infrastructure Protection

Ensuring continuous power and protecting data integrity

Power Resiliency

Power is the foundation of technology. We can't control power availability, but we can mitigate issues.

UPS (Uninterruptible Power Supply)

Short-term backup power for blackouts, brownouts, surges.

- Offline/Standby UPS
- Line-interactive UPS
- On-line/Double-conversion UPS

Generators

Long-term power backup requiring fuel storage. Can power entire buildings. Takes minutes to start—use UPS during startup.

Journaling

Prevent data corruption when power fails during writes.

The Problem

Power outage while writing data = corrupted data. Recovery is complicated.

The Solution

- Write journal entry before data
- Write data to storage
- Update journal after write

Continuity of Operations (COOP)

Not everything goes according to plan. Disasters cause disruptions—we need alternatives.

The Challenge

We rely on computer systems—technology is pervasive. When systems fail, business stops.

Alternative Processes

- Manual transactions
- Paper receipts
- Phone calls for approvals

Requirements

- Document alternatives before problems occur
- Test procedures regularly
- Train staff on manual processes

Key Insight: COOP planning ensures business can continue even when technology fails. The goal is resilience, not just recovery.

COMPREHENSIVE SECURITY

Building Secure, Resilient Infrastructure

Modern infrastructure security requires a **holistic approach** combining cloud-native architectures, robust network segmentation, comprehensive data protection, and resilient systems.

Cloud-Native

Scalable, flexible architectures

Defense in Depth

Layered security controls

Always Available

Resilient by design

From cloud deployments to disaster recovery

Every component plays a vital role in protecting organizational assets. Security professionals must balance availability, cost, and protection while planning for the unexpected.

Based on Professor Messer's CompTIA Security+ SY0-701 Course Notes