SECURITY+ STUDY GUIDE TABLE OF CONTENTS

Chapter 1: Security Fundamentals

Module A: Security concepts

CIA Triad

The parts of CIA are confidentiality, integrity, and availability.

Risks, Threats, and Vulnerabilities

Risk – The chance of harm coming to an asset
Threat – Anything that can cause harm to an asset
Vulnerability - Any weakness an asset has against potential threats

Security Standards Organizations

CIS – Center for Internet security
IEEE – Institute of Electrical and Electronics Engineers
IETF – Internet Engineering Task Force
ISO – International Organization for Standardization
ISOC – Internet Society
ITU – International Telecommunication Union
NIST – National Institute of Standards and Technology
NSA – National Security Agency
W3C – World Wide Web Consortium

Security Controls

Administrative – Organizational policies and training
Technical – Technological solutions
Operational – Day to day employee activities
Physical – Physical safety and security devices
Preventive - Proactive controls which act to prevent loss
Detective - Monitoring controls that detect and/or record
Corrective - Follow-up controls used to minimize the harm caused and prevent recurrence
Deterrent - Visible controls designed to discourage attack or intrusion

Confidentiality Controls

Least privilege - Users are given only the permissions they need to perform their actual duties
Need to know - Data access is restricted to those who need it
Separation of duties - Tasks broken into components performed by different people
Access controls - Access restricted to authorized users
Encryption - Data made unreadable without proper key
Steganography - Secret messages concealed inside of ordinary ones

Integrity Controls

Hashing - Digital fingerprints used to detect file alteration
Digital signatures - Hashing and encryption used to prove a file's origin
Backups - Spare copies of data kept in safe storage
Version control - Formal preservation and tracking of multiple file versions

Availability Controls

Redundancy – Multiple or backup systems designed for immediate or quick recovery

Fault tolerance – Systems that continue functioning after components fail
Patch management – Application of software updates with minimal service disruption

Defense in Depth
Comprehensive security controls that exist on all levels of an organization. Usually defines multiple layers in which an organization needs to be secured.
e.g. Data
Application
Host
Internal Network
Perimeter Network
Physical facility
Users and organization

Events and Incidents
True positive – Problem occurred and was detected
True negative – No problem, and no alert
False positive – Alert triggered by benign event
False negative – Real problem went undetected

Module B: Risk management

Risk Assessment
1. Identify assets at risk
2. Conduct threat assessment for each asset
3. Analyze business impact for each threat
4. Determine likelihood of threat doing damage
5. Prioritize risks by weighing likelihood vs. potential impact
6. Create risk mitigation strategy

Identifying Assets
Information and data
Computing hardware and software
Business inventory
Building or other physical facilities
Cash or other financial assets
Personnel
Branding and business reputation
Business relationships, including partner assets in organization's keeping

Threat Assessments
Environmental accident
Natural disaster
Equipment failure
Supply chain failure
Human error
Malicious outsider
Malicious insider

Impact Analysis
Replacement cost
Revenue or opportunity loss
Production loss
Human costs
Reputation
Legal consequences

Privacy Impact Assessment
Ensure compliance with external regulations and internal policies on privacy
Analyze potential privacy risks and impacts
Evaluate security controls to minimize risks

Threat Probability
MTTF – Mean time to failure
MTTR – Mean time to repair
MTBF – Mean time between failures
MTBSI – Mean time between service incidents

Quantitative Risk Assessment Values
SLE – Single loss expectancy is cost of any single loss
ARO – Annual rate of occurrence is expected number of times given loss may occur per year
ALE – Annual loss expectancy is expected cost per year from threat (SLE × ARO).

Risk Assessment
Quantitative
    Single loss expectancy
    Annual rate of occurrence
Qualitative

Risk Management
Avoidance
Transference
Mitigation
Deterrence
Acceptance
Residual risk

Mitigation Techniques
Technology controls
Policies and procedures
Routine audits
Incident management
Change management

Automated Security Tools

Device or system configuration tools
Continuous monitoring and alert systems
Configuration validation tools
Vulnerability scanners
Remediation tools
Patch management software
Automated trouble shooters
Application testers

Module C: Vulnerability assessment

Vulnerability Assessments,
Baseline review
Determining attack surface
Reviewing code
Reviewing architecture
Reviewing design

Vulnerability Scans
Intrusive vs. non-intrusive
Credentialed vs. non-credentialed
Goals:
- Missing or misconfigured security controls
- Open ports
- Weak passwords or encryption
- Misconfigured security controls
- Unsecured data
- Compromised systems
- Exploitable vulnerabilities
- Unpatched systems

Penetration tests
Black box – no attacker knowledge of the system
White box – Full attacker knowledge of system
Gray box - Partial attacker knowledge systems

Network Reconnaissance
Passive reconnaissance
Active reconnaissance
Vulnerability analysis

Penetrating Networks
Escalate privileges:
- Gathering user names or password hashes
- Gaining additional privileges
- Finding exploitable information
- Installing malware

Establishing persistence
- Installing backdoors
- Creating alternate accounts
- Compromising authentication systems

Pivot:
- Perform reconnaissance on internal networks
- Create tunnels to bypass firewalls and other boundaries
- Exploit trust relationships

Chapter 2: Understanding attacks

Module A: Understanding Attackers

Types of Hackers

Black hat – criminal hackers
White hat – Security experts who hack for legal purposes
Grey hat – Hackers that are neither white nor black hats

Attacker Qualities

1. Intent: Some hackers are after specific resources or information, others will take whatever they can find, and others just want to deny service or destroy information.
2. Sophistication: Some attackers are relatively inexperienced, others use much more subtle methods.
3. Resources: Some attackers are groups working to a common cause, while some lone attackers have access to powerful resources.
4. Location: Some attacks require physical proximity, while others can be conducted from anywhere in the world.
5. Target information: Some attackers might know little about your organization, while others might have critical information about your assets.

Attacker Types

Script Kiddies
Hacktivists
Organized criminals
Competitors
Insiders
Nation states
Advanced persistent threats (APTs)

Module B: Social engineering

Social Engineering Principles

Authority
Intimidation
Consensus/Social proof
Scarcity

Urgency
Familiarity
Trust

Phishing
Spear phishing – targets specific users
Whaling – Singles out high-profile targets
Vishing – Applies phishing techniques to voice calls

Physical Intrusion
Shoulder surfing – eavesdropping on sensitive reading or conversations
Tailgating – tagging behind someone into a secure area
Dumpster diving – stealing sensitive data from the trash

Social Engineering Defenses
User training – information sharing guidelines, don't share passwords, ignore suspect requests
Policies – Least privilege/need to know, logoff, data disposal
Technical controls – mantraps, spam filters, network controls

Module C: Malware

Malware Vectors
Virus – attaches malicious code to another file
Worm – replicates itself by exploiting system vulnerabilities
Trojan horse – masquerades as a useful program
Logic bomb – lies dormant until a specific condition is met
Watering hole – injection on a trusted site or service used by actual targets

Malware payloads
Backdoor – hidden way into a system or application
Botnet – large number of controlled systems
Ransomware – attempts to extort money to undo damage
Spyware – secretly records user activity
Adware – Presents ads to the user

Hidden Malware
Polymorphic malware – changes signatures
Stealth malware – hides from antimalware programs
Rootkit – compromises boot or OS functions to avoid detection

Malware Defenses
Legitimate sourcing – for all hardware and software
Antimalware – antivirus and specialized scanners
System permissions – restricting user installation of applications
Security updates – browsers and addons as well as OS
Network security – Firewalls, IDS, spam filters
Policies and training – Unknown sites, phishing links, removable media

Module D: Network attacks

Network Probes
Xmas attack – too many flags set
Fuzzing – random data input
Banner grabbing – normal request used to gather return data

Spoofing
Can mimic or pretend to be an IP address, MAC address, Email address, etc.

Redirection
ARP poisoning – performed by inside attackers
DNS poisoning – More difficult but works on larger networks
Pharming – similar to phishing but with compromised DNS
VLAN hopping – bypasses VLAN segmentation

Denial of Service Variants
Ping of death – oversized packets or malformed packets
Syn Flood
Permanent DOS
Unintentional DOS

Password Cracking
Brute force – try all combinations in sequence
Dictionary attack – try entries from a list
Birthday attack – finds hash collisions
Rainbow table – uses pre-compiled hash list
Pass the hash – Uses hash stolen from a single compromised system

Man in the Middle Attacks
Replay attack
Session replay
Session hijacking
Downgrade

Wireless Attacks
Wardriving – searching for open hotspots
Rogue AP – unauthorized hotspot
Bluejacking – radio interference
Blue snarfing – theft of information
Evil twin – rogue AP used for MitM

Module E: Application attacks

Application Exploits
Privilege escalation
Directory traversal – reaching additional folders on target computer
Arbitrary code execution – running malicious code on target computer
Resource exhaustion

Input Manipulation
Header manipulation – changing values in headers used by communication protocol
Memory manipulation – sending input that affects variables and other values
Injection – sending specifically formatted input

Memory Vulnerabilities
Buffer overflow – sending too much information to the application
Integer overflow – setting integer variable to value that exceeds maximum size to store it
Pointer dereference – directly retrieve value that a pointer points to
Memory leak – cause application to allocate memory but never release it

SQL Injection
Unfiltered escape characters – special characters used by SQL
Improper input types – placing wrong data types into fields
Blind injection – gathering information through page output changes
Signature evasion – hiding signs of attack from IDS

Other Injection Techniques
NoSQL injection – targets non-relational databases
LDAP injection – targets network directory services
XML injection – targets XML databases
Command injection – targets remote command shells
DLL injection – targets running processes

Cross-site scripting
Stored/Persistent – script uploaded as permanent content
Reflected/Non-persistent – script temporarily placed in error field or search response
DOM-based – script run entirely in the client browser

Chapter 3: Cryptography

Module A: Cryptography concepts

Classical ciphers
Substitution ciphers – vulnerable to frequency based attacks
Transportation ciphers – vulnerable to partial solution attacks
Steganography – hides existence of secret message, digital variants

Digital Encryption
Uses – transport, storage, memory, cryptographic obfuscation
Methods – symmetric, asymmetric, cryptographic hashing
XOR functions

Key Strength
Key length – n = 2 to the n power combinations

Key length vs effective strength – advancing computing power requires stronger encryption over time, varies by type of encryption key security

Symmetric Algorithms
DES – obsolete, 56-bit key
3DES – three 56-bit keys, but effectively 80-bit
AES – NSA standard, 128 to 256-bit key
Blowfish – first strong public domain cipher, variable key size
Twofish – improved blowfish, AES competitor
Serpent – AES finalist, powerful but slow
RC4 – stream cipher, old but common
CAST – popular family, includes CAST-128 and CAST-256

Key Life Cycles
Key duration – static and ephemeral
Key generation
Key exchange – in band and out of band
Perfect forward secrecy

Asymmetric Encryption
Public and private keys – one key encrypts, opposite decrypts
Uses – key exchange, authentication and non-repudiation
Drawbacks – longer keys, slower performance

Asymmetric Algorithms
RSA – Key generated from two prime numbers, up to 4096-bit key, used for digital signatures
DSA – Adopted as NIST standard, uses one-way problem called discrete logarithm
ECC – based on exotic mathematics, higher performance and shorter keys than RSA
DH – first openly published public-key system, many variants
Quantum cryptography – quantum key distribution

Cryptographic Hashes
One-way functions – easy to verify, hard/impossible to recover
Data integrity – creates fingerprint of data
Data identification – hash table
Key generation – pseudorandom string
Password storage – user password hashed and compared to stored has, salting for additional security

Hash Algorithms
MD5 – 128-bit, obsolete
SHA-1 – 160-bits, being phased out
SHA-2 – SHA 256 and SHA 512
SHA-3
Password hashes – NTLM, bcrypt, PBKDF2

Module B: Public key infrastructure

Digital Certificates
Also known as public key certificates
Contents – public key, owner identity, digital signatures attesting to authenticity
Not to be confused with digital signatures – certificates proves identity of a user or a system

Certificate Encodings
DER
PEM
CER
P12
PFX
P7B

Certificate Authorities
CA signs and revokes certificates
Root certificates – out of band distribution
Certificate generation – limited purpose, multi domain, wildcard, extended validation

Certificate Generation
1. Applicant generates key pair, keeps private key
2. Applicant presents public key and CSR to CA
3. CA verifies applicant identity according to CPS
4. CA signs and disseminates certificate

Certificate Revocation
Certificate revocation list – list of all revoked certificates
Online Certificate Status Protocol – shows status of a particular certificate

Key Pinning
Stating pinning – browser's publisher pins keys of high traffic sites
Dynamic pinning – uses IETF standard HTTP public key pinning, pins key to check against every subsequent contact

Key Archival and Recovery
Private keys – backed up along with system
Compromise – back up key stores and corresponding certificates separately from other data
Dedicated hardware storage modules – contain valuable keys, may include secure backup functions

Chapter 4: Network fundamentals

Module A: Network components

Network Models
OSI Model – Important educational and theoretical tool
TCP/IP – Designed by US DOD, maintained by IETF, Dominant standard of internet

Data Link Layer
Combined with physical layer in TCP/IP
Contains technologies that can handle addresses, traffic direction and security (ex: MAC addresses, Switches, VLANs)

MAC address
A.K.A. physical addresses
Represent physical devices
Used for address filtering

Switches
Direct local traffic
Tracks addresses with a MAC table
Are vulnerable to MAC spoofing

VLANs
Separate broadcast domains on same physical switch
Collection of methods rather than single standard
    Port based, dynamic, and protocol based

The Network Layer
Extends beyond broadcast domain
Allows for larger networks by reducing congestion and preventing switching loops
Uses more intelligent protocols for routing and logical addressing

Routers
Joins two broadcast domains
Separates subnets
Can communicate with other routers
Is aware of surrounding network structure

ICMP
Used for control and error messages
Needed for core network functions
Includes several message types
    Echo request and reply (ping)
    Host unreachable
    Source quench
    Redirect
    Time exceeded

Wi-Fi Signals
2.4 GHz – most common with relatively long range but a small number of channels

5 GHz – more expensive with shorter range but with more channels
60 GHz – Very high data rate but can't pass through walls, requires line of sight

Antenna types
Omnidirectional and directional

Industrial Control Systems
SCADA – Large scale distribution systems, information gathering with limited control
DCS – Process control systems, direct control with limited information gathering
*Neither are designed for security

Module B: Network addressing

IPv4 Addresses
Comprised of Network ID and Host ID
Have Classful and Classless addresses
Classful – Class A/B/C/D/E

Special IPv4 Addresses
Broadcast – 255.255.255.255
Loopback – 127.0.0.0
Private Addresses – 10.0.0.0 /8, 172.16.0.0 /12, 192.168.0.0 /17
APIPA – 169.254.0.0 /16

IPv6
Massive address range (much higher than IPv4)
Easier network configuration
Increased efficiency and enhanced security
Compatibility issues

IPv6 Address Types
Loopback - ::1 /128
Link-local – fe80:: /10 which is equivalent to APIPA
Site-local – similar to IPv4 private
Global - 2000:: /3
Multicast – will begin with ff

DHCP
Server contains pool of available network addresses called scope
Addresses assigned dynamically or by reservation
DHCP server options – default gateway, DNS server addresses, Time server or time zone
*If DHCP server is not on client's local segment, routers can be DHCP relay agents

Module C: Network ports and applications

Transport Protocols
End to end communications
Uses ports or sockets for host-level multiplexing
The two most common protocols are TCP and UDP

TCP
Connection oriented
Reliable
Error correction
Flow control
Sequencing

UDP
Connectionless
Unreliable
Fast
Used for time-sensitive data, small data exchanges

Port Ranges
System ports – assigned to major TCP/IP standards (1-1023)
User ports – assigned to any application which registers for one (1024-49151)
Private ports – used by private applications or temporary uses (49152-65535)

Application Protocols
Restrict plaintext protocols
Combine insecure protocols with others that provide security
Use lower layers of security such as VPN, Wi-FI encryption
Network segmentation

Remote Access Protocols
Telnet – insecure, text-based terminal connections on TCP port 23
Secure Shell – Secure telnet replacement, uses TCP port 22
Remote Desktop Protocol – Windows proprietary remote access protocol, TCP port 3389
Simple Network Management Protocol – v1 and v2 are obsolete, v3 is secure used on UDP ports 161 and 162

Resource Sharing Protocols
LDAP – Directory service on LAN, uses TCP 389
NetBIOS – Session-layer API used by multiple applications
SMB – Allows Windows folder sharing on LAN
FTP – File access on LAN or internet, replaced by FTPS and SFTP, TCP port 20 and 21
TFTP – simplified FTP protocol, UDP port 69
NTP – Used to synchronize clocks between networked devices

Hypertext Transfer Protocol
Insecure plaintext protocol
Uses TCP port 80
HTTPS – Encrypted using SSL or TLS, uses TCP port 443

Email Protocols
SMTP – Only used to send email between servers or from clients to servers
POP – Used by clients to retrieve mail from servers, uses TCP port 110
IMAP – Used by clients to retrieve mail from servers, stores messages permanently on the server
MAPI – Propriety Microsoft Exchange protocol for sending and receiving

TCP/IP Tools
Ipconfig – Windows, displays, or refreshes IP settings
Ifconfig – Unix, displays or configures IP settings
Netstat – displays variety of network information
Nbtstat – Windows, displays diagnostic information for NetBIOS over TCP/IP
Arp – displays IPv4 ARP cache
Nslookup – Performs DNS lookups and displays IP address
Ping – tests reachability of host
Traceroute/tracert – displays hop-by-hop path to given host
Pathping – Windows, pings every hop along route to determine latency

Chapter 5: Securing networks

Module A: Network security components

Network ACLs
Packet filtering – MAC address, IP address, port number, protocol
Is either an implicit deny or allow

Switch Security Features
Port security – Allows or denies traffic based on source MAC address
MAC filtering – Useful, but easier to circumvent
Loop protection – Helps increase network availability by preventing accidental loops

Network Access Control
Guest network – Separate access point with only internet access
Posture assessment – Ensures client meets security rules, acts as a quarantine network
Agents – can be persistent or non-persistent

Intrusion Detection and Prevention

Signature-based – looks for telltale signs of known attacks
Stateful protocol analysis – looks for abnormal protocol use
Anomaly-based/Heuristic – looks for unusual behavior patterns

Honeypots and Honeynets
Decoy system – has weak or flawed security and is isolated from the rest of the network
Honeynet – network of honeypots
Used for testing and criminal investigations

Application Layer Security
Application layer firewall – web application firewall
Content filter – web filter and spam filter

Load Balancing Techniques
SSL acceleration
Data compression
Health checking
TCP offloading and TCP buffering

Unified Threat Management
Firewall
IDS
IPS
DMZ interface
NAT or proxy server
Network access control
VPN endpoint

Module B: Transport encryption

SSL and TLS
Upper layer protocols – SSL 1.0-3.0 and TLS 1.0-1.2
Certificate based – Asymmetric key exchange, symmetric bulk encryption

Secure Shell
Designed to replace Telnet and rlogin
Uses public key cryptography – X.509 is only one option available

Secure Email
Secures message text, not just transfer
S/MIME - Uses X.509 certificates, Only common in high-security enterprise environments
PGP - Uses OpenPGP certificates on web of trust model, Commercial and free support

Secure VoIP
Secured by using TLS and RTP with secure RTP

Wireless Encryption
Layer 2 encryption
WEP - Extremely weak due to serious flaws in RC4 IV.
WPA - Based on draft 802.11i, TKIP is a stronger but still flawed RC4 cipher
WPA2 - Based on draft 802.11i, AES mode is strongest Wi-Fi encryption

WPA Authentication
WPA-Personal - Uses pre-shared password hashed with SSID to create key, Convenient but only one key for whole hotspot
WPA-Enterprise - 802.1X using authentication server, EAP-TLS or PEAP authentication, allows individual credentials
WPS - Convenient, but insecure and should be disabled

VPN Solutions
GRE – tunneling but no security
PPTP – PPP packets over GRE, not very secure
L2TP/IPSEC – can be very secure and is natively supported by most OS
SSL/TLS – secure, but supported mostly via third-party
SSH – typically used to tunnel single applications

IPsec
IKE – Negotiates secure connections
Authentication header – provides data integrity and source
Encapsulating Security Payload – encrypts packet payload itself
AH and ESP can be used separately or together

Module C: Hardening networks

Segmenting Networks
Collision domains – No privacy without encryption, is mostly found in Wi-Fi hotspots
Broadcast domains – limited traffic control, separated by routers
VPNs
Airgaps – no connection to internal or external network

Hardening Network Hosts
Keep list of hosts, owners, and purposes
Perform updates
Disable unnecessary services
Configure firewalls
Policies for temporary network hosts
Onboarding and offboarding procedures

Monitoring

Securing Network Infrastructure
Harden devices like hosts
Use up to date firmware
Allocate network addresses carefully
Enable router and switch security
Deploy network security systems

Securing Perimeter Networks
Open only necessary ports
Minimize value of perimeter and bastion hosts
Harden specialized security appliances

Securing Wireless Access Points
Harden like other network appliances
Use strong encryption
Disable WPS
Use 802.1X
Choose a unique SSID
Use guest networks for untrusted clients
Place WAP securely

Module D: Monitoring and detection

Monitoring Tools
Network analyzer – captures and analyses network traffic
Interface monitor – examines specific network interface
Port mirrors – copies traffic from a port
Wireless analyzers – tests wireless congestion and reception
SNMP management software – monitoring or remote management
Syslog – centrally managed logs

Syslog
Header – unique ID including timestamp and generating device ID
Facility – type of program that generated the message
Severity level – ranges from 0 (emergency) to 7 (debug)

Placing Monitoring Tools
Some sensors built into devices
Place network taps and port mirrors on chokepoints
Feed large volumes of data through collection systems

Vulnerability Scanners

Protocol analyzer
Port scanner
Network mapper
Password cracker
Wireless scanner
Exploitation framework

Security Audits
Logs
Incident response reports
User activities
Device configurations
Installed applications

Incident Reports
Alarms
Alerts
Trends

Chapter 6: Securing hosts and data

Module A: Securing data

Classification Levels
Top Secret – Grave damage could be done to national security
Secret – Less grave, but still national security risk
Confidential – Could cause damage to national security, but is less sensitive than secret
Unclassified – all other information

Personally Identifiable Information
Can either distinguish an individual or linked to an individual (ex: name, address, bank number, biometric data)
Educational Institutions – must protect student records
PCI-DSS – policy for the payment card industry

Data Ownership Roles
Data owner
Data custodian
Data Steward
Data user
Privacy officer

States of Data
Data in transit

Data at rest
Data in use

Data Life Cycle
1. Creation/Acquisition
2. Use/Storage
3. Retention/Archival
4. Wiping/Disposal

Share Permission
Read – view file names, subfolders, and data
Change – read permissions plus adding, changing and deleting
Full control – change, plus can change NTFS permissions

Storage Encryption
Removable drive encryption
Archive file encryption
Transparent database encryption
File or full dusk encryption

Encryption Hardware
Hardware-based disk encryption
Smart card
USB encryption
Trusted platform module
Hardware security module

Windows Encryption
Encrypting file system – encrypts individual files and folders, intended for personal files
BitLocker – protects entire volumes or computers, controlled by administrator

BitLocker
Encrypts entire volumes
Can be used without TPM
Three authentication methods – Transparent operation mode, user authentication mode, USB key mode

Secure Media Destruction
Pulverizing – hydraulic or pneumatic processing
Pulping – paper recycling reduces documents to liquid slurry
Incineration – burning into unrecognizable ash

Module B: Securing hosts

Code Signing

Signature verifies only that signer claims it is safe
Private signing keys can be compromised
Code signing gives protection only if OS configured to check for signatures

Hardening Operating Systems

Secure operating systems
Account control
Access control
Unnecessary services
Directory services
Updates

Securing peripherals

External ports
External storage devices
Digital cameras
Shoulder-surfing

Security Software

Antivirus
Firewall
Anti-spyware
Pop-up blockers
HIDS
File Integrity Monitor

Removing Malware

1. Identify symptoms
2. Quarantine
3. Disable system restore
4. Repair infected system
5. Update system and schedule future scans
6. Enable System Restore and create restore point
7. Educate end user and document findings

Quarantining Systems

Isolate removable storage devices or backups
Disable all network shares, file sharing applications, or ongoing connections to other computers
Limit network connectivity

Remediating Infected Systems

Always use updated tools

Combine multiple tools
Run multiple scans
Try safe mode, restore environments, bootable rescue discs, or removal tools target to specific infection
Scan removable media

Securing Repaired Systems
Update all potentially vulnerable software
Schedule regular security scans and updates
Disable unnecessary services
Examine system and application settings

Following Up On Repairs
Discuss findings with involved users
Document findings and steps taken
Report findings to admins and management

Software Changes
Patch – typically targets a single problem
Hotfix – Very specific, niche, or high urgency
Service pack – Large compilation of patches
Upgrade – New software version
Maintenance release – smaller than a service pack

Static Environments
Embedded devices – Network appliances, printers, TVs, HVAC
Kiosks
Smart devices – Internet of Things
SCADA/ICS – Industrial environments
Mobile devices
In-vehicle computing systems – emerging field
Legacy systems – no longer receiving updates

Alternative Threat Mitigation
Security layers
Control redundancy and diversity
Network segmentation
Application firewalls
Wrappers
Firmware version control

Module C: Mobile device security

Mobile Deployment Models

COBO – Corporate owned, business only
BYOD – Bring your own device
COPE – Corporate owned, personally enabled
CYOD – Choose your own device
VDI – Virtual desktop infrastructure

Mobile Data Protection
Device location software – Find my iPhone, Android Device Manager
Remote wipe
Inventory control
Asset tracking
Full device encryption
Storage segmentation

Mobile Application Security
Application whitelisting
Key and credential management
Geotagging
Encryption
Push notifications
Transitive trust authentication

Chapter 7: Securing network services

Module A: Securing applications

Software Assurance
Ensure use of secure design – OWASP, NIST and other published standards, handles PII appropriately
Development and operations work together with stakeholders

Waterfall Development Model Steps
1. Requirements
2. Analysis
3. Design
4. Development
5. Testing
6. Maintenance

Secure DevOps Practices
Security automation
Continuous integration
Baselining
Immutable systems

Infrastructure as code

Program Life Cycle
Development
Compile
Linking
Distribution
Installation
Load time
Runtime

Securing Code Principles
Least privilege – restrict privilege of users and applications
Input validation - evaluate input before processing
Input sanitization – delete dangerous characters or add escape characters
Cryptography – protect data and applications
Data exposure – session tokens, passwords and PII protect from untrusted users
Error and exception handling – Fail-safe error handling, high detail error logging

Input validation
Improper characters
Unicode characters
Improper length
Improper values
SQL code
Browser code

XSS Prevention
1. Never insert untrusted data except in allowed locations
2. HTML escapes
3. Attribute escapes
4. JavaScript escapes
5. CSS escapes
6. URL escapes
7. Sanitizing library

Fuzzing
Application fuzzing – tests I/O functions
Protocol fuzzing – tests network protocols
File format fuzzing – tests file reading/parsing functions

Provisioning
Network provisioning – ensures network resources are available and accessible
Server provisioning – setting up server to host application or service

User provisioning – creation and maintenance of user accounts and attributes
Deprovisioning – orderly freeing up of resources

Module B: Virtual and cloud systems

Virtual Server Benefits
VMs using different OS can share host without conflict
VMs are easier to back up, restore, or move
Easier to change or upgrade hardware on hosts

Software-Defined Networking
Control plane – makes decisions about overall flow of traffic
Data plane – does work of moving individual frames and packets through network

Virtual Security Benefits
Snapshots – allows easy reversion when problems occur
Sandboxing – isolated from outside host
Security control testing
Patch compatibility
Availability/elasticity – convenient for load balancing and restoration

Cloud Service Models
Software as a service – subscription based access to applications or databases
Platform as a service – access to computing platform that can be used to host applications
Infrastructure as a service – access to computing and network resources themselves

Cloud Security
Still subject to network attacks
Using off-premises service requires secure communications
Control given to another entity
Attacks on cloud services can affect many services
Varying privacy policies

Chapter 8: Authentication

Module A: Authentication factors

The AAA Process
Security principals
Authentication – verified identification of a principal
Authorization – specifying accessible resources
Accounting – tracking user actions

Authentication
Knowledge – something you know
Possession – something you have
Inherence – something you are
Behavior – something you do
Location – somewhere you are

Digital Credentials
Digital certificate – verifiable cryptographic signature
One time password – generated by pseudorandom algorithm
Hardware token – stores OTP generator or certificate
Software token
Magnetic stripe card – not secure at all
Smart card – contains cryptographic chip, CAC, PIV or SIMs

Biometric Factors
Fingerprint scanner
Retinal Scanner
Iris Scanner
Facial recognition
Voice recognition

Module B: Authentication protocols

PPP Authentication
PAP – insecure plaintext exchange
CHAP – somewhat secure but vulnerable
MS CHAP – improved CHAP, still not very secure
EAP – message format supporting a wide variety of authentication methods

Radius
Designed for dial-in
Used for PPP and wireless networks
Client-server system – client is remote access server not user workstation
PPP protocols used for relaying credentials

Radius Authentication Process
1. NAS requests authentication
2. NAS sends access request to server
3. Server evaluates credentials, replies to NAS
4. NAS responds to client to either accept, reject or challenge

TACACS+

Advantages over RADIUS:

- TCP rather than UDP
- More complete encryption
- Fully separates all three AAA steps
- Supports non-IP protocols

Disadvantages vs. RADIUS:

- Resource intensive
- Proprietary
- Primal intended for network devices

RAS

Used by Windows Server
Server directly authenticates connection
RRAS includes routing capability
Allows Windows server to as an ISP
Not to be confused with RDP

802.1X

Used mostly for WPA Enterprise
RADIUS server using EAP
Less secure for wired networks

Kerberos

Widely used SSO system – authentication server is trusted third party
Realm – basic Kerberos network unit
Principal – node belonging to a realm
Key distribution center – Authentication server and Ticket granting server

Kerberos Authentication Steps

1. Client authenticates with AS
2. AS gives a ticket granting ticket (TGT)
3. Client presents TGT to TGS
4. TGS gives resource ticket
5. Client requests resource
6. Resource server grants access

LDAP

Simplified version of X.500
Centralized access to database with network information
Queries used in scripts or sent as URLs
Active directory uses LDAP and Kerberos
Intended for trusted networks
Secure LDAP is more secure, but still not considered safe on the internet

SAML
XML based SSO (Google and Salesforce)
Principal contacts service provider first
Allows many authentication mechanisms

Chapter 9: Access control

Module A: Access control principles

Access Control Models
DAC – object owner controls access, common in file systems
MAC – administrators assign security labels and is common for military and high security environments
R(Rule)BAC – administrators define access rules, used by routers and firewalls
R(Role)BAC – administrators define permissions for roles which users belong to
ABAC – administrators define attributes for resources, users, and environments

NTFS File Permissions
Principals – owner and any number of groups
SID – security identifier, identifies a principal
ACE – access control entry, permissions for a SID
DACL – contains all ACEs applying to one principal

Role Based Access Control
Elements of a MAC and DAC
No strict ownership content
Permissions assigned centrally
Roles are similar to groups
Permissions typically additive

Rule Based Access Control
Rules set by administrator
Simple and widely used (Network ACLs, and Software whitelists/blacklists)
Rule types – dynamic and static

Module B: Account management

Account Types
User
Privileged
Shared/Generic
Guest

Service

Active Directory Objects
User
Contact
Computer
Printer
Shared folder
Group (security and distribution)
Organizational Unit

Group Scopes
Domain local:
- Visible in own domain
- Can contain most objects
- Can belong to only other domain local groups
- Best used to assign permissions

Global:
- Visible everywhere
- Can contain objects in same domain
- Can belong to any universal or domain local group
- Best used to organize users

Universal
- Visible everywhere
- Can contain objects from any domain
- Can belong to any universal or domain local group
- Best used to nest global groups

Managing User Accounts
Define policies and then enforce them
- Strong but manageable passwords
- Lockout policy
- Credential management
- Disable unneeded accounts
- Assign group permissions
- Avoid generic accounts

Continuous review
- Enable auditing logs
- Review user access settings

Using Security Templates
Use Group Policy Editor console to apply
Use Microsoft Management Console to:
- Create, compare config to template, and apply

Chapter 10: Organizational security

Module A: Security policies

Regulatory Compliance

The Sarbanes-Oxley Act of 2002
The Federal Information Security Management Act
The Health Insurance Portability and Accountability Act
The Family Educational Rights and Privacy Act
The Gramm-leach-Bliley Act
The Payment Card Industry Data Security Standard

Policy Framework

NIST – NIST 800 series describes the cybersecurity standards and best practices for US federal government
ISO – ISO 27000 series is very broad policy framework containing security guidelines for all sorts of organizations
COBIT – Control Objectives for Information and Related Technologies published by ISACA
ITIL – focused on the service aspect of IT

Security Policies by Role

Managerial Staff:
- Legal or regulatory requirements
- Who has access to what
- Activities, processes and actions necessary to enact
- How employees are expected to comply
- Consequences for noncompliance

IT administrators and technicians
- Best practice and security goals
- Technological standards
- Procedure documents
- User permission policies
- Data disposal policies

Types of Policies

Acceptable use policies
- Secure practices and guidelines for use of network resources
- Codified expectations of user privacy
- Creating and maintaining passwords

Asset management policies
- Tracking of hardware and software

Incident Response policies
    Steps to be taken in response to incidents
Disaster planning and business continuity policies
    Steps to be taken to secure assets, protect staff and maintain business operations during disruptions
Change management policy
    Guidelines for updating policies and procedures
Standard operating procedures
    Steps for routine tasks

Password Policies

Length – 8 to 12 characters recommended
Complexity – mix of letters, numbers and special characters
Duration – 30 to 90 day replacement
History – 12 to 24 prior passwords stored
Sharing and Storage – prohibit where possible, secure where not

Secure Personnel Policies

Least privilege – limits damage done by malice, error or attacker
Mandatory vacations – uncovers fraud or ongoing mistakes
Rotation of duties
Separation of duties – enables employees to check each others' work
Recertification – regular review and approval process
Clean desk policy – prevents data loss or theft

Asset Management

IT Assets:
    Computers and network appliances
    Peripherals and other devices
    Data and storage media
    Software and software licenses
    Supporting infrastructure
Asset roles:
    Owner
    Custodian
    User

Business Agreements

Service level agreement – formal definition of a service provided to or by the organization

Memorandum of understanding – a less formal agreement of mutual goals between two or more organization

Interconnection security agreement – a security focused document that specifies the technical requirements in forming a data connection between two parties

Business partnership agreement – a written agreement defining the general relationship between business partners

Non disclosure agreement – legal agreement outlining proprietary or confidential information that may not be disclosed

Adverse Action Policies

Checks to perform in relation to benefits

Reporting requirements:

- What to report to whom
- How quickly action must be reported

Privacy requirements for background check

Remedies subject can pursue to dispute or correct results

Social Media Risks

Use can be time consuming

Use single sign on with shared credentials

Many employees use same passwords for personal accounts as for work

Postings can reveal sensitive information

Postings commonly used in social engineering attacks

Employee behaviors can be liability for employer

Module B: User training

Role Based Training

End users:

- Common threats and how to avoid them

Customer facing employees

- Social engineering and public reputation

Privileged users:

- Elevated privileges means more risk

Administrators:

- Detailed procedures and evolving threats

Incident response teams:

- Response procedures and forensics

Management

- High level view of assets and general threats

Handling Data

Data should be classified by nature

- Labeling, storage and access permissions

Special data should be handled appropriately

- PII, HIPAAA, PCI-DSS, Customer and partner data

Data transit

- Secure network protocols, mobile devices and removable storage

Data disposal

Module C: Physical security and safety

Facility and Location Concerns
Location issues – crime, disaster, utilities, emergency
Perimeter – sturdy, sensors and cameras, visibility
Barriers
Secure doors/windows
Visibility – lighting, escape routes

Secure Entryways
Conventional locks
Electronic locks – passcode, ID badge, biometrics, fail secure vs fail safe
Guards
Mantrap
Entry Logging

HVAC Systems
Temperature range
Humidity range
HVAC settings
Air Flow
Sudden Changes

EMI Shielding
Electromagnetic interference
Radio frequency interference
Sources – motors, microwaves, HVAC, industrial equipment
Protections – shielded cables, faraday cage, TEMPEST standards

Fire Suppression
Fire extinguishers:
- Class A for solids
- Class B for liquids
- Class C for electrical
- Class D for metals
- Class K for cooking oils/fats

Fixed systems:
- Sprinklers, halon/inert gas

Chapter 11: Disaster planning and recovery

Module A: Business continuity

Continuity Planning

Business continuity plan (BCP)
: Comprehensive plan with risk analysis, controls, and service restoration procedures

Business impact analysis (BIA)
: Assessment of critical business functions

Disaster recovery plan (DRP)
: Technical plan for specific disaster type

IT contingency plan
: Restoration plan for IT systems

Continuity of operations plan (COOP)
: Procedure for temporary site during recovery

Crisis communications plan
: Internal and external

Succession plan
: Procedures for sudden changes of personnel

Creating a BCP

1. Perform a risk assessment, much like for normal security planning
2. Create a BIA
3. Design the BCP and its supporting recovery plans and controls
4. Implement and test the plan
5. Analyze the results to apply further refinement

Creating a BIA

1. Identify functions critical to sustained business operations
2. Identify resources used by each critical function
3. Prioritize critical functions
4. Identify threats to each function
5. Determine mitigation techniques for each threat

Disaster Recovery Plans

System documentation
Reserve resources
Vendor lists
Backup policies
Recovery procedures
Personnel list
Emergency contacts

Module B: Fault tolerance and recovery

Recovery Objectives

Recovery time objective

Maximum expected amount of down time in case of a failure

Recovery point objective

Maximum expected period of time for which data will be lost in the case of disaster

Alternate Sites and Spare Parts

Replacement parts – hot spare is ready to go, cold spare is ready to install
Hot site – fully equipped backup location that is ready in hours
Cold site – Space and utilities but no hardware
Warm site – some hardware, but not ready to go

Data Backups

Archive bit – marks data needing backup
Full backup – all data on volume
Incremental backup – backs up only files with set archive bit
Snapshot – quickly capture state of system

Creating Backup Policies

1. Identify what data is important to backup
2. Determine retention requirements
3. Choose backup strategy and schedule
4. Plan data security
5. Assign personnel responsibilities
6. Create and apply a backup testing schedule

Module C: Incident response

Forensic Evidence

Evidence admissible in court
Testimony – sworn statement, oral or written
Real evidence – physical object relevant to the case
Demonstrative evidence – a representation of an object or event
Digital evidence – evidence recorded in a digital format

Collecting Evidence

1. Secure access to systems and data
2. If necessary, access evidence through eDiscovery
3. Classify evidence by order of volatility
4. Capture evidence
5. Take hashes
6. Analyze data

7. Assemble findings

Incident Response Process

1. Preparation
2. Identification
3. Containment
4. Investigation
5. Eradication
6. Recovery
7. Lessons learned

Identifying Incidents

1. Rely on multiple sources
2. Examine anything unusual
3. Evaluate the incident's nature
4. Evaluate incident scope and severity
5. Escalate the incident appropriately

Eradicating Problems

1. Clean up damage
2. Harden network against recurrence
3. Notify relevant personnel

Restoring Service

1. Create service restoration plan
2. Certify restored system are operational and secure
3. Formally restore services
4. Continue monitoring