

CompTIA Security+ (SY0-701) Day 2 Notes

Hashing and Obfuscation

Hashing

- Mathematical “meat grinders” – you can't reverse the process
- Generate unique "fingerprints" for any data they are fed
- Used to verify the integrity of data or to conceal the data
- Small changes to inputs result in large changes to outputs
 - MD5 ("password") = 5f4dcc3b5aa765d64d8327deb882cf99
 - MD5 ("Password") = dc647eb65e6711e15537528212b3964
- Collisions occur when two inputs yield the same output
 - Important that collisions are exceedingly difficult to generate and therefore practically never happen
 - **Note:** MD5 is cryptographically broken and should not be used in modern systems

Hashing Use Cases

- Cryptographic Applications
- Data Integrity Verification
- Password Storage and Verification
- Efficient Data Retrieval
- Detecting Duplicates
- Blockchain and Distributed Systems

Salting

- Adding non-secret, random data into the algorithm along with the password/passphrase/key to generate a result that would be significantly different if the same password/passphrase/key is used more than once
- Example: Two passwords that are the same can be “salted” differently
 - My Password = securityrocks
 - My Salt = wh6q

- Hashed = b3e513cd1098dc46c03c0be9969840c1
- Your Password = securityrocks
 - Your Salt = pl0z
 - Hashed = a00b9c5cc442312708286dd3c4f552d7

Key Stretching

- A technique used to enhance the security of cryptographic keys or passwords
- Makes them more resistant to brute-force and dictionary attacks
- Common algorithms: PBKDF2, bcrypt, scrypt, Argon2
 - Example:
 - Cryptographic key = "mypassword"
 - Key derivation function = PBKDF2
 - Salt = "b5322c2cf31bcf4a2a3ab81e4e3c19fc"
 - Iterations = 100,000

Steganography

- Hiding secret data within an ordinary, non-secret file or message
- Common formats:
 - Images
 - Video
 - Audio

Tokenization

- Replacing sensitive data with a non-sensitive equivalent, referred to as a "token"
- Tokens are random or pseudorandom values that have no direct correlation to the original data
- Purpose: protect sensitive information while allowing functional use without exposing real content
- Used when organizations do not need to retain the data's original format or structure

Data Masking

- Replacing sensitive data with a non-sensitive equivalent of the same type and format

- Example: johndoe@gmail.com → J****@****.com
- Example: 555-12-3456 → 555-12-**** (format preserved)
- Purpose: protect sensitive information while maintaining usability for testing, reporting, or analytics

Public Key Infrastructure (PKI)

- Solution to verify ownership of public keys
- Made up of a Certificate Authority (CA) and supporting infrastructure
- PKI provides the means to bind public keys to their owners and distribute them securely
- Consists of hardware, software, people, policies, and procedures needed to manage certificates

Certification Authority (CA)

- Trusted third party
- Issues, signs, and publishes certificates
- Issues Certificate Revocation Lists (CRLs)
 - List of invalid (revoked) certificates
 - Online Certificate Status Protocol (OCSP) provides real-time status
- Maintains archives of status information
- May retain copies of data encryption private keys for recovery (government/legal compliance)

Registration Authority (RA)

- Verifies certificate requests for the CA
- Performs identity proofing
 - Face-to-Face, Remote, or Automated Registration
- Handles revocation requests
- A CA may have multiple RAs
- RA's public key is trusted by the CA

CA Verification Options

- **Domain Validated (DV)** – Proves control of a domain
- **Organization Validated (OV)** – Proves domain control + legitimate business registration
- **Extended Validation (EV)** – Proves domain control + registered business + human interview

Certificate Types

- **Wildcard** – Covers all subdomains of a domain
- **Self-Signed** – Not issued by a CA (not trusted externally)
- **SSL/TLS Certificate** – Authenticates websites, servers, or entities
- **Code Signing** – Digitally sign applications to prove authenticity
- **User/Client** – Authenticate and authorize users
- **Computer/Device/Machine** – Authenticate and authorize devices
- **Root** – Used to identify the Root CA (self-signed)

Certification Revocation List (CRL)

- Published by CAs at regular intervals
- Responsibility of users/clients to download and check
- Disadvantages:
 - Latency in revocation process since lists are updated periodically

Online Certificate Status Protocol (OCSP)

- Alternative to CRLs

- Real-time check if a certificate is revoked or suspended
- More efficient than downloading large lists

Key Escrow

- Safeguard against loss of private keys
- Securely stores a copy of private keys with a trusted third party
- Ensures recovery of encrypted data when the original private key is unavailable, lost, or legally required
- **Risk:** Escrow agents can be compromised or coerced, introducing potential security concerns

Blockchain and Public Ledgers

Open Public Ledger

- Distributed and transparent record-keeping system accessible to the public

Blockchain

- A distributed database or ledger shared among a computer network's nodes
- Commonly used for cryptocurrency but also for secure record-keeping
- Benefits:
 - Cryptographic security
 - Fraud prevention
 - Transparency and trust
 - Decentralization (no central authority)

- Keys:
 - Public Key → The “address” in the blockchain
 - Private Key → Secret credential required to sign transactions

Data Encryption

- Ensures confidentiality, integrity, and security of sensitive information
- Protects data at rest and in transit

At Rest Options:

- Full Disk – Encrypt entire disk (e.g., BitLocker)
- Partition – Encrypt specific partitions
- Volume – Encrypt logical disk volumes
- File – Encrypt individual files
- Database – Encrypt entire databases
- Record – Encrypt specific records within a database

TPM, HSM, KMS, and Secure Enclave

Trusted Platform Module (TPM)

- Security chip embedded in a system
- Provides secure storage of cryptographic keys, remote attestation, and secure boot
- Typically used with Secure Boot

Hardware Security Module (HSM)

- Specialized hardware device for strong cryptographic security
- Manages and safeguards cryptographic keys
- Performs cryptographic operations securely
- Protects sensitive information

Key Management System (KMS)

- Centralized software or hardware for securely generating, storing, distributing, rotating, and managing cryptographic keys

- Ensures confidentiality, integrity, and availability of keys
- Provides controlled access for authorized users and devices

Secure Enclave

- Isolated and protected region within hardware or software
- Provides secure execution of sensitive operations, data, and code
- Protects against unauthorized access even if the host OS is compromised

Section 2.0 Threats, Vulnerabilities, and Mitigation

2.1 Compare and Contrast Common Threat Actors and Motivations

Unskilled Attacker (Script Kiddies)

- **Attributes:** External, minimal funding, low sophistication (uses publicly available tools)
- **Motivations:** Curiosity, bragging rights, disruption

Hacktivists

- **Attributes:** External, sometimes loosely affiliated, variable skills, moderate resources (often DIY)
- **Motivations:** Philosophical/political beliefs, ethics, disruption/chaos

Organized Criminals

- **Attributes:** External, well-funded via illicit means, professional, agile
- **Motivations:** Primarily financial gain (fraud, extortion, ransomware, blackmail, data exfiltration)

Nation States / State Actors

- **Attributes:** External, very large resources & funding, highly sophisticated tools, zero-day capabilities
- **Motivations:** Espionage, data exfiltration, cyber warfare, often sponsor Advanced Persistent Threats (APTs)

Insider Threats

- **Attributes:** Internal (trusted access), varies widely in skill, moderate resources (access is their “resource”)
- **Motivations:** Revenge, financial gain, blackmail

Shadow IT

- **Attributes:** Internal (unauthorized), often no formal support, varies in sophistication
- **Motivations:** Convenience, user wants/needs

2.2 Explain Common Threat Vectors and Attack Surfaces

Threat Vector: The specific method or pathway through which a cyberattack is launched or a security breach occurs.

Attack Surface: The collection of all potential entry points and vulnerabilities in a system, network, or organization that could be exploited by attackers.

Message-Based Vectors

- **Email**
 - Threat Vectors: Phishing, malware distribution, spoofing, impersonation
 - Attack Surface: User inboxes, email servers
- **SMS (Short Message Service)**
 - Threat Vectors: SMS phishing (smishing), malware distribution, SIM card swap
 - Attack Surface: Mobile devices
- **Instant Messaging**
 - Threat Vectors: Malware distribution, social engineering, on-path attacks
 - Attack Surface: IM platforms, end-user devices

Image-Based (.PNG, .JPEG)

- Threat Vectors: Steganography (hiding malicious code or data in image files), malicious image files, phishing/social engineering
- Attack Surface: End-user devices, websites and web apps, email/messaging platforms, social media

File-Based (.PDF, .DOC)

- Threat Vectors: Malicious attachments, downloads, USB flash drives, P2P sharing
- Attack Surface: End-user devices, websites and web apps, email/messaging platforms, file storage/sharing services

Voice Calls

- Threat Vectors: Call interception, caller ID spoofing, vishing, VoIP vulnerabilities, call relay attacks
- Attack Surface: Mobile and landline phones, VoIP systems and providers, caller ID services, networks

Removable Devices

- Threat Vectors: Malware distribution, unauthorized remote access, data exfiltration/leakage
- Attack Surface: End-user devices, corporate networks, cloud storage services

Vulnerable Software

- **Client-Based**
 - Threat Vectors: Bugs in client applications, drive-by downloads, zero-day exploits, phishing
 - Attack Surface: End-user devices, network, internet
- **Agentless**
 - Threat Vectors: Server/service vulnerabilities, web application flaws, denial-of-service (DoS) attacks, unauthorized access
 - Attack Surface: Server/network infrastructure, cloud services

Unsupported Systems and Applications

- Threat Vectors: Software vulnerabilities, malware, ransomware
- Attack Surface: Legacy systems, unsupported applications, networks

Insecure Networks

- Threat Vectors: Unauthorized access, on-path attacks, data exfiltration, unsolicited messages/files
- Attack Surface: End-user applications/devices, wired/wireless network devices, insecure protocols/services

Open Service Ports

- Threat Vectors: Port scanning, service exploitation, DoS, unauthorized access
- Attack Surface: Network infrastructure, individual systems, internet-facing devices

Default Credentials

- Threat Vectors: Brute force attacks, password spraying, public internet research
- Attack Surface: End-user devices, applications, servers, network devices, embedded systems

Supply Chain

- **Managed Service Providers (MSPs)**
 - Threat Vectors: Weak authentication, credential theft, unpatched software, on-path attacks, DoS
 - Attack Surface: MSP software, tools, and infrastructure
- **Vendors**
 - Threat Vectors: Weak authentication, credential theft, unpatched software, on-path attacks, DoS
 - Attack Surface: Development, distribution, or delivery of software, hardware, or services
- **Suppliers**
 - Threat Vectors: Weak authentication, credential theft, unpatched software, on-path attacks, DoS
 - Attack Surface: Supplier systems/services that impact customer/client security

Human Vectors / Social Engineering

- **Social Engineering:** Psychological manipulation technique used to exploit human behavior via email, text, phone, websites, and more
 - **Pretexting:** Creating a fabricated scenario to obtain information from a target
 - **Impersonation:** Pretending to be someone else to deceive the target
 - **Misinformation/Disinformation:** Using falsified information to mislead the target (often seen in phishing, smishing, spear phishing)
 - **Brand Impersonation:** Using a trusted company's identity to trick targets

Human Vectors / Social Engineering

- **Social Engineering:** Psychological manipulation technique used to exploit human behavior via email, text, phone, websites, and other channels.
- **Pretexting:** Creating a fabricated scenario to obtain information from a target.
- **Impersonation:** Pretending to be someone else to deceive the target.
- **Disinformation:** Intentionally using false or misleading information to deceive the target, often seen in phishing, smishing, and spear phishing.
- **Brand Impersonation:** Using a trusted company's identity to trick targets.

Variations of Phishing

Phishing

- An email-based attack.
- Designed to deceive recipients into taking specific actions, such as clicking a link or opening an attachment.
- Can target anyone, but often focuses on groups more likely to respond.

Smishing

- An SMS-based attack.
- Designed to deceive recipients into taking specific actions, such as clicking a link or opening an attachment.
- Can target anyone, but often focuses on groups more likely to respond.

Vishing

- A voice-based attack.
- Designed to deceive recipients into providing sensitive information, making financial transactions, or taking actions that benefit the attacker.
- Can target anyone, but often focuses on groups more likely to respond.

Spear-Phishing / Spear-Smishing / Spear-Vishing

- A targeted and personalized form of phishing, smishing, and vishing.
- Attacker customizes messages for specific individuals or organizations.
- Involves research to gather information about the target, such as their name, role, company, or interests, making the message appear more convincing.
- Goal: deceive a specific individual or organization into transferring funds, disclosing confidential information, or compromising a system.

Whaling Email / Whaling SMS / Whaling Voice

- A highly targeted form of phishing, smishing, and vishing aimed at executives or key decision-makers.
- Attacker customizes messages based on detailed research about the target.
- Goal: trick high-level individuals into transferring funds, revealing confidential information, or compromising a system.

Business Email Compromise (BEC)

- A cybercrime involving scammers using email to trick individuals into sending money or divulging confidential company information.
- Scammer poses as a trusted figure requesting payment or sensitive data.
 - False Invoice Scheme
 - CEO Fraud
 - Lawyer Impersonation
 - Account Compromise

Watering Hole Attack

- Targets a specific group or organization.
- Involves compromising websites or online resources known to be frequented by the target audience.

Typosquatting

- Attacker registers domain names similar to legitimate websites to exploit typing errors.
- Also known as URL hijacking or domain mimicry.
- Often used in combination with phishing emails to increase credibility.
- Example domains:
 - www.facebook.com
 - www.gooogle.com