INFORMATION SECURITY (IS)

Information: Processed, structured data with meaning and value
Information security: Protection of the CIA of information
IS Importance: minimize downtime, protect processed/stored information, safe operation of applications, safeguarting assets from theft/misuse
Non-repudiation: Prevents parties from denying their actions
Accountability: Ability to trace actions back to a person
Authentication: Verifies the identity of a user or system
Authorization: Determines actions an entity is allowed to do
Access control: Restrict access to resources based on rules
Security policy: A rule/expectation for protecting information
Compliance: Adherence to laws, regulations, and standards
Information types: Personal, business, financial, intellectual, system
Components of an Information System (IS): Software, Hardware, Data, People, Procedures, Networks
Bottom-Up: Implementations happen before policies
Top-Down: Initiated by management, more effective
McCumber cube: x: CIA (what), y: IS (where), z: Ctrl (how)
(C)onfidentiality: Prevent unauthorized access to info
(I)ntegrity: Protect reliability and correctness of information
(A)vailability: Ensure uninterrupted access to information
Information states: In **storage**, in **transit**, in **use**
Control: A measure designed to reduce the potential risk of an attack by eg. **Policy, Education, Technology**
(S)poofing: Pretending to be someone else
(T)ampering: Unauthorized data modification or altering
(R)epudiation: Denying actions without proof
(I)nformation disclosure: Exposing sensitive information
(D)enial of service: Making systems or services unavailable
(E)levation of privilege: Gaining unauthorized rights
Intellectual property: Legal rights protecting creations of the mind: Copyright, (Registered) Trademarks, Patents, Trade Secrets
Trademark: Protects brand identifiers such as names, logos, or symbols
Patent: Protects inventions and technological solutions

THREAT CATEGORIZATION

SOCIAL ENGINEERING

Manipulating people to reveal confidential information
Phishing: Forged emails impersonating legitimate entities
Spear Phishing: Targeted phishing to specific individuals
Vishing: Voice-based phishing over phone or video calls
Smishing: SMS / Text-based phishing

SOFTWARE ATTACKS

Exploiting vulnerabilities in software to gain access/steal data
Virus: Malware that attaches to programs and spreads
Worms: Self-replicating malware that spreads over a network
Trojan Horse: Malicious SW disguised as legitimate apps
Ransomware: Encrypts victim data, asks payment to restore
Rootkits: SW hides malicious acts, maintains priv. access

DENIAL OF SERVICE

Overloading one or multiple systems to make it unavailable
DoS: Single source denial of service attacks
DDoS: DoS performed by multiple attackers/devices
Botnet: Network of compromised devices controlled by an attacker and used to together to flood a target with traffic
SYN-Flood Attack: Sending many TCP connection requests without completing them
Reflection Attack: Attacker spoofs victim's IP, sends requests to a service so that it sends (many) replies to victim

WEB APPLICATION ATTACKS

Exploiting vulnerabilities in websites/servers hosting websites
SQL Injection: Insert malicious SQL commands into an input
Cross-Site Scripting (XSS): Inject malicious scripts into website that execute in users' browsers to steal data. Relies on reflected input. Often uses `<script>`. Defense: limit amount of user input chars
Cross-Site Request Forgery (CSRF): Trick logged-in user's browser into sending reqs to a webapp on attacker's behalf
Broken Authentication: Weak auth mechanisms allow attackers to gain unauthorized access (password/session)

PASSWORD / AUTHENTICATION ATTACKS

Compromising login systems to gain unauthorized access
Rainbow Table Attacks: Precomputed hash lookup tables to reverse weakly hashed passwords back into plaintext
Password Spraying: Trying a few common passwords like "password" across many accounts to avoid lock-/timeouts
Credential Stuffing: Using leaked credentials from previous breaches to attempt logins on other services
Brute Force Attack: Repeatedly try many username & password combinations until they gain access to an account

PHYSICAL THREATS

Bypass technical cntrols by accessing physical infrastructure
Theft of devices: Physically steal hardware to gain direct access to stored data, credential, internal systems, …
Hardware tampering: Modify/implant malicious components in to intercept data, bypass security, or disrupt operations
Power disruption: Interrupt or manipulate power supply impacting availability and business continuity
Environmental damage: Environmental events that damage infrastructure, causing data loss, downtime, …

INFORMATION SECURITY MANAGEMENT (ISM)

Information security governance: System by which IS strategy is controlled to ensure that it supports business objectives, manages risk appropriately, and complies with legal and other regulatory requirements. (**what**)
Information Security Management System (ISMS): Framework used to manage and protect assets through policies, processes and controls (**how**)
Enterprise Information Security Policy (EISP): High-level Information security policy that sets the strategic direction and scope for all an organization's security efforts
- **Statement of Purpose**: Scope, objectives, and purpose
- **Info Security Elements**: Core principles & concepts (CIA)
- **Need for IS**: IS importance & legal/ethical responsibility
- **IS Responsibilities and Roles**: Organizational structure

Security Awareness and Training: Educational programs to ensure employees know their security responsibilities
Monitoring, Measurement and Audits: Ongoing evaluation of control effectiveness and ISMS performance
Issue-specific security policy: Detailed, targeted guidance to instruct people in the use of a specific resource

POLICY

Practices: Ex. actions that illustrate compliance with policies
Policy: Instructions that dictate certain behavior within an org
Standard: Details of what must be done to comply with policy
Guidelines: Non-mandatory recommendations (reference)
Procedures: Step-by-step instructions to assist employees
De jure standard: Formally evaluated and approved by org
De facto standard: Widely adopted/accepted by public group
What does a policy do?: Establishes authority, account., responsib. Foundation for standards, procedures, guidelines
Who is responsible for policies?: Created by senior mgmt. Enforced by mgmt. Employees responsible for compliance
How is it enforced?: Communicate, integrate into standards, monitor compliance, disciplinary measure on violation
Cyber Resilience Act (EU): Requires secure-by-design digital products and vulnerability management

DESIGNING EFFECTIVE POLICIES

1) Development: Must align with organizational goals, business risks and legal requirements
2) Distribution: to all affected entities in a timely manner
3) Comprehension: Readable for, available to and read by all
4) Compliance: Formally agreed to by act or affirmation
5) Enforcement: Uniformly applied to all affected entities
6) Review: Reviewed regularly in a changing environment

RISK ANALYSIS

Identify Assets → Identify Threats → Identify Vulnerabilities → Assess Likelihood → Assess Impact → Determine Risk Level
Asset: Item of value belonging to an organization. eg:
Information: Customer data, intellectual property, code
Technical: Services, applications, databases, networks
Physical: Servers, devices, facilities, infrastructure
Human: Employees, administrators, contractors
Business Process: Critical operational workflows
Threat: An event or action with the potential to cause harm by exploiting a vulnerability. eg: power outage, vishing

CLASSIFYING ASSETS

Public: Information that can be shared without risk
Internal: Information for organization internal use only
Confidential: Sensitive info, could cause harm if disclosed
Restricted: Highly sensitive,strictly limited,strongly protected

SECURITY CONTROLS

Administrative/Management Controls: Policies, procedures, security training, security governance
Technical / Logical Controls: Firewalls, encryption, access control systems, system hardening
Physical Controls: Physical locks, surveillance cameras, secure access badges, turnstiles
Preventive Controls: Stop incidents before they occur. eg. Firewalls, access control, encryption
Detective Controls: Identify incidents when they occur. eg. Intrusion detection, log monitoring, SIEM, CCTV
Corrective Controls: Limit damage, restore systems after an incident. eg. Backups, system restore, incident response
Deterrent Controls: Discourage malicious behavior. eg. Warning banners, monitoring notices, disciplinary policies
Compensating Controls: Reduce risk when a primary control cannot be implemented. eg. Network isolation, layered security, alternative safeguards
Business continuity: Ensures critical operations continue during disruptions. Objectives: maintain operations, minimmize impact, protect assets, recover fast

SECURITY AND AWARENESS TRAINING

1) **Awareness**: basic information, **what**
2) **Training**: detailed knowledge, **how**
3) **Education**: depth of knowledge, **why**

GAP ANALYSIS

Define target framework → Assess curr state → Identify gaps, assess risk → Eval, prioritize gaps → Create remediation plan

SECURITY FRAMEWORK

NIST Cybersecurity Framework: Framework for managing cyber risk: Identify, Protect, Detect, Respond, Recover. ISO 27000 is a certifiable international standard, where the NIST does not have certification.
CIS Controls: Defines 18 practical technical security controls

THREATS

Attack: Act that intends to damage, steal or degrade assets
Vulnerability: A weakness in a system that can be abused
Exploit: A method used to take advantage of a vulnerability
Risk: The likelihood of a threat exploiting a vulnerability and the potential harm that could cause = Vulnerability + Threat
Threat vector: Path, method, or delivery mechanism that a threat uses to reach an asset and exploit a vulnerability
Attack surface: ∑ of threat vectors hackers can use to attack

RISK MANAGEMENT (RM)

The process of identifying, assessing, prioritizing and mitigating threats to an asset from an organisation
Risk management process: Implementation, analysis, evaluation of the risk management framework (**doing**)
- **Risk assessment**: Identification, analysis, and evaluation of risk as initial parts of risk management
- **Risk treatment & Risk Owner**: Application of safeguards or controls to reduce the risks to an acceptable level
  1) **Risk identification**: Where and what is the risk?
  2) **Risk analysis**: How severe is the current level of risk?
  3) **Risk evaluation**: Is the current level of risk acceptable?
  4) **Risk treatment**: How do I bring risk to acceptable level?

Risk management framework: Structure of the strategic planning and design of risk management efforts (**planning**)
1) **Exec Governance & Support**: Support by mgmt & usrs
2) **FW Design**: Define methods,risk appetite strategy
3) **Framework Implementation**: Rollout of the plan
4) **Monitoring & Review**: How effective is entire system?
5) **Continuous Improvement**: Adaption to new threats

Risk appetite (strategic): The quantity of risk that organizations are willing to accept, to achieve their goals
Risk tolerance (specific): The acceptable risk organizations are willing to accept for a specific asset
Residual risk: Remaining risk after controls were applied
Common Vulnerabilities and Exposures (CVE): Standard identification number for vulnerabilities
Common Vulnerability Scoring System (CVSS): Severity scores for vulnerabilities based on CIA (14d to be remediated)

QUANTITATIVE RISK ANALYSIS

1) Assign Asset Value (AV)
   1) Identify the organization's information assets.
   2) Classify them.
   3) Categorize them into useful groups.
   4) Prioritize them by overall importance.
2) Calculate Exposure Factor (EF = Damage/AV)
   percentage of loss that an organization would experience if a specific asset is violated by a realized risk
3) Calculate single loss expectancy (SLE = AV × EF)
   Exact amount of loss if an asset were harmed by a threat
4) Assess the annualized rate of occurrence (ARO)
   Expected occurrence frequency of a threat within a year
5) Derive the annualized loss expectancy (ALE=SLE × ARO)
   possible yearly cost of all instances of a realized threat against an asset
6) Perform cost/benfit analysis of countermeasures

Safeguard: Reduce the ARO and/or reduce the SLE
Annual cost of a safeguard (ACS): $ / year
ALE with safeguards (ALE2): ALE with updated ARO/SLE
Value of a safeguard: ALE1 - ALE2 - ACS. Negative = bad (you shouldn't spend more on a safeguard than the value of the asset itself)
Risk Evaluation: Compare risk with risk appetite of the org
Important Indicators (Business Impact): Maximum Tolerable Downtime (MTD) Recovery Point Objective (RPO) Recovery Time Objective (RTO) Work Recovery Time (WRT)
Risk treatment:
- **Mitigation**: Apply safeguards to eliminate remaining risk (Firewall, Training)
- **Transfer**: Shift risks to other areas/entities (Outsourcing)
- **Acceptance**: Leave assets vulnerability facing the current risk level (after formal evaluation).
- **Termination**: Remove asset from the environment

Risk mitigation:
- Fix vulnerabilities
- Applying controls (tools, processes, rules to mitigate risk)
- Reduce final impact (If vulnerabilities happen)
  - **Endpoint Detection and Response (EDR)**: Software watching for sus behaviour, responds with measures
  - **Extended Detection and Response (XDR)**: Like EDR but watching everywhere (not just on endpoints)

IDENTITY & ACCESS MANAGEMENT (IAM)

Provisioning and protecting digital ids & access permissions
Subject: Active entity that accesses a passive object.
users, programs, processes, services, computers
Object: Passive entity that provides information to subjects. files, databases, computers, programs, services, printers
Physical controls: To prevent, monitor, or detect direct contact with systems: guards, fences, motion detectors
Technical or logical controls: To manage access and provide protection for resources. auth, encryption, ACL
Administrative controls: Policies and procedures. hiring practices, background checks, security training
Identification: Claiming an identity, eg. typing a username
Authentication: Verifying validity of claimed id, eg. password
1) Something you know, eg. password
2) Something you have, eg. smartcard
3) Something you are/something you do, eg. biometrics
4) Somewhere you are / aren't (secondary factor)

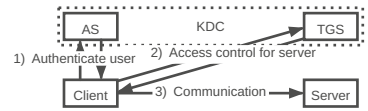
Multifactor Auth: Using two or more factors
Synchronous Dynamic Password Tokens: Generate time-based passwords that are synched with an auth server (TOTP)
Asynchronous Dynamic Password Tokens: Generate passwords based on algorithm and incr. counter, remain valid until used (HOTP)
Biometric access:
- **False Reject Rate (FRR)**: Authorized users who are denied access
- **False Accept Rate (FAR)**: Unauthorized users who are granted access
- **Crossover Error Rate (CER)**: Point where FRR == FAR

(1) Basic Authentication: Username/pw transmitted in the clear
(2) One Time Passwords: Basic auth but used only once
(3) Challenge / Response: Password and one-time challenge
(4) Anonymous Key Exchange: Exchange credentials over unauthenticated secure channel, eg. diffie-hellmann
(5) Zero-Knowledge Password Proofs: Does not permit offline-based password attacks
(6) Server Certificates + User Authentication: Transmit user password over unilaterally authenticated secure channel
(7) Mutual Public Key Authentication: Bilateral use of public key signatures

Attack	*1*	*2*	*3*	*4*	*5*	*6*	*7*
Passive Password Sniffing	✗						
Offline Brute Force Password Attack	✗		✗	✗			
Active Man-in-the-Middle Attack	✗	✗	✗	✗			
Identity Theft on Server	✗	✗	✗	✗	✗	✗	
CA Compromise						✗	✗

KERBEROS

Client encrypts timestamp inside the authenticator, sends it to KDC. If KDC verifies that the time is within a specified amount (def=5min), then OK. **Tickets issued by KDC also have expiration time**. Uses **symmetric key encryption** (DES). KDC stores a list of **hashes** of the principals' passwords. Because hash is used as the symmetric key (Master Key), an attacker with the hash can impersonate user without needing plaintext password. Password itself never traverses the network.



Principal: A Kerberos participant
Principal's Master Key: Long-term secret between the principal and KDC. Used to en-/decrypt authentication tickets.
Kerberos Ticket: Temporary credential for network services
Authentication Server (AS): Verifies client, gives TGT
Ticket Granting Server (TGS): Grants services, gives ST
Ticket Granting Ticket (TGT): Given by the AS
Service Ticket (ST): Given by the TGS
Key Distribution Center (KDC): Verifies & manages auth credentials, distributes session keys to users and services

RADIUS

Remote Authentication Dial-In User Service provides centralized Authentication, Authorization and Accounting (AAA)
1) User requests access from Network Access Server (NAS)
2) NAS prompts the RADIUS server for credentials
3) RADIUS server evaluates the request and returns one of:
   – Access-Accept: User authenticated, NAS grants access
   – Access-Reject: Invalid credentials, NAS denies access
   – Access-Challenge: Server requires more info (MFA)
4) Connected: NAS sends Accounting-Request (log session)

Attack	*Kerberos*	*RADIUS*
Passive Password Sniffing		
Offline Brute Force Password Attack	✗	✗
Active Man-in-the-Middle Attack		✗
Identity Theft on Server		
CA Compromise		✗

AUTHORIZATION

Access Control — Discretionary — Mandatory
Nondiscretionary — Lattice-based — Role-/Task-based
Discretionary access control (DAC): Every object has an owner, the owner can grant or deny access (sharing drive)
Nondiscretionary access control (NDAC): Access controls that are implemented by a central authority (HIPAA/DSG)
Lattice-based access control (LBAC): Assigns users a matrix of authorizations for particular areas
Mandatory access control (MAC): Labels applied to both subjects and objects (classified documents ↔ glowies)
Role-based access control (RBAC): Privileges are tied to a role or job (project info ↔ project manager)
Task-based (TBAC) access control: Privileges are tied to a task (access to server room ↔ technician's time slot)
Auditing: A subject's actions are tracked and recorded
Accounting: Consumption of resources by a subject is measured, metered, and collected.
Salting: Adds unique random value password before hashing, prevents same passwords from producing same hash
Access Aggregation Attacks (passive): Aggregate nonsensitive info to learn sensitive info (Reconnaissance attck)
Password Attacks (brute-force): Online (accounts) vs Offline (steal account database and crack the passwords)
Dictionary Attack (brute-force): Discover passwords by using every possible password in a predefined database
Birthday Attack (brute-force): Finding collisions. MD5 is not collision free, SHA-3 is safe against collisions
Sniffer Attacks: Application that captures traffic traveling over the network. Encrypt all sensitive data, Use OTP.

CRYPTOGRAPHY

Objectives: Confidentiality, Integrity, Auth, Non-repudiation
Steganography: Embedding secret messages within content
Nonce: Unique number for each usage. Makes sure that key is not re-used. Nonce is public, (shared) key is private
One-Way Functions: Easily produces output values but makes it impossible to retrieve the input values
Reversability: Being able to undo the operation of encryption
Ciphertext/Cryptogram: Encrypted message
Cipher: Encryption algorithm. Set of rules for en-/deciphering
Key/Cryptovariable: Usually a very large binary number
Key space: Range of numbers from 0 to 2^n, where n is the bit size of the key. A 128-bit key is $\in \{0, ..., 2^{128}\}$
Initialization vector (IV): Random bit string, same length as the block size and is XORed with the message to create unique ciphertext every time same message is encrypted
Kerkhoff's Principle: Security stems from the secrecy of the key and not the secrecy of the algorithm
Shannon's Principles:
- **Confusion**: Relationship between the plaintext and the key is complicated. S-Box, substitution
- **Diffusion**: Change in plaintext results in multiple changes spread throughout the ciphertext. P-Box, permutation

SP-Network: Repeated substitution and permutation
One-Time-Pad (OTP): XORing all bytes with one-time block of same size. Technically unbreakable
Hashing: Maps data to fixed-size output. Should be: random, diffused, fast, deterministic, irreversible, collisionless
- **Password storage**: Prefer slow hash functions (PBKDF2, bcrypt, argon2)
- **Summarizing data**: Prefer fast hash functions (MD5, SHA-1/2/3)

Data integrity (symmetric enc): Encrypt msg, then hash w/ shared key
HMAC: Hash based MAC, splits a key in two and hashes twice, not vulnerable to length extension attack
SHA-1: Insecure, fast
SHA-2: 256/512-bit variants secure (lower = insecure), current standard
SHA-3: (KECCAK), flexible, ≈ as secure as SHA-2
KMAC 128/256: SHA-3 based KECCAK MAC
bcrypt: Salted, GPU-resistant
Argon2: Highly secure, configurable
AES: Advanced Encryption Standard (SP-Net). XOR, SubBytes, ShiftRows, MixColumns, repeat (128 bit block size)
Ephemeral public keys: Used for communication
Long-term public keys: Used for authentication

SYMMETRIC CRYPTOGRAPHY

Relies on shared secret key, distributed to all members before communication. No non-repudiation or message integrity.
Stream ciphers: Approximate OTP by generating infinite random keystream, work on messages of any length, nonce guarantees uniqueness, fast, no guaranteed integrity
Block ciphers: Take input of fixed size and return output of same size, use confusion and diffusion (SP-Network) **AES**
Electronic Code Block (ECB): Encrypt blocks sequentially with same key. Weak to redundant data divulging patterns
Cipher Block Chaining (CBC): XOR the IV with first input, then XOR output with next input. Not parallelizable
Counter Mode (CTR): Encrypt counter to produce stream cipher and XOR it with message. Parallelizable. **AES**

ASYMMETRIC CRYPTOGRAPHY

Relies on mathematically linked key pairs. $n \in \mathbb{N} \setminus \{0\}, z \in \mathbb{Z}$
– Encrypting a message so only one specific recipient can read it. → Recipient's public key
– Decrypting a message that was sent to me. → My own private key
– Producing a digital signature on a message. → Signer's private key
– Verifying a digital signature. → Signer's public key

Public-key enc: pubkey (e, n) **encrypt**, privkey (d) **decrypt**
Digital signing: privkey (d) **sign**, pubkey (e, n) **verify**
Discrete logarithm: $f(g, a, p) = g^a \bmod p$ (Diffie-Hellman)
Primitive root: g is primitive root of p if
$g \bmod p, g^2 \bmod p, ..., g^n \bmod p$ are distinct
Integer Factorization: $f(p, q) = p \cdot q$ (RSA)
Euler's Theorem: $\gcd(z, n) = 1 \Rightarrow z^{\varphi(n)} \equiv 1 \bmod n$
Totient:

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ has a multiplicative inverse in } \mathbb{Z}_n\}$$

$\varphi(n)$ = Nr. of elements in $\mathbb{Z}_n$ with mult. inv.
= Amount of Numbers $1 \le q \le n$ with $\gcd(q, n) = 1$
$= |\mathbb{Z}_n^*|$

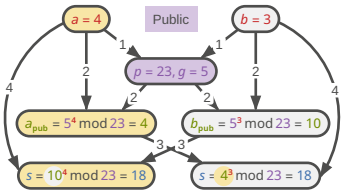
1) $n \in \mathbb{N}$ prime $\Rightarrow \varphi(n) = n - 1$
2) $n \in \mathbb{N}$ prime, $p \in \mathbb{N} \setminus \{0\} \Rightarrow \varphi(n^p) = n^{p-1} \cdot (n - 1)$
3) $m, n \in \mathbb{N} \setminus \{0\}, \gcd(m, n) = 1 \Rightarrow \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

RSA: Rivest-Shamir-Adleman: Signing, use DH for Encryption. Weak for short messages, add OAEP
1) Choose two prime numbers p, q
2) Calculate $n = p \cdot q$
3) Calculate $\varphi(n) = (p - 1)(q - 1)$
4) Choose a, b, so that $a \cdot b \equiv 1 \bmod \varphi(n)$
5) Forget $p, q, \varphi(p \cdot q)$

Public key is now n, b, private key is n, a

– Encrypt: $z = c^a \bmod n$
– Decrypt: $c = z^b \bmod n = c^{ab} \bmod n$
Optimal Assymetric Encryption Padding (OAEP): Introduces IV and hashes it `[0x00 | maskedSalt | maskedDB]`
Probabilistic Signature Scheme (PSS): Hash, Salt, Pad, RSA
DSA: Digital Signature Algorithm
DSS: Digital Signature Standard
DH: Diffie Hellman, share secret over insecure channel

1) Agree on **public parameters** (prime and generator)
2) Combine **private key** with **the parameters**
3) Send resulting **public keys** to each other
4) Combine other **pubkey** with **priv key** to get shared **secret**



ECC: Elliptic Curve Cryptography $y^2 = x^3 + ax + b$
ECDSA: Elliptic Curve Digital Signature Algorithm
ECDH: Elliptic-Curve Diffie Hellman. Uses elliptic-curve point multiplication instead of modular exponentiation. Faster, shorter keys.
ECDHE: ECDH Ephemeral
Perfect forward secrecy: Ephemeral DH KEX, forces new key exchange for every new session (refreshing website)

POST-QUANTUM CRYPTOGRAPHY

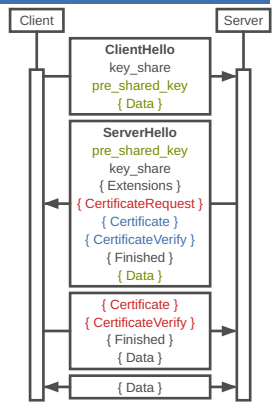
Quantum Computer: Factoring, Discrete Log, Hashing, Asymmetric Crypto (RSA), Symmetric Crypto (HMAC)

TRANSPORT LAYER SECURITY (TLS)

TLS < 1.2 insecure, 1.2 if configured correctly, 1.3 secure
TLS version 1.2 supports insecure ciphers, requires more pkgs for connection establishment, doesn't have 0-RTT.

TLS 1.3

Establishes a shared secret with perfect forward secrecy. → ECDHE
Proves the server's identity (and optionally the client's) via a digital signature. → RSA / ECDSA / EdDSA signatures
Derives traffic keys and IVs from the handshake secret. → HKDF
Provides confidentiality (AES) + integrity (MAC/HMAC) for application data in a single primitive. → AEAD cipher
Certificate not visible in cleartext, handshake encrypted at Server Hello
– Only in mutual auth
– Only present in 0-RTT
– NOT present in 0-RTT
– { Encrypted }

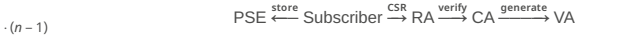


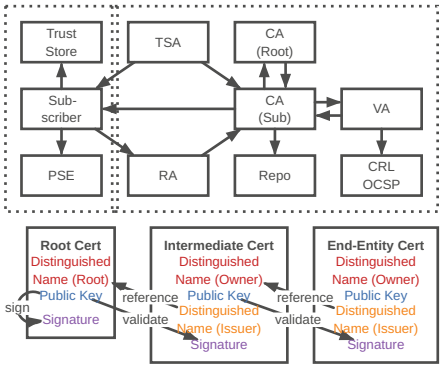
AEAD: Authenticated encryption with associated data. (GCM, ChaCha20/Poly1305)

ChaCha20: Preferred over AES if CPU doesn't have AES instruction set
MAC: Message Authentication Code. Confirms that message came from stated sender (authenticity) and has not been changed (integrity)
GCM: AES Galois Counter Mode → MAC

PUBLIC KEY INFRASTRUCTURE (PKI)

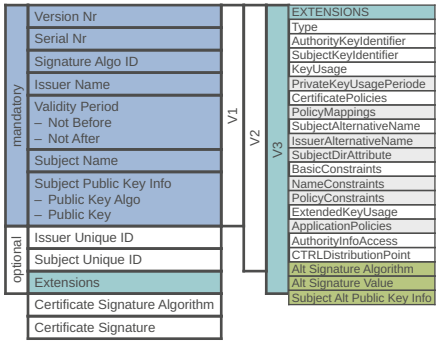
A set of roles, policies, hardware and software needed to manage digital certificates and public-key encryption. Provides trust.





X.509V3

Multiple domains can use the same certificate (if only server-side SSL)



RA: Registration Authority, validates CSR
CP: Certificate Policies
CPS: Certificate Practice Statements
CA: Certificate Authority, trusted certificate issuer
CSR: Certificate Signing Request (creates)
CRL: Certificate Revocation List (signs)
VA: Validation Authority, validates integrity of certificates
TSA: Time Stamp Authority
Subscriber: Client / Certificate holder
PSE: Personal Security Environment
Certificate pinning (HPKP): Explicitly trusts only one certificate, all other root anchors are ignored. Used to prevent MITM/rogue CA. 3 different models: root, intermediate CA, end entity pinning. Poses big risk, because certificates are no longer fully validated. Legacy since 2017.
Truststore: Central (private) storage for certificates. Decides which CAs are trustworthy. Controlled by OS/Browser/etc
Keystore: Central (private) storage for private keys
Hybrid cryptosystem: Var. methods for optimal use-cases Hashing: Digital fingerprint, Symmetric crypto: Bulk encryption, Asymmetric crypto: Signing/exchanging keys
Cipher suites: enc_kex_signature_WITH_bulk-enc_mac
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
OCSP: Certificate Status Protocol
CT: Certificate Transparency
Chain of trust: Evaluated back to root CA to conclude trustworthiness
Root certificate: Self-signed cert on top of PKI chain (truststore). Root certs come already installed on client's machine
Intermediate certificate: Faster cert replacement, less usage of root cert
Revocation: Happens bc. private key was leaked. Client checks with CA
Creation: CSR include pubkey of sub, unsigned signature, signature hash algo. RA investigates if ID/pubkey match with domain. CA creates cert with validity period, key usage, signature signed with priv. key of CA
Verification: Client checks if signature in certificate can be decrypted with pubkey of issuer as well as with pubkey of root cert on client's machine

E-MAIL

Cert necessary before sending enc. mails. Sender of enc. mail uses receiver's pubkey to encrypt email. pubkey of user is embedded into cert.
Multipurpose Internet Mail Extensions (MIME): Contains various header fields and is split into multiple body parts
Secure MIME (S/MIME): Provides signatures + encryption. Central auth. sign-then-encrypt
Encapsulated S/MIME: Content within CMS SignedData Obj. Protected agains modifications
Encrypted S/MIME: Content within CMS EnvelopedData Obj. Protected against transfer encoding changes
Pretty Good Privacy (PGP): Uses Key pairs, no central auth (direct trust/indirect trust). encrypt-then-sign
Sign-then-encrypt: signer knows message, signature hidden, oracle attacks, no integrity, recipient could re-encrypt
Encrypt-then-sign: signature ensures integrity, signer might not know message, recipient could re-sign
Sender Policy Framework (SPF): Specifies which servers may send email for domain (DNS TXT: SMTP MAIL FROM)
DomainKeys Identified Mail (DKIM): PKI based on DNS
Domain-based Message Authentication, Reporting, and Conformance (DMARC): Combines SPF + DKIM

WEB

Common Weakness Enumerations (CWE): Classification of types of vulnerabilities (eg. XSS, SQL Injection)
Open Web Application Security Project (OWASP): Community-driven project for web application security
Broken Auth: Can bypass identity checks/impersonation
Broken Access Control: Eg. get data by changing URL ID
Avoidance Insecure Direct Object References (IDOR): prevents this (eg. UUIDs, server-side auth checks)
Centralized Access Control Logic: Handle in backend
Injection: SQL, Cross-site Scripting (XSS), Shell
(1) Secure Programming: Prepared statements
(2) Infrastructure security: DB Least privileges, WAF
(3) Secure Programming: No logs 4 user, Anon error msgs
Reflected XSS: Data provided by web client is used immediately by server to generate a page of results for that user
Stored XSS: Data provided by web client is stored in a database. This data is then presented to the user unencoded
DOM-based XSS: Original client side JS embeds attacker's payload (eg. from URL) into DOM → `eval()` or `innerHTML`
(1) Secure Programming: Input sanitization
(2) Security Mechanisms: CSP, Headers, WAF

CYBER KILL CHAIN

A model developed by Lockheed Martin in 2011
1) Reconnaissance: Gather information on the target
– Social media, DNS Lookup, Legal info
2) Weaponization: Construct custom weapon to attack target
Exploit: Office macro execution, malicious PDF
Payload: Remote Access Tool, Ransomware, Spyware
Weapon: Phishing Email, Crafted Network Request
3) Delivery: Transmit the weapon to the target
– USB Drops, drive-by downloads, phishing mails
4) Exploitation: Vulnerability is triggered or the target tricked
5) Installation: Establish persistence, install backdoors
– Scheduled tasks, startup folders
6) Command & Control (C2): Compromised host connects to the attacker
– DNS tunneling, HTTPS to legitimate-looking domain
7) Actions on Objectives: Exfiltration, encryption, sabotage, lateral movement

Beaconing: Most C2 traffic beacons: small periodic check-ins, often jittered, tiny in volume but constant in rhythm
Defense-in-depth mapping: Each control (EDR, IDS, backup) maps to phases. Gaps = phases without coverage
Dwell time matters: Median dwell time = 10 days for an attacker to move between phases, undetected
Metric you can measure: Time from phase-1 artefact entering your environment to phase-7 impact
Detections, not tools: Buying appliance without knowing which phase it improves coverage on is expensive theatre
MITRE ATT&CK: Matrix of 14 tactics, hundreds of techniques

INCIDENT RESPONSE

ESCALATION PATH

Event: Any observable occurrence in a system. A user logs in, a file is created, a packet arrives. Most events are routine
Alert: Automated notification from a security tool that an event matched a detection rule and may warrant investigation
False positive: Alert/suspected adverse event that turns out to be benign
Adverse event: Event w/ possibly bad consequences, worth investigating
Incident: A confirmed adverse event that threatens the confidentiality, integrity, or availability of information assets
Data breach: Incident with unauth. access/disclosure of protected data

PIPKIN'S INDICATORS

Possible: Weak signals, worth logging but not acting on alone
Probable: Strong signals, typically trigger investigation
Definite: Confirmed incidents, activate the IR plan
Classifier's dilemma: (Confusion Matrix)

True Positive	False Positive
False Negative	True Negative

DETECT AND RESPOND

"Prevent Everything": If the perimeter holds, we are safe
"Assume Breach" Mindset: Design for fast detection and fast containment, not just for prevention.
MTTD (Mean Time to Detect): Initial compromise - first alert
MTTR (Mean Time to Resp.): First alert - incident contained
Dwell Time (MTTD + MTTR): Total time attacker was active
SOC (Security Operations Centre): The always-on monitoring function. Runs the SIEM, triages alerts, drives day-to- day detection. (T1 triage, T2 investigation, T3 engineering).
CSIRT (Computer Security Incident Response Team): Handles confirmed incidents end-to-end. Often virtual, pulled together when needed: IT, legal, comm, mgmt
CERT (Computer Emergency Response Team): National or sector-level coordination bodies (e.g., GovCERT.ch)
In-House vs. Managed: Many organisations outsource SOC functions to an MSSP (Managed Security Service Provider). CSIRT responsibilities usually stay in-house.
Short-term containment: Stops immediate bleeding fast, temporary (block IPs, disable acc, isolate hosts, temporary filtering rules)
Long-term containment: Hardens environment, persistent (network segmentation, key rotation, rebuild bastion hosts)

NIST IR PROCESS

1) Preparation: Policy, plan, team, tools, training
2) Detection & Analysis: Spot signals, classify them
3) Containment, Eradication & Recovery: Stop the bleeding, remove the attacker, restore services. Short/Long-Term
4) Post-Incident Activity: Lessons learned, feed back to Prep

COMMON IR MISTAKES

Unclear Chain of Command: Attacker uses the confusion
No Central operations center: Decisions are undocumented
Containing too slowly: Fear of "making it worse"
Wiping evidence b4 Forensics: Rebuilding infected server
Skipping after-action Review: Same mistakes next year
No tested Backups: Everyone assumes the backups work

INTRUSION DETECTION SYSTEMS (IDS)

IDS: Monitors systems, flags activity, raises alerts
Intrusion Prevention System (IPS): IDS that takes action
Signature-based detection: Match traffic with known pattern
Anomaly-based detection: Alert on deviations from "normal"
Stateful Protocol Analysis: IDS understands network protocols (HTTPS)
Heuristic & Behavioral Rules: Rules describing suspicious sequences
AI-Assisted Classification: ML trained on labelled samples
Hybrid in Practice: Real-world products blend all the above

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

1) Sources: Endpoints, firewalls, servers, identity providers
2) Collectors: Agents, syslog receivers, API, log forwarders
3) Parse & Normalize: Map every log into a common schema
4) Correlate & Store: Detection rules, ML, search index
5) Consume: Alerts to the SOC, dashboards, search, reports

SIEM: Collect, normalize, correlate, alert. Human response.
Security Orchestration, Automation and Response (SOAR): On top of SIEM. Runs playbooks: isolate, disable
Extended Detection and Response (XDR): Vendor-bundled detection. Lighter alt. to SIEM+SOAR, vendor lock-in.
In real enterprises: SIEM + SOAR is the classic stack
Volume Problem: Avg company produces 20+GB logs/day
Correlation Problem: Attacks touch several systems
Retention Problem: Forensics need logs from 90+ days ago
Compliance Problem: PCI-DSS, ISO 27001, FINMA, NIS2
Alert Fatigue: Many low-quality alerts, analysts stop reading
Garbage In / Garbage Out: Incomplete, mis-parsed logs
Ingestion Cost: Most SIEMs price per GB per day
Tuning Debt: Rules that fit last year do not fit this year
Skills Gap: Detection engineers/threat hunters needed

OPEN-SOURCE INTELLIGENCE (OSINT)

Collecting, analyzing, decisions based on public information
Cyber Threat Intelligence (CTI): Proactive collection, processing, and analysis of information about threats
External sources: CI vendors, Subscription service
Internal sources: Logs, Alerts, Dedicated teams
Advanced persistent Threat (APT): Threat actor, typically nation state
APT Attack: Attacker gains network access, stays there undetected for a long time. Often associated with zero-day attacks

1) Strategic Level for Executives & Management: Who is attacking, why?
2) Operational Level for SOC Teams & Analysts: How does a specific attack unfold?
3) Tactical Level for SIEM systems & Firewalls: Which concrete indicators do I need to block?

ETHICAL HACKING

Validate, audit and report on system/software vulnerabilities
Black Hat: Malicious, destructive hacker, anonymous
Grey Hat: Possess Black hat skills, focus on offense+defense
White Hat: Possess Black hat skills, focus on defense
Script Kiddie: Use tools without knowing what they are doing
Cyber Terrorist: Skilled attacker with ideological purpose
State Sponsored: Hackers employed by the government
Hacktivist: Hacking in order to pursue a political or social aim
Pentesting: Manual process, in-depth analysis
Vulnerability scanning: Automated, periodic
Penetration Testing Execution Standard (PTES): Community-driven industry standard, e2e pentesting methodology
NIST 800-115: Technical Guide, Government-oriented
EC-Council: Global organization providing cysec certs
Black-box Testing: No internal info, Attacker's perspective
Gray-box Testing: Limited knowledge, Realistic auth, Insider-based threat modeling
White-box Testing: Full internal knowledge, Deep analysis
Statement of Work (SoW): Activities to be performed, timeline, location, scope. → Master Service Agreement (MSA)
Non Disclosure Agreement (NDA): Uni-/Bi-/Multilateral

MALICIOUS CODE

User-Dependent Malware: Most malware rely on user interaction or unsafe behavior to propagate
Self-Replication Threats: (Worms) – no human involvement
Computer Viruses: Propagation and payload execution
Drive-by downloads: Unintentional dl of malicious code
Obfuscation: C2 technique, for staying undetected (adding junk data to protocol trraffic, steganography, encoding payload)
Buffer overflow: Allow modifying contents of system's memory by writing beyond the allocated space
Backdoor: Undocumented command sequences that allow individuals with knowledge of the backdoor to bypass normal access restrictions.
MBR infection: Read MBR → Exec malware → Start OS
File infection: Infect exe files, self-contained, easily detected
Service injection: Inject into trusted runtime processes
Macro infection: Written in embedded macro lang (Excel)
Fileless techniques: RAM, resistant to signature-based detection
Multipartite Viruses: Use more than one propagation technique
Stealth Viruses: Hide themselves, trick antivirus
Polymorphic Viruses: Modify their code as they travel. Signature differs, antivirus vendors cracked the code of many
Encrypted Viruses: Use cryptographic techniques, include decryption routine segment, use different keys (polymorph)
Logic Bombs: Lie dormant until some event triggers them
Keystroke logging: Record the keys struck on a keyboard
Trojan Horses: Appears "kind", carries hidden (malware) payload
Ransomware: Encrypts files with key known only to hacker
Worms: Propagate themselves without human intervention
TOCTTOU: Time-of-check to time-of-use, relies on timing of the execution of two events (difference between them)
Spy-/Adware: windows

ANTIVIRUS & ENDPOINT SECURITY

"Disinfects" malware, removing malicious code, quarantines otherwise
Signature-based: Database of characteristics of viruses, most common
Heuristic-based: Analyze the behavior of software
Data integrity: Detect Unauthorized file modifications (hash)
Endpoint Security: EDR tools capture all sys events. Behavioral Analysis, Automated Response and Remediation
DMZ: Demilitarized zone. Net in between scary outside and safe inside

IT/OT

OT: Operational Technology, Software & Hardware for monitoring of industrial machinery/processes
IT/OT - convergence: Traditionally isolated OT-Systems are digitalized and intertwined with IT through e.g. use of IoT
Ensuring Operations: Supply Chain/Operational Reliability
Company-wide Synergies: Complexity, Costs
Enhancing & Leveraging Expertise: Flexibility, Costs, Skilled Workers
Comprehensive Cybersecurity: Risk Mitigation
Compliance with Regulations: Costs
Data Transparency: Planning Accuracy

IOT

Feature	*IT (Office/IT)*	*IoT (Connected)*	*OT (Industrial)*
CIA Prio	C > I > A	I > C > A	A > I > C
Asset Focus	Servers, Laptops, Databases	Smart Dev, Trackers, Cams	Motors, Robots, Sensors
OS Type	Windows, Linux, MacOS	Embedded / Lightweight Linux	Real-time (RTOS) Proprietary
Lifecycle	3–5Y Short-lived	2–7Y Fast-paced	15–30Y Legacy S.
Patching	Regular (e.g. "Patch Tuesday")	OTA (Over-the-Air) targeted	Rare (only during downtime)
Failure Impact	Data loss, Reputation damage	Mass manipulation, Botnets	Physical damage, Risk to life

Typical vulnerabilities: Default pass, no encryption, outdated firmware
Attack vectors: Botnets, MITM, Supply chain attacks

FUTURE

Security-by-Design, Zero-Trust Architectures, Automated patch mgmt & standardization, Compliance with standards