Notes: Security Engineering – Chapter 1

Introduction

Security engineering = designing systems that remain dependable despite malice, error, or accident.

Needs cross-disciplinary expertise: cryptography, software/hardware security, psychology, law, economics, system engineering.

Requires adversarial thinking (like chess – anticipate moves/attacks).

Failures can affect:

- Human life & environment (nuclear safety)
- Economy (ATM systems, payments)
- Privacy (medical records)
- Entire industries (utilities, alarms)

Framework for Security Engineering

Four elements must align:

Policy – what's to be achieved (goals).

Mechanism – tools & controls (e.g., ciphers, access control).

Assurance – how much confidence in the mechanisms.

Incentives – motivations of defenders & attackers.

Example: 9/11 & airport security

- Failures were often policy-related, not mechanism-related.
- "Security theatre" = visible but ineffective controls (TSA checks vs cockpit doors).
- Incentives often drive policy toward looking secure vs being secure.

Case Studies: Banks

Core bookkeeping:

- Threat = insider fraud (1% staff fired yearly for dishonesty).
- Defenses = double-entry, dual authorization, transaction monitoring, enforced holidays.

ATMs:

- Early widespread cryptography use.
- Fraud via "phantom withdrawals".

Online banking:

- Attacks shifted to customers (phishing).
- Countered by SMS codes, but SIM swap fraud evolved.

High-value messaging:

- Used for large transfers, securities, trade.
- Defenses = bookkeeping + crypto + access control.

Branches:

- Physical structures = “theatre.”
- Real protection = alarms + monitoring + cryptography.

Case Studies: Military Bases

Communications:

- Encrypted messages not enough; adversary may locate source.
- Used **low-probability-of-intercept (LPI)** radios → influenced modern Bluetooth.

Electronic warfare:

- Jamming, spoofing, denial techniques pioneered in military before civilian cybercrime.

Information classification:

- Multi-level systems (“Secret” vs “Top Secret”).
- Access control foundations.

Nuclear security:

- Led to biometrics, fiber alarms, strong authentication.
- **Lesson**: Long-term software maintenance crucial (now extends to consumer devices like cars).

Case Studies: Hospitals

Medical device usability:

- Infusion pump errors kill thousands yearly.
- Risk rises with hackable devices.

Patient records:

- Must restrict access (e.g., nurses only for 90 days of care).
- EU law stricter than HIPAA.

Anonymization challenge:

- Medical + contextual data often re-identifies patients.

New risks:

- WannaCry (2017) shut down hospital networks → no backups for digital workflows.
- Accessory authentication = fragility in supply chains.

Case Studies: Home

- Banking & healthcare systems extend into homes.
- Cars:
- Early key fobs encrypted; newer proximity keys vulnerable to relay attacks → theft increase.
- Phones:
- Use SIM authentication but vulnerable to IMSI catchers & SIM swaps.
- Prepayment meters:
- Secure codes for electricity/gas, used even in off-grid villages.
- Smart homes:
- Alarms, IoT, assistants (Alexa, Google Home).
- Increasing surveillance risk.
- Example: EU banned insecure children's watches (unencrypted comms).

Key Definitions

- System: can mean hardware, OS, apps, users, or whole ecosystem. Confusion = vulnerabilities.
- Principals: entities in security (person, role, device, channel).
- Identity: correspondence between principals. Often misused as just "name."
- Trusted vs Trustworthy:
- Trusted = failure breaks policy.
- Trustworthy = won't fail.
- Secrecy / Confidentiality / Privacy:
- Secrecy = technical limitation of access.
- Confidentiality = duty to protect info.
- Privacy = right to personal info & space.
- Authenticity vs Integrity: authenticity = integrity + freshness.
- Hack: system rule-permitted but unintended/undesired behavior (e.g., legal loopholes, exploits).
- Vulnerability: property that could lead to failure.
- Security failure: breach of policy.
- Security policy: concise statement of protection goals.
- Security target: detailed implementation spec.
- Protection profile: generalized spec for cross-comparison.

Summary

- “Security” = overloaded term, means different things depending on perspective (corp vs employee).
- Expect conflict, confusion, and language misuse as security also becomes a tool for control/power.
- Engineers must formalize security goals clearly and separate reality from “security theatre.”