Chapter 2

Threats and Security Processes

IT security processes

Approach to IT security depends on the system to protect

- **Networks and single systems**: first step is to be clear about the attacker(s) and which specific **threats** they pose
- Complex IT **infrastructures**: need to be clear about which **assets** are worth protecting, then look at those systems in turn
- **Organizations** making use of IT infrastructures: often defined by legal necessity (regulation) for following specific IT security **processes** (focus is more on change management than on single solutions)

As this course is mostly about technical security measures, will start with threats and then continue with higher levels of abstraction

Network and systems security

Designing a secure system means asking the right questions first

1. Who are the (potential) attackers?
2. What are their (assumed) capabilities?
3. Which threats follow from those capabilities?
4. What are the potential consequences of successful attacks?
5. What is the risk associated with these threats?
6. What are potential safeguards against these threats?
7. Which risks need to be accepted?

Only then does it make sense to think about technical approaches!

Threat model

Threat modeling is (and/or):

- A description of the security issues the designer cares about
  → *"What is the threat model for DNSSec?“*
- A description of a set of computer security aspects – a set of possible attacks to consider for a specific system
  → *“What is the threat model for our SCADA installation?”*

Starting points

- Attacker-centric (see previous slide)
- Software-centric (e.g. used by Microsoft)
- Asset-centric (often used in military circles)

Potential threats to communication and data

- **Passive attacks** (eavesdropping): very difficult to detect, best safeguard is cryptography
  - *release of message contents*
  - *traffic analysis* often works on meta data → encryption of content does not help – see e.g. data retention laws in most countries (currently **still** illegal in EU), NSA/GCHQ mass data surveillance

- **Active attacks**: typically unable to protect against, goal is therefore to detect
  - *replay*
  - *masquerade*
  - *modification*
  - *denial of service*

GCHQ "FLYING PIG" and NSA "QUANTUMHAND" programs

Active attacks are more expensive than passive

→ force attackers into active

Example for threat model

Dolev-Yao model for interactive cryptographic protocols

- Formal model for mathematical proofs of protocols
- Well-established as the “standard” model against which new cryptographic protocols are tested

Informal definition

- Protocol messages are exchanged between two (or multiple) trusted parties
- The network communication is untrusted and subject to attack
- An attacker may overhear, intercept, and synthesize any message
  - ➔ full control of the channel with all capabilities of active “on-path-attack” / “man-in-the-middle” / “person-in-the-middle”: add, remove, change, delay, reorder, etc.
- All potential threats from previous slide covered

Potential threats to computer systems

- **Physical access**
  - cannot trust boot loaders, OS protection mechanisms
  - do not assume RAM to be volatile → cold boot attacks
  - always have to assume physical access for mobile devices

See e.g. Android threat model

- **Remote exploitation** over network
  - running OS or applications at risk
  - data in memory is at risk (even when encrypted at rest)

NSA "TURBINE" program automatically using "TAO" implants

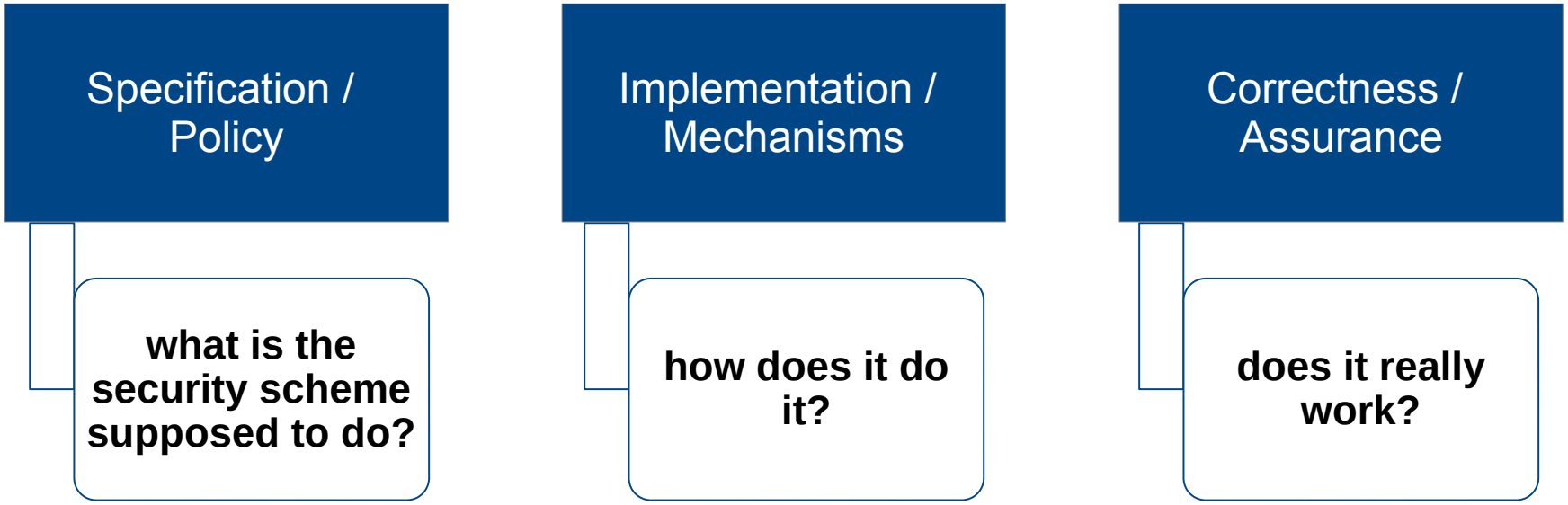
- **Local exploitation** by applications
  - goal is mostly to escalate privileges

Security management

= formal process of answering the questions:

- Ensures that critical assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified – or accept them

Computer security strategy



Management support

- IT security policy must be supported by senior management
- Need IT security officer
  - provide consistent overall supervision
  - liaison with senior management
  - maintenance of IT security objectives, strategies, policies
  - handle incidents
  - management of IT security awareness and training programs
  - interaction with IT project security officers
- Large organizations need separate IT project security officers associated with major projects and systems
  - manage security policies within their area

Security policy

= formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

- Factors to consider:
  - value of the assets being protected
  - vulnerabilities of the system
  - potential threats and the likelihood of attacks
- Trade-offs to consider:
  - ease of use versus security
  - cost of security versus cost of failure and recovery

Security risk assessment

- Critical component of process

- Ideally examine every organizational asset
  - not feasible in practice

- Approaches to identifying and mitigating risks to an organization's IT infrastructure:
  - baseline
  - informal
  - detailed risk
  - combined

Threat identification

Threat sources

- Threats may be
  - **natural events** (“disasters”) or **human-made**
  - **accidental** or **deliberate**
  - evaluation of human threat sources should consider:
    - motivation
    - capability
    - resources
    - probability of attack
    - deterrence

- Any previous experience of attacks seen by the organization also needs to be considered

Vulnerability identification

- **Identify exploitable flaws or weaknesses** in organization's IT systems or processes – determines applicability and significance of threat to organization
- Need **combination of threat and vulnerability** to **create a risk to an asset**
- Outcome should be a **list of threats and vulnerabilities** with brief descriptions of how and why they might occur

Analyze risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls
- Specify consequence should threat occur
- Derive overall risk rating for each threat
  ➔ **risk = likelihood threat occurs x cost to organization**
- Hard to determine accurate probabilities and realistic cost consequences
  - so use **qualitative, not quantitative**, ratings, e.g.

Qualitative assessments: likelihood input

Example *likelihood/probability* levels

- **rare**: only in exceptional circumstances
- **unlikely**: not usually expected
- **possible**: may occur, difficult to judge because of externals
- **likely**: will probably occur sometime, should be no surprise
- **almost certain**: question is more when than if

Qualitative assessments: cost input

Example *cost/consequence* levels

- **insignificant**: impact less than a few days, minor cost to rectify; no tangible detriment
- **minor**: impact less than a week, can be rectified by single team/project
- **moderate**: impact less than 2 weeks, needs management involvement, may require ongoing future cost; public may be aware of event
- **major**: impact less than 2 months, needs higher management and significant cost to rectify, substantial ongoing cost expected; public needs to be notified, loss of organizational outcomes is expected
- **catastrophic**: impact more than 3 months, top management intervention required; significant harm to organization, loss of confidence, regulatory impact, and/or criminal legal action against key personnel likely
- **doomsday**: collapse of the organization to be expected

Qualitative assessments: risk output

Example *risk* levels

- **low (L)**: can be managed through routine procedures
- **medium (M)**: can be managed through specific monitoring and response procedures
- **high (H)**: requires ongoing management by team leaders, regular monitoring and review of procedures
- **extreme (E)**: requires detailed management by executive level, substantial adjustments to organizational control expected (modifying overall goals and processes)

Qualitative assessments: Mapping inputs to output

	doomsday	catastrophic	major	moderate	minor	insignificant
Almost certain	E	E	E	E	H	H
likely	E	E	E	H	H	M
possible	E	E	E	H	M	L
unlikely	E	E	H	M	L	L
rare	E	H	H	M	L	L

Example risk register

Asset	Threat / vulnerability	Existing controls	Likelihood	Cost / consequence	Risk level	Risk priority
Internet gateway	Outside network attacker	Single admin password only	possible	moderate	high	1
Destruction of data center	Fire, flood, etc.	None (no disaster recovery plan), but irregular backups exist	unlikely	major	high	2

Risk treatment

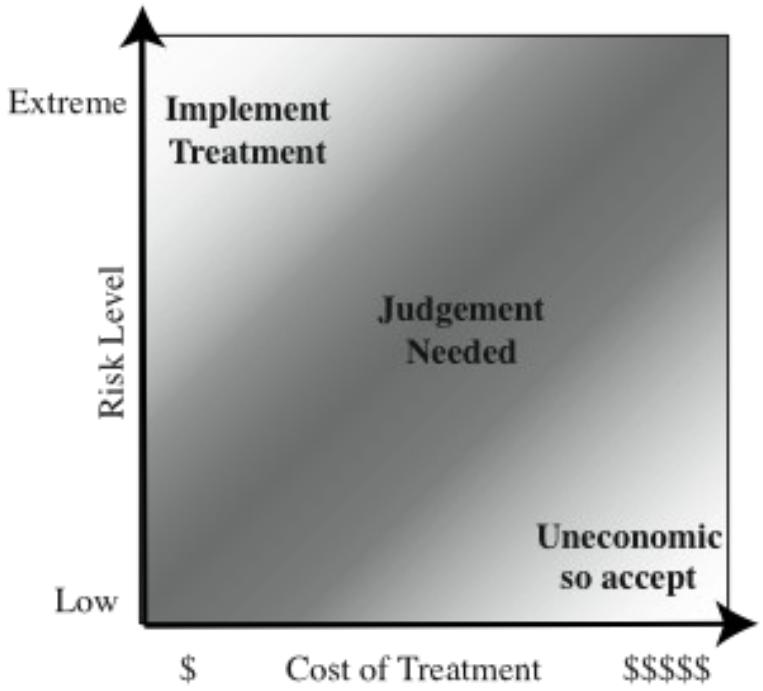
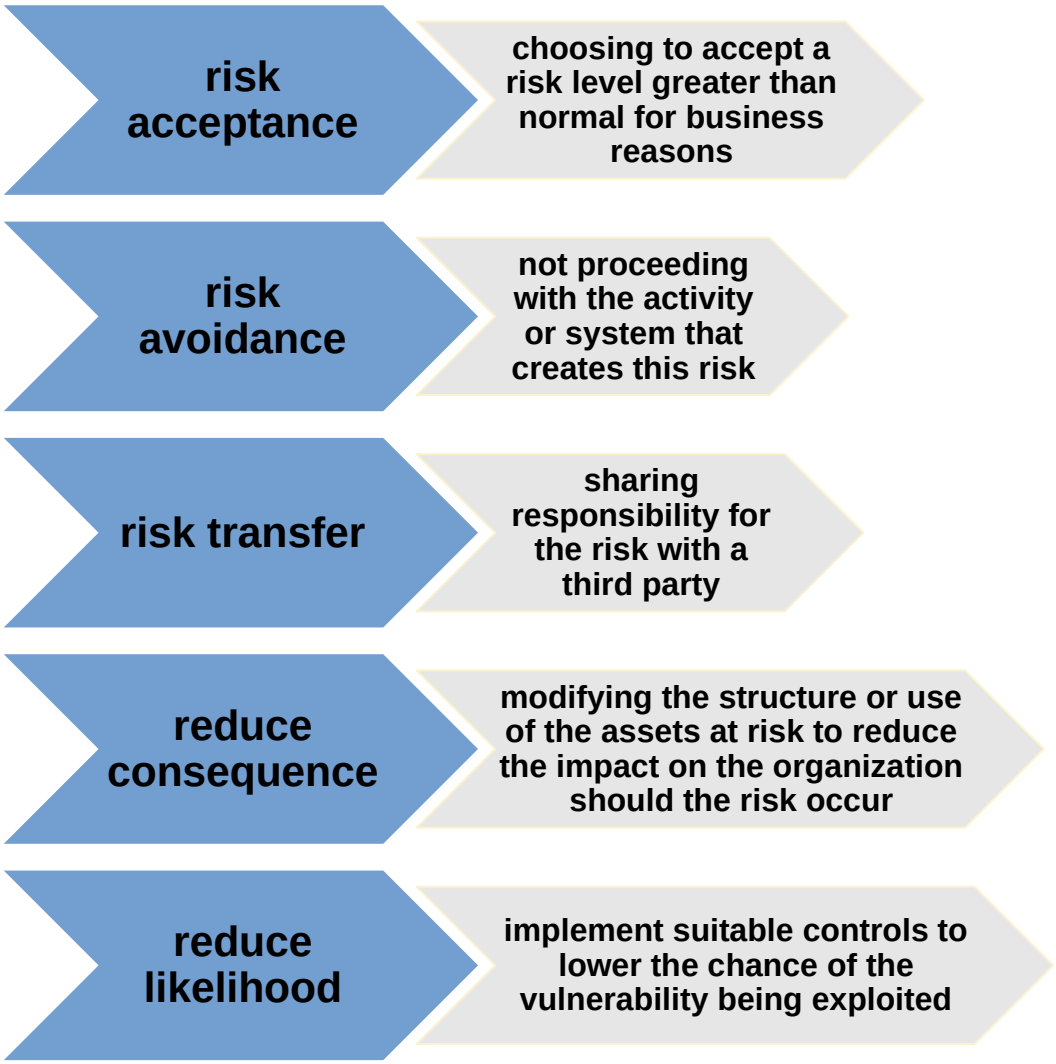


Figure 14.5 Judgment About Risk Treatment

Risk treatment alternatives



Security implementation requires all four complementary courses of action:

Detection

- intrusion detection systems
- detection of denial of service attacks
- detect those attacks that cannot (yet) be prevented

Response

- upon detection, being able to halt an attack and prevent further damage
- analyze reasons for attack

Prevention

- secure encryption algorithms
- prevent unauthorized access to encryption keys
- code security

Recovery

- use of backup systems
- documented recovery procedures

Security functional area requirements

(primarily)
Technical measures

- access control
- identification & authentication
- system & communication protection (confidentiality)
- system & information integrity

Overlapping technical and management measures

- configuration management
- incident response
- media protection (e.g. backup media)

(primarily)
Management controls and procedures

- awareness & training
- audit & accountability
- certification, accreditation, & security assessments
- contingency planning
- maintenance
- physical & environmental protection
- personnel security
- risk assessment
- systems & services acquisition

Assurance and evaluation

- **Assurance**
  - the *degree* of confidence one has that the security measures work as intended to protect the system and the information it processes
  - encompasses both system design and system implementation
- **Evaluation**
  - process of examining a computer product or system with respect to certain criteria
  - involves testing and formal analytic or mathematical techniques

A note on Cybercrime / computer crime

- Cybercrime: "*criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity*"
- Categorize based on computer's role:
  - as target
  - as storage device
  - as communications tool
- More comprehensive categorization seen in Cybercrime Convention, Computer Crime Surveys