Security

- Security covers a wide range of issues.
- When thinking about security, start from the application, not from the technology.
- Attacks may exploit weak points of the “business model” rather than technical flaws.
- Security problems can rarely be eliminated, but they can be managed.

Security

- Systems may fail for various reasons.
- Reliability deals with accidental failures.
- Usability addresses problems arising from operating mistakes made by users.
- Security deals with intentional failures: a decision by somebody to do something (s)he is not supposed to do.
- Reasons: crime, malice, curiosity, stupidity, ...

Security is a People Problem

- Technical solutions can only address a part of the problem.
- Technical measures should be managed in a wider security culture.
- The legal system defines the boundaries of acceptable behaviour.
- Social engineering is a powerful attack method.
- Protection of the assets of an organisation is the responsibility of management.
- Security measures may restrict people in working patterns, so could ignore security rules if security instructions do not come from authority but from other branch of the organisation.

Security Awareness

- effective security policies must be supported by top management: needs clear document explaining general rules.
- users are not the enemy but are required to protect their own assets.
- Not every member in an organisation has to become a security expert, but all members should know:
  - Why security is important
  - What is expected of them
  - Which good practices to follow

The Price of Security

- Price paid for security should not exceed the value of the assets you want to protect.
- To decide what to protect you should perform some kind of risk analysis.
- know your assets and understand how they might be damaged.
- Total cost of security measures is more than the cost of “security technology” (e.g. firewalls or intrusion detection systems).

Assets

- Hardware: laptops, servers, routers, PDAs, mobile phones, smart cards, ...
- Software: applications, operating systems, database systems ...
- Data and information: data for running your business, design plans, digital content, data about customers, ...
- Services and revenue
- Reputation of enterprise, trust, brand name
- Employees’ time

Damage

- Disclosure of information, espionage
- Modification of data
- Necessary resources not available when needed
- Identity spoofing (identity “theft”)
- Unauthorised access to services
- Lost revenue
- Damaged reputation
- Theft of equipment
- ...

Security policies

- Question: Is this system secure?
- Answer: Wrong question; please be more specific about your protection requirements.
  - Protect PC from virus and worm attacks?
  - No unauthorized access to corporate LAN?
  - Keep sensitive documents secret?
  - Verify identity of partners in a business transaction?
- Security policies formulate security objectives.

Types of Policies

- Organisational security policy: laws, rules, and practices that regulate how an organisation manages and protects resources to achieve security policy objectives.
  - Organisations must comply with given regulations
- Automated security policy: restrictions and properties that specify how a computing system prevents violations of organisational security policy.
  - A detailed technical specification

Security Metrics

- very useful if we could measure security to convince managers or customers of benefits of a new security mechanism,
- First: obtain values for security relevant factors.
  - Some values can be established objectively, other values are subjective.
- Second: consolidate measurements into a single value used for comparing current security state with past state.
  - the values given to management for making security comparisons are called security metrics.

Security Metrics

- Ideally, a security metric gives quantitative result, not just qualitative statement about security of product or system.
  - Product: a package of software, firmware and/or hardware, designed for use within a multiplicity of systems.
  - System: aspecific IT installation, with a particular purpose and operational environment.
- Security metrics for a product: number of security flaws (bugs) detected, or the attack surface, i.e. the number of interfaces to outside callers or the number of dangerous instructions in the code.
- These measurements deliver quantitative results but do they really measure security?
- Secure products can be deployed in insecure ways!

Security Metrics

- Security metrics for a system: check configurations of the products deployed; may be valuable status information but does not give quantitative results.
- Alternatively measure: the cost of mounting attacks
  - Time an attacker has to invest in the attack.
  - Expenses the attacker has to incur.
  - Knowledge necessary to conduct the attack.
- The cost of discovering an attack is often much larger than the cost for mounting the attack; when attack scripts are available, launching attacks can be easy.
- Another alternative: focus on the assets in the system and measure the risks these assets are exposed to.

Overview of Risk Analysis

- Areas of engineering and business developed own disciplines and terminology for risk analysis.
- Within IT security, risk analysis is being applied
  - comprehensively for all information assets of an enterprise,
  - specifically for the IT infrastructure of an enterprise,
  - during the development of new products or systems, e.g. in software security.
- Informally, **risk** is the possibility that some incident or attack can cause damage to the enterprise.

Attacks

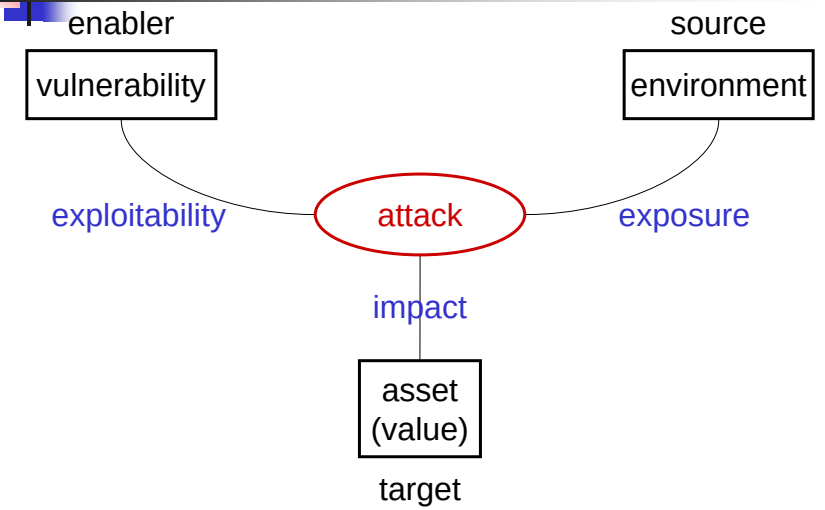
- An attack against an IT system is a sequence of actions, exploiting weak points in the system until the attacker's goals is achieved.
- To assess the risk posed by an attack, evaluate the amount of damage and the likelihood for the attack to occur, which depends on attacker's motivation and difficulty in mounting the attack, which, in turn, depends on the security configuration of the system under attack.

Risk Analysis

- To organize the process of risk analysis, look at assets, vulnerabilities, and threats.
- Risk is a function of assets, vulnerabilities, and threats:

  Risk = Assets × Threats × Vulnerabilities
- During risk analysis, values are assigned to assets, vulnerabilities, and threats.

Factors in Risk Analysis



Quantitative or Qualitative?

- Quantitative risk analysis: values taken from a mathematical domain like a probability space.
  - For example, assign monetary values to assets and probabilities to threats and then calculate expected loss.
- Qualitative risk analysis: values taken from domains that do not have an underlying mathematical structure.
  - Risk calculated based on rules that capture the consolidated advice of security experts.

Valuation of Assets

- Assets such as hardware can be valued according to their monetary replacement costs.
- For other assets such as data and information this is more difficult.
  - If business plans are leaked to competition or private data about customers is leaked to the public, there are indirect losses due to lost business opportunities
  - For lost or stolen equipment, consider value of data stored on it, and value of services that were running on it
- Value assets according to their importance.
- As a good metric for importance, ask yourself how long your business could survive when given asset has been damaged: a day, a week, a month?

Vulnerabilities

- Weaknesses of a system that could be accidentally or intentionally exploited to damage assets.
- Typical vulnerabilities in an IT system are:
  - Accounts with system privileges where the default password, such as “MANAGER”, has not been changed.
  - Programs with unnecessary privileges or known flaws.
  - Weak access control settings on resources, e.g. having kernel memory world writable.
  - Weak firewall configurations that allow access to vulnerable services.
- Sources for vulnerability updates: CERTs (Computer Emergency Response Teams), SANS, BugTraq, ...

Rating Vulnerabilities

- Rate vulnerabilities according to their impact (level of criticality):
  - vulnerability that allows an attacker to take over a systems account is more critical than vulnerability that gives access to an unprivileged user account.
  - vulnerability that allows an attacker to completely impersonate a user is more critical than a vulnerability where the user can only be impersonated in a single specific service.
- Vulnerability scanners provide a systematic and automated way of identifying vulnerabilities.
- Some vulnerability scanners also give a rating for vulnerabilities they detect.

Microsoft Severity Rating System

- Critical: Exploitation could allow propagation of Internet worm without user action.
- Important: Exploitation could compromise the confidentiality, integrity, or availability of users data, or the integrity or availability of processing resources.
- Moderate: Exploitability mitigated to a significant degree, e.g. by default configuration or by auditing.
- Low: Exploitation extremely difficult, or impact is minimal.

Common Vulnerability Scoring Scheme

Basic metrics		Temporal metrics	Environmental metrics	
Access vector	Confidentiality impact	exploitability	Collateral damage potential	Confidentiality requirement
Access complexity	Integrity impact	Remediation level	Target distribution	Integrity requirement
Authenti-cation	Availability impact	Report confidence		Availability requirement

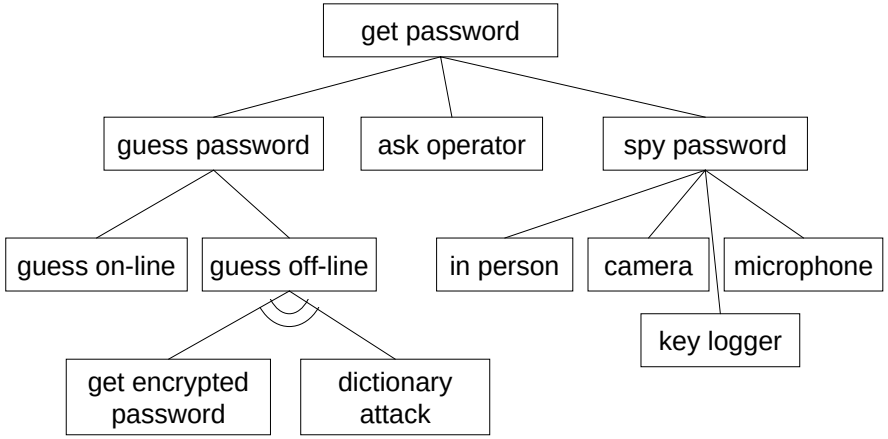
Threats

- Threats: actions by adversaries who try to exploit vulnerabilities to damage assets.
- Various ways for identifying threats:
  - Categorize threats by the damage done to assets.
  - Identify source of attacks. Would adversary be member of your organisation or outsider, contractor or former member? Has adversary direct access to your systems or is attack launched remotely?

Attack Trees

- To analyze how an attack is executed in detail.
- Attack may start with innocuous steps, gathering information needed to gain privileges on one machine, then jump to another machine, until the final target is reached.
- To get a fuller picture of potential threats, attack trees can be constructed.

Attack Tree – example



Rating Threats

- Rate threats according to their likelihood.
- The likelihood of a threat depends on
  - difficulty of the attack,
  - motivation of the attacker,
  - number of potential attackers.
- Attack scripts automate attacks; likely to be available to large set of attackers.
- Hence, such attacks rated more likely than individual hand-crafted attack.

Calculating Risk

- In quantitative risk analysis, expected losses computed based on monetary values for assets and probabilities for likelihood of threats.
  - Advantage: uses well established mathematical (probability) theory
  - Drawback: ratings obtained often quite imprecise and based on educated guesses.
  - Quality of results cannot be better than quality of inputs provided.
- Quantitative risk analysis works in some areas.
- More often we can only obtain ratings where there is no justification to have these inputs processed by an established mathematical calculus.

Calculating Risk

- In qualitative risk analysis, rate
  - assets on a scale of *critical – very important – important – not important*.
  - vulnerabilities on a scale of *has to be fixed immediately – has to be fixed soon – should be fixed – fix if convenient*.
  - threats on a scale of *very likely – likely – unlikely – very unlikely*.
- For finer granularity of scaling you could use numerical values from 1 to 10.
- Guidance needed on how to assign ratings.
- The mapping of the ratings for assets, vulnerabilities, and threats to risks often given by a table that reflects the judgement of security experts.

Risk Mitigation

- Risk analysis produces a prioritized list of threats, with recommended countermeasures to mitigate risk.
- Analysis tools usually have a knowledge base of countermeasures for the threats they can identify.
- General risk mitigation strategies:
  - Accept risk (and live with it); there may be good reasons to do so.
  - Avoid risk: eliminate a vulnerability that causes the risk; drop product feature that has a vulnerability.
  - Limit risk: use controls to make a threat less likely.
  - Transfer risk: buy insurance.

Summary

- Security management creates the context in which individual security mechanisms operate.
- Without good security management, even strong security mechanisms may be ineffective
- Risk analysis gives management information about the risks an organisation faces and the countermeasures that can be taken.
- Security management guidelines and risk analysis methods can be described as organized common sense.