Managing Security

Vítor Francisco Fonte, vff@di.uminho.pt, University of Minho, 2025

Overview

- Managing security
- Measuring security
- Security policies
- Security standards
- Risk and threat modelling

Security Management

- **A management decision**
  - Significant financial cost
  - Significant organisational impact
- **Why do it?**
  - The cost of doing nothing
  - Legal or regulatory compliance
  - Competitive advantage
- **How to do it?**
  - Analyse risks and threats
  - Standards and best practices
- **Security policy**
  - Objectives, procedures and controls
  - Technical and organisational measures

Security Management

- Security is a **“people problem”** as technology is not enough
- **Legal systems define boundaries of acceptable behaviour**
  - Data protection, computer misuse
- **Management is ultimate responsible for security in an organisation**
  - Users have to cooperate and comply to the laid out rules
  - Correct deployment and operation of technical measures
  - Make it clear that security measures have full support of senior management

Security Management

A challenge for the organisation

- Tradeoffs:
  - **Security vs. convenience**
  - **Cost vs. investment**
- Impacts on the organisation:
  - **Structure, procedures, financials**
- Impacts on people and entities:
  - **Staff** and **management**
  - **External entities** (suppliers, customers, partners)

Security Management

Assets, attacks and attackers

- **Assets**
  - What, where, value?
- **Vulnerability, exploitability and exposure:**
  - Publicly known, what kind, how, from where?
  - Social engineering, technical exploitation threats
- **Attacks**:
  - Complex, automated, costly, opportunistic?
  - Conditions determine viability and yield of an attack
- **Attackers**:
  - Motivations, resources, skill sets?

Security Policies

- ***Crucial*** component of **security management** in an organisation
- Can be an **informal security policy** document:
  - **Why security matters** for members and for the organisation,
  - **What is expected** from each of its members, and
  - **Which security practices** they should follow.
- Supported by **security-awareness training**
  - And announced and non-announced exercises

Security Policies

- Or a thorough, **structured document**, stemming from a two-step process:
  - Systematic assessment of **information security risks;**
  - Definition and enforcement of **risk mitigation measures.**
- Often follows a **standard** or a well-established **code of best practice**
- **Compliance** with standards may actually be **required**:
  - Involves scrutiny by external, independent consultants and auditors.

Security Policies

- **Security policy**:
  - A statement that defines the security ***objectives*** of an organisation;
  - It has to state ***what*** needs to be protected;
  - It may also indicate ***how*** this is to be done.
- **Security policy objective**:
  - A statement of intent to protect an identified asset.
- Applicable to very **different contexts** with **different granularities**.

Security Policies

- How to meet the objectives at the organisational level:
  - **Organisational security policy**: The set of laws, rules, and practices that regulate how an organisation manages, protects, and distributes resources to achieve specified security policy objectives.
- Organisational security policies can be supported by technical means:
  - **Automated security policy**: The set of restrictions and properties that specify how a computing system prevents information and computing resources from being used to violate an organisational security policy.
  - E.g. Define access control lists and firewall settings, stipulate the services that may be run on user devices, and prescribe the security protocols for protecting network traffic.

Security Policies

IT product and service development

- What about **organisations developing IT** services and products?
- Project teams must have deep understanding of:
  - Execution environment and **expected threats**;
  - **Compliance requirements** for specific categories of data;
  - **Common** software development **weaknesses**;
  - Understand and implement **risk mitigation strategies and practices**.
- IT organisations must **define and implement security-focused policies**

Security Standards

- Set of **criteria or guidelines** that organisations can follow to **protect sensitive information**, ensuring it remains confidential, integral, and available.
- Provides a **structured approach** to managing **security risks**.
- Developed and maintained by well-established international, national, or sectorial organisations.
- May serve as a blueprint for achieving **regulatory compliance** by appointed accreditation registrars.

Security Standards

Compliance

- Compliance with **specific standards** can be **required** in specific sectors:
  - E.g. PCI DSS (financial, international), HIPAA (health, US)
- Compliance with **other standards** can be **voluntary:**
  - Can be seen as a **codes of best practice**
  - E.g. **ISO/IEC 27001** and supporting standards (general, international)

ISO/IEC 27000 Series

ISO 27001

- **ISO 27001** is the standard for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS) within the context of an organisation (scope).
- Includes requirements for the assessment and treatment of information security risks.
- **Generic requirements**, applicable to all organisations, regardless of type, size or nature.
- Organisations can apply for **certification** by **accreditation registrars**. Requires recertification audits every three years to maintain compliance.

ISO/IEC 27000 Series

ISO 27001 organisation management requirements

- Systematically **examine the organisation's information security risks**, taking account of the threats, vulnerabilities, and impacts;
- **Design and implement** a coherent and comprehensive suite of **information security controls** and/or **other forms of risk treatment** (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to **ensure that the information security controls continue to meet the organisation's information security needs** on an ongoing basis.

ISO/IEC 27000 Series

Stages of ISO 27001 certification process

The current state of an organisation is compared to the standard; any identified shortcomings must be addressed.

- **Stage 1** is a preliminary review of the ISMS. It includes checks for the existence and completeness of key documentation, such as the organisation's information security policy, Statement of Applicability (SoA), and Risk Treatment Plan (RTP).
- **Stage 2** is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation.
- **Ongoing** involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard.

ISO/IEC 27000

ISO 27001 key areas of focus

- **Organisational controls**: Address organisational structures, policies, procedures, and responsibilities related to information security.
- **People controls**: Security awareness, training, and management of personnel, including access controls and security clearances.
- **Physical controls**: Physical security of information assets, including access to premises, equipment, and data storage.
- **Technological controls**: Implementing security measures using technology, such as firewalls, intrusion detection systems, and encryption.

ISO/IEC 27000 Series

Supporting (supplemental) documents

- Guidance for **implementation** of information **security controls**:
  - **ISO 27002** provides the original reference documentation.
  - **ISO 27017** refines and expands 27002 for cloud services, applicable to both cloud service providers and customers.
- Another relevant supporting document:
  - **ISO 27005** provides guidance on systematically identifying, assessing, evaluating and treating information security risks.

Measuring Security

- Well-founded management decisions heavily relies on inputs
  - E.g. Which product alternative is the most secure? What is the expected return on investment?
- **Measurements**:
  - Values may be obtained for security-relevant factors
- **Metrics:**
  - Measurements can consolidated in a single value
- Examples:
  - Number of known security flaws
  - Size of an attack surface (external-facing interfaces)

Measuring Security

In practice

- **Unfortunately it is hard to measure security in a meaningful way:**
  - How comparable is a particular metric on two slightly different products?
  - How relevant is the comparison of different metrics on the same product?
  - How relevant is actually the value of a measurement or a metric?
- Even if a measurement of a product is **indicative of its potencial security**
  - A **secure product** can always be **deployed in an unsecured manner**
  - So, how to measure security of a deployed product or system?

Measuring Security

In practice

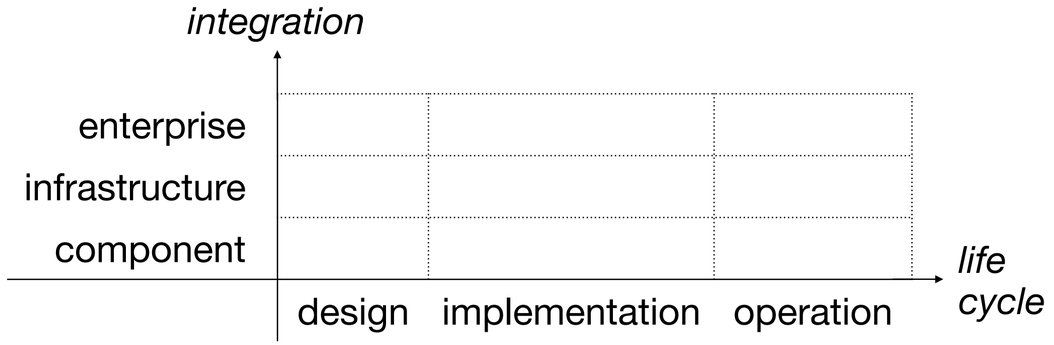
- At best, we may have **acceptable metrics** for **individual aspects** of security
  - May be useful for **comparison** of the **current state** against a **baseline**
- Alternatively:
  - Estimate the **cost of mounting an attack**
  - Estimate the **risks the assets are exposed to**

Risk and Threat Analysis

- Informal definition of **risk**:
  - The possibility some incident or attack can cause damage to an organisation
- Need of a structure and systematic approach to risk analysis:
  - Note that damage to an asset may facilitate a next attack step
  - Danger of getting lost in details of particular security problem
  - Danger of failing to establish a comprehensive overview of the risks

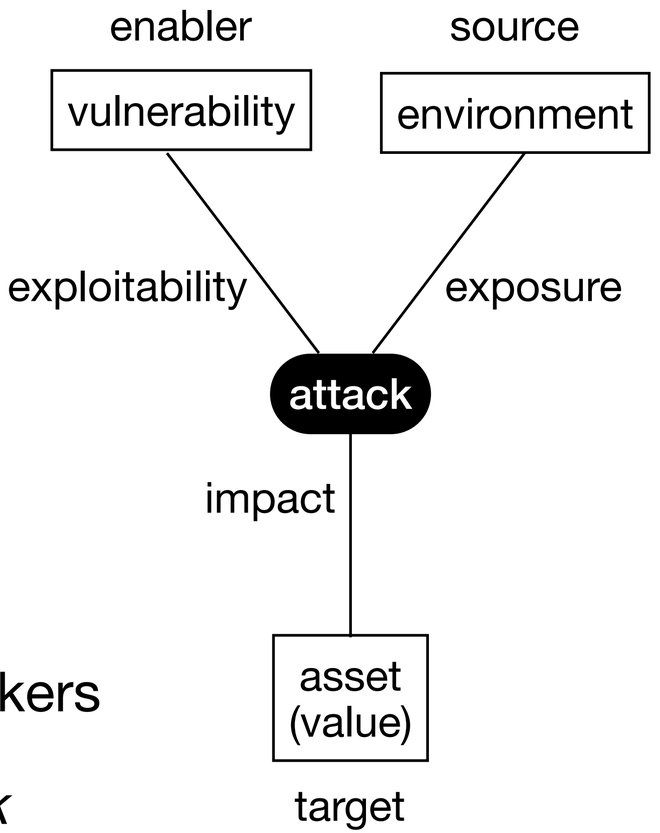
Risk and Threat Analysis

- Different ways of structuring the assessment of potential damage:
  - Risk analysis, threat analysis, vulnerability scoring
  - Different names and focus, same objective
- Different **phases** and **granularity**:
  - Design, implementation and operation
  - Component, infrastructure, organisation



Risk Analysis
Factors

- To assess the **risk of an attack**:
  - Evaluate its **impact** to the value of an asset
  - And the **likelihood** of occurrence
- **Likelihood** of occurrence depends of:
  - **Exploitability** of the vulnerabilities
  - **Exposure** of the system to attackers
  - Also of perception of impunity, number of potential attackers
  - *And of security configurations of the system under attack*



Risk and Threat Analysis

- A **system** consists of **resources** and of **agents** operating on those resources
  - Resources are assets
  - Agents are subjects (in Access Control)
- Corruption of:
  - Resource: confidentiality, integrity, availability
  - Agent: authentication, authorisation, non-repudiation

Assets

- All risk and threat analysis must **Identify** and **value** the **assets**
- **Identifying assets:**
  - Hardware, software, data and information, ***reputation***
- **Value of assets:**
  - Monetary replacement cost and indirect costs (e.g. loss of business)
  - According to their importance (e.g. survivability of organisation without asset)

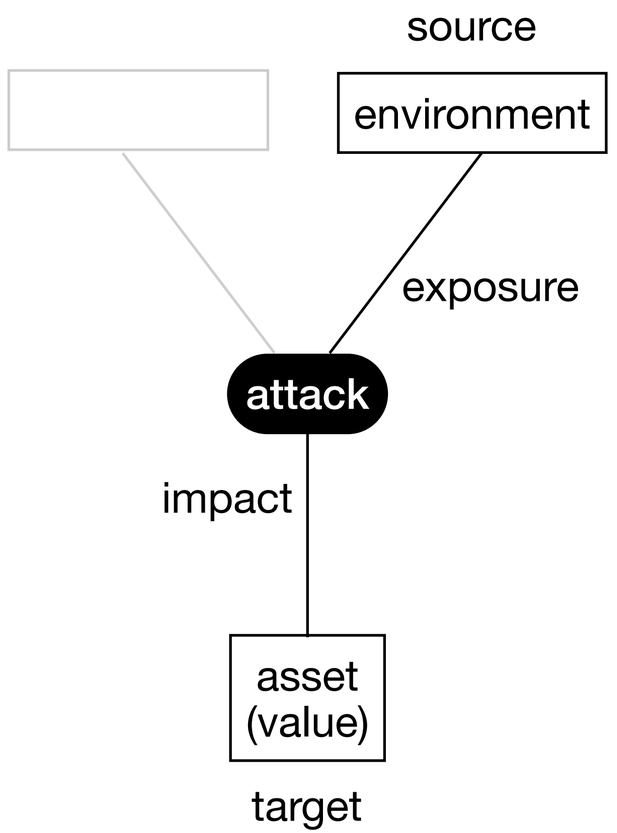
Threats

- **Threat:**
  - Undesirable negative impact on an asset
  - Materialises when an attack succeeds
- **Categorising threats by source** (who/where is the adversary?):
  - A member, a contractor, a former member, direct access to systems?
- **Categorising threats by impact**:
  - E.g. Microsoft’s STRIDE threat model

Threat Analysis

Factors

- **Threat analysis**: risk analysis at the **design stage**
- **Conceptual model** with assets, agents, and (perhaps) the environment
- **No implementation vulnerabilities** to consider
- For each threat it rates the **impact** (potential damage) and the **exposure**
- Points out **security features** that must be part of the system design



Threat Analysis

The STRIDE threat modelling

- **S**poofing identities: an agent pretends to be somebody else; this can be done to avoid responsibility or to misuse authority given to someone else. **Control: Authentication.**
- **T**ampering with data: an agent violates the integrity of an asset; e.g. security settings are changed to give the attacker more privileges. **Control: Integrity.**
- **R**epudiation: an agent denies having performed an action to escape responsibility. **Control: Non-Repudiation.**
- **I**nformation disclosure: an agente violates the confidentiality of an asset; information disclosed to the wrong parties may lose its value (e.g. trade secrets). **Control: Confidentiality.**
- **D**enial of service an agent violates the availability of an asset; denial-of-service attacks can make resources unavailable. **Control: Availability.**
- **E**levation of privilege: an agent gains more privileges beyond its entitlement. **Control: Authorisation.**

Vulnerabilities

- **Vulnerability:**
  - **Weakness** of a system that could be accidentally or intentionally **exploited** to **damage assets**
  - E.g. incorrect privileges on accounts or on programs, insecure configuration settings, software flaws, weak access control on resources
- **Risk analysis** must:
  - Performed at the **implementation or deployment stages** of a system
  - Must **identify vulnerabilities** and **their exploitability**
  - Can be partially automated or assisted by **vulnerability scanning tools**

Vulnerabilities

Common Vulnerabilities and Exposures (CVE)

- **Common Vulnerabilities and Exposures (CVE)**: searchable database of publicly disclosed cybersecurity vulnerabilities maintained by MITRE.
  - Project information and searchable database: http://cve.org/
- **National Vulnerability Database (NVD)**: database maintained by NIST that provides information about CVEs, including CVSS scores.
- **CVE Details**: database that provides additional information about CVEs, such as exploits and advisories.

Vulnerabilities

Simplified structure of a CVE record

- **CVE ID**: A unique identifier in the format "CVE-YYYY-NNNNN" (where YYYY is the year and NNNNN is a sequence number).
- **CVE Numbering Authority (CNA)**: Vendor, researcher, open source, CERT, hosted service, bug bounty provider, and consortium organisations authorised by the CVE Program.
- **Title and brief description**: A concise title and explanation of the security vulnerability or exposure.
- **Affected products and versions**: Information about the software, hardware, or systems that are vulnerable.
- **References**: Links to relevant vulnerability reports, advisories, and other resources.
- **Other metadata**: Information about the CVE record, such as the status (e.g., PUBLISHED, REJECTED), who requested it, and when it was requested.

Vulnerabilities

Example of a CVE entry

- **CVE ID**: CVE-2025-0001
- **CNA:** Switzerland National Cyber Security Centre (NCSC)
- **Title and description**: Authenticated Arbitrary File Read Vulnerability. Abacus ERP versions older than 2024.210.16036, 2023.205.15833, 2022.105.15542 are affected by an authenticated arbitrary file read vulnerability.
- **Affected products and versions**: Affected from 0 before 2024.210.16036, …
- **References**: https://borelenzo.github.io/stuff/2025/02/15/CVE-2025-0001.html
- **Status**: PUBLISHED
- **CWE:** CWE-36 - Absolute Path Traversal
- **CVSS**: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N, score 6.5 (medium)

Vulnerabilities

Useful resources for developers to enhance software security

Top 10 CWE 2024 (general software)

1. Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')
2. Out-of-bounds Write
3. Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')
4. Cross-Site Request Forgery (CSRF)
5. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
6. Out-of-bounds Read
7. Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')
8. Use After Free
9. Missing Authorisation
10. Unrestricted Upload of File with Dangerous Type

Source: https://cwe.mitre.org/top25/

Top 10 OWASP 2021 (web-based software)

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery

Source: https://owasp.org/www-project-top-ten/

Common Vulnerability Scoring System

- Helps to **prioritise vulnerability remediation** efforts
- Standardised way to **evaluate the severity** of security flaws **(vulnerabilities)**
- Adopted by:
  - National Vulnerability Database (NVD): https://nvd.nist.gov/
  - Open Source Vulnerability Database (OSVDB): https://osv.dev/
- More information about CVSS: https://www.first.org/cvss/

Common Vulnerability Scoring System

- Vulnerabilities **numerically scored** according to a set of **metric groups** (0-10)
- **Overall scores** for specific combination of metric groups
  - Can be translated into **qualitative representation** (eg. Low)
- Assessments can also be **represented as a vector strings** (compressed textual representation of the values used to derive the score)
  - E.g. CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Score calculator: https://www.first.org/cvss/calculator/4-0/
  - Can also be used as https://www.first.org/cvss/calculator/4-0#<*vector-string*>

Common Vulnerability Scoring System

CVSS 4.0 overview

- **CVSS 4.0 metric groups:**
  - Base and Threat (mandatory)
  - Environmental (optional)
  - Supplemental (optional, do not affect scores, new in 4.0)
- **CVSS 4.0 scores:**
  - Base, Base+Threat, Base+Environmental, Base+Threat+Environmental

Common Vulnerability Scoring System

CVSS 4.0 metric groups

- **Base Metrics** (*mandatory*): Represent the intrinsic characteristics of a vulnerability that are constant over time and across user environments.
  - Attack Vector (AV), Attack Complexity (AC), User Interaction (UI), Privileges Required (PR), Vulnerability Exploitability (E), Vulnerability Outcome (Confidentiality VC, Integrity VI, Availability VA), Safety (S)
- **Threat Metrics** (*mandatory*): Represent the current exploitation status of the vulnerability.
  - Exploit Maturity (E), Remediation Level (RL), Report Confidence (RC)

Common Vulnerability Scoring System

CVSS 4.0 metric groups

- **Environmental Metrics** (*optional*): Accounts for the characteristics of a vulnerability that are relevant to a specific user's environment.
  - Modified Base Metrics (customised values of Base metrics), Security Requirements (Confidentiality CR, Integrity IR, Availability AR, Safety SR)
- **Supplemental Metrics** (*optional*): Provide additional context but *do not impact the numeric score*. They help organisations better understand the risk.
  - Automatable (AU), Recovery (RE), Value Density (V), Vulnerability Response Effort (RE), Provider Urgency (PU)

Common Vulnerability Scoring System

CVE-2022-41741

- **Description**:
  - A vulnerability in the module ngx_http_mp4_module might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The attack is only possible if an attacker can gain privileged access to the host running NGINX, place a specially crafted audio or video file within the webroot, and then trigger NGINX to process the specially crafted file.
- **Base score: 7.3**
  - CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Common Vulnerability Scoring System

CVSS 4.0 for CVE-2022-41741: Base metric group

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialised conditions or advanced knowledge are required.
Attack Requirements	Present	Multiple conditions that require target specific reconnaissance and preparation must be satisfied in order to achieve successful exploitation of this vulnerability.
Privileges Required	Low	An attacker must be able to place a file within the web root to be processed by NGINX.
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Integrity	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Availability	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Subsequent System Confidentiality	None	There is no impact to the subsequent system confidentiality.
Subsequent System Integrity	None	There is no impact to the subsequent system integrity.
Subsequent System Availability	None	There is no impact to the subsequent system availability.

Attacks

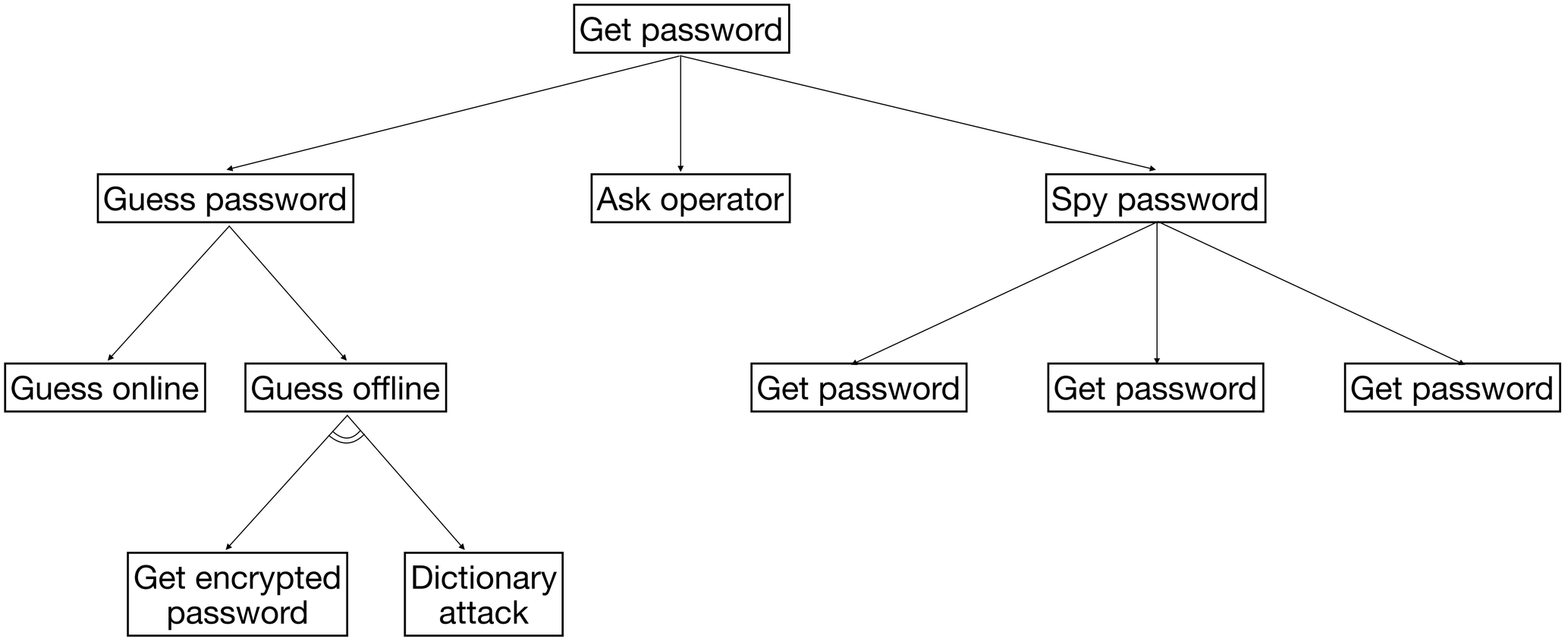
- **Attack:**
  - Sequence of actions, performed by an attacker
  - In order to achieve a security goal
  - E.g. information gathering, gain of access
- A **threat** materialises when an **attack succeeds**
  - How to **assess a threat** to the system (conceptual stage)?
  - How to **assess the risk** of an attack (implementation/deployment stage)?

Attack Trees

- Formalised and structured method for **threat analysis**
- The **root is a threat** to the system
- A **node is a goal** that **must be achieved** for the **attack succeed**
- A goal may be broken up in **subgoals**
- **AND** node: to reach that goal all subgoals must be achieved
- **OR** node: to reach that goal one of the subgoals must be achieved

Attack Trees

Attack tree for obtaining a user password



Attack Trees

Estimating impact and/or likelihood of an attack

- **Values can be assigned to edges:**
  - Estimated cost of achieving a goal, or the likelihood of achieving it, etc…
- Values can be used for:
  - Identification of the **cheapest**, or the **more likely attack** to succeed
- **Requires significant experience:**
  - Unreasonable results? Values may have to be adjusted
  - Taking too long? Stop breaking up subgoals

Estimating the Severity of an Attack

- **Severity of an attack:**
  - Likelihood it will be **launched**, likelihood it will **succeed**, **damage** it might do
- **Likelihood depends of:**
  - **Difficulty** of attack, existing **countermeasures**
  - M**otivation** of attacker, **number of potential attackers,**
- **The DREAD methodology:**
  - Systematic **measure of the severity of an attack**
  - **Complements** the **STRIDE** threat modelling

Estimating the Severity of an Attack

The DREAD methodology

- **Quantitative assessment of the severity of a threat:**
  - Severity is rated on a set of **factors**
  - According to a **scale**
- **Overall severity:**
  - **Sum of the ratings** for each factor (or average)
- **Requires** a lot of **experience:**
  - Ratings are **subjective**

Estimating the Severity of an Attack

The DREAD methodology

- **The DREAD factors:**
  - **D**amage potential: Relates to the values of the assets being affected.
  - **R**eproducibility: Attacks that are easy to reproduce are more likely to be launched from the environment than attacks that only work in specific circumstances.
  - **E**xploitability: Captures the effort, expertise, and resources required to launch an attack.
  - **A**ffected users: The number of assets affected contributes to the damage potential.
  - **D**iscoverability: Will the attack be detected? In the most damaging case, an organisation may never know that the system has been compromised.

Estimating the Severity of an Attack

The DREAD methodology

- **How DREAD works:**
  - **Identify threats**: The first step is to identify potential security threats and vulnerabilities.
  - **Assess each threat**: Each threat is then assessed based on the five DREAD factors, typically using a scaled grading system.
  - **Prioritise threats**: By evaluating and scoring each threat based on the DREAD factors, organisations can determine the severity of each threat and prioritise which ones should be addressed first.

Estimating the Severity of an Attack

DREAD assessment of a potential SQL injection in an online bank

- **Damage potential**: 9 (High). A successful SQL injection could lead to unauthorised access to sensitive user data, financial data breaches, and potentially significant financial loss.
- **Reproducibility**: 6 (Moderate). The vulnerability might be reproducible, but the exact steps might depend on the input sanitisation measures in place.
- **Exploitability**: 9 (High). SQL injection vulnerabilities are well-known and readily exploitable, with readily available tools and techniques.
- **Affected users**: 9 (High). Potentially all users of the online banking platform could be affected.
- **Discoverability**: 9 (High). SQL injection vulnerabilities are easily detectable through automated vulnerability scanners and penetration testing.
- **Overall severity**: 8.4 (High). High-severity threat.

Quantitative and Qualitative Risk Analysis

- Informal calculation of **risk:**
  - *Assets x Threats x Vulnerabilities*
- In this formula “Threats” stands for:
  - Potential negative impact on assets, and
  - Likelihood damage will occur

Quantitative Risk Analysis

- **Quantitative risk** analysis takes ratings from a **mathematical domain**:
  - Assign monetary value to assets
  - Assign probabilities to attacks, and
  - Calculate the expected loss.
- Unfortunately, inputs are often just **educated guesses**:
  - Quality of the results cannot be better than the quality of the inputs
  - Lack of precision in the inputs **does not justify mathematical treatment**

Qualitative Risk Analysis

- **Qualitative risk** analysis takes ratings from domains with **no mathematical structure**:
  - Assets could be rated on a scale of “critical", “very important”, “important”, “not important”
  - Criticality of vulnerabilities could be rated on a scale of “has to be fixed immediately”, “has to be fixed soon”, “should be fixed”, “fix if convenient”.
  - Threats could be rated on a scale of “very likely”, “likely”, “unlikely”, “very unlikely”.

Qualitative Risk Analysis

- **CVSS** and **DREAD** follow a **qualitative risk** analysis approach
- CVSS:
  - Individual ratings are mapped to weights that serve as input to a combination algorithm that calculates a risk value (0 to 10)
- DREAD:
  - A risk value is the result of averaging the five ratings (scale The average of the five ratings is the risk value (1 to 10)

Countermeasures: Risk Mitigation

- Result of a risk analysis:
  - Prioritised list of threats, together with
  - Recommended countermeasures to mitigate risk.
- Note that risk analysis tools often come with a **knowledge base of countermeasures** for the threats they can identify.

Countermeasures: Risk Mitigation

Return on Security Investment (ROSI)

- Risk analysis can be used for calculating the **Return on Security Investment**

$$ROSI = \frac{Benefits\ of\ Investment - Cost\ of\ Investment}{Cost\ of\ Investment}$$

- Example: ROSI of Preventing a data breach

  If a security investment prevents a data breach that would cost €500,000 and the investment cost is €200,000, the ROSI would be 150% (€500,000 - €200,000) / €200,000 = 150%

Countermeasures: Risk Mitigation

Return on Security Investment (ROSI)

- Helps justify cybersecurity investments by demonstrating the financial value of risk reduction and cost avoidance:
  - **Justifies cybersecurity investments**: Helps demonstrate the value of security investments to stakeholders.
  - **Prioritises security initiatives**: Enables organisations to focus on the most critical security investments.
  - **Improves security posture**: Encourages organisations to proactively address security risks.

Countermeasures: Risk Mitigation

STRIDE threat & mitigation techniques

Threat Type	Mitigation Techniques
Spoofing Identities	1. Appropriate authentication 2. Protect secret data 3. Don’t store secrets
Tampering with data	1. Appropriate authorization 2. Hashes 3. MACs 4. Digital signatures 5. Tamper resistant protocols
Repudiation	1. Digital signatures 2. Timestamps 3. Audit trails

Threat Type	Mitigation Techniques
Information disclosure	1. Authorization 2. Privacy-enhanced protocols 3. Encryption 4. Protect secrets 5. Don’t store secrets
Denial of service	1. Appropriate authentication 2. Appropriate authorisation 3. Filtering 4. Throttling 5. Quality of service
Elevation privilege	1. Run with least privilege

Countermeasures: Risk Mitigation

Threat profiles

- Once threats and corresponding countermeasures are identified, it is possible to derive a **threat profile** with the following criteria:
  - **Non mitigated threats**: Threats which have no countermeasures and represent vulnerabilities that can be fully exploited and cause an impact.
  - **Partially mitigated threats**: Threats partially mitigated by one or more countermeasures and can only partially be exploited to cause a limited impact.
  - **Fully mitigated threats**: These threats have appropriate countermeasures in place and do not expose vulnerabilities.

Countermeasures: Risk Mitigation

Baseline protection

- Always do risk analysis before deciding on security measures, right?
  - Results may already be outdated when by the end of this process
  - Costs may be difficult to justify to management
- In practice, organisations may opt for **baseline protection**
  - Analysis of security requirements for typical cases, and
  - Recommends security measures deemed adequate.

Countermeasures: Risk Mitigation

BSI IT baseline protection (IT-Grundschutz)

- Provided by the German Information Security Agency (BSI)
- Purpose: The primary goal is to provide a structured and systematic approach to securing information technology in organisations, ensuring an adequate and appropriate level of security. Based on ISO/IEC 27001.
- Methodology: Uses a modular approach, with standardized security measures and recommendations for various aspects of IT security, including organisational, personnel, infrastructural, and technical measures.
- Key components:
- Risk Assessment: Identifying and evaluating potential security risks within the organization.
- Security Measures: Implementing well-proven technical, organizational, personnel, and infrastructural safeguards.
- Action Implementation Plan: Developing a plan to address identified risks and implement necessary security measures.
- Continuous Monitoring and Maintenance: Regularly checking for compliance with the ISMS and maintaining the security measures.

Countermeasures: Risk Mitigation

BSI IT baseline protection (IT-Grundschutz)

- **Provider:** German Information Security Agency (BSI).
- **Purpose**: The primary goal is to provide a structured and systematic approach to securing information technology in organisations, ensuring an adequate and appropriate level of security. Based on ISO/IEC 27001.
- **Targets**: Designed for companies, authorities, and other stakeholders active in the field of critical data security.
- **Methodology**: Uses a modular approach, with standardised security measures and recommendations for various aspects of IT security, including organisational, personnel, infrastructural, and technical measures.

Countermeasures: Risk Mitigation

BSI IT baseline protection (IT-Grundschutz)

- Key components:
  - **Risk assessment**: Identifying and evaluating potential security risks within the organisation.
  - **Security measures**: Implementing well-proven technical, organisational, personnel, and infrastructural safeguards.
  - **Implementation plan**: Developing a plan to address identified risks and implement necessary security measures.
  - **Continuous monitoring and maintenance**: Regularly checking for compliance with the ISMS and maintaining the security measures.
- A compendium provides a detailed catalog of security measures and recommendations, helping organisations implement the baseline protection effectively.

Countermeasures: Risk Mitigation

BSI IT baseline protection (IT-Grundschutz)

- Main steps of the process:
  - The IT network is defined.
  - IT structure analysis is carried out.
  - Protection needs determination is carried out.
  - A baseline security check is carried out.
  - IT baseline protection measures are implemented.
- More information: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html