Zurich University of Applied Sciences

zh aw

10. Security Risk Analysis

Prof. Dr. Marc Rennhard
Institut für angewandte Informationstechnologie InIT
ZHAW School of Engineering
rema@zhaw.ch

Content

- Introduction to Security Risk Analysis
- The basic process to perform security risk analysis
- NIST 800-30: A very simple but also limited methodology to perform security risk analysis
- OWASP Risk Rating Methodology: A more structured approach towards security risk analysis
- Risk Mitigation: What can we do if we identify risks that are "too high"

Goals

- You understand the purpose of security risk analysis during the secure software development process
- You know the basic security risk analysis process and can apply it when performing threat modeling or security testing
- You know the risk rating methodologies according to NIST 800-30 and OWASP and can apply them to perform risk analysis yourself

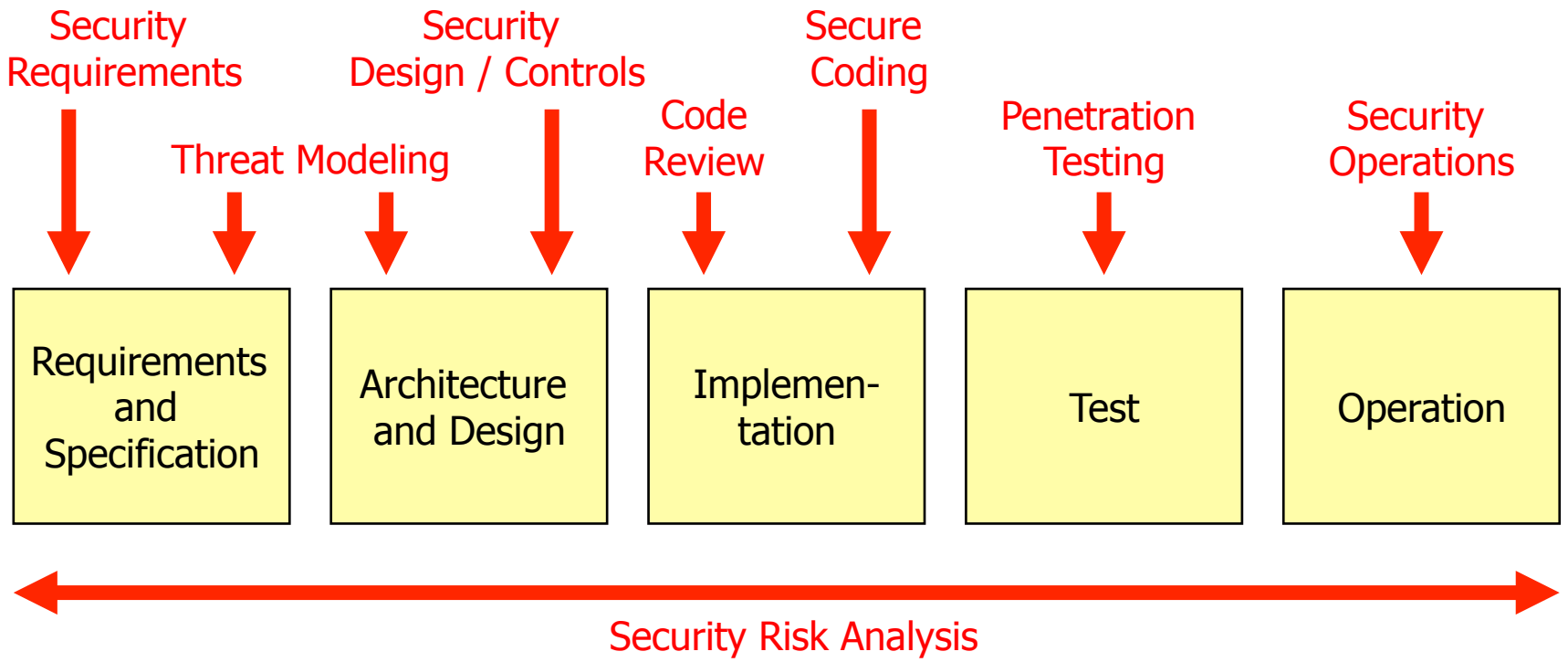
Zurich University of Applied Sciences

zh aw

Introduction to Security Risk Analysis

Security Risk Analysis (1)

- The goal of security risk analysis is to rate the risk (the criticality) of system weaknesses to make reasonable decisions about "where to make security investments"
- Security risk analysis is a horizontal activity during secure software development as it supplements many of the other activities



Security Risk Analysis (2)

Zurich University of Applied Sciences

Some examples where security risk analysis is useful:

- During threat modeling
  - To assess the risk of the uncovered vulnerabilities, which allows making reasonable decisions with respect to necessary additional security requirements
- When performing code reviews
  - To assess the risk of a discovered bug, which provides the basis to make the right decisions about the necessity of corrective measures
- During penetration testing
  - Like code reviews: To assess the risk of a discovered vulnerability to make the right decisions about the necessity of corrective measures
- During operations
  - To assess the risk of operational issues, e.g. whether redundant systems should be used and how frequently backups should be made

Security Risk Analysis (3)

- Risk analysis in general should be an essential activity during any software project and goes beyond security risks, e.g.:
  - Technical risks (are there technical risks that may endanger the project from working as specified?)
  - Personnel risks (are there single persons in the project team that would be difficult to replace?)

- Here, the focus is on security risks, i.e. risks that could endanger one or more of the security goals: confidentiality, integrity, availability

- In addition, we focus on risks that arise due to malicious use by internal or external attackers
  - There are also security risks due to accidents or non-intentional misuse, e.g. incorrect handling of backup tapes, which should be considered as well

Quantitative Risk Analysis

- One way to do risk analysis is to express risks as financial loss, or Annualized Loss Expectancy (ALE)
- It is calculated as follows:
  - SLE: Single Loss Expectancy
  - ARO: Annualized Rate of Occurrence

$$ALE = SLE \times ARO$$

- Example:
  - We expect that our user database is compromised every 5 years (ARO = 1/5), with an SLE of CHF 100'000 → ALE = 20'000 CHF/year
- Advantages: Shows the costs of risks and the maximum amount of money one should spend to fix the problem
- Disadvantages: very difficult to make reasonable guesses for SLE and ARO, e.g.
  - What's the financial loss of a website defacement
  - How many times will an SQL injection vulnerability be exploited in a year?

Qualitative Risk Analysis

- As a result, a qualitative risk analysis is often preferred in security risk analysis
- Given a threat, qualitative risk analysis estimates the likelihood of occurrence and the resulting impact of the attack
- Likelihood and impact are not expressed in numbers, but in a relatively small number of levels (e.g. 3 or 5)
  - More than 5 levels does hardly make sense due to the qualitative nature of the approach
- Based on the determined levels for likelihood and impact, a risk value is "calculated", using also only a few levels
- Risks above a certain level usually must be reduced with appropriate countermeasures

Zurich University of Applied Sciences

zh aw

Security Risk Analysis – The Process

Security Risk Analysis – The Process (1)

We identify 4 steps in the (qualitative) security risk analysis process:

1. Identify security threats that should be risk-rated by describing the following for each threat:
   - The actual attack that is used
   - The threat agent (who attacks)
   - The vulnerabilities that are involved / exploited
   - Security controls (if any) that are already in place that help protecting from the threat

This step is covered in other chapters of this course:

- Finding and Exploiting Vulnerabilities in Web Applications (chapter 7)
- Threat Modeling (chapter 9)
- Penetration Testing (chapter 11)
- Security Testing with Tools (Security Lab)

Security Risk Analysis – The Process (2)

2. For each threat, estimate the likelihood of a successful attack and its business impact
3. For each threat, determine the risk based on likelihood and impact
4. Risk mitigation: For each threat and associated risk, decide on the actions to be taken (if necessary), e.g. additional security requirements or specific security controls

Covered in this chapter

The actual selection of corrective measures is covered in other chapters of this course:

- Secure Programming (chapters 3 & 4)
- Security Controls (chapter 5)
- Java Web Application Security (chapter 8)

Methods to Perform Security Risk Analysis

- To actually perform the security risk analysis process, it's best to use one of several methods that were proposed to perform this task
  - Basically, the methods are similar to each other in the sense that they usually follow the 4 steps

- Here, we introduce two methods:

- NIST 800-30: Risk Management Guide for Information Technology Systems
  - A very simple methodology that shows the basic idea of qualitative risk analysis without providing much guidance to pick appropriate values for likelihood and impact

- OWASP Risk Rating Methodology
  - Basically an extension of NIST 800-30 that provides more help / guidance to pick appropriate values for likelihood and impact

Zurich University of Applied Sciences

zh aw

Security Risk Analysis – NIST 800-30

NIST 800-30 – Likelihood Determination

- The likelihood of successful attack is described as high, medium, or low

- The three levels are defined / described as follows:

Likelihood Value	Definition
High	The threat agent is highly motivated and sufficiently capable, and controls to prevent the risk from occurring are ineffective.
Medium	The threat agent is motivated and capable, but controls are in place that may impede successful materialization of the risk.
Low	The threat agent lacks motivation or capability, or controls are in place to prevent or at least significantly impede the risk from occurring.

NIST 800-30 – Impact Determination

- Likewise, there are three levels to determine the impact:

Magnitude of Impact	Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

NIST 800-30 – Risk Determination

- The overall risk is then determined according to the following table
  - It's basically simply a "product" of likelihood and impact

	Impact		
Likelihood	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

- Description of the risk levels:
  - High – indicates a strong need for corrective measures; an existing system may continue to operate, but corrective actions should be implemented as soon as possible
  - Medium – indicates that corrective actions are needed and should be implemented within a reasonable time (e.g. next major release)
  - Low – indicates that the system's decision authorities must determine whether corrective actions are needed or decide to accept the risk

NIST 800-30 – Example (1)

- A tax consulting company with 1'000 employees develops its own financial accounting system (contains all financial data: revenue, salary…)
- Ten financial accountants will have access to read / modify data
- The core components of the system have already been designed and you are given the task to do some threat modeling to find security-critical vulnerabilities before implementation begins
- You identify this threat: accountants may modify the data in non-legitimate ways and can deny having done this
  - They could offer their co-employees to "tune" their salaries a bit – of course for financial compensation
- You discover that there's absolutely no logging / auditing mechanism to track changes made by the accountants → vulnerability!
- As a side note, "morale" among the employees is not so great due to recent salary cuts…

NIST 800-30 – Example (2)

- So what's the risk of this threat?
- Looking at the guidance provided by NIST 800-30, that's not so easy to determine…
- Likelihood can be rated Medium – High:
  - The employees are somewhat motivated to carry out such an attack (Medium)
  - Controls to discover who has performed the attack are missing, which means there's a high probability the attack will be carried out (High)
- Impact can be rated Medium
  - There may be some financial loss but likely not too much (Low)
  - Reputation may take a serious hit if this becomes public (High)
  - No injuries expected (Low)
- So the risk of this threat is Medium and we likely should do something…

NIST 800-30 – Discussion

- Risk analysis according to NIST 800-30 is certainly a start, but the provided guidelines to assess likelihood and impact are minimal
- This lack of guidance will likely mean that different security analysts will likely interpret the levels in a different way
  - As a result, it is likely that different security analysts may determine significantly different risk values for the same threats
- The approach does not provide an integrated way to document why a particular level for likelihood or impact was selected
  - This makes it difficult for 3rd persons to understand / verify the values assigned by others
- Especially beginners in security risk analysis would prefer a somewhat more structured approach to determine likelihood and impact

Zurich University of Applied Sciences

zh aw

Security Risk Analysis – OWASP Risk Rating

OWASP Risk Rating

- We have seen that NIST 800-30 provides little help / guidance to pick appropriate values for likelihood and impact
- To overcome this, the OWASP Risk Rating method uses – for both likelihood and impact – a set of factors that must be rated
  - Each factor is rated from 0 – 9 (higher = bigger likelihood / impact)
  - For each factor, examples are provided to help choosing reasonable values
  - The ratings of the factors are then used to estimate the likelihood and impact, which again determines the resulting risk
- Likelihood factors:
  - Threat agent factors to rate e.g. skill and motive
  - Vulnerability factors to rate e.g. ease of exploitation and difficulty to detect a successful attack
- Impact factors:
  - Technical impact factors to rate e.g. loss of availability or confidentiality
  - Business impact factors to rate e.g. loss of money or reputation

OWASP Risk Rating – Threat Agent Factors (Likelihood)

- Skill level: How technically skilled is this group of threat agents?
  - No technical skills (1), some technical skills (3), advanced computer user (4), network and programming skills (6), security penetration skills (9)
- Motive: How motivated is this group of threat agents to find and exploit this vulnerability?
  - Low or no reward (1), possible reward (4), high reward (9)
- Opportunity: What conditions and resources are required for this group of threat agents to find and exploit this vulnerability?
  - full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
- Size: How large is this group of threat agents?
  - Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

(Note: you can assign any value 0 – 9 for each factor, the descriptions are only examples for reasonable value selection)

OWASP Risk Rating – Vulnerability Factors (Likelihood)

- Ease of discovery: How easy is it for this group of threat agents to discover this vulnerability (just finding it, not yet exploiting it)?
  - Practically impossible (1), difficult (3), easy (7), automated tools available (9)
- Ease of exploit: How easy is it for this group of threat agents to actually exploit this vulnerability (once it has been found)?
  - Theoretical (1), difficult (3), easy (5), automated tools available (9)
- Awareness: How well known is this vulnerability to this group of threat agents (awareness of the attacker with respect to the existence of the vulnerability)?
  - Unknown (1), hidden (4), obvious (6), public knowledge (9)
- Intrusion detection: How likely is an exploit to be detected?
  - Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

OWASP Risk Rating – Impact Factors

- When considering the impact of an attack, one can consider the technical or the business impact

- Usually, business impact is more important

- However, you may not have access to all the information required to figure out the business consequences of a successful exploit
  - In this case, providing details about the technical impact and the technical risk will enable the appropriate business representatives to make a decision about the business risk

OWASP Risk Rating – Technical Impact Factors

- Loss of confidentiality: How much data could be disclosed and how sensitive is it?
  - Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
- Loss of integrity: How much data could be corrupted and how significant is the damage?
  - Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
- Loss of availability: How much service could be lost and how vital is it?
  - Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
- Loss of accountability: Are the threat agents' actions traceable to an individual?
  - Fully traceable (1), possibly traceable (7), completely anonymous (9)

OWASP Risk Rating – Business Impact Factors

- Financial damage: How much financial damage will result from an exploit (direct damage by the attack and effort to recover from it)?
  - Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- Reputation damage: Would an exploit result in reputation damage that would harm the business (long-term damage)?
  - Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
- Non-compliance: How much will regulations by governments (e.g. laws) or other companies be violated by an exploit?
  - Minor violation (2), clear violation (5), high profile violation (7)
- Privacy violation: How much personally identifiable information could be disclosed?
  - One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

OWASP Risk Rating – Likelihood Determination

- The likelihood of successful exploitation is determined by taking the average of the threat agent and vulnerability factors

- Example:

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportu-nity	Size	Ease of discovery	Ease of exploit	Aware-ness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood: 4.375							

OWASP Risk Rating – Impact Determination

- The impact of successful exploitation is determined individually for technical and business impact, again by computing the average

- Example:

Technical impact factors				Business impact factors			
Loss of confiden-tiality	Loss of integrity	Loss of availability	Loss of accounta-bility	Financial damage	Reputa-tion damage	Non-com-pliance	Privacy violation
5	7	5	9	7	5	1	6
Overall technical impact: 6.5				Overall business impact: 4.75			

- If possible, use the business impact value in the further risk calculation (if you have enough information to make educated estimations)
  - Otherwise, use the technical impact value

OWASP Risk Rating – Risk Determination

- The computed values (likelihood, impact) are mapped to high, medium, and low as follows:
  - Likelihood 4.375 → Medium
  - Technical impact 6.5 → High
  - Business impact 4.75 → Medium

Likelihood and impact levels	
0 to <3	Low
3 to <6	Medium
6 to 9	High

- And the overall risk is determined according to the following table

	Impact		
Likelihood	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Info	Low	Medium

  - So we have a technical risk of High and a business risk of Medium

OWASP Risk Rating – Example (1)

Let's again rate the risk of the threat identified in that financial accountants system of the tax consultant company

- Threat agent factors:
  - Skill level: threat agents (accountants) have advanced user skills (4)
  - Motive: atmosphere among employees is not so great (salary cut), there may be financial gain (5)
  - Opportunity: access to the system is possible from within the company, no special resources are required (7)
  - Size: only financial accounting staff have access (3)
- Vulnerability factors:
  - Ease of discovery: difficult to detect as the lack of missing logging is not obvious, maybe one could start with an "accidental" minor modification and see if anyone notices (3)
  - Ease of exploit: once found, this is very easy (7)
  - Awareness: there have been rumors that only little logging is done (4)
  - Intrusion detection: no logging at all (9)

OWASP Risk Rating – Example (2)

- Business impact factors:
  - Financial damage: some limited direct damage can be expected (people getting too much salary, effort to recover from the attack) (3)
  - Reputation damage: significant brand damage to be expected if a successful attack became public (9)
  - Non-compliance: no impact as there are no special compliance requirements for this company (0)
  - Privacy violation: no disclosure of personal identifiable information (0)

OWASP Risk Rating – Example (3)

- Likelihood determination:

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportu-nity	Size	Ease of discovery	Ease of exploit	Aware-ness	Intrusion detection
4	5	7	3	3	7	4	9
Overall likelihood: 5.25 (Medium)							

- Business impact determination:

Business impact factors			
Financial damage	Reputa-tion damage	Non-com-pliance	Privacy violation
3	9	0	0
Overall business impact: 3.0 (Medium)			

- So we still get a risk rating of Medium (just like with the NIST 800-30 method before)
  - But due to the more structured approach, there's more confidence in the result
  - And the reasoning (values for the factors) is documented and can be followed by other persons

OWASP Risk Rating – Exercise (1)

- You are performing a penetration test of a custom e-shop web application with 50'000 registered users
- You discover an SQL injection vulnerability that allows to read the stored credit card information of all users from the shop's database
- Discovering and exploiting the vulnerability each required several days of skillful probing, automated tools did not help at all
- The application employs extensive logging (web logs, DB logs…) and log files are inspected regularly
- The vulnerability can be exploited "from the Internet", no login is required
- A user recently reported in a public web forum that he had found an SQL injection vulnerability in this e-shop, without disclosing any details
- Your task: asses the risk of the threat that an attacker can read all credit card information from the application

OWASP Risk Rating – Exercise (2)

- Likelihood determination:

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportu-nity	Size	Ease of discovery	Ease of exploit	Aware-ness	Intrusion detection

- Business impact determination:

Business impact factors			
Financial damage	Reputa-tion damage	Non-com-pliance	Privacy violation

Zurich University of Applied Sciences

zh aw

Risk Mitigation

Risk Mitigation

- Once the risks have been determined, one must decide what further actions have to be taken → risk mitigation

- Risk mitigation means that the following must be done for the threats included in the risk analysis:
  - Prioritize the threats according to the risk rating
    - This should make sure that the most critical threats are handled first – and not the ones that are easiest to mitigate
  - Decide what to do with the threats (risk mitigation options)
  - If necessary, propose, design and implement corrective actions to reduce or avoid the risk of a threat

- Once risk mitigation has been completed, update your risk analysis documentation
  - Determine the new risk values that take the corrective actions into account
  - Check if there are no unacceptable risk levels remaining

Risk Mitigation Options

With every threat / risk, you can decide to do one of the following:

- Risk Acceptance
  - Accept the risk, e.g. because it's so small that any corrective action would be pointless / financially not reasonable (e.g. risk rating is Low)
- Risk Reduction
  - Implement corrective measures to either reduce the likelihood or the impact (or both) to reduce the risk to an acceptable level
- Risk Avoidance
  - Avoid the risk completely, e.g. by removing the functionality with which it is associated
- Risk Transfer
  - Transfer the risk to someone else, e.g. buying insurance
- Risk Ignorance
  - You know there's a (possibly high) risk, but you simply ignore it

Risk Reduction

- With software projects, risk reduction is often the selected mitigation option

- The risk of a threat can be reduced by either reducing the likelihood or the impact (or both)
  - Likelihood is usually easier to reduce than impact, as it can often be reduced using appropriate measures to make "the attack more difficult"

- It is important to select cost-effective strategies to reduce a risk
  - Obviously, the costs to reduce a risk should not be greater than the expected financial damage from the threat
  - It is not necessary to find the best solution to reduce a risk, but to find a cost-effective solution that reduces the risk to an acceptable level
  - Note that a selected solution may also have negative side effects (e.g. on usability) and may even result in new threats / risks (e.g. encrypting a backup tape may create problems during recovery)

Risk Reduction – Example

- The OWASP Risk Rating factors are also helpful to think about ways to reduce a risk
  - The high values obviously provide the most reduction potential

- Example: some options to reduce likelihood (and therefore risk) in the financial accountants system of the tax consultant company

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportu-nity	Size	Ease of discovery	Ease of exploit	Aware-ness	Intrusion detection
4	5 → 3	7 → 2	3	3	7	4	9 → 3

Reduce motivation by treating employees "better"

Enforce 4-eyes principle to modify critical data

Improve intrusion detection by employing strict logging and log inspection

Security Risk Analysis – Final Remarks (1)

- Security risk analysis is always subjective – performing the analysis in a team increases the likelihood that the outcome is sound
- Don't try to be over-precise:
  - It does not significantly matter whether you assign 4 or 5 to a specific factor, as we only do a coarse-grained rating Low – Medium – High
  - To be on the safe side, be a bit pessimistic when choosing the values
- Always compare the determined risk values with your "gut feeling": Do the values make sense?
  - If there are significant discrepancies, validate the assigned values for correctness
- Adapting the risk methodology to your needs is possible, e.g. with OWASP Risk Rating:
  - Adding additional factors (e.g. "customer loss")
  - Weighting factors (reputation may count "more" in your organization if you are, e.g., a security provider)

Security Risk Analysis – Final Remarks (2)

- With iterative software development processes, risk analysis should be part of several iteration (just like, e.g., threat modeling)
  - Because any extension of the system (new requirements, use cases, design extensions, functionality etc.) can result in new threats and therefore risks and can affect the risks of already known threats
- But even when a system is in operation, risk analysis should be reviewed periodically
  - E.g. because new attack methods (and therefore threats) surface from time to time or because new powerful automated attack tools have appeared
- Security risk analysis is useful beyond secure software development
  - E.g. when performing a penetration test or in general when doing security assessments of systems / companies as an external security analyst

Summary

- The goal of security risk analysis is to rate the criticality of system weaknesses to make reasonable decisions about "where to make security investments"
- Security risk analysis complements other security activities such as threat modeling and security testing
- Risk is determined as a function of likelihood and impact
- The NIST 800-30 approach is a very simple method that provides only little help to pick realistic values for likelihood and impact
- OWASP Risk Rating is a more structured approach by using a set of factors, for which values can be assigned
  - Also supports documentation and provides a basis for risk reduction
- The final step of risk analysis is risk mitigation, which means deciding about what options must be taken to reduce risks to acceptable levels (if necessary)