ESSoS 14
Engineering Secure Software and Systems

Tutorial on Risk Management

International Symposium on Engineering Secure Software and Systems (ESSoS'14)

Bjørnar Solhaug

Munich, February 26, 2014

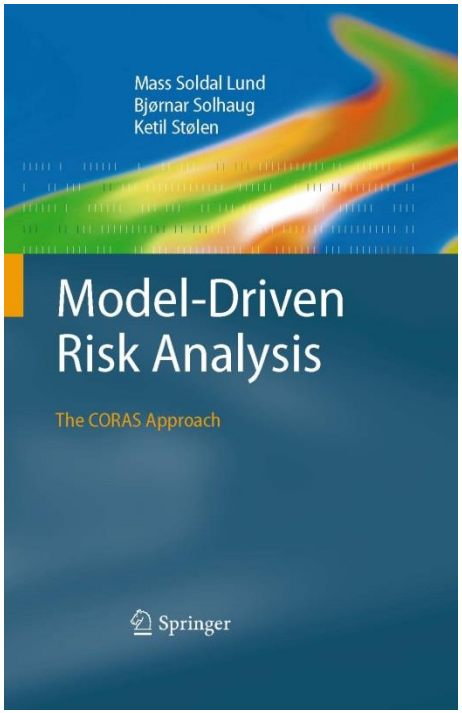
RASEN

NESSoS

EMFASE

Me

- Bjørnar Solhaug
  - Bjornar.Solhaug@sintef.no
  - www.solhaugb.byethost11.com
- Research scientist at SINTEF ICT since 2010
  - www.sintef.no
- MSc in Logic, Language and Information, University of Oslo, 2004
- PhD in Information Science, University of Bergen, 2009
- Coauthor of the book on Model-Driven Risk Analysis



Overview

- Part I – Background
  - Risk management
  - Information security risk management
  - Standards, definitions and terminology
- Part II – Risk assessment process
  - Exemplified presentation of activities, challenges and techniques
- Part III – Selected issues
  - Risk estimation
  - Uncertainty
  - Reasoning about likelihoods

Part I
Background

Risk Management

What is Risk?

- Health
- Safety
- Security
- Compliance (legal and regulatory)
- Environmental protection
- Product quality
- Reputation
- Defense
- Finance
- …

Risk – General Definition

- Risk is the effect of uncertainty on objectives [ISO Guide 73]
  - An effect is a deviation from the expected – positive and/or negative
  - Objectives can have different aspects (financial, health, safety, security)
  - Uncertainty is the state of deficiency of information related to understanding or knowledge of an event, its consequence or likelihood

- This definition is general and covers both offensive and defensive management of risk

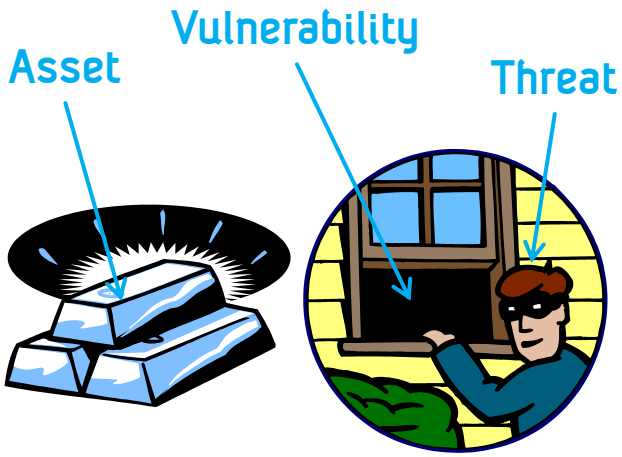
Risk – Specific Definition

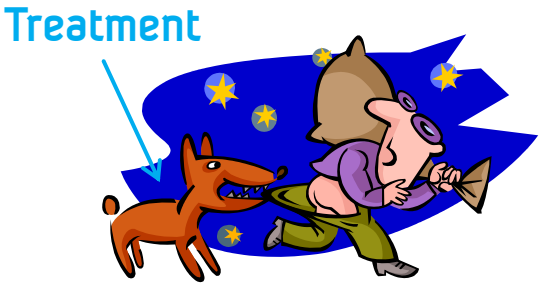
- A **risk** is the combination of the consequences of an event and the associated likelihood of occurrence [ISO Guide 73]

- The **consequence** is in terms of degree of harm to an asset
- The **likelihood** is the chance of something happening, e.g. in terms of probability or frequency

- **Risk level** is the magnitude of risk in terms of the combination of consequence and likelihood

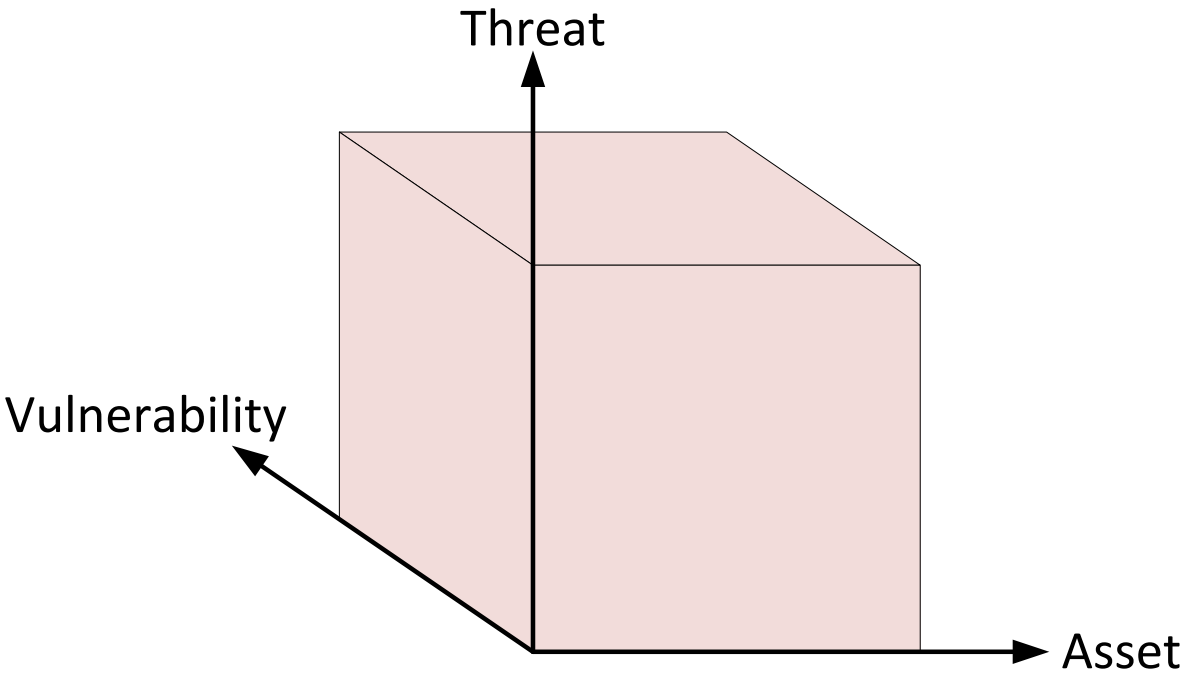
Risk Ingredients



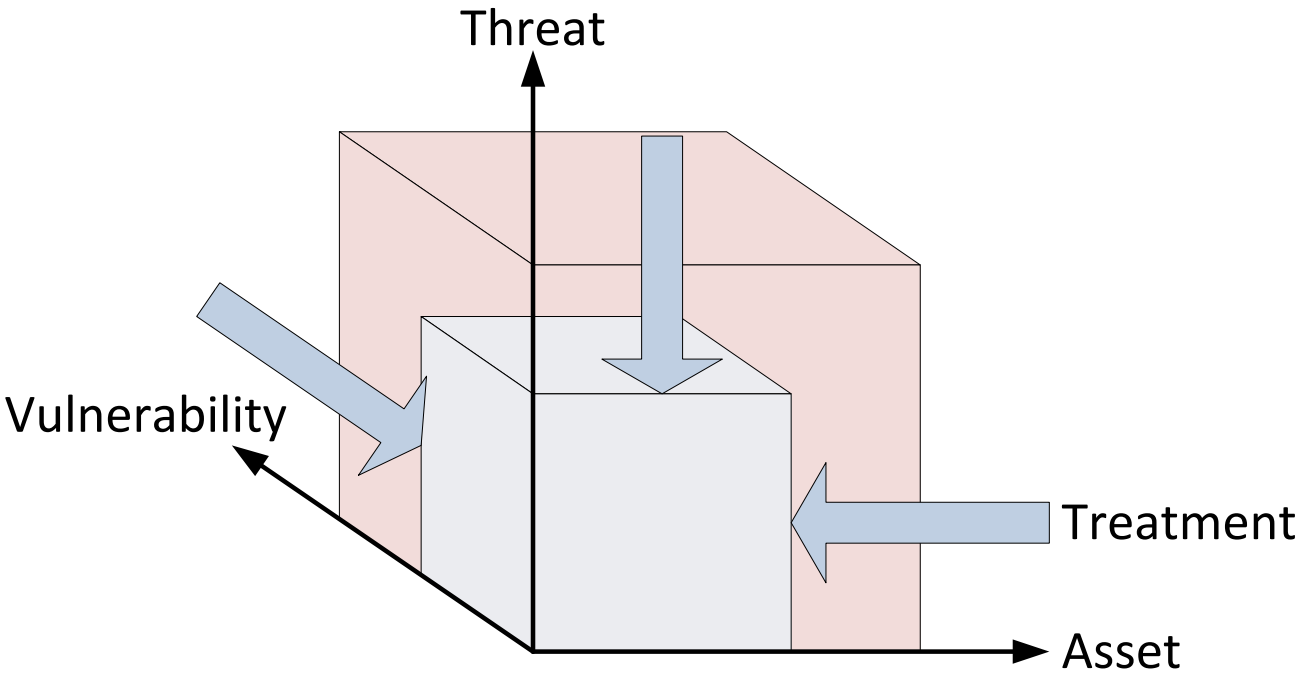


- What is needed for risks to occur?
- A **threat** is an initial cause of a risk
  - Cf. risk source [ISO Guide 73]
- A **vulnerability** is a property that opens for a threat to cause an event with a consequence
- An **asset** is something of value and that requires protection
  - Cf. objective [ISO Guide 73]
- Without all these three ingredients there is no risk
- A **treatment** is a means to reduce (modify) risk

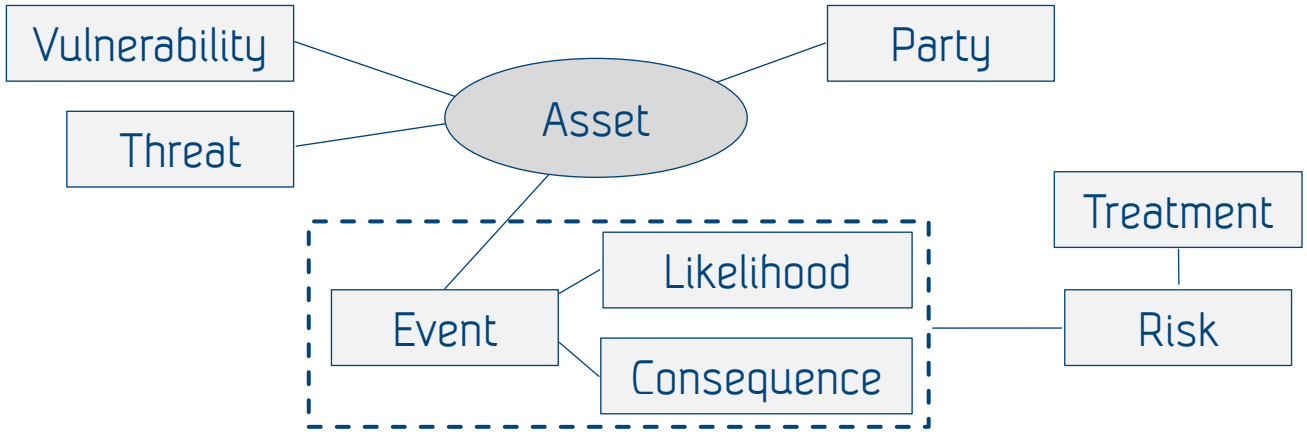
Risk Ingredients



Risk Ingredients

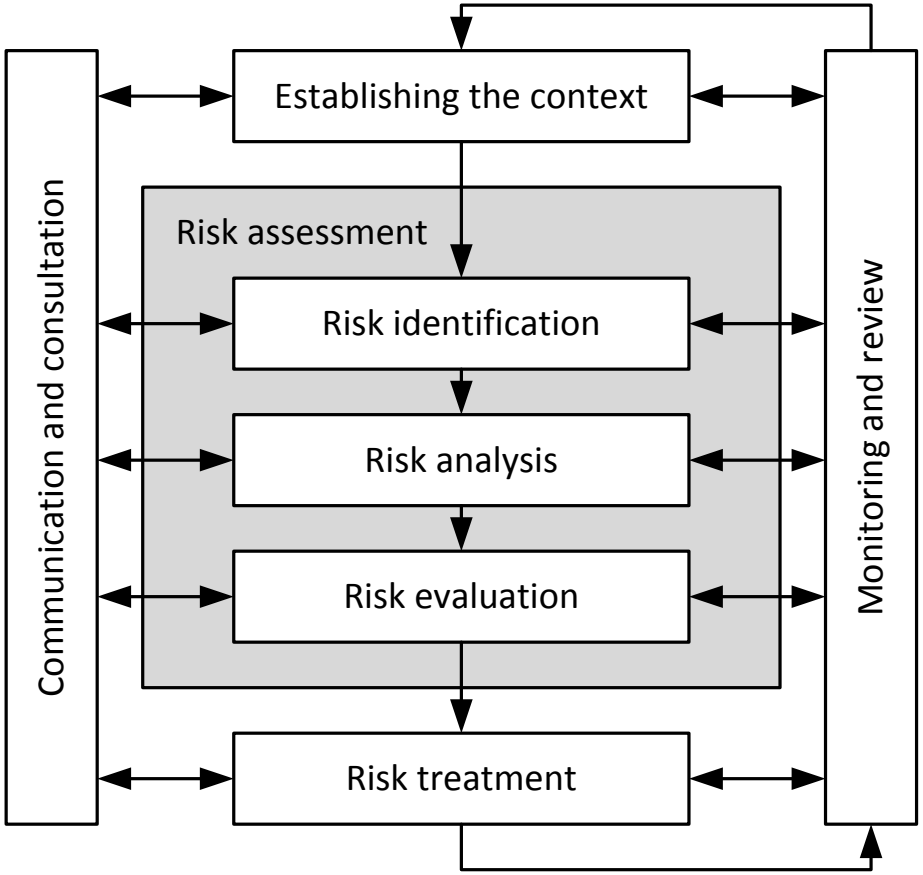


Main Concepts of Risk Analysis



- A **party** is an entity on whose behalf a risk analysis is conducted
  - Note: "Party" is *not* the same as "stakeholder" and "asset owner" in ISO Guide 73
- An **asset** is something to which a party assigns value and hence for which the party requires protection
- We often use the term **unwanted incident** instead of **event**

Risk Management Process



ISO 31000

Information Security Risk Management

Security Risk

- Security
  - Security risks relate to events that compromises assets, operations or objectives
  - The events comprise those undertaken by actors with intentions (adversaries)

- Information security [ISO/IEC 27000]
  - Information security risk is the potential that a threat will exploit a vulnerability of an asset and thereby cause harm
  - Information security is the preservation of confidentiality, integrity and availability of information
  - An information asset is knowledge or data of value
  - Risk is the combination of the probability of an event and its consequence

Security Risk – Definitions

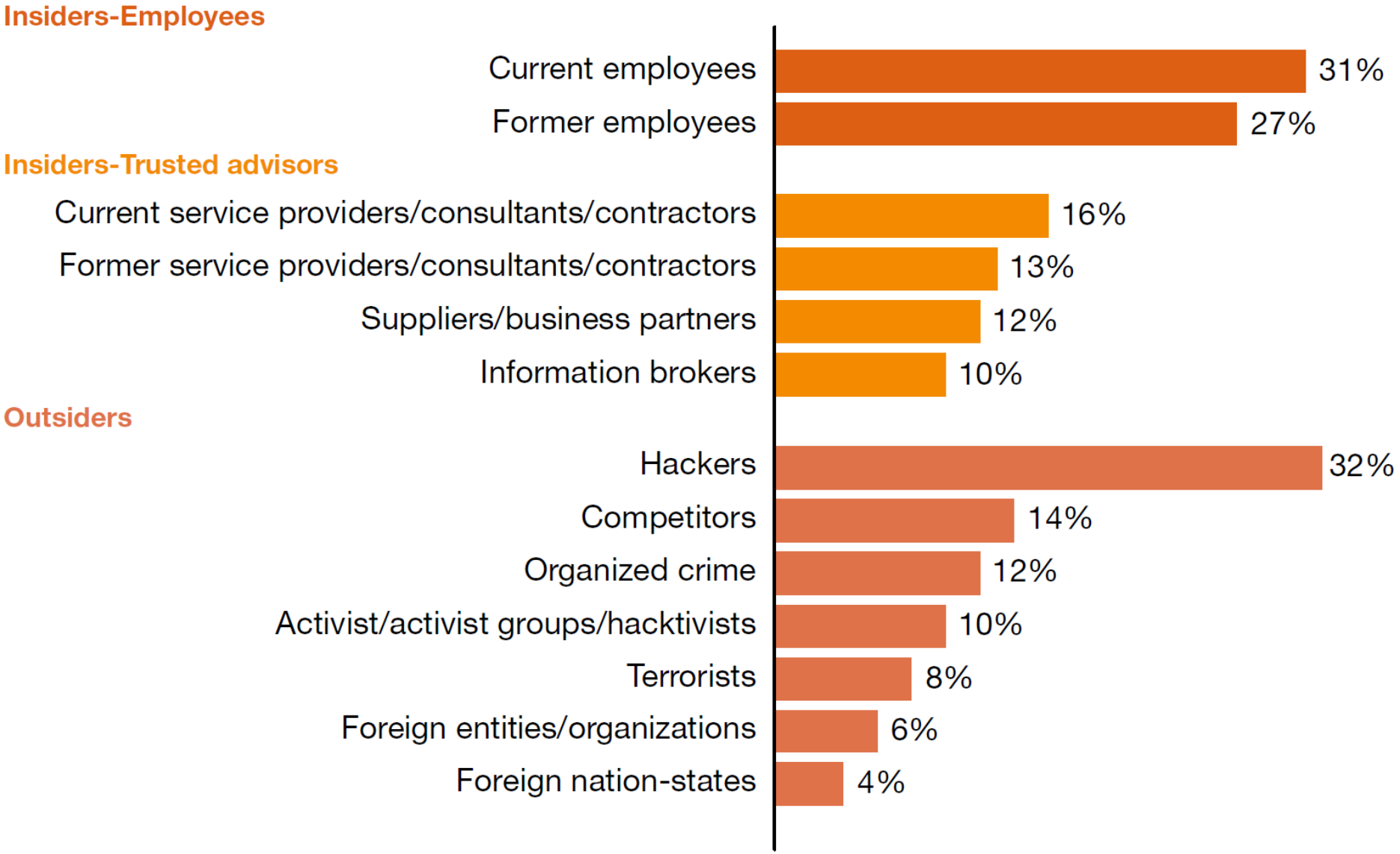
- Properties of information security:
  - **Confidentiality:** Property that information is not made available or disclosed to unauthorized individuals, entities or processes
  - **Integrity:** Property of protecting the accuracy and completeness of assets
  - **Availability:** Property of being accessible and usable upon demand by an authorized entity
- Further properties that are often considered:
  - **Authenticity:** Property that an entity is what it claims to be
  - **Accountability:** Responsibility of an entity for its actions and decisions
  - **Non-repudiation:** Ability to prove the (non-)occurrence of a claimed event or action and its originating entities
  - **Reliability:** Property of intended behavior and results

Threats to Information Security

- Threats may be deliberate, accidental or environmental
- Threats may be internal or external
- Examples
  - Physical damage (fire, destruction of equipment, corrosion,…)
  - Natural events (flood, seismic phenomena,…)
  - Loss of essential services (cooling, power,…)
  - Compromise of information (remote spying, eavesdropping, theft of media, disclosure, tampering with HW/SW,…)
  - Technical failure (equipment failure, software malfunction,…)
  - Unauthorized actions (use of equipment, copying of software, corruption of data,…)
  - Compromise of functions (abuse of rights, forging of rights,…)

Human Threat Sources

- Hacker
- Computer criminal
- Terrorist
- Industrial espionage
- Insiders (including accidental, e.g. poorly trained or negligence)
  - 58% of information security incidents attributed to insider threat [Infosecurity, 3 May 2013]
  - The BYOD phenomenon is a significant factor



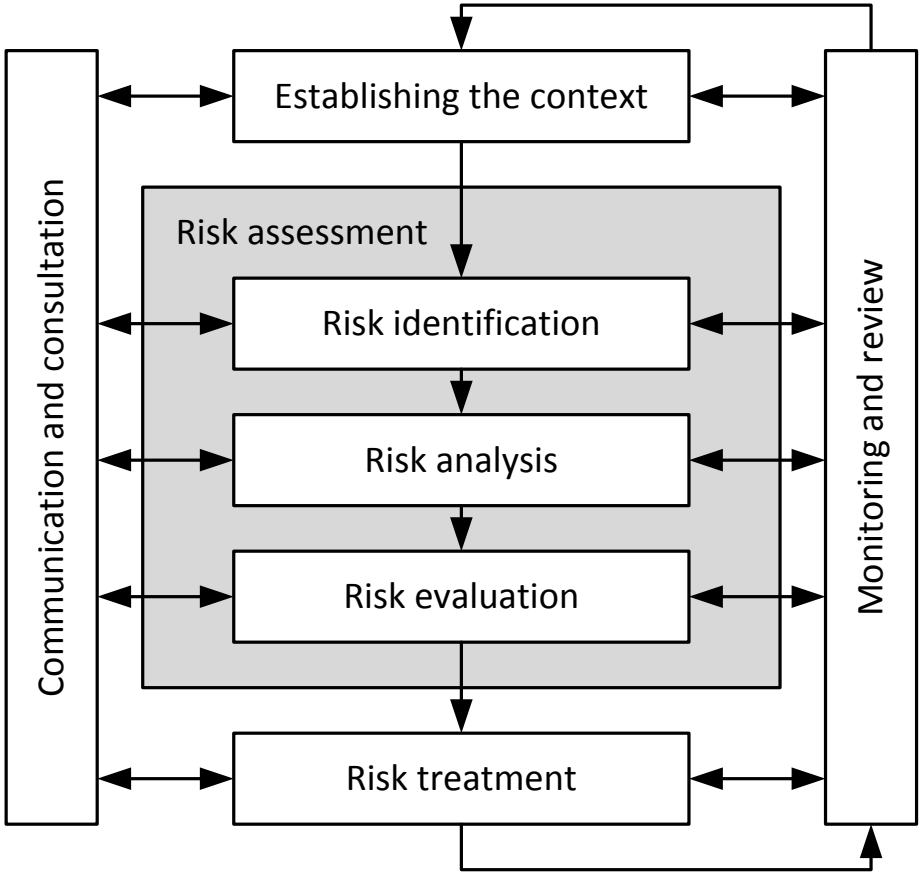
Source of incidents [The Global State of Information Security Survey 2014, PwC]

Summary

- Useful standards to know
  - ISO 31000 on risk management
  - ISO 27000 on information security terminology
  - ISO 27005 on information security risk management
- Essentials of ISO 31000
  - All kinds of risks
  - Focus is on achieving the objectives of an organization
  - Both offensive and defensive – Balance risk and opportunity
- Essentials of ISO 27005
  - Information security risk
  - Focus is on protecting the information assets of an organization
  - Defensive – Protect what you have

Part II
Risk Assessment Process

Risk Management Process

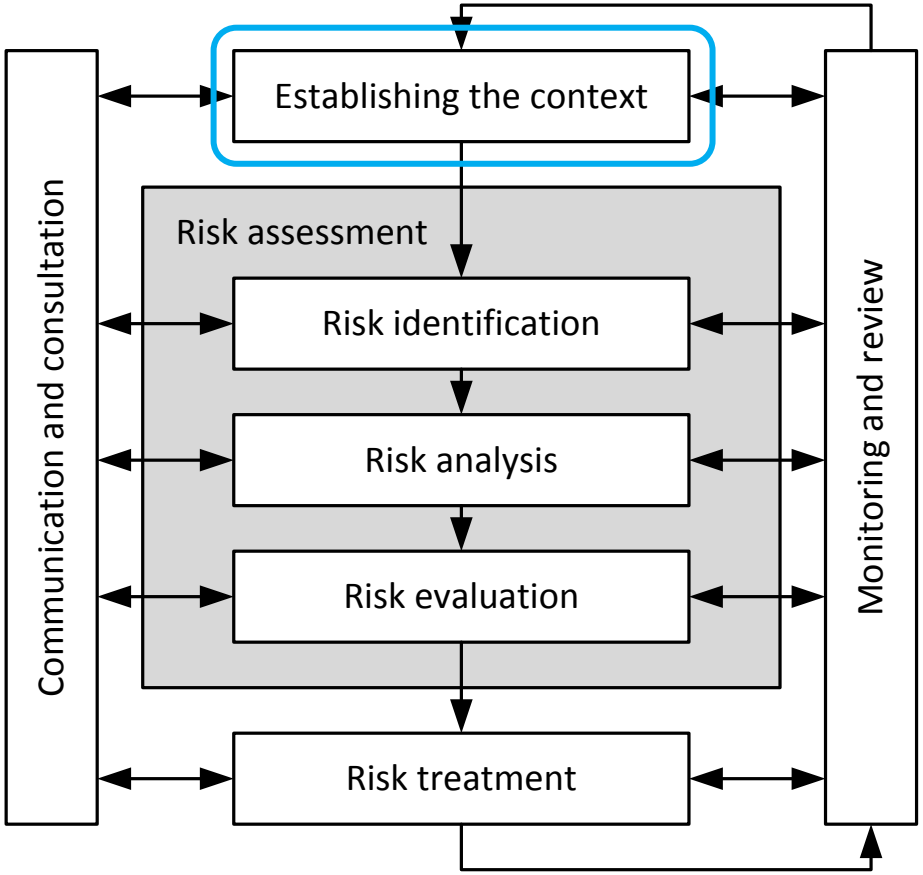


Risk Management Process

- Information security risk management should be a continual process
- Continual activities:
  - **Communication and consultation:** Information sharing, planning and decision making among relevant stakeholders
  - **Monitoring and review:** Monitoring of risks and their factors, as well as the organization context
- Iterative sequence of activities conducted on regular basis:
  - Establishing the context
  - Risk identification
  - Risk analysis
  - Risk evaluation
  - Risk treatment

Focus of the remainder of this tutorial

Risk Management Process



Establishing the Context

- The context establishment is to define and document the target and objectives of the analysis
  - External context
  - Internal context
  - Target of analysis
  - Assumptions
  - Scope and focus
  - Assets
  - Likelihood and consequence scales
  - Risk evaluation criteria
- The correctness and completeness of the context establishment is crucial
  - The correctness and validity of the risk assessment depends on this

Target Description

- The target of analysis must be documented in a way that can be understood by all relevant stakeholders
- The target description must be at a level of abstraction and details that is adequate for the desired abstraction level of the risk analysis
- The target description serves as a basis for the risk identification
  - Should show all relevant applications, components, roles, actors, business processes, data flows, etc.
  - Risks are identified by systematically searching for vulnerabilities, attack points, misuses, etc.
- It is recommended to document the target using a precise, unambiguous and well-understood notation
  - E.g. UML, BPMN, DFD, …

Running Example

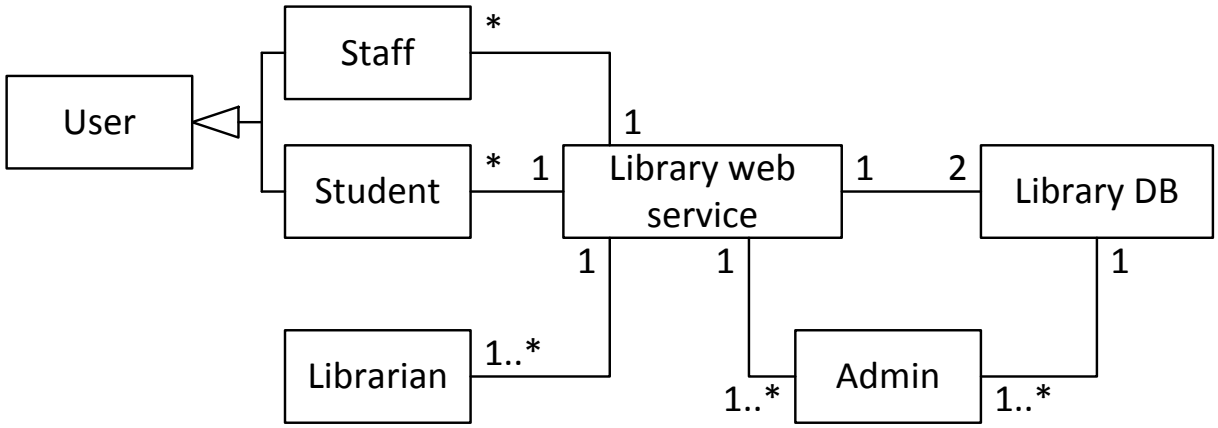
- The example is based on an OWASP example of a college library website
  - https://www.owasp.org/index.php/Application_Threat_Modeling
- The website provides online services for searching for and requesting books
- The users are students, college staff and librarians

- Note
  - The examples shown in the slides are small illustrations
  - A full risk assessment requires larger models of higher granularity

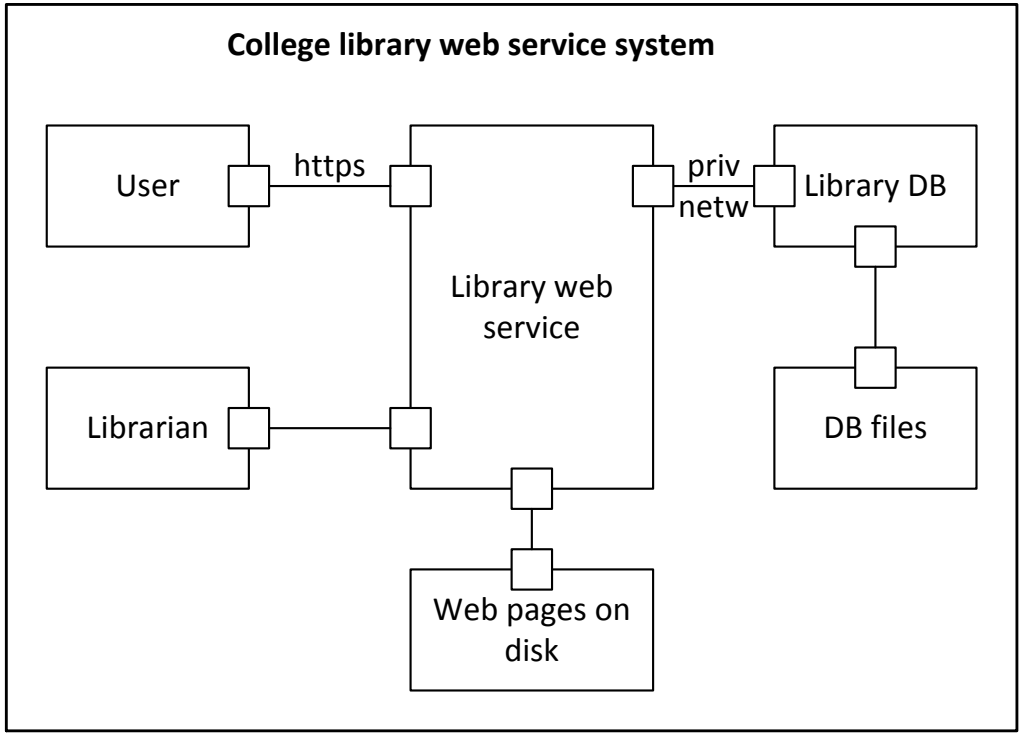
Modeling the Target of Analysis

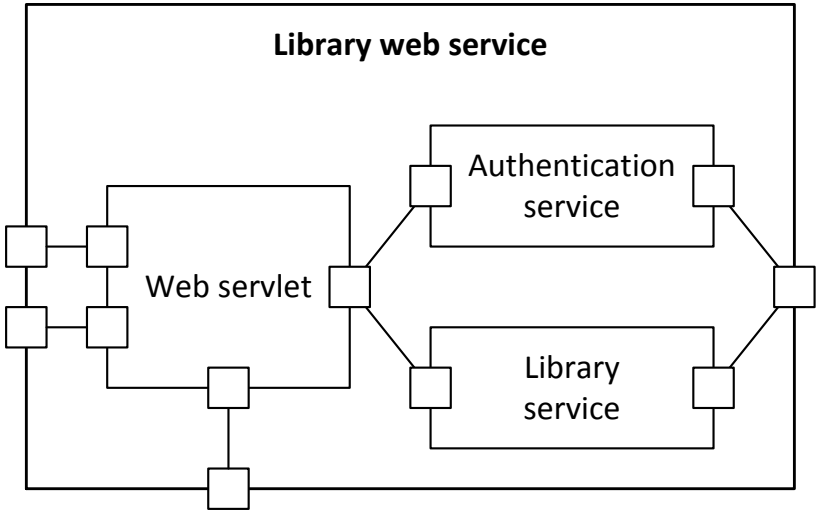
- It is often useful to describe the target using different kinds of diagrams
- We should provide, for example
  - Conceptual overview
  - Architecture
  - Activities
  - Data flows
  - Interactions
  - …
- Describing the target of analysis can also be done in prose, or by using tables/templates
  - Tables are often useful for more light-weight assessments

Target Description – Conceptual Overview



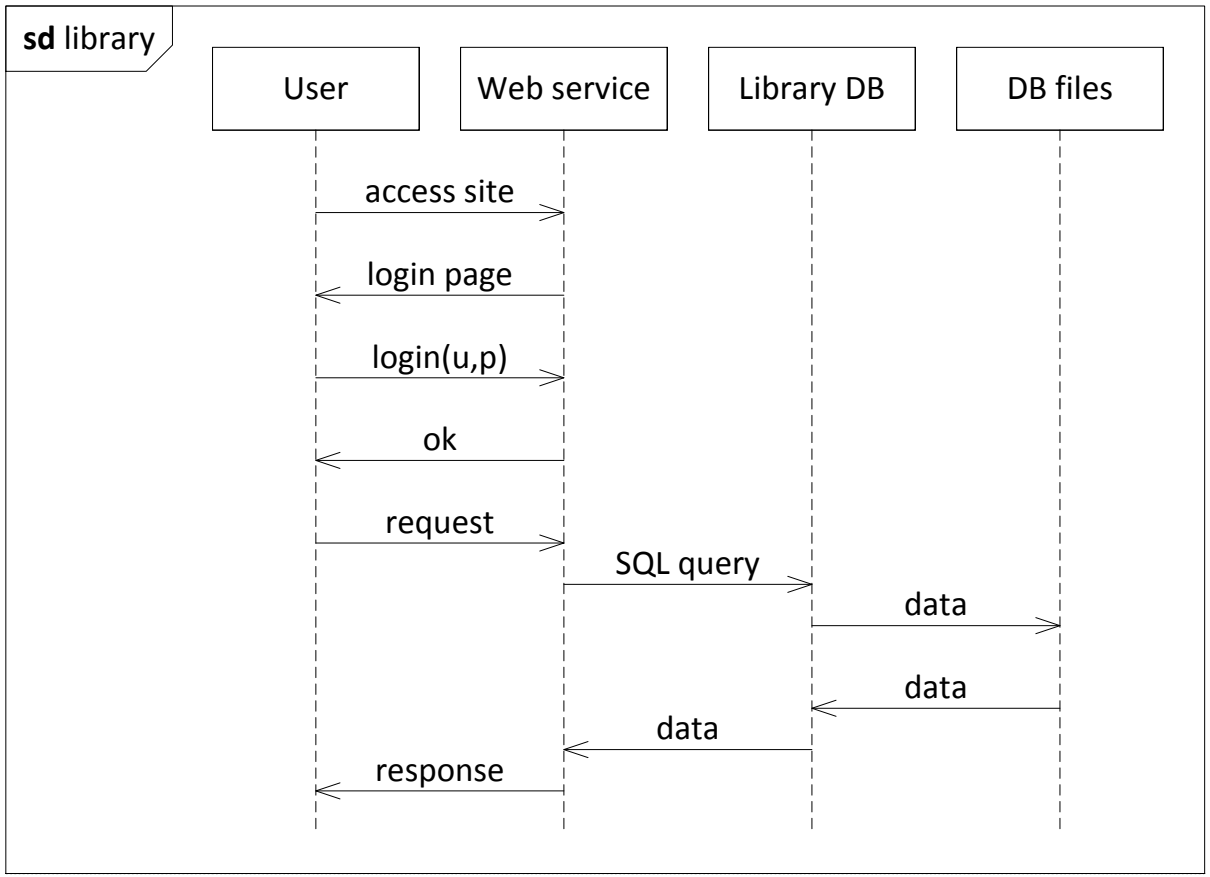
Target Description – Overall Architecture



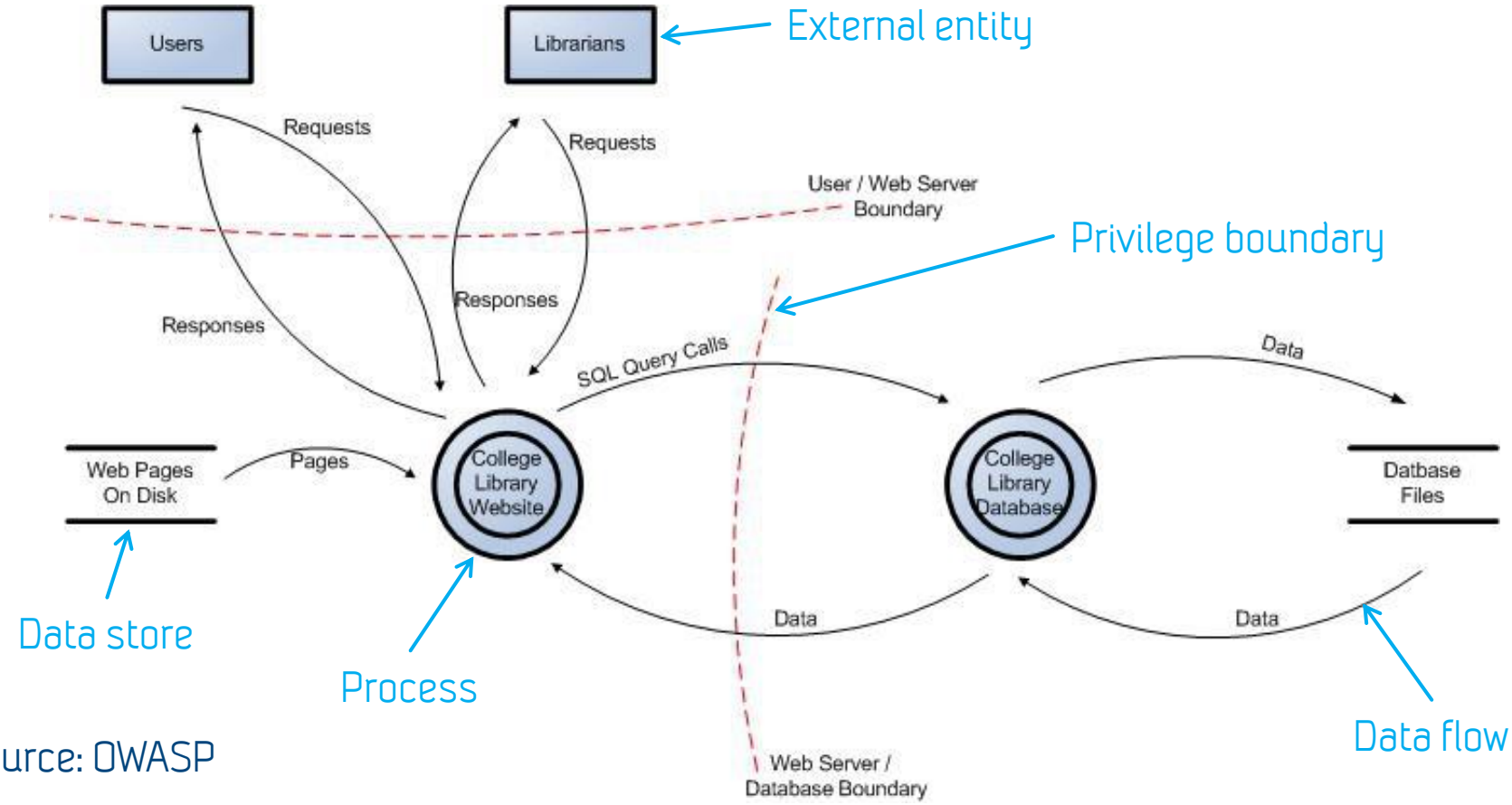


Internal structure of component

Target Description – Interactions

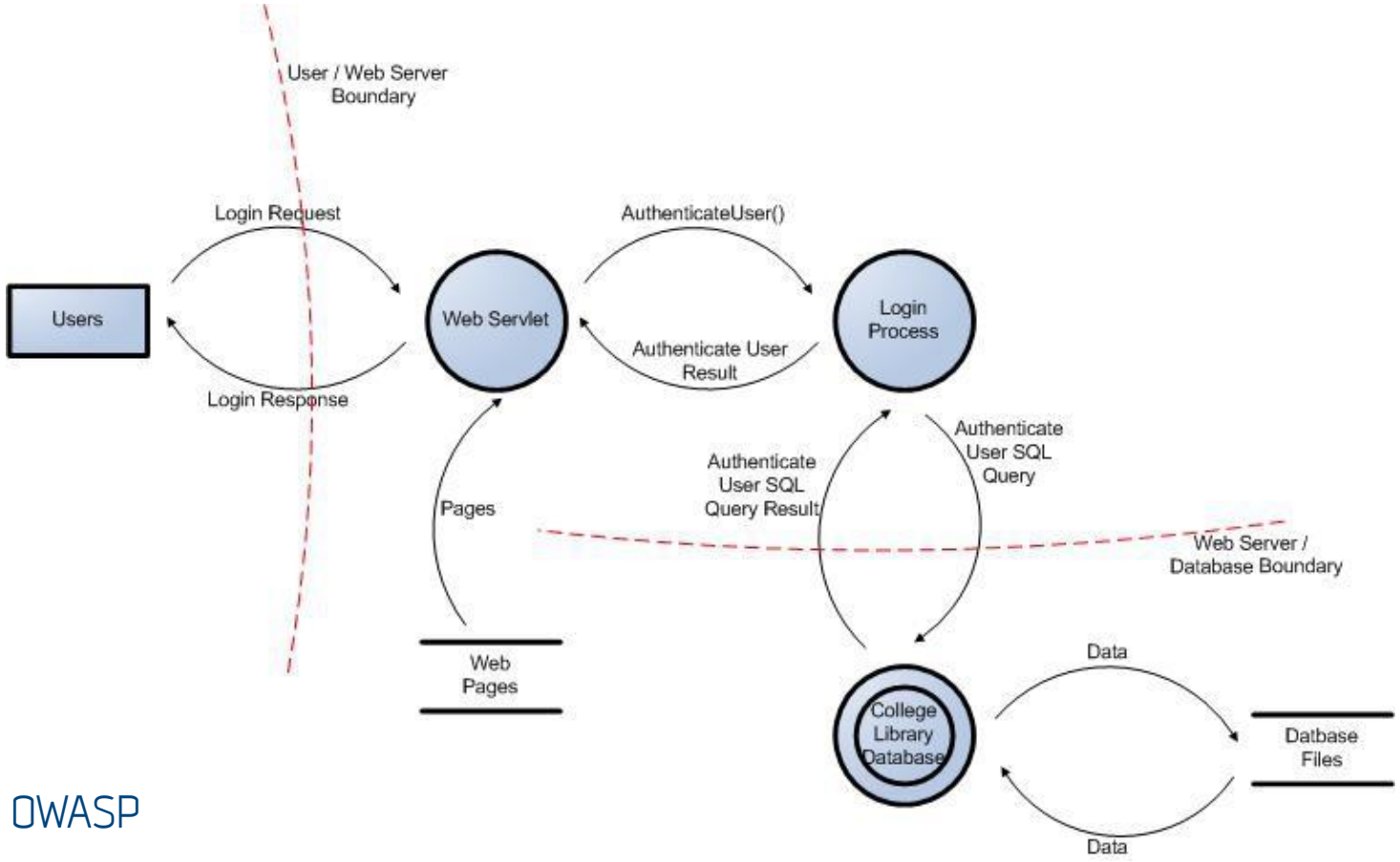


Alternative Example Using DFD – Library Website



Source: OWASP

Alternative Example Using DFD – User Login



Source: OWASP

Assumptions

- All assumptions for the analysis must be made explicit and documented
- The risk assessment is valid only under the assumptions made
- An assumption may be something we hold as true and do not investigate further
- An assumption may also be a requirement or precondition for specific parts of the target
- Examples
  - There are no malicious insiders
  - Power supply never fails
  - System requirements are fulfilled (OS, CPU, RAM)
  - Communication is encrypted
  - …

Asset Identification

- An asset is anything that has value to the organization and which therefore requires protection
  - Information, services, software, physical, people, reputation, image,…
- Information and software security often focus on information assets and service assets

- The identified assets specify the focus of the analysis
- The risk identification, analysis and evaluation are with respect to the identified assets only

- The identified assets may be ranked and/or assigned value

Asset Identification – Library Website Example

- Confidentiality of personal user data
- Availability of web service
- Integrity of databases

- For brevity, the assets will in the following be referred to as "confidentiality", "availability" and "integrity", respectively

Likelihood and Consequence Scales

- The scales define the values we use for estimating likelihoods and consequences for the identified unwanted incidents
- These estimates are used to derive the risk levels and evaluate the risks
- The scales can be continuous, discrete or by intervals
- The values can be qualitative or quantitative

- Quantitative scales may be by probabilities or frequencies for likelihoods, and e.g. monetary loss or number of DB entries affected for consequences
- Qualitative scales may be by
  - natural language terms (like "often" and "rare", "insignificant" and "catastrophic")
  - general descriptions of how often it is experienced by how many

Likelihood Scale Example – Qualitative

Likelihood	Definition
Unlikely	Has never occurred yet throughout the total lifetime of the system
Rare	Only very few similar incidents on record when considering a large traffic volume or no records on a small traffic volume
Possible	Several similar occurrences on record - Has occurred more than once for the same user
Likely	A significant number of similar occurrences already on record - Has occurred a significant number of times for the same user
Certain	A very high number of similar occurrences already on record- Has occurred a very high number of times for the same user

Likelihood Scale Example – Quantitative by Frequencies

Likelihood	Definition
Unlikely	[0,1› : 1 year
Rare	[1,5› : 1 year
Possible	[5,20› : 1 year
Likely	[20,50› : 1 year
Certain	[50,∞› : 1 year

The defined frequency intervals must be adequate for the target of analysis and its scope

Likelihood Scale Example – Quantitative by Frequencies

Likelihood	Definition
Unlikely	[0, 0.01›
Rare	[0.01, 0.1›
Possible	[0.1, 0.25›
Likely	[0.25, 0.75›
Certain	[0.75, 1]

The defined probability intervals must be adequate for the target of analysis and its scope; the probability of occurrence is with respect to a given period

Consequence Scale Example – Qualitative

Consequence	Definition
Insignificant	Generally tolerable and easy to manage or recover from
Minor	Tolerable if easy to recover from or if not very frequent
Moderate	Several occurrences over time can potentially put the service provider out of business
Major	Failure to recover can potentially put the service provider out of business
Catastrophic	Can potentially put the service provider out of business

Consequence Scale Example – Quantitative

Consequence	Definition
Insignificant	Range of [0%, 1%› of records are leaked
Minor	Range of [1%, 10%› of records are leaked
Moderate	Range of [10%, 20%› of records are leaked
Major	Range of [20%, 50%› of records are leaked
Catastrophic	Range of [50%, 100%› of records are leaked

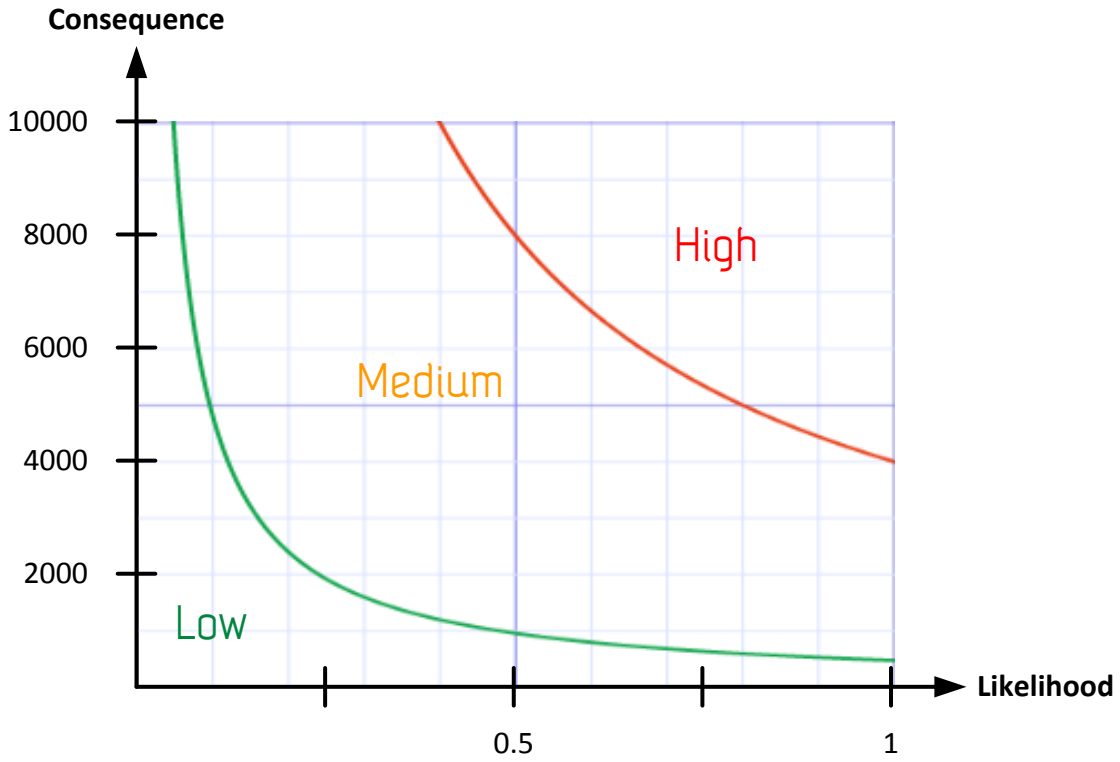
Note: We often need to define one consequence scale for each asset, for example

- Service availability in terms of downtime
- Confidentiality in terms of number/share of entries that are leaked
- Integrity in terms of number/share of entries that are affected

Risk Evaluation Criteria

- The risk evaluation criteria specifies the risk tolerance
- In order to define the criteria, we first need to define the risk function
- The risk function is a mapping from consequence and likelihood to risk level
  - Can be by using risk matrices or by a mathematical function (such as multiplication)
- For cases in which we have several assets with different consequence scales, we may need to define one set of criteria for each asset

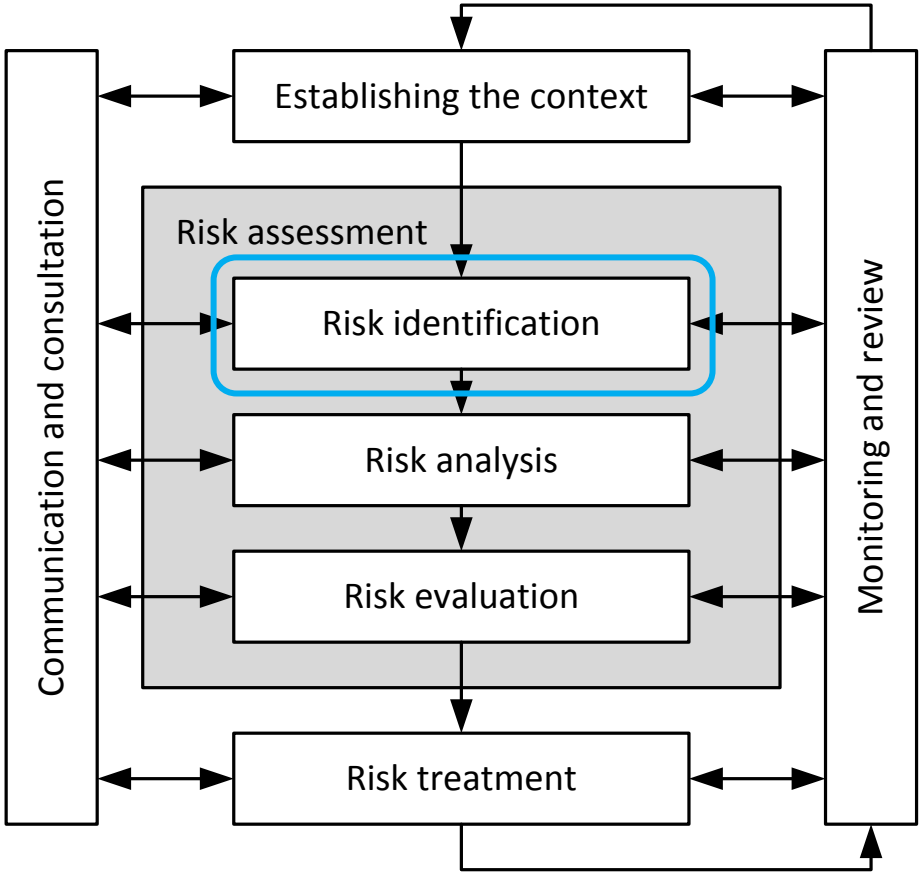
Risk Evaluation Criteria Example – Continuous Scales



Risk Evaluation Criteria Example – Risk Matrix

	Insignificant	Minor	Moderate	Major	Catastrophic
Unlikely	1	2	3	4	5
Rare	2	3	4	5	6
Possible	3	4	5	6	7
Likely	4	5	6	7	8
Certain	5	6	7	8	9

Risk Management Process



Risk Identification

- This activity involves the identification and documentation of the risks and their causes
  - Threats (natural or human, deliberate or accidental)
  - Vulnerabilities
  - Scenarios
  - Incidents
- The risk identification shall be with respect to the identified assets only
- There are numerous techniques and formats available for risk identification and documentation
  - ISO 31010 gives an overview and classification of assessment techniques
  - ISO 27005 gives lists of threats and vulnerabilities
  - Several organizations publish repositories of risk sources

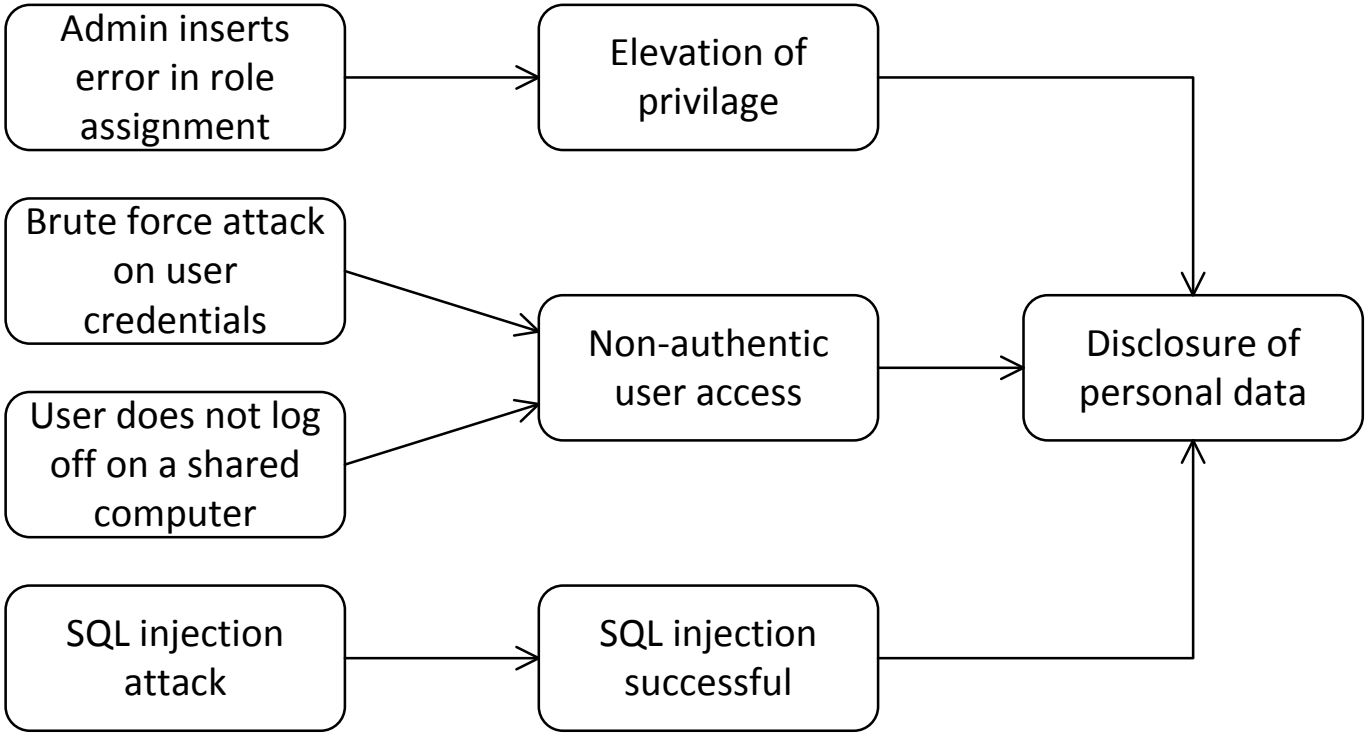
Which Technique to Choose?

- Need to determine what we wish to document, what kind of analyses we wish to conduct, the level of granularity, the available time and resources, etc.
  - Tables and checklists are useful for quick-and-dirty, high-level assessments
  - Fine-grained modeling techniques are useful for detailed assessments and more rigorous analyses
- Consider also the underlying terminology: Which risk elements to we seek to identify, document and reason about?
- We moreover need to determine how to gather the information
  - Interviews, brainstorming, testing, examination of logs and historical data, …
- Examples of techniques:
  - ISO 27005 table formats, event trees, attack trees, Bayesian networks, MS threat modeling, …

Note

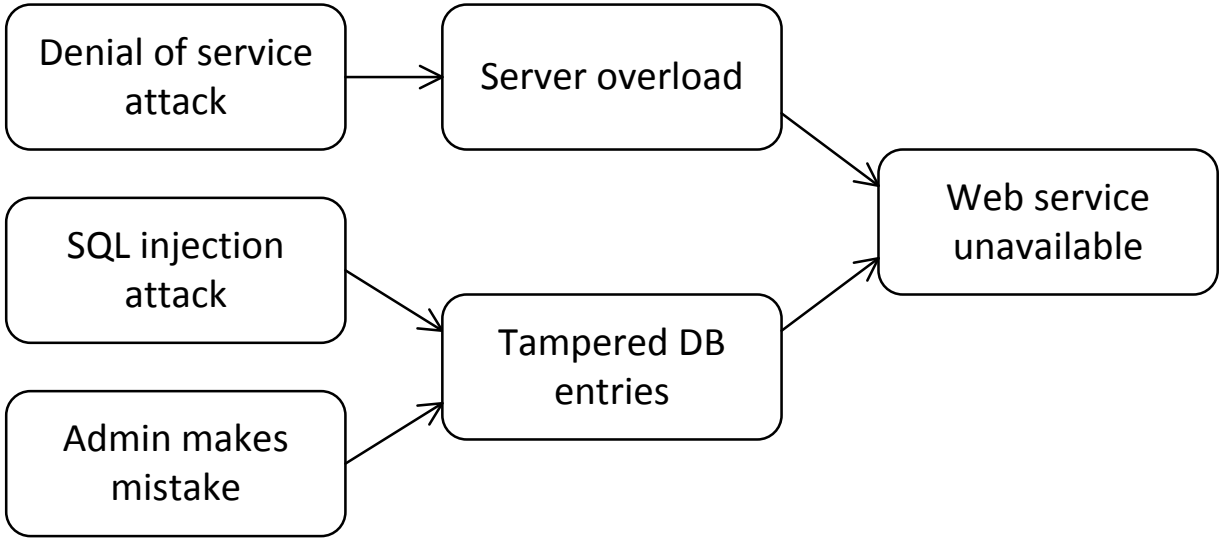
- The diagrams shown in this presentation are not using a specific risk modeling notation
- It is a "dummy notation" used to exemplify some of the key elements of risk modeling and risk assessment in general

Risk Modeling – Library Example: Confidentiality

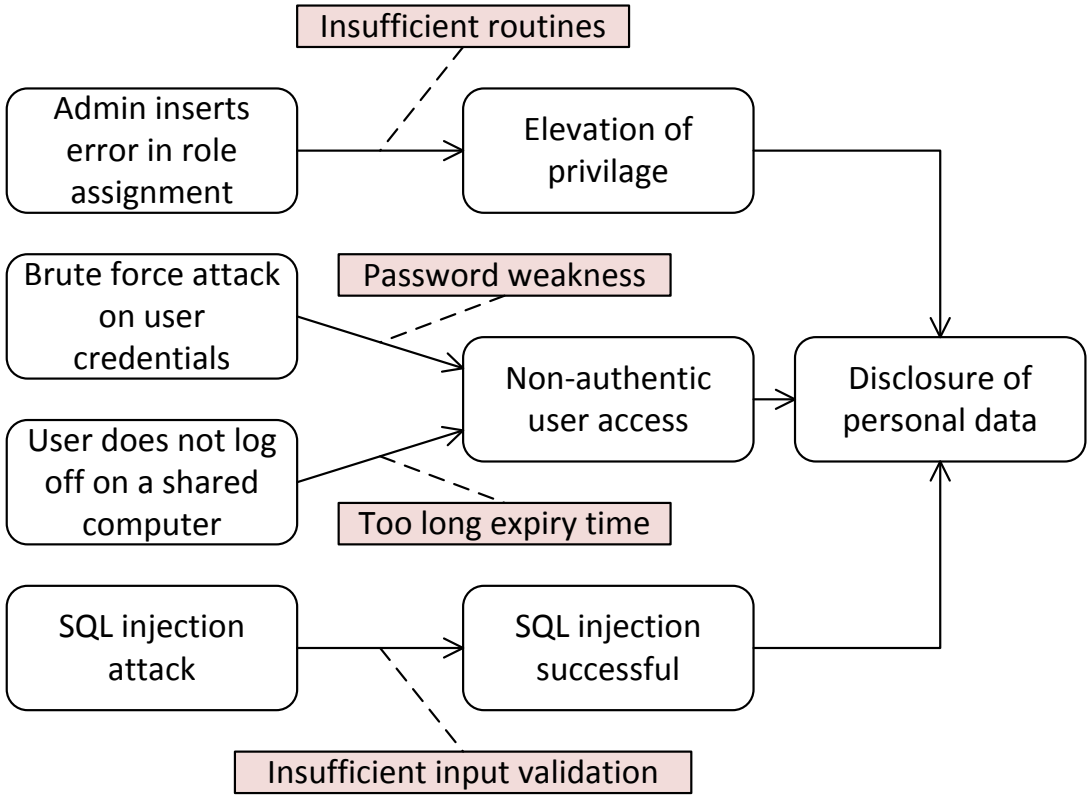


Note: Multiple ingoing arrows to a scenario are OR composition

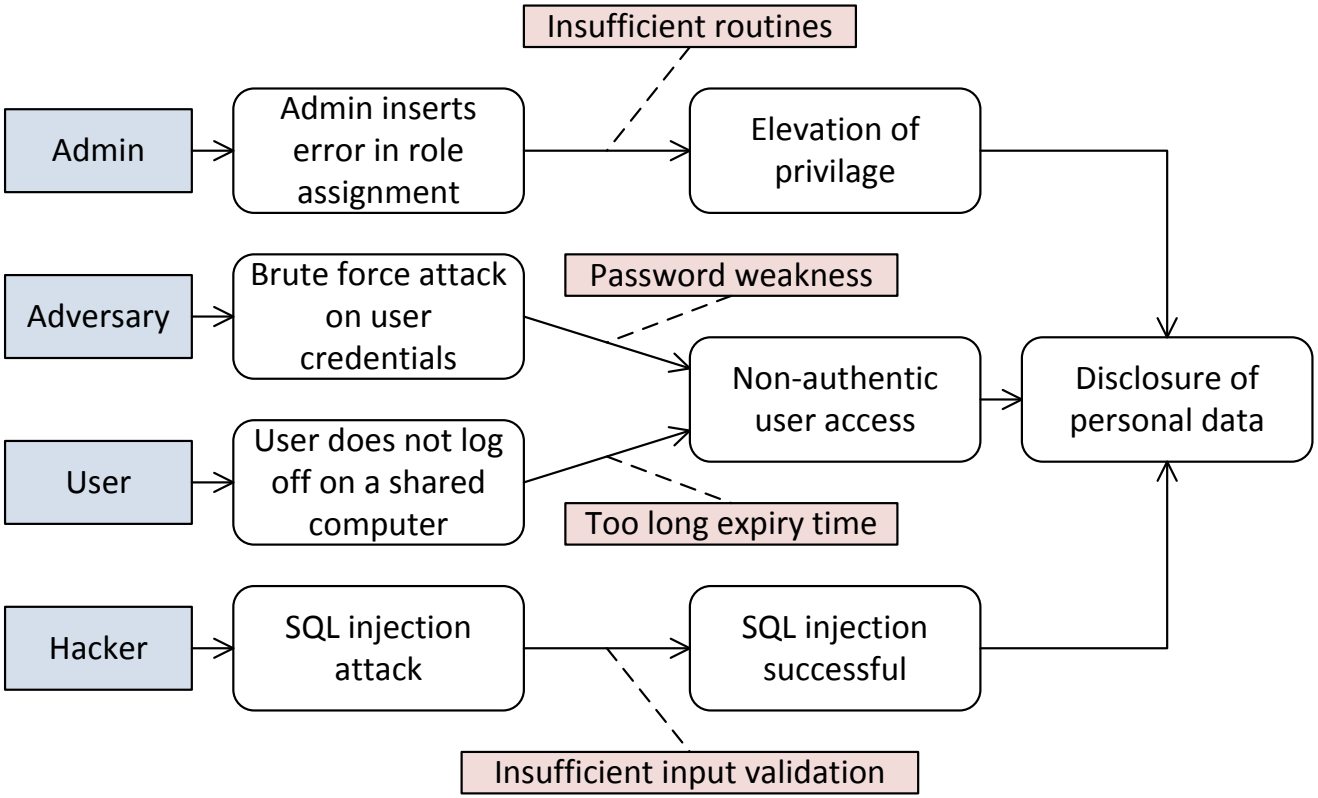
Risk Modeling – Library Example: Availability



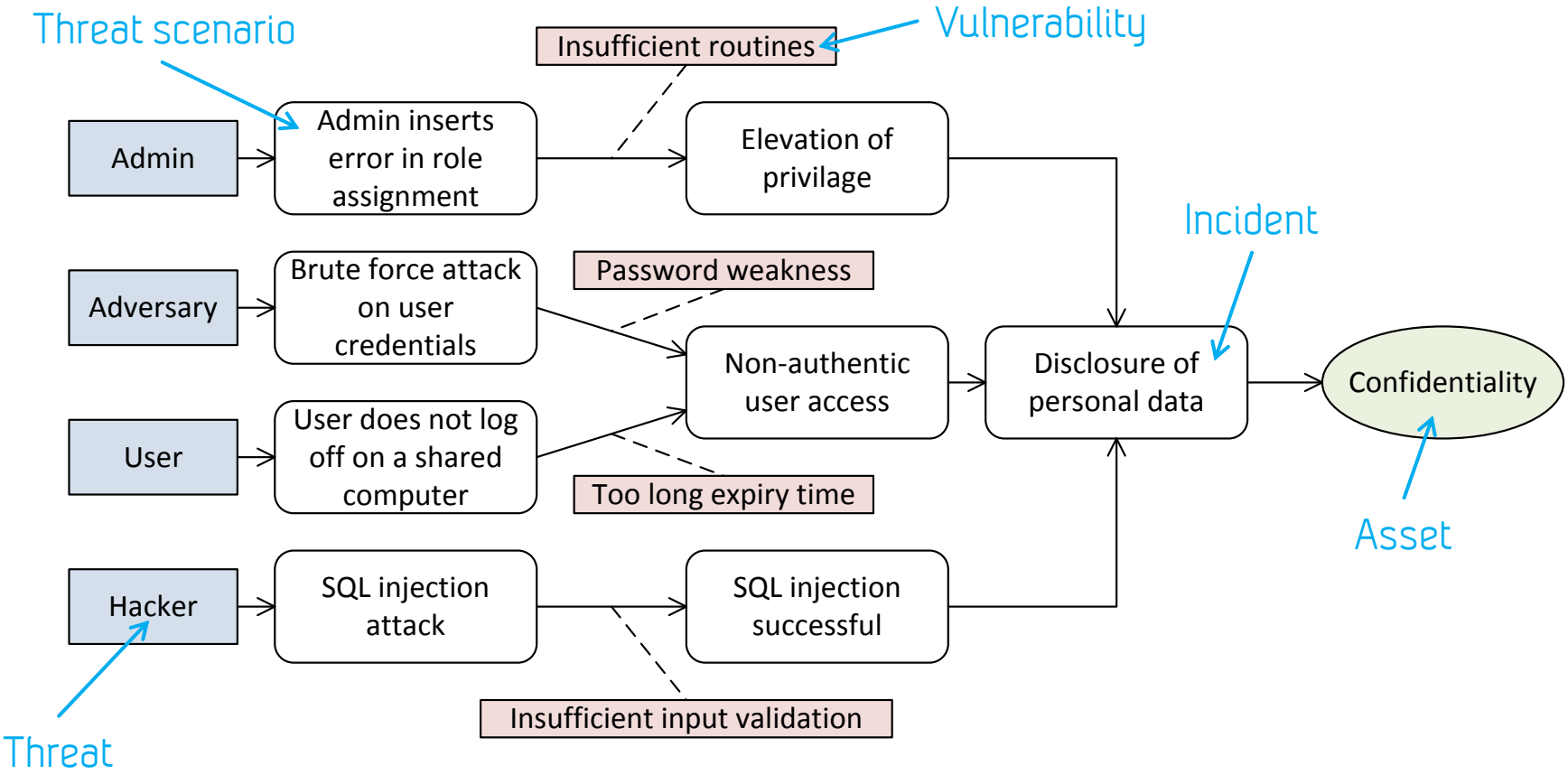
Risk Modeling – Library Example: Vulnerabilities



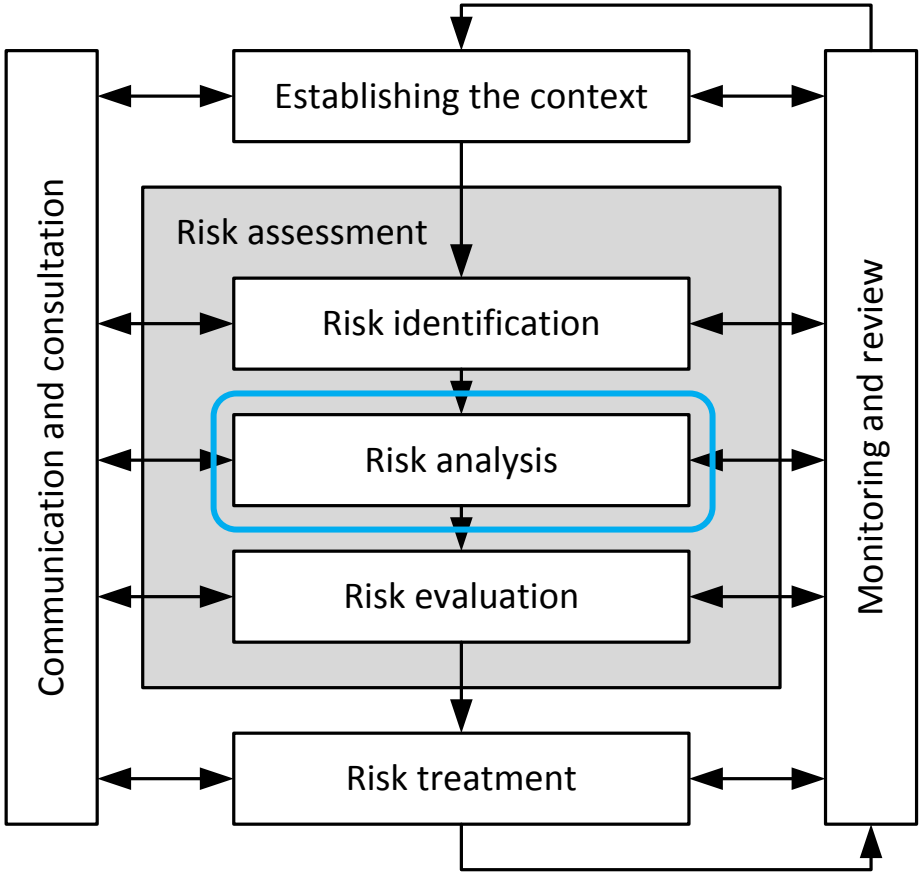
Risk Modeling – Library Example: Threats



Risk Modeling – Library Example: Assets



Risk Management Process

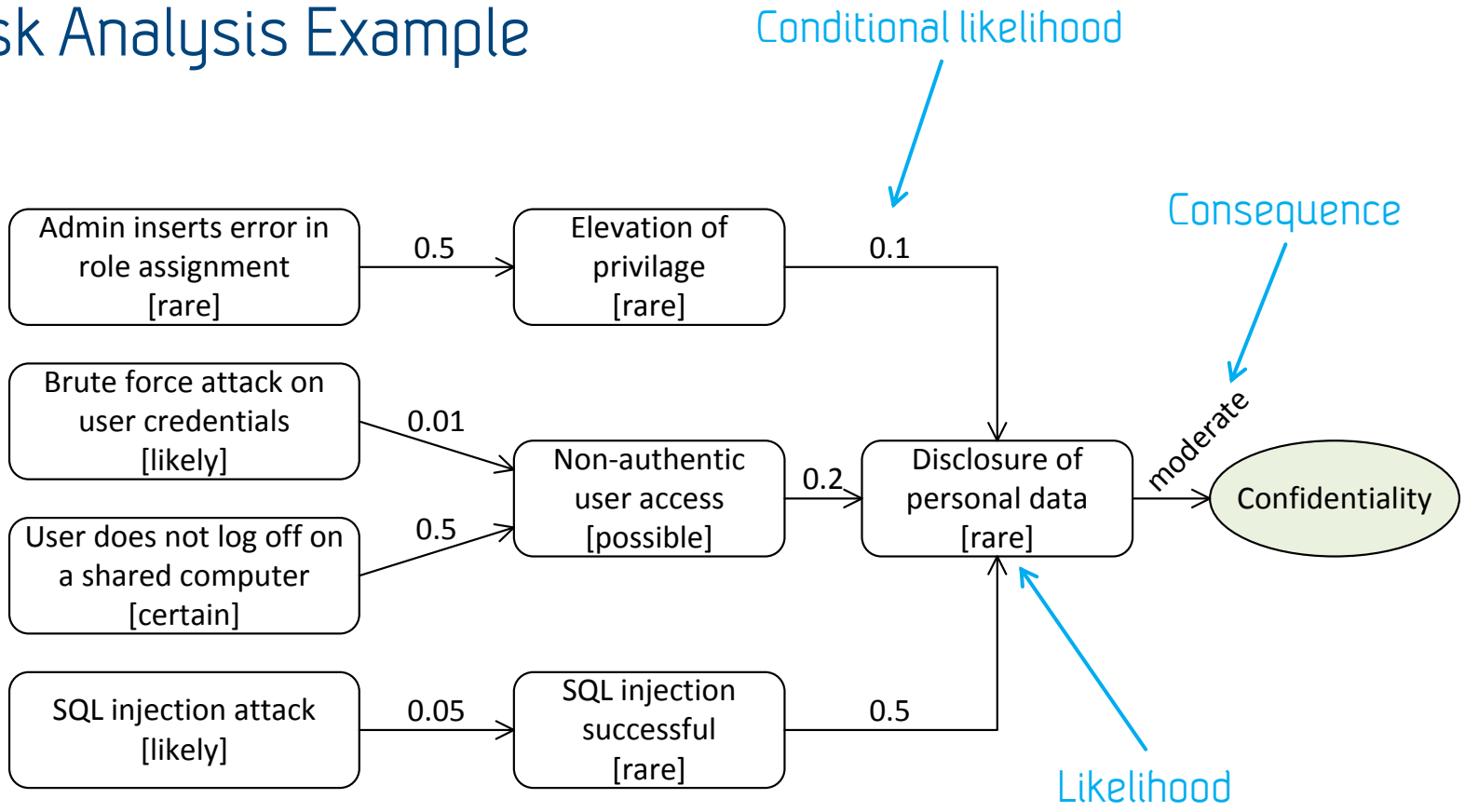


Risk Analysis

- The objective of this activity is to estimate the likelihood of incidents and their consequences for the assets they harm
- Qualitative or quantitative, depending on our choice of scales and criteria
- The data is gathered from historical data, interviews, brainstorming, testing, …

- In addition to estimating likelihoods of incidents, the risk analysis should seek to identify the most important sources of risk
  - Deliberate threats (motivation, required skills, required time and resources,…)
  - Vulnerabilities and existing controls
  - Likelihood of preceding threat scenarios
  - Conditional likelihoods

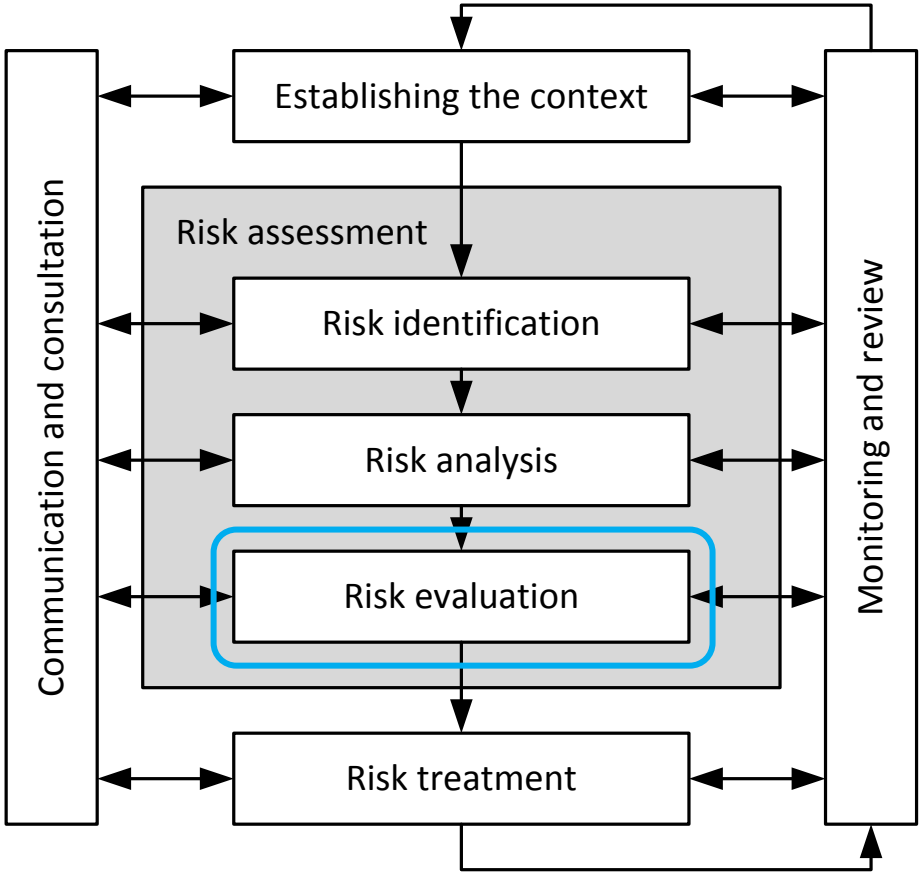
Risk Analysis Example



Risk Analysis – Some Guidelines

- Try to estimate the likelihood of each scenario, relation and incident separately
- Use rules for reasoning about likelihoods to identify possible mutual inconsistencies
  - Inconsistencies may indicate elements for which there are mistakes or misunderstandings
- Use rules to calculate missing estimates when estimation cannot be done directly
- Take into account whether the diagram is complete or not
- Take into account statistical dependencies

Risk Management Process



Risk Evaluation

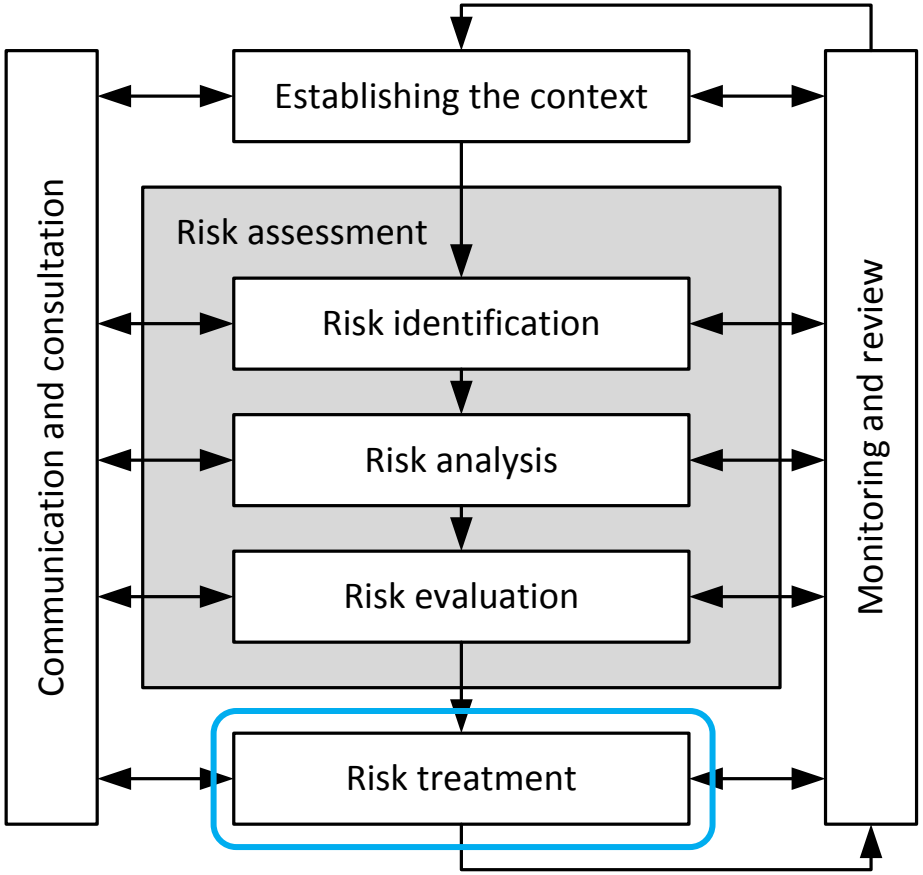
- This activity is to determine which risks are acceptable and which risks need to be considered further for possible treatment
- Risk are evaluated by comparing them against the predefined risk evaluation criteria

- Note that for each incident, we must consider all assets the incident may harm
- Need also to consider the aggregation and combinations of risks

Risk Evaluation Example

	Insignificant	Minor	Moderate	Major	Catastrophic
Unlikely					
Rare			DFD		
Possible			WSU		
Likely					
Certain					

Risk Management Process



Risk Treatment

- This activity is to identify controls for mitigating unacceptable risks
- Treatments are to reduce, retain, avoid or share risks

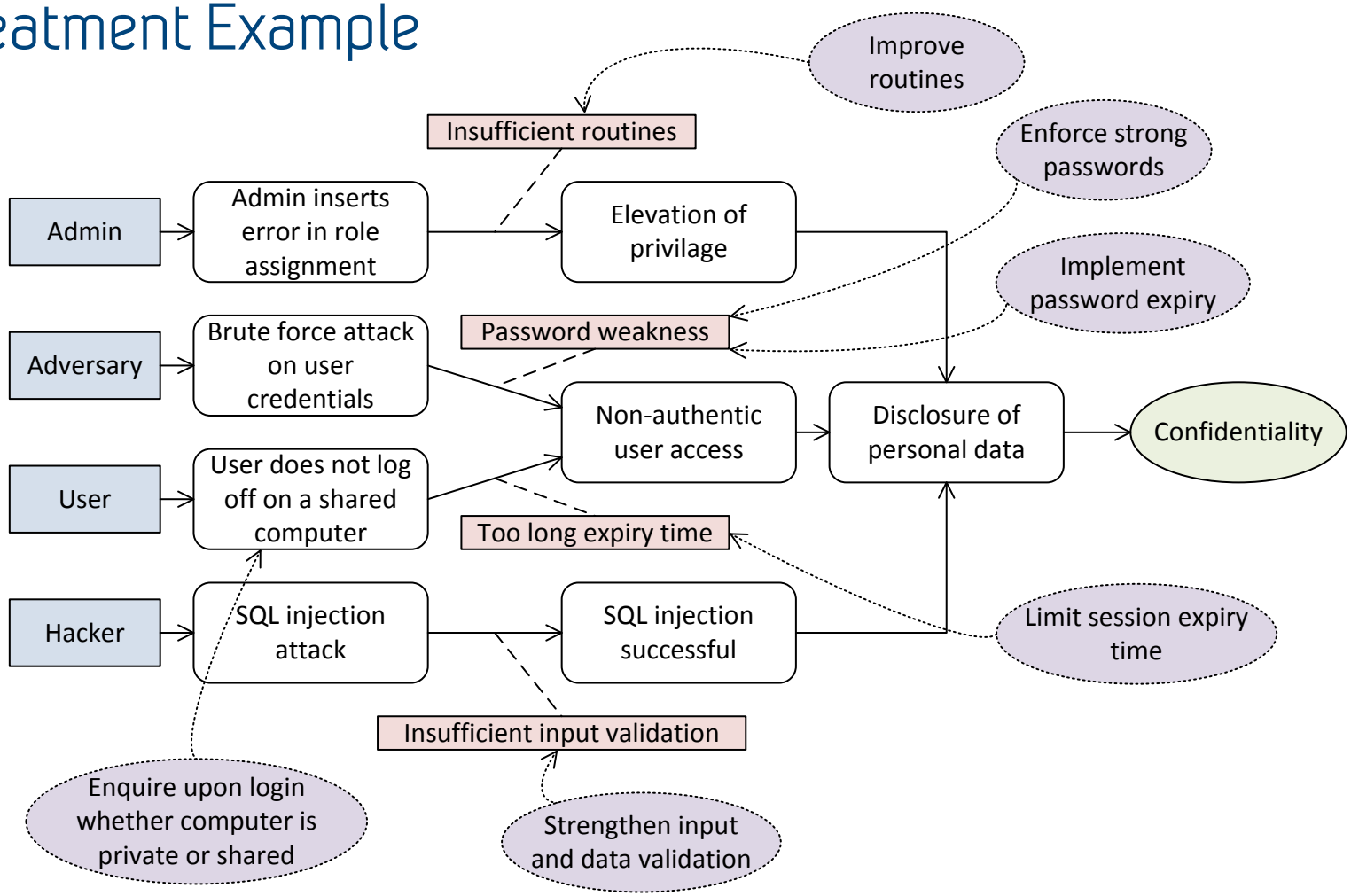
- For each identified treatment, its cost and benefit should be estimated, and the residual risk should be assessed
  - Note: Even risks that in principle are unacceptable cannot be treated at any cost
- The activity is concluded by specifying and documenting a risk treatment plan

Risk Treatment Options

- The options are not mutually exclusive and can often be used in combination
  - Reduce: Implement controls to reduce likelihood and/or consequence of incidents
  - Retain: Accept the risk (by informed decision)
  - Avoid: Terminate the activities or processes that lead to the risk
  - Share: For example by insurance, contracts, outsourcing, sub-contracting

- ISO 27001 comes with a list of controls that can be considered

Risk Treatment Example



Part III
Selected Issues

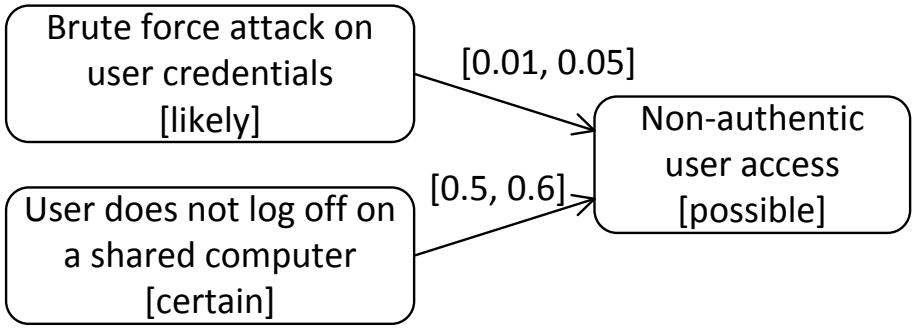
Uncertainty

- Uncertainty is inherent to risk and risk assessment
- In risk assessment we are confronted with two kinds of uncertainty
  - Aleatory
  - Epistemic
- Aleatory uncertainty is due to the inherent randomness of systems and pertains to chance
  - E.g. the tossing of a coin or the cards a poker player receives
  - It is an uncertainty that cannot be removed from systems (without redesign)
- Epistemic uncertainty pertains to ignorance or lack of evidence
  - It is an uncertainty that we actively seek to reduce by gathering more information and evidence (by empirical studies)

Uncertainty of Risk

- Risk assessment is about predicting future scenarios or outcomes
- For each identified outcomes we may e.g. assign a probability $p \in [0,1]$
- In cases of perfect knowledge and where p is close to 0 or 1, the outcome is almost certain
  - No epistemic uncertainty and little/no aleatory uncertainty
- If p is close to 0.5 the outcome is increasingly uncertain (aleatory)
- Should knowledge be imperfect we additionally have a degree of epistemic uncertainty
  - This can be documented e.g. by using an interval $P \subseteq [0,1]$
  - The correct probability is then assumed to be a value $p \in P$

Modeling Uncertainty



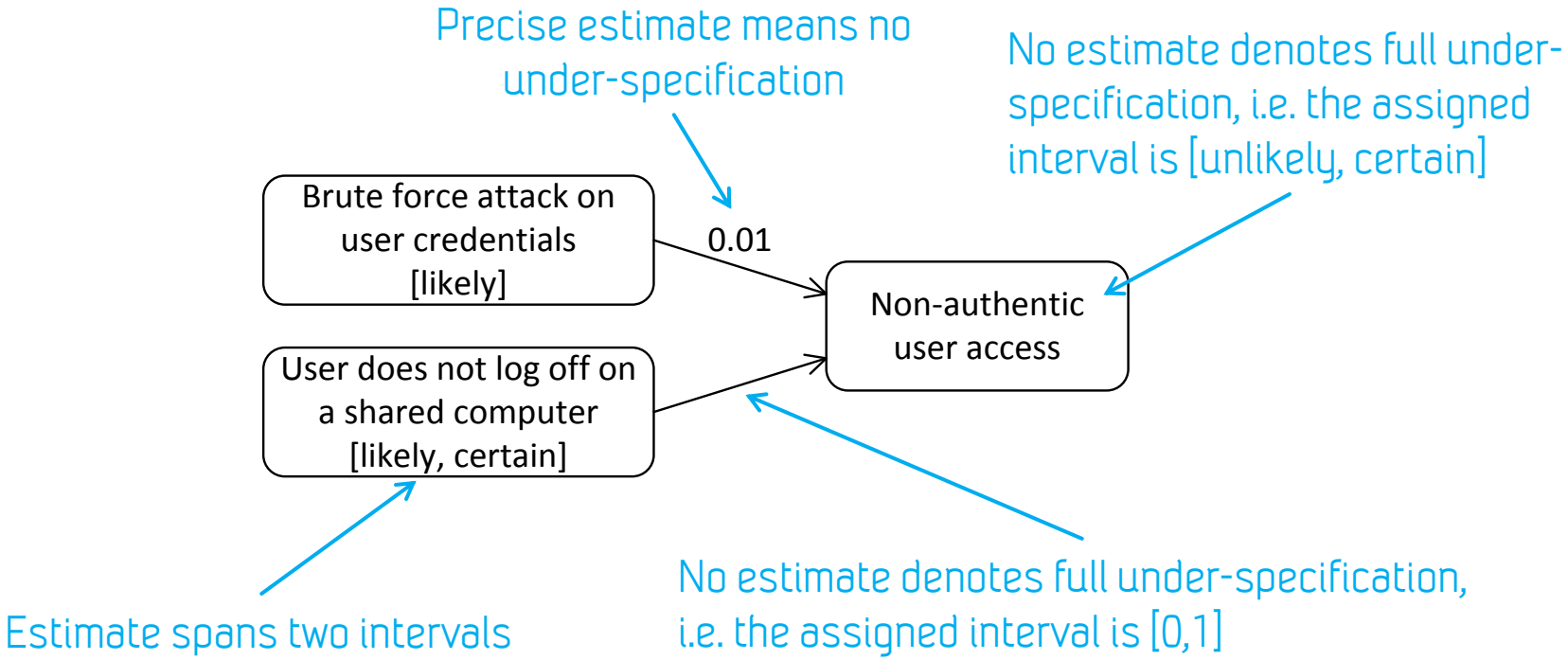
- In our examples we used intervals for likelihood estimates
  - If the model is correct, the correct likelihoods are within the respective intervals
- We do not explicitly distinguish between aleatory and epistemic uncertainty

- Some approaches to risk assessment use exact values in combination with an estimate of uncertainty
  - This is a possible option, but should be used with care
  - Strive to keep things simple and intuitive to understand!

- Remember: Some degree of uncertainty in risk assessment is unproblematic
  - Eventually, we only need to be able to distinguish between risk levels when the difference is significant for the evaluation and decision making

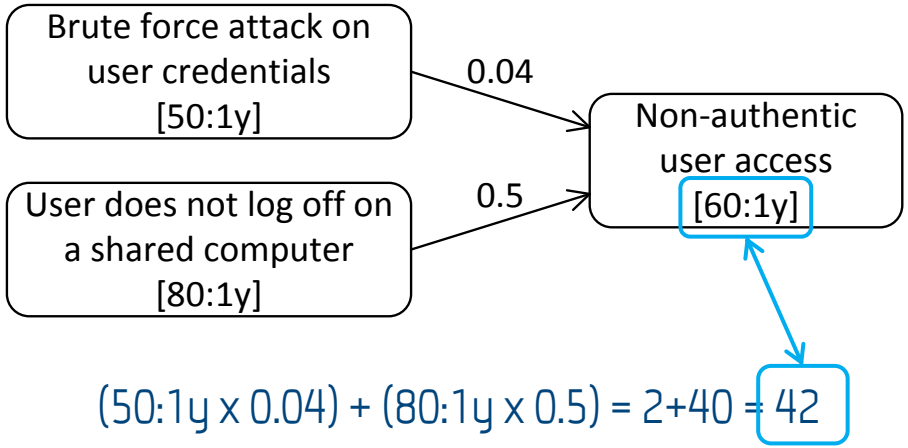
Under-specification of Likelihoods

- The use of intervals is a form of under-specification
- By increased knowledge, the under-specification (uncertainty) is reduced



Completeness of Diagrams

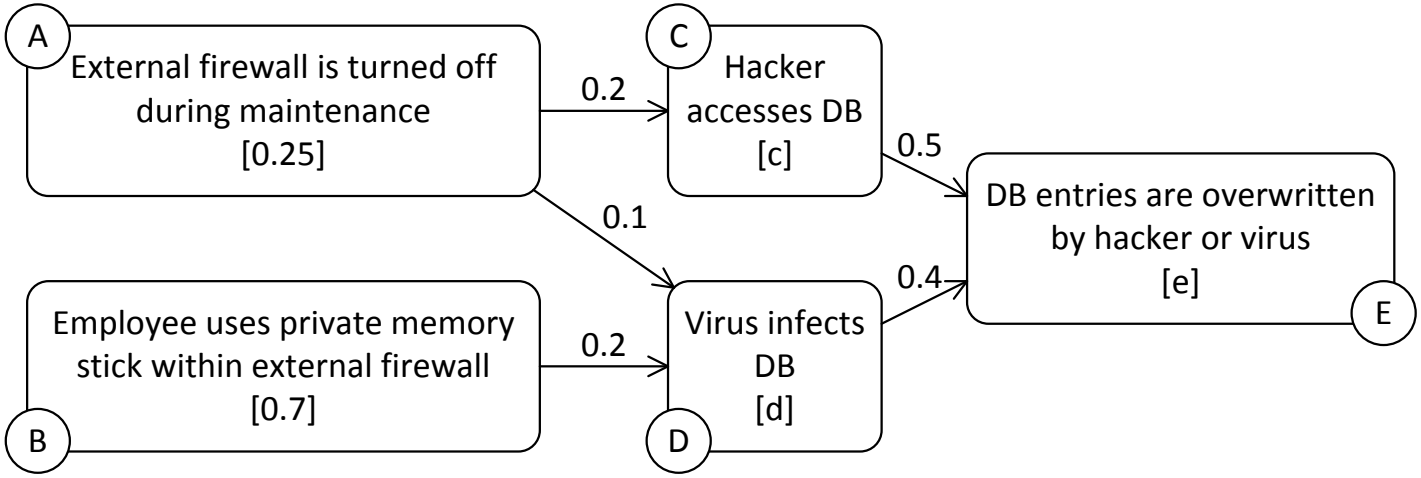
- If the diagram is complete we have modeled all sources of risk
  - In that case we can calculate likelihoods based on preceding scenarios
- If the diagram is incomplete there are risk sources that are not accounted for
  - This is most common in any risk analysis
  - In that case we can calculate lower bounds of likelihoods



The diagram is consistent if incomplete and inconsistent if complete

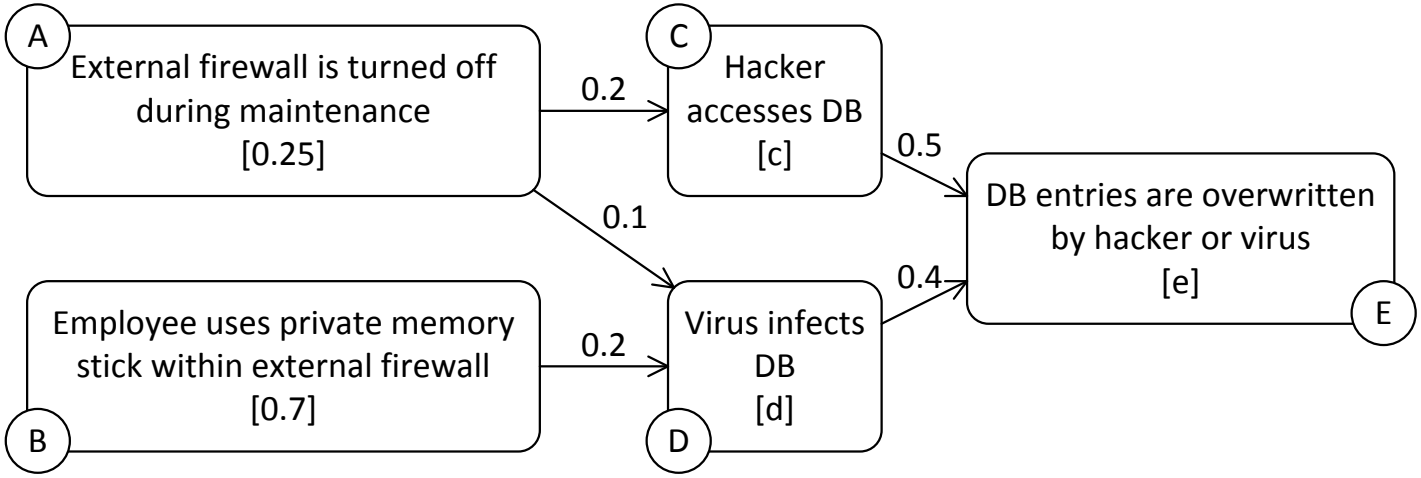
Example: Reasoning with Probabilities

- Assume the diagram is complete
- A and B are statistically independent
- C and D are not statistically independent



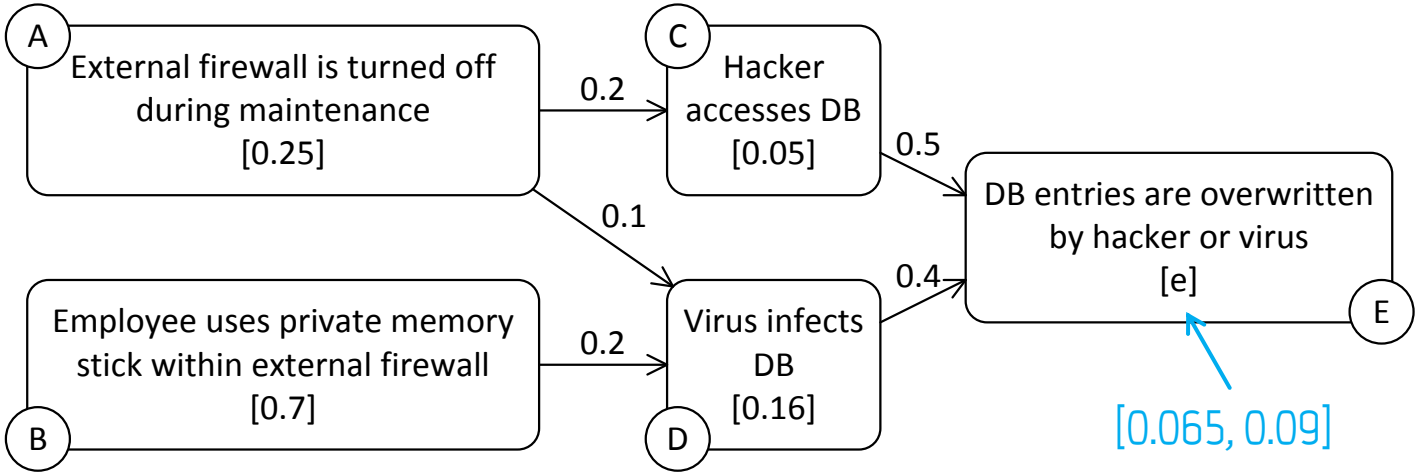
Example: Reasoning with Probabilities

- c = 0.25 x 0.2 = 0.05
- d is calculated from A and B
  - A) 0.25 x 0.1 = 0.025
  - B) 0.7 x 0.2 = 0.14
  - d = 0.025 + 0.14 – (0.025 x 0.14) = 0.1615



Example: Reasoning with Probabilities

- C and D are neither statistically independent nor mutually exclusive
- We can therefore calculate only the lower and upper bounds of E
  - e cannot be higher than the sum of the contribution from C and D
  - e cannot be lower than the max of the contributions from C and D
- Max: (0.05 x 0.5) + (0.1615 x 0.4) = 0.025 + 0.0646 = 0.0896
- Min: 0.0645



Concluding Recommendations

- Define the terminology you use and make sure it is commonly understood
- Do not underestimate the importance of establishing the context and describing the target of analysis
  - Develop precise documentation
  - Actively seek for possible misunderstandings
  - Specify and document all assumptions
- Focus on the identified assets
- Ensure that the semantics of the models are well-defined and understood

- Keep things as simple as possible!

Thank You!

- Acknowledgments:

www.nessos-project.eu

www.rasenproject.eu

https://securitylab.disi.unitn.it/doku.php?id=emfase