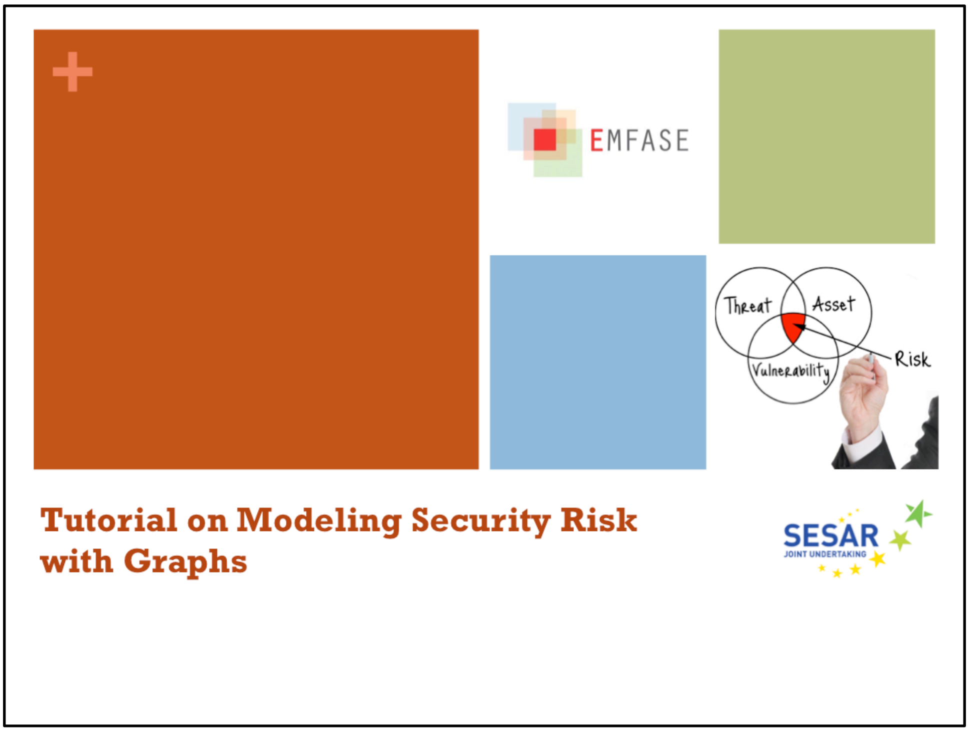
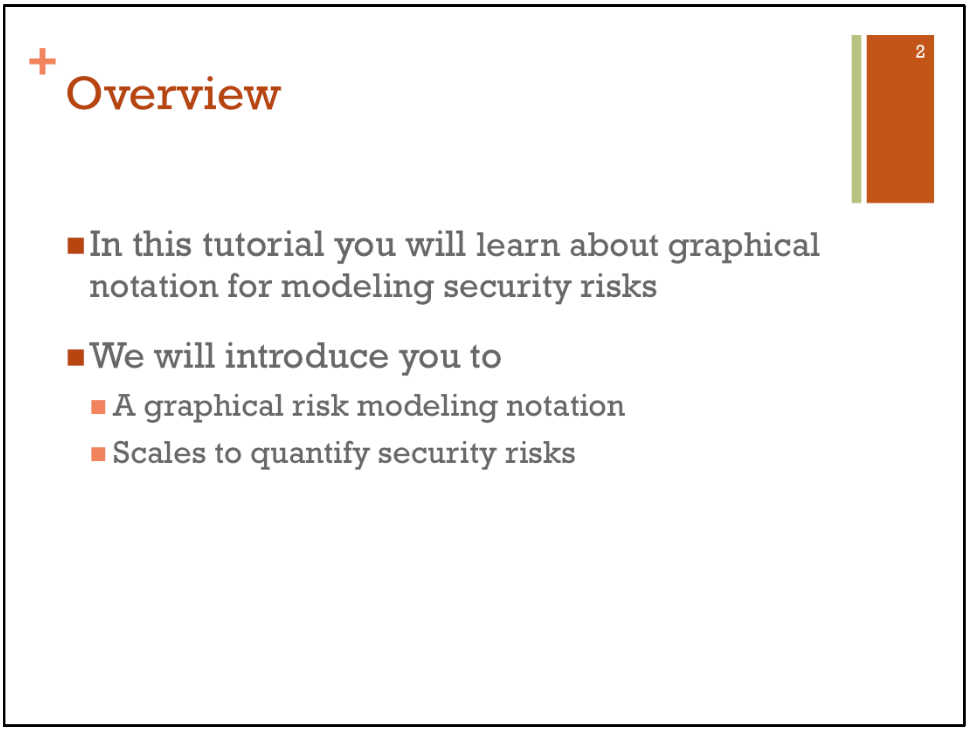


Tutorial on Modeling Security Risk with Graphs

This tutorial is on modeling security risks using graphs. It is targeted to security professionals as well as anyone is interested in knowing more about security risk modeling.

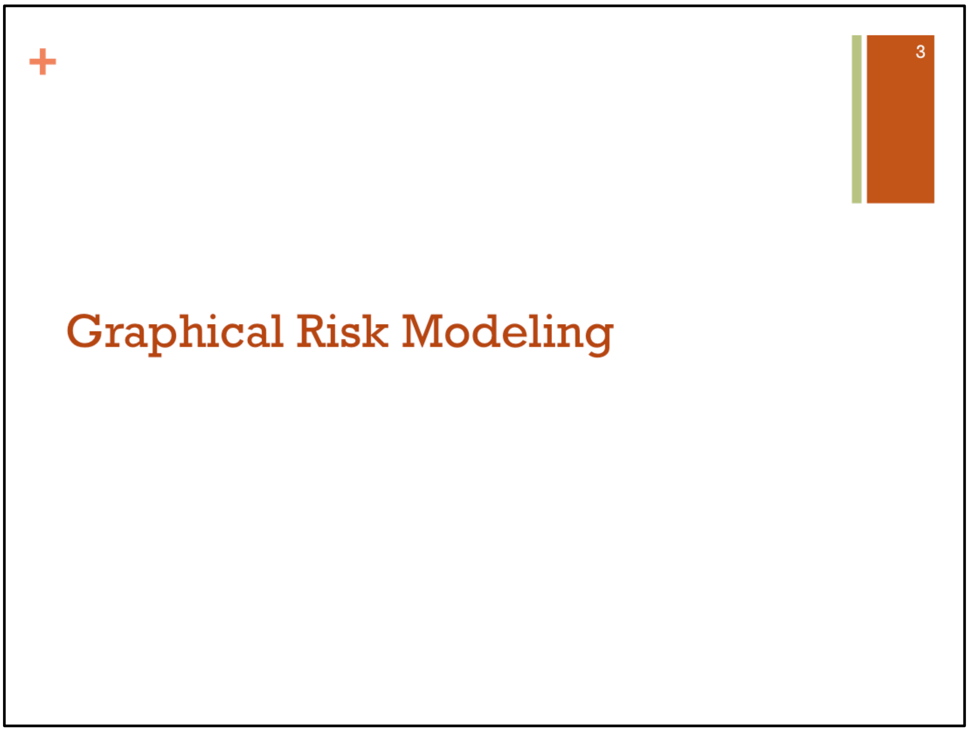


+ Overview

2

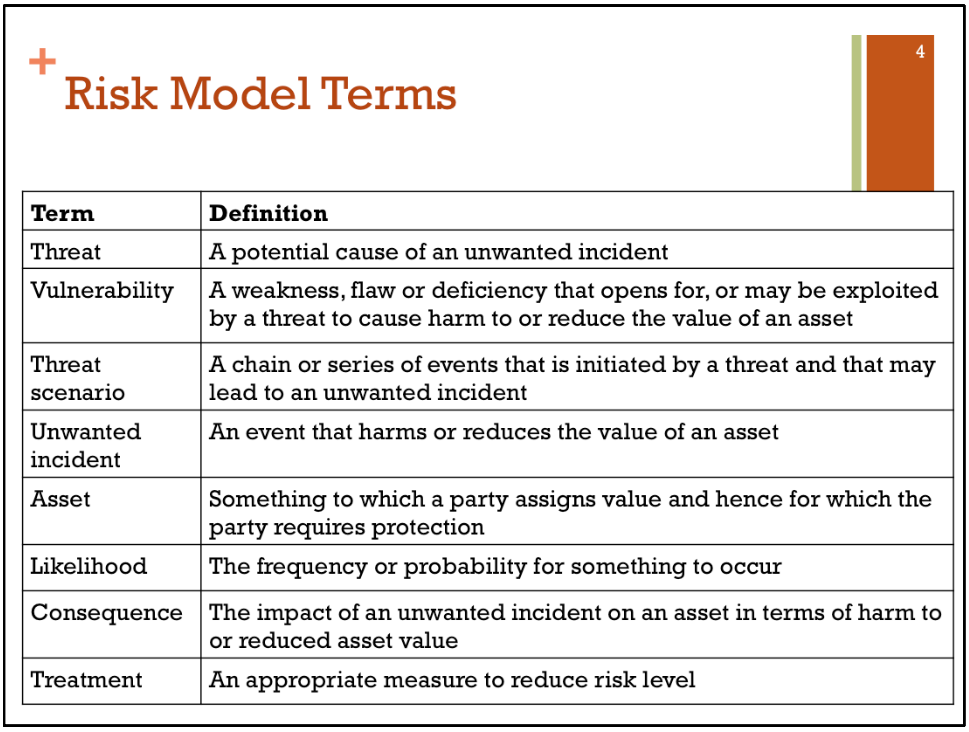
- In this tutorial you will learn about graphical notation for modeling security risks
- We will introduce you to
  - A graphical risk modeling notation
  - Scales to quantify security risks

This tutorial will give you the basics to model security risks using graphs. We will introduce you to a graphical approach based on UML to identify, communicate and document security risks. We will also explain you how to evaluate security risks.



Graphical Risk Modeling

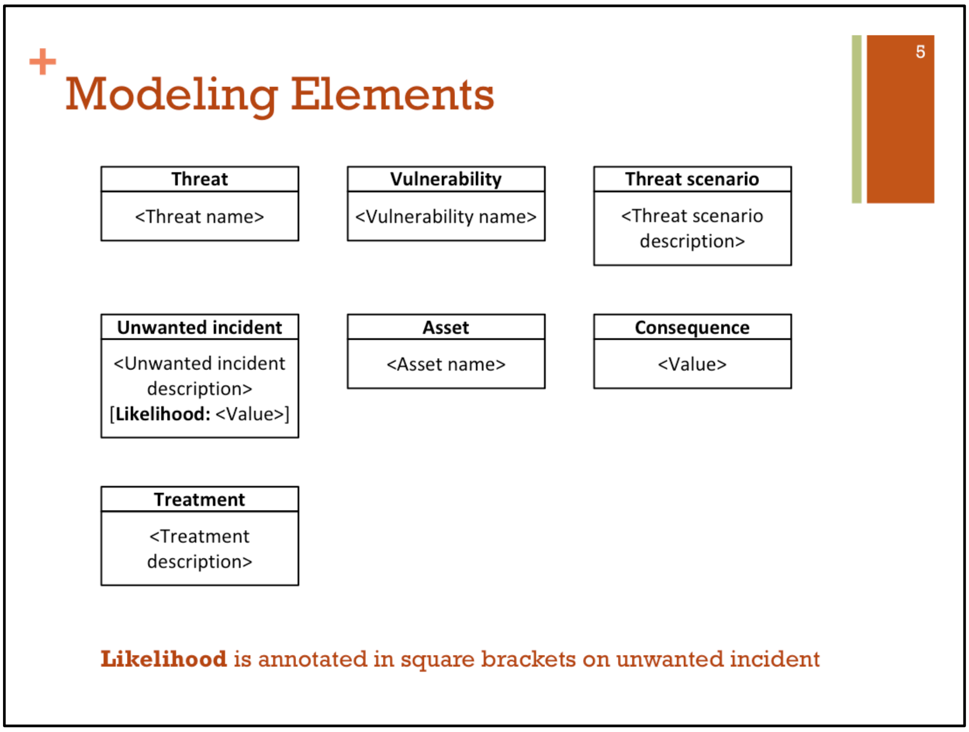
Let’s get started with the UML based approach to model security risks



+ Risk Model Terms

Term	Definition
Threat	A potential cause of an unwanted incident
Vulnerability	A weakness, flaw or deficiency that opens for, or may be exploited by a threat to cause harm to or reduce the value of an asset
Threat scenario	A chain or series of events that is initiated by a threat and that may lead to an unwanted incident
Unwanted incident	An event that harms or reduces the value of an asset
Asset	Something to which a party assigns value and hence for which the party requires protection
Likelihood	The frequency or probability for something to occur
Consequence	The impact of an unwanted incident on an asset in terms of harm to or reduced asset value
Treatment	An appropriate measure to reduce risk level

The UML-based graphical notation uses a set of standard concepts used in security risk analysis which you can see in the slide.



5

Modeling Elements

Threat
<Threat name>

Vulnerability
<Vulnerability name>

Threat scenario
<Threat scenario description>

Unwanted incident
<Unwanted incident description>
[**Likelihood:** <Value>]

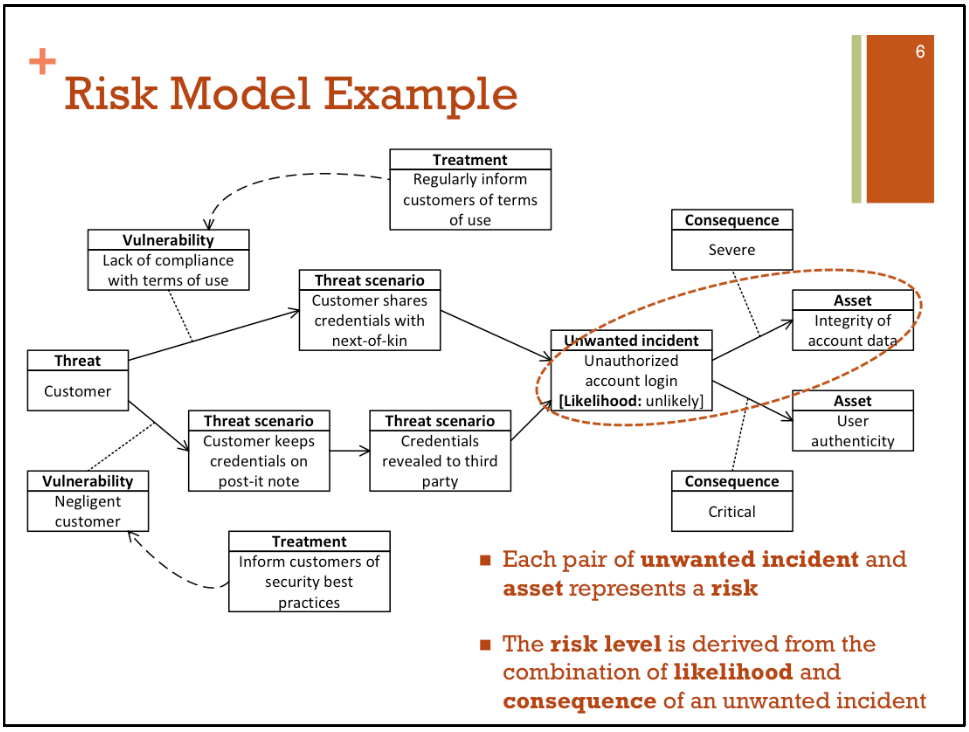
Asset
<Asset name>

Consequence
<Value>

Treatment
<Treatment description>

Likelihood is annotated in square brackets on unwanted incident

Each concept is graphically represented as a UML class. Each class is represented by a box which contains two parts. The top part specifies the name of the security concept, e.g. Threat or Vulnerability. The bottom part contains the name of the instance of the concept. If the class represents an unwanted incident, the likelihood of the unwanted incident is represented in the bottom part of the box with the unwanted incident name.



Risk Model Example

Treatment
Regularly inform customers of terms of use

Vulnerability
Lack of compliance with terms of use

Consequence
Severe

Threat scenario
Customer shares credentials with next-of-kin

Asset
Integrity of account data

Threat
Customer

Unwanted incident
Unauthorized account login
[Likelihood: unlikely]

Asset
User authenticity

Threat scenario
Customer keeps credentials on post-it note

Threat scenario
Credentials revealed to third party

Vulnerability
Negligent customer

Consequence
Critical

Treatment
Inform customers of security best practices

- Each pair of **unwanted incident** and **asset** represents a **risk**
- The **risk level** is derived from the combination of **likelihood** and **consequence** of an unwanted incident

Here a risk model represented in the UML notation is provided.

The threat customer initiates two different attack scenarios:

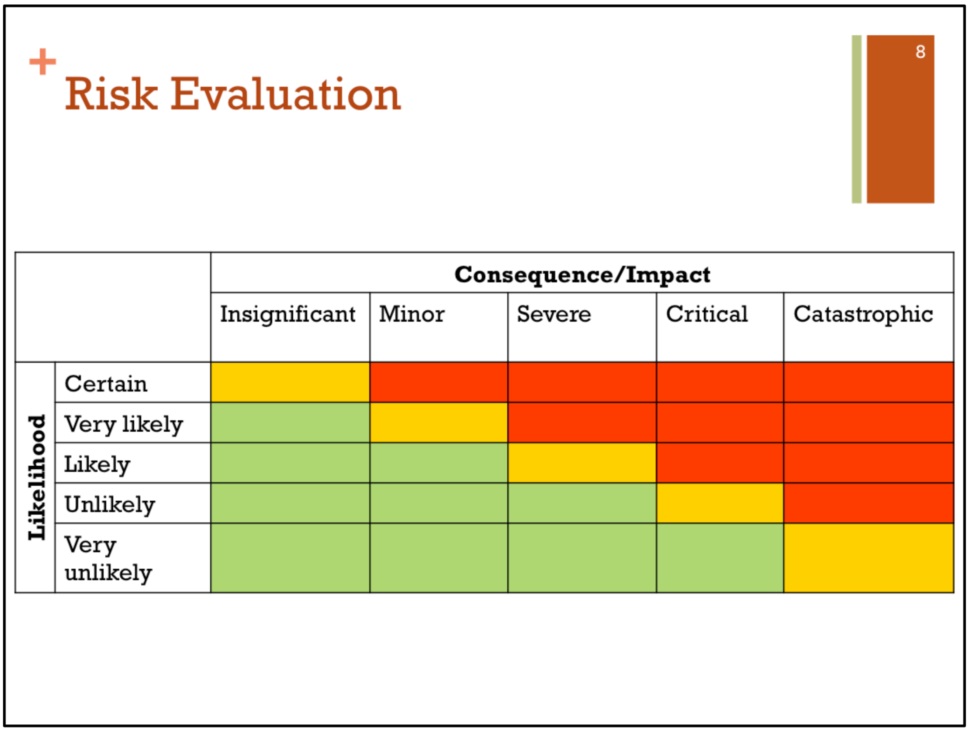
Scenario 1. The customer exploits vulnerability “Lack of compliance with terms of use” to initiate the threat scenario “Customer shares credentials with next-of-kin”
Scenario 2. The customer exploits vulnerability “Negligent customer” to initiate the threat scenario “Customer keeps credentials on post-it note” which leads to the threat scenario “Credential revealed to third party”.

Both scenarios lead to the unwanted incident “Unauthorized account login” which impacts the assets “Integrity of account data” and “User authenticity”.

The risk of the unwanted incident "Unauthorized account login" is given by the likelihood that it occurs and the consequences that it has on the assets
- “Integrity account data" and
- “User authenticity”
The likelihood of the unwanted incident “Unauthorized account login" is a label of the unwanted incident
Consequences are specified by the arrows from the unwanted incident.
To reduce the risk, we need to mitigate the two threat scenarios.
The first one is mitigated by the treatment “Regularly inform customers of terms of use", while the second one is mitigated by the treatment “Inform customers of security best practices"

HOW TO EVALUATE SECURITY RISKS

The next section is dedicated to the evaluation of the security risks.



Risk Evaluation

		Consequence/Impact				
		Insignificant	Minor	Severe	Critical	Catastrophic
Likelihood	Certain	🟨	🟥	🟥	🟥	🟥
	Very likely	🟩	🟨	🟥	🟥	🟥
	Likely	🟩	🟩	🟨	🟥	🟥
	Unlikely	🟩	🟩	🟩	🟨	🟥
	Very unlikely	🟩	🟩	🟩	🟩	🟨

Risk value of an unwanted incident of a threat scenario is computed on a risk evaluation matrix.

The matrix has on the rows the possible values that the likelihood can assume, and as columns the possible values that the consequence of impact can assume.

The entries of the map represent risk values:

- Risk values represented in green are risks that can be accepted
- Entries denoted in orange are risks that need to be monitored
- Red entries are risks that need to be treated. So a possible counter measure or treatment needs to be identified and implemented

Thank you for your attention