EMFASE

Tutorial on Modeling Security Risk with Tables

SESAR JOINT UNDERTAKING

Thanks to Poste italiane PT for the provision of the Scenario

Overview

- In this tutorial you will learn about tabular notations for modeling security risks
- We will introduce you to
  - NIST 800-300 Tabular Risk Modeling Notation
  - Scales to quantify security risks

NIST 800-30

NIST 800-30 Terms

Term	Definition
Overall likelihood	The likelihood that a threat event results in adverse impact
Level of impact	The degree of impact in terms of harm to assets
Security control	Safeguards or countermeasures to protect the confidentiality, integrity and availability of a system and its information

NIST 800-30 Terms

Term	Definition
Threat event	An event (or scenario) or situation that has the potential for causing undesirable consequences or impact
Threat source	The adversarial, accidental, structural or environmental exploitation of a vulnerability
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source
Impact	A harmful event that may occur given the potential for threats exploiting vulnerabilities
Asset	Operations, individuals, physical or non-physical entities that can be harmed due to a threat event and its impact

NIST Example

Threat event	Threat source	Vulnerability	Impact	Asset	Overall likelihood	Level of impact	Security control
Customer shares credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized account login	Integrity of account data	Unlikely	Severe	Regularly inform customers of terms of use
Customer shares credentials with next-of-kin	Customer	Lack of compliance with terms of use	Unauthorized account login	User authenticity	Unlikely	Critical	Regularly inform customers of terms of use
Customer keeps credentials on post-it note which is revealed to third party	Customer	Negligent customer	Unauthorized account login	Integrity of account data	Unlikely	Severe	Inform customers of security best practices
Customer keeps credentials on post-it note which is revealed to third party	Customer	Negligent customer	Unauthorized account login	User authenticity	Unlikely	Critical	Inform customers of security best practices

Risk level

Same risk, but other causes

Scales Risk and Criteria

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

EMFASE

SESAR JOINT UNDERTAKING

Thank you for your attention

Thanks to Posteitaliane PT for the provision of the Scenario