SESAR Security Risk Assessment Exercise

Federica Paci
University of Trento

What are we going to do

- Go this Dropbox folder
  - https://www.dropbox.com/sh/34a1pdbc0w3tn46/AACDN_nXVOowlc06z9zQpfJRa?dl=0
  - Read the file HouseBurglaryCase.pdf (10 min)
  - Download the file SecRAM-exercise-template.xlsx
  - We go through each step of SecRAM methodology
    - You apply the step to the application scenario (20 min)
    - We discuss together the results (15 min)

Training Material

- SecRAM guidelines and catalogues is confidential material
- The distribution of the material is on Wed 15th after the class
- We will ask you to sign a Non Disclosure Agreement
- Please download the Non Disclosure Agreement
- https://www.dropbox.com/s/6qie2olfzsd5msn/2014-Trento-SecurityEngineering-NDA.pdf?dl=0
- Fill it in with your personal data
- Return it on Wed 15th and you will get a personal copy of the training material

The scenario: Going on holidays

- Leave the key of the house to a trusted neighbour
- Leave a copy of the key of the house to the daughter
- No pets, intrusion alarm
- Printed Documents (passport, credict cards …) are kept in a locker
- Scanned documents are saved on the personal computer

Primary Assets Identification

- **GOAL:** List Primary Assets
- They are intangible entities
- What kind of information are processed/used in your target of analysis?
- What kind of services are executed/provided in your target of analysis?

Primary Asset Identification

Primary Asset ID	**Primary Asset**	**Type**
PA_1	Primary Asset 1	
PA_2	Primary Asset 2	
PA_3	Primary Asset 3	
.....		

Impact Assessment

- **GOAL:** Identify Impact on the CIA of primary asset
- For each primary asset x and for each security impact area y ask yourself the following questions
  1. If the confidentiality of primary asset "x" is compromised what would be the worst impact on the impact area "y"?"
  2. If the integrity of primary asset "x" is compromised what would be the worst impact on the impact area "y" ?"
  3. "If the availability of primary asset "x" is compromised what would be the worst impact on the impact area "y" ?"

Impact Assessment

Primary Asset	CIA	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact
Primary Asset 1	C								
	I								
	A								

Supporting Assets Identification

- **GOAL**: List all Supporting Assets
- They are tangible entities that enable the primary assets
- For each primary asset ask yourself the following questions:
  1. When and how is the primary asset used, by whom and for what purpose?
  2. When and how can the use of the primary asset be interrupted or prevented?
  3. How can a threat or other circumstances interrupt or prevent the use of the primary asset?
  4. Link the primary asset to at least a supporting asset

Supporting Assets Identification

	Primary Asset		
Supporting Asset	Primary Asset 1	……	…….
Supporting Asset 1			
Supporting Asset 2			

Threat Scenarios

- **GOAL**: Identify threats exploiting supporting asset vulnerabilities
- For each supporting asset

1. What can happen on this supporting asset if the confidentiality, integrity or availability is affected?
2. Use the catalogue of threats
3. Identify the impact of the threat scenario on confidentiality, integrity and availability of the primary asset (via supporting asset)
   a) The impact (Overall Impact) is inherited from the primary asset

The threat scenarios table

Supporting Assets	**Threats**	**Primary Assets**		
		One-Time Password		
		C	I	A
Supporting Asset 1	Threat A	5		
	Threat B	5	4	

Same as Overall Impact

Risk Evaluation

- **GOAL**: Assess the risk level of a threat
- For each threat
  1. Consider the maximum impact of all the CIA (Inherited Impact)
  2. Assume that the Inherited Impact and the Reviewed Impact are equal
  3. Assess the likelihood of the threat using risk assessment matrix
  4. Compute the risk level of the threat from the impact and likelihood using risk assessment matrix

The Impact Evaluation table

Maximum impact of all CIA

Supporting Assets	**Threats**	**Primary Assets**			**Inherited Impact**	**Reviewed Impact**
		Primary Asset 1				
		C	I	A		
Supporting Asset 1	Threat A	5			5	5
	Threat B	5	4		5	5

The Risk Assessment table

Supporting Assets	**Threats**	**Reviewed Impact**	**Likelihood**	**Risk Level**
Mobile Device	Theft	5	4	High
	Malicious Code	5	3	High

Risk Treatment

- **GOAL:** Identify security control to mitigate the risks
- For each threat with risk level "High"
  1. Select at least a security control from the catalogue

The Risk Treatment table

Supporting Assets	**Threats**	**Reviewed Impact**	**Likelihood**	**Risk Level**	**Controls**
Supporting Asset 1	Threat A	5	4	High	Control X Control Y
	Threat B	5	3	High	Control Z Control H