Asset-Oriented Threat Modeling (TrustCom 2020)

Improve the threat modeling process to provide a security assistance to architects during system design

Nan MESSE \textsuperscript{1} Vanea Chiprianov \textsuperscript{2} Nicolas Belloir \textsuperscript{2} Jamal El-Hachem \textsuperscript{2} Régis Fleurquin \textsuperscript{2} Salah Sadou \textsuperscript{2}

\textsuperscript{1}Université Toulouse - Jean Jaurès / SM@RT, IRIT, Toulouse
\textsuperscript{2}Université Bretagne Sud / ArchWare, IRISA, Vannes

7 novembre 2021
Plan

Problem statement

Structuring threat modeling

Proof-of-concept

Conclusion
Problem statement

- Threat enumeration is often held in brainstorming meetings, which is a subjective and unstructured activity.
Problem statement

- Threat enumeration is often held in brainstorming meetings, which is a subjective and unstructured activity

**Brainstorming**

- Knowledge gap
- Lack of guidance
- Lack of formalized process
- High dependence on participants
Problem statement

- Threat enumeration is often held in brainstorming meetings, which is a subjective and unstructured activity.

**Brainstorming**

- Knowledge gap
- Lack of guidance
- Lack of formalized process
- High dependence on participants

- The current threat modeling processes require a certain security knowledge level, making it a non-trivial task for participants with limited security knowledge.
Requirements

1. There is a need of a guidance in brainstorming that is more prescriptive, formal, reusable and less dependent on the aptitudes and knowledge of the participants
Requirements

1. There is a need of a guidance in brainstorming that is more prescriptive, formal, reusable and less dependent on the aptitudes and knowledge of the participants.

2. There is thus a need to propose a method that can be easily used or understandable by security novices.
Requirements

1. There is a need of a guidance in brainstorming that is more prescriptive, formal, reusable and less dependent on the aptitudes and knowledge of the participants

2. There is thus a need to propose a method that can be easily used or understandable by security novices

3. There is a need of a common language or a common concept that can be understood by all participants.
### An inventory of industrial threat modeling processes

<table>
<thead>
<tr>
<th>Phase</th>
<th>Activity</th>
<th>Asset Identification</th>
<th>Threat Enumeration</th>
<th>Threat Prioritization</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Identify security goal</td>
<td>Model domain</td>
<td>Identify asset</td>
<td>Identify threat</td>
</tr>
</tbody>
</table>

‘Anything that has value to an organization’

---

Plan

Problem statement

Structuring threat modeling

Proof-of-concept

Conclusion
A novel refinement of “asset”

<table>
<thead>
<tr>
<th>Asset</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Asset (DA)</td>
<td>Anything that has value for domain experts, towards the fulfilment of the function and goal of system, together with the assurance of its properties.</td>
</tr>
<tr>
<td>Vulnerable Asset (VA)</td>
<td>Anything that has value for security experts. It has vulnerabilities that can be menaced by threats.</td>
</tr>
<tr>
<td>Vulnerable Domain Asset (VDA)</td>
<td>Anything that has value for domain experts, but also has vulnerabilities that can be menaced by threats.</td>
</tr>
</tbody>
</table>

2. Asset: anything that has value to an organization. (ISO27001)
An asset-based reference model
An asset-based reference model

Raspberry Pi is a Single-board Computer
Raspberry Pi has a GPS Module
GPS Signal depends on a GPS Module
The B-Tree structure

Structure:

```
\[ \text{Root} \]
\[ \text{is} \]
\[ \text{is} \]
\[ \text{is} \]

\[ \text{Key2} \quad \text{depends} \quad \text{Key1} \]
\[ \text{has} \]
\[ \text{Child1} \]
\[ \text{Child2} \]
\[ \text{Child3} \quad \text{...} \]
```

Example:

```
\[ \text{Single-board Computer} \]
\[ \text{is} \]
\[ \text{has} \]

\[ \text{GPS Signal} \]
\[ \text{depends} \]

\[ \text{ARM CPU/GPU} \quad \text{GPS Module} \]
\[ \text{has} \]
\[ \text{Raspberry Pi} \]
```

9/20
Asset identification process: major tasks

1. Brainstorming
2. VA Library
3. Domain Asset (DA)
4. Vulnerable Domain Asset (VDA)
5. Select
6. Compare Similarity
7. Modifiable GPS Signal
Building VA library

Extraction of VA from CAPEC$^3$ respecting B-Tree structure

1000 - Mechanisms of Attack

- Engage in Deceptive Interactions - (156)
  - Content Spoofing - (148)
  - Checksum Spoofing - (145)
  - Spoofing of UDDI/ebXML Messages - (218)
  - Intent Spoof - (602)
  - Counterfeit GPS Signals - (627)
  - Carry-Off GPS Attack - (628)
- Identity Spoofing - (151)

3. https://capec.mitre.org/
Some rules to extract VAs and their relations basing on CAPEC

- **Rule 1**: 'contaminate' | 'poison' | 'leverage' | 'manipulate' | 'abuse' | 'exploit' | 'misuse' + VA (Ex. 'Poison web service registry');
- **Rule 2**: VA + 'manipulation' | 'poisoning' | 'tampering' | 'alteration' (Ex. 'Web service protocol manipulation');
- **Rule 3**: VA + 'injection' | 'inclusion' | 'insertion'; VA = 'Untested' + VA + 'Input' (Ex. 'XML injection', VA = 'UntestedXMLInput');
- **Rule 4**: 'childOf' → 'is' | 'has' (Ex. 'SOAP manipulation' is a 'web services protocol manipulation'; 'XML injection' has 'DTD injection');
- **Rule 5**: 'canFollow' → 'depends'. 
Plan

Problem statement

Structuring threat modeling

Proof-of-concept

Conclusion
Microsoft SDL threat modeling process

WebSphere Application Server Version 7.0:

Microsoft SDL threat modeling tool\(^4\)

---

I. Integrating our process into Microsoft SDL threat modeling process – DA
II. Integrating our process into Microsoft SDL threat modeling process – VA
III. Integrating our process into Microsoft SDL threat modeling process – VDA

Result: 14 threats found
A reusable BASH prototype for security experts

Figure – An excerpt of BASH application result

5. https://github.com/lunanan/ArchwareExtraction
Plan

Problem statement

Structuring threat modeling

Proof-of-concept

Conclusion
Conclusion

Structuring the threat modeling process:

- An asset-based reference model
- An asset identification process
- Extraction of VA to build a VA library
- Integrating with current threat modeling process such as the Microsoft SDL one

Perspectives:

- Evaluating the asset identification process with industrial case studies
- Automating the security knowledge base extraction