Asset-Oriented Threat Modeling (TrustCom 2020)

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

Nan MESSE [1] Vanea Chiprianov [2] Nicolas Belloir [2] Jamal El-Hachem [2] Régis Fleurquin [2] Salah Sadou [2]

[1] Université Toulouse - Jean Jaurès / SM@RT, IRIT, Toulouse

[2] Université Bretagne Sud / ArchWare, IRISA, Vannes

7 novembre 2021

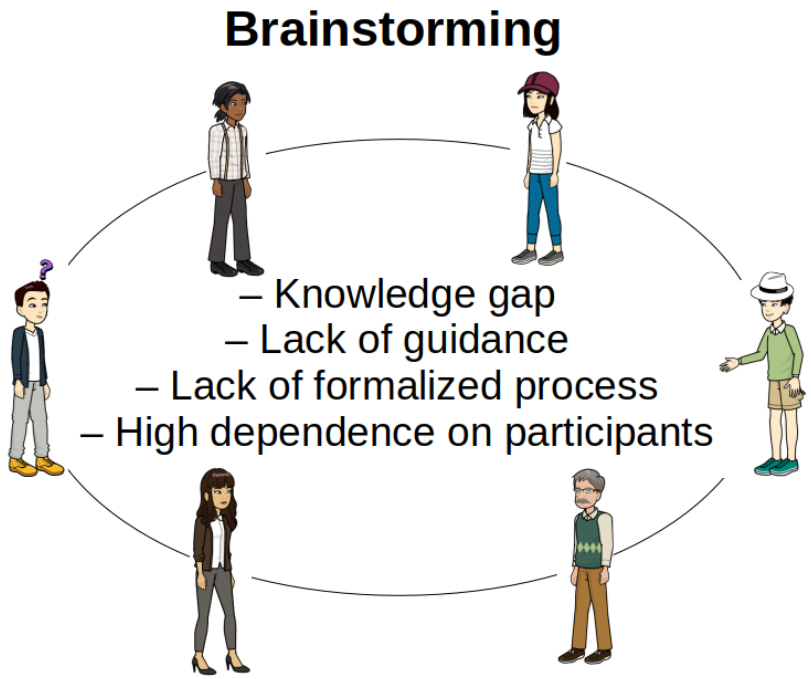
Plan

Problem statement

- Threat enumeration is ofen hold in brainstorming meetings, which is a subjective and unstructured activity

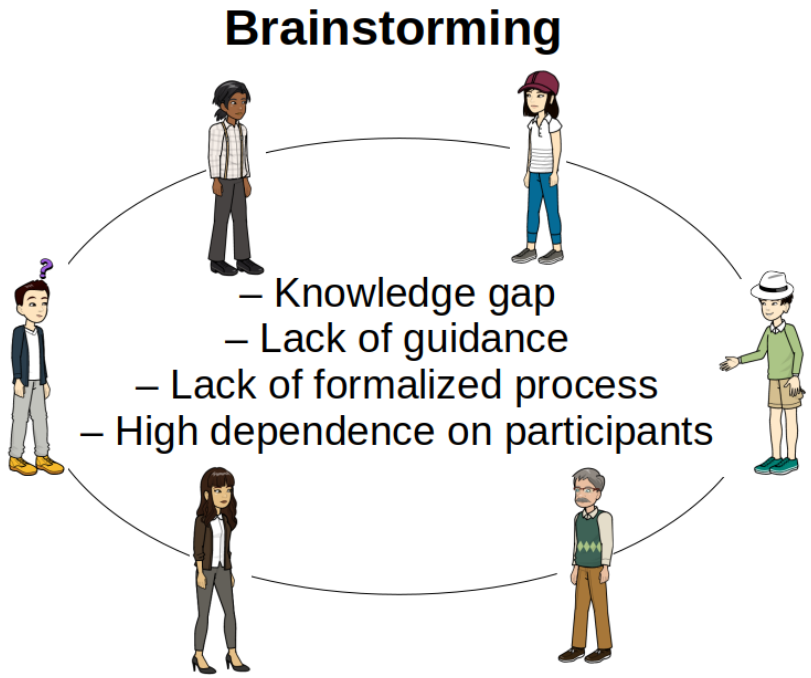
Problem statement

- Threat enumeration is ofen hold in brainstorming meetings, which is a subjective and unstructured activity



Problem statement

- Threat enumeration is ofen hold in brainstorming meetings, which is a subjective and unstructured activity



- 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

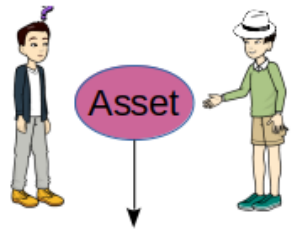
1. There is a need of a guidance in brainstorming that is more prescriptive, formal, reusable and less dependent on the aptitudes and knowledge of the participants
2. There is thus a need to propose a method that can be easily used or understandable by security novices

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

Phase	Asset Identification			Threat Enumeration				Threat Prioritization		Mitigation	
Activity / Paper	Identify security goal	Model domain	Identify asset	Identify threat	Enumerate &document threat	Describe attacker	Identify vulnerability	Rate threat	Assess risk	Mitigation	Verification
Torr (2005) [15]		X		X						X	X
Shostack (2008) [12]		X			X					X	X
Scandariato (2013) [11]		X		X	X						
Beckers (2013) [1]		X	X	X	X	X					
Dhillon (2011) [4]		X		X					X	X	
Steven (2010) [13]	X	X		X			X				
Kamatchi (2016) [6]		X	X	X	X			X			

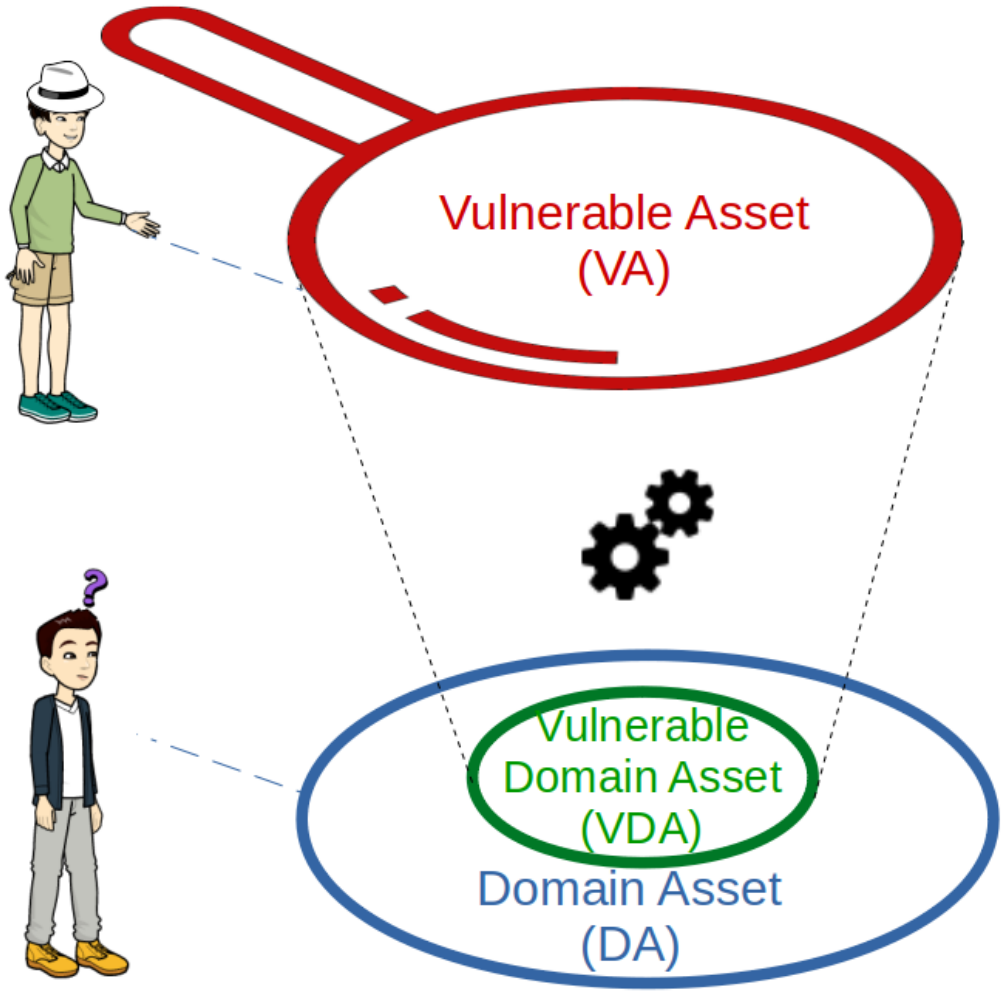


'Anything that has value to an organization'

1. Joel Brenner. "ISO 27001 : Risk management and compliance". In : *Risk management* 54.1 (2007), p. 24.

Plan

A novel refinement of "asset"

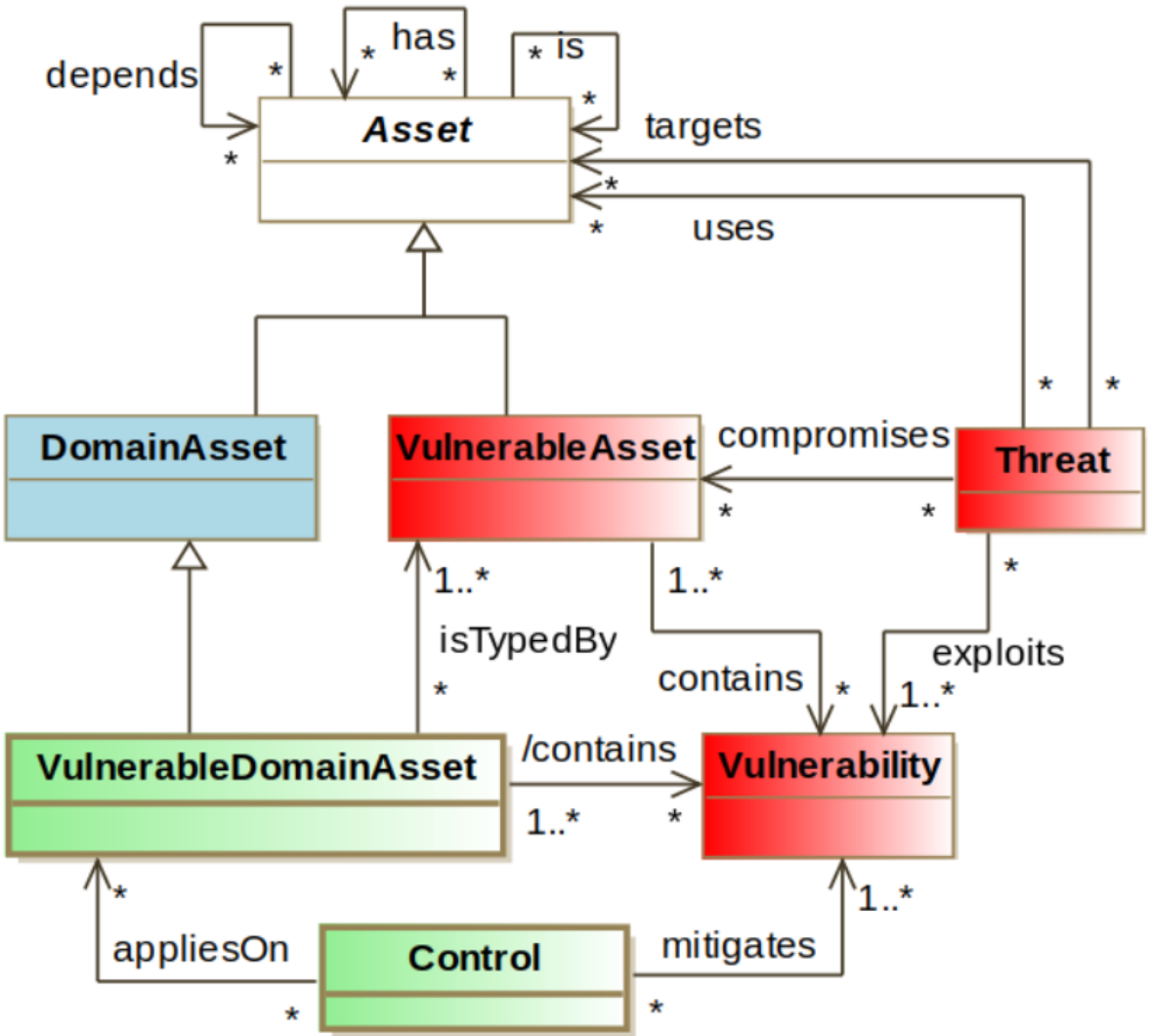


Asset	Definition
Domain Asset (**DA**)	Anything that has value for domain experts, towards the fulfilment of the function and goal of system, together with the assurance of its properties.
Vulnerable Asset (**VA**)	Anything that has value for security experts. It has vulnerabilities that can be menaced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

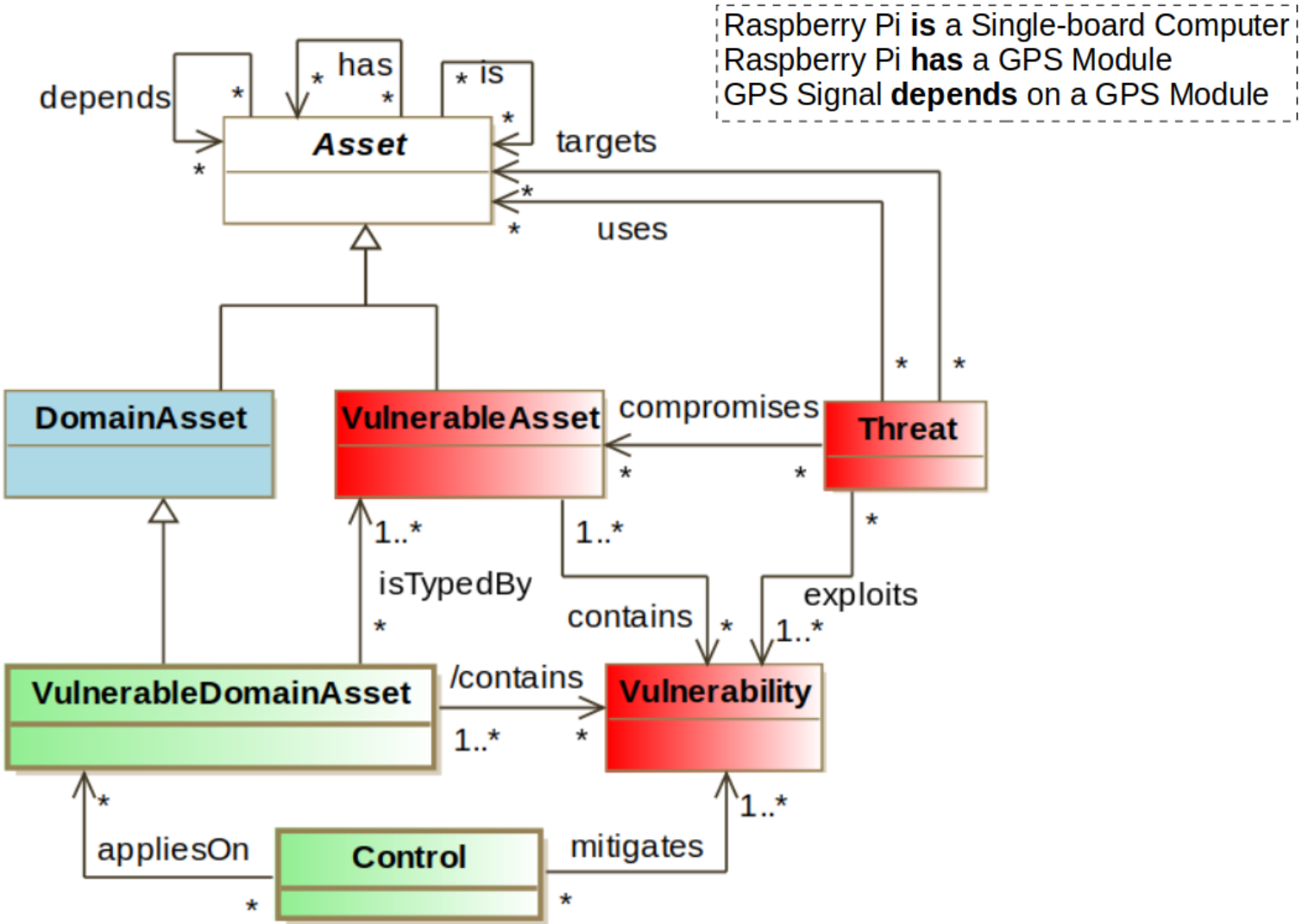
2

2. **Asset: anything that has value to an organization. (ISO27001).**

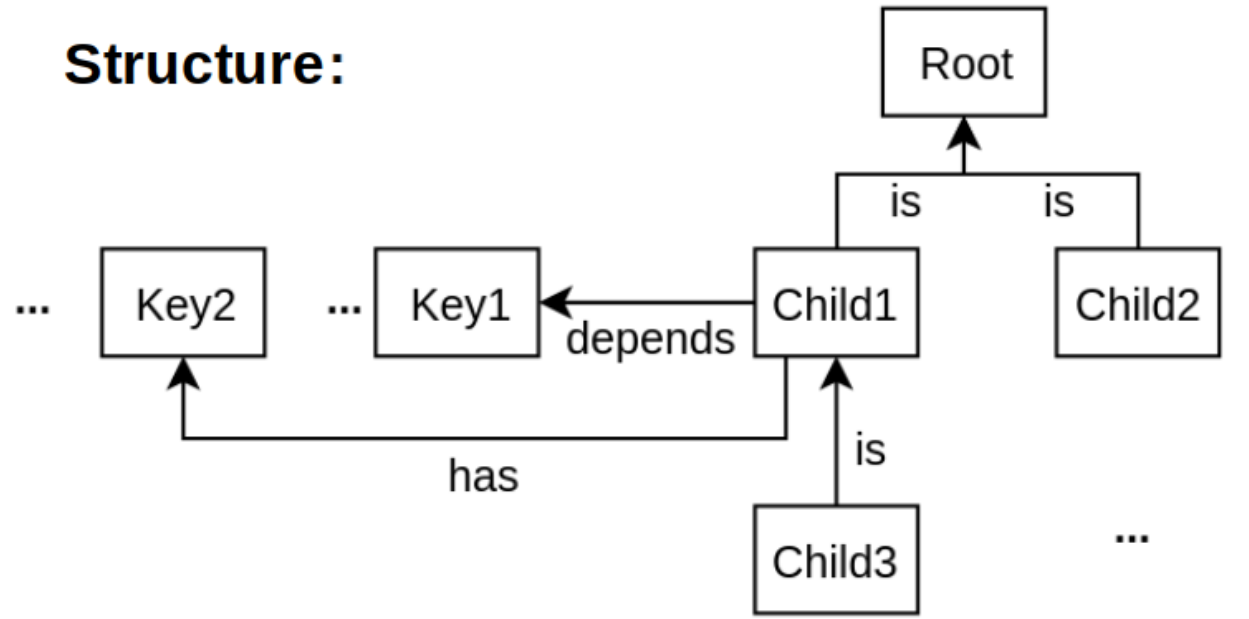
An asset-based reference model

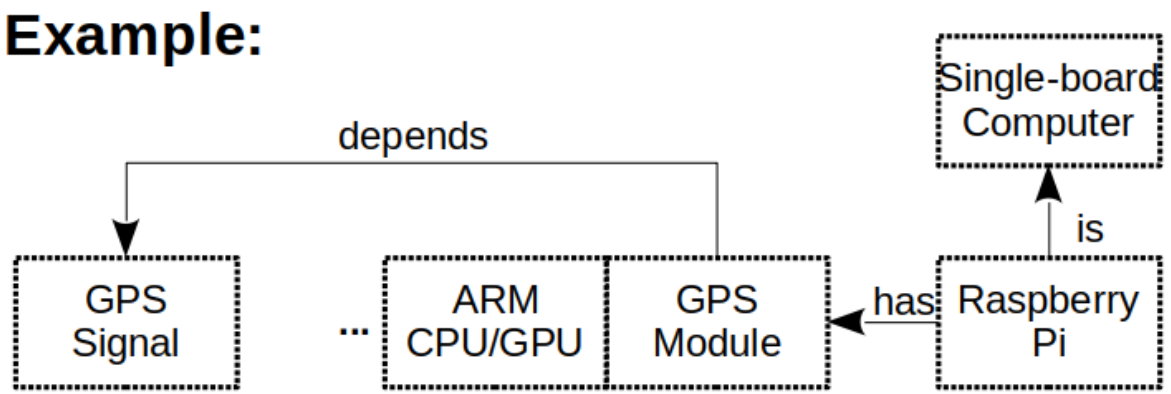


An asset-based reference model

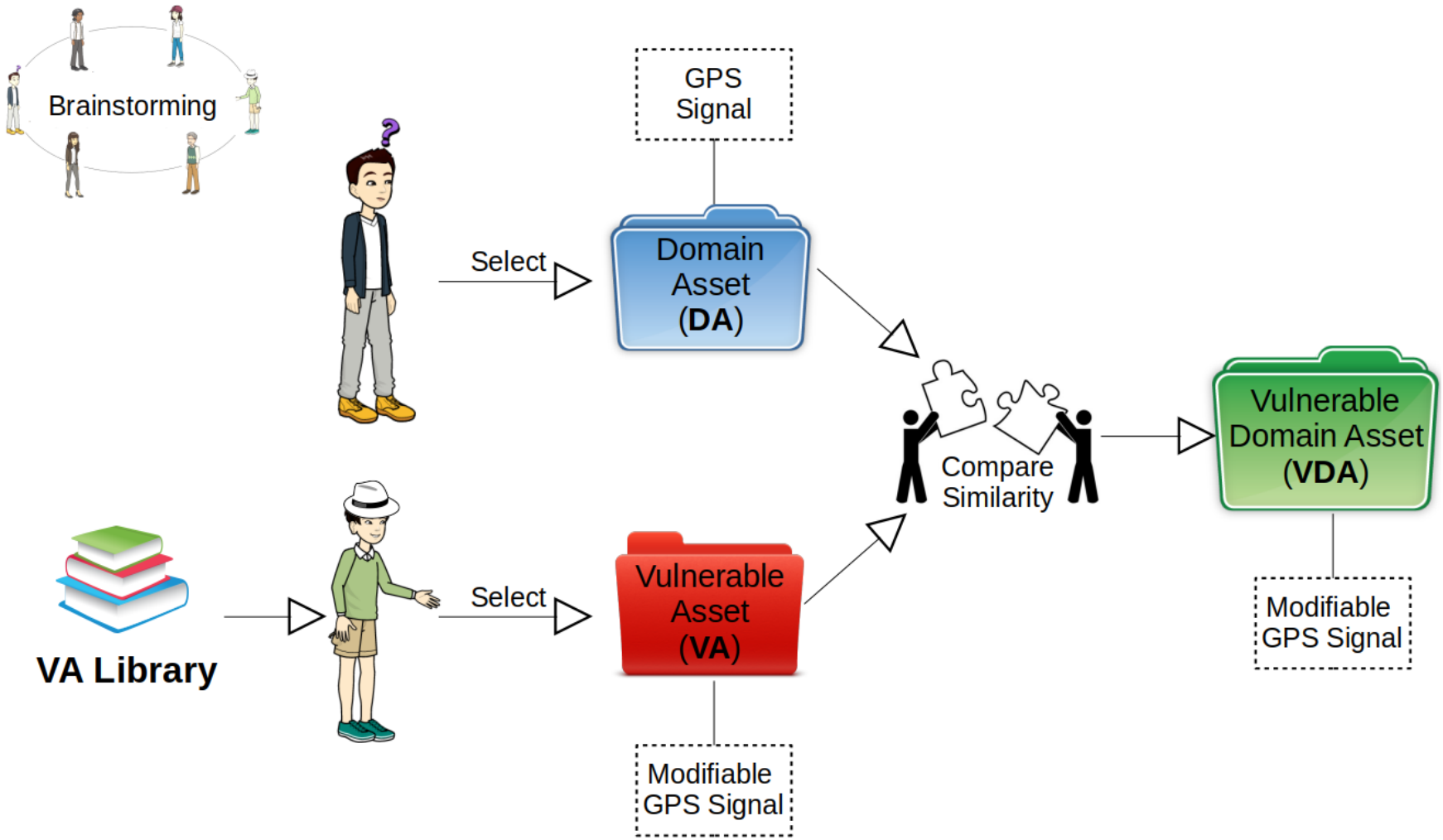


The B-Tree structure





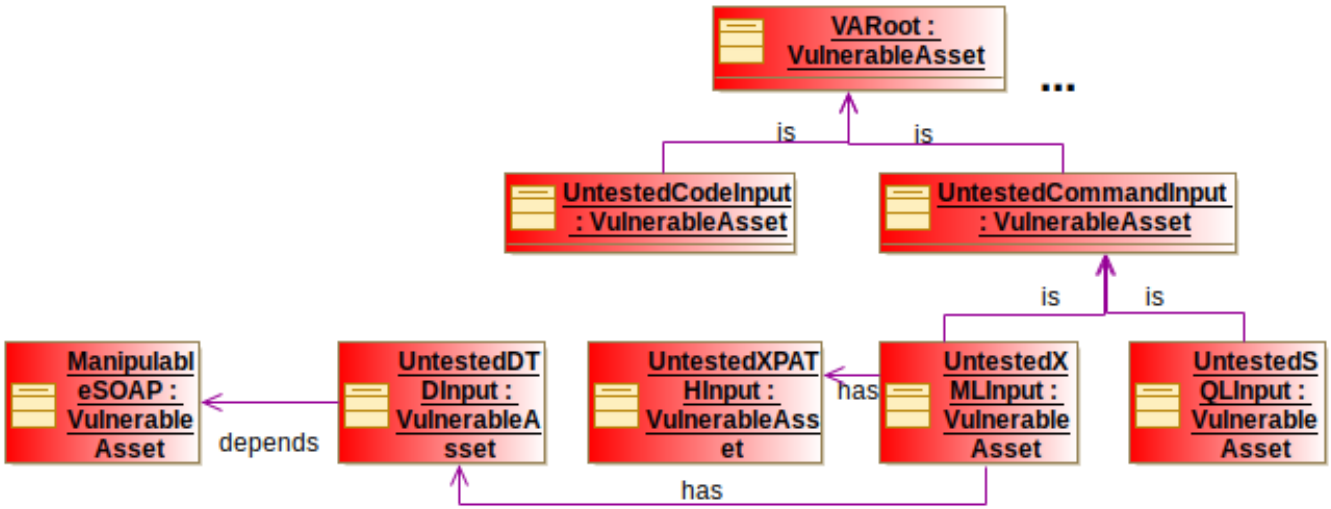
Asset identification process : major tasks

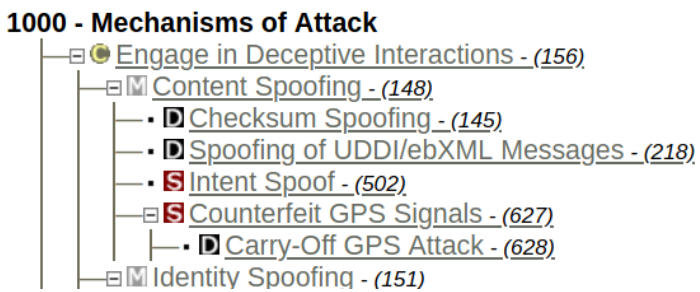


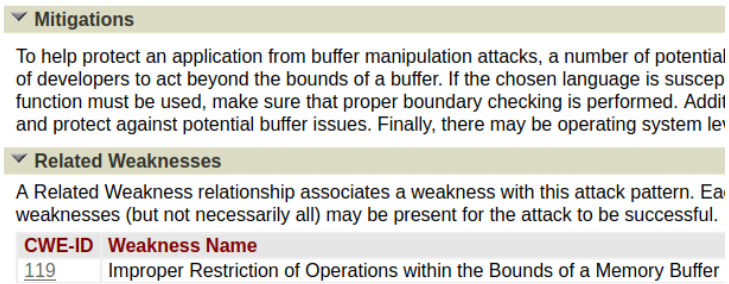
Building VA library

VA Library

Extraction of VA from CAPEC [3] respecting B-Tree structure







3. https ://capec.mitre.org/

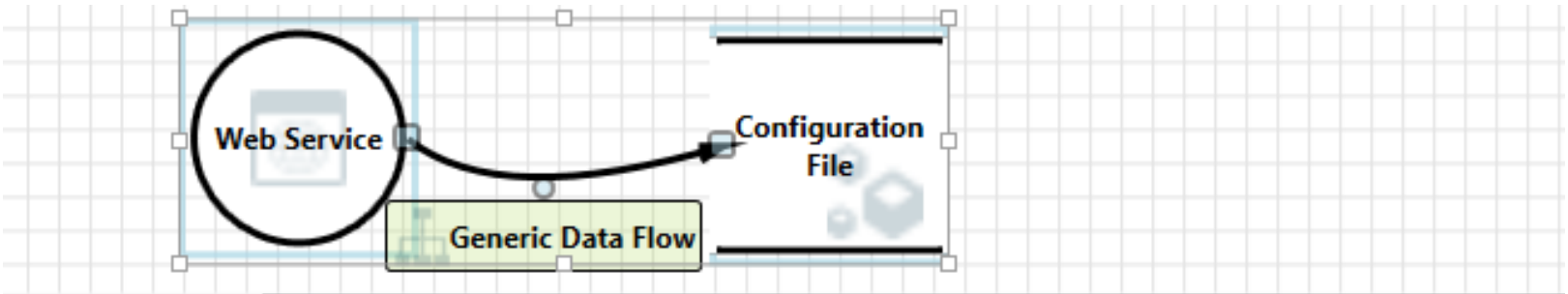
Some rules to extract VAs and their relations basing on CAPEC

- **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' $\rightarrow$ 'is' | 'has' (Ex. '**SOAP** manipulation' *is* a '**web services protocol** manipulation' ; '**XML** injection' *has* '**DTD** injection') ;
- **Rule 5** : 'canFollow' $\rightarrow$ 'depends'.

Plan

Microsoft SDL threat modeling process

WebSphere Application Server Version 7.0 :



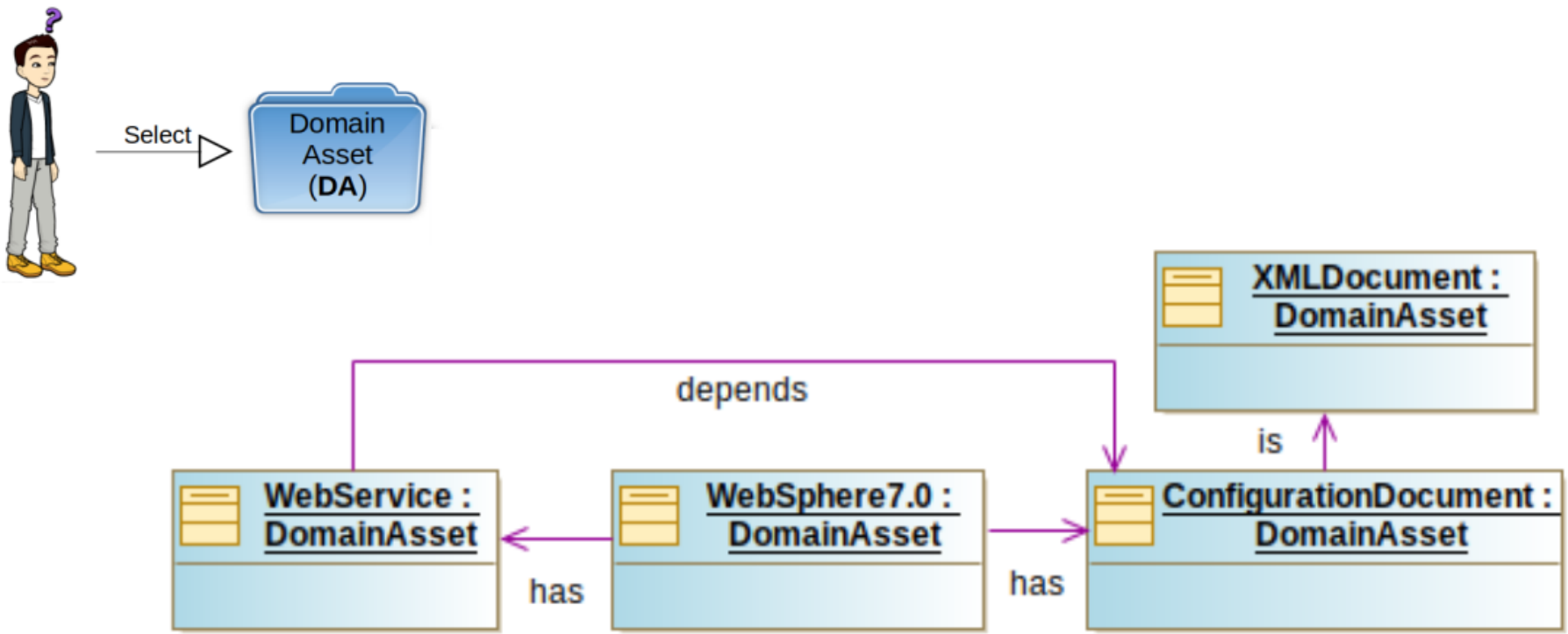
Threat List

ID	Diagram	Title	Category
0	Diagram 1	Spoofing of Destination Data Store Configuration File	Spoofing
1	Diagram 1	Potential Excessive Resource Consumption for Web Service or Configuration File	Denial Of Service

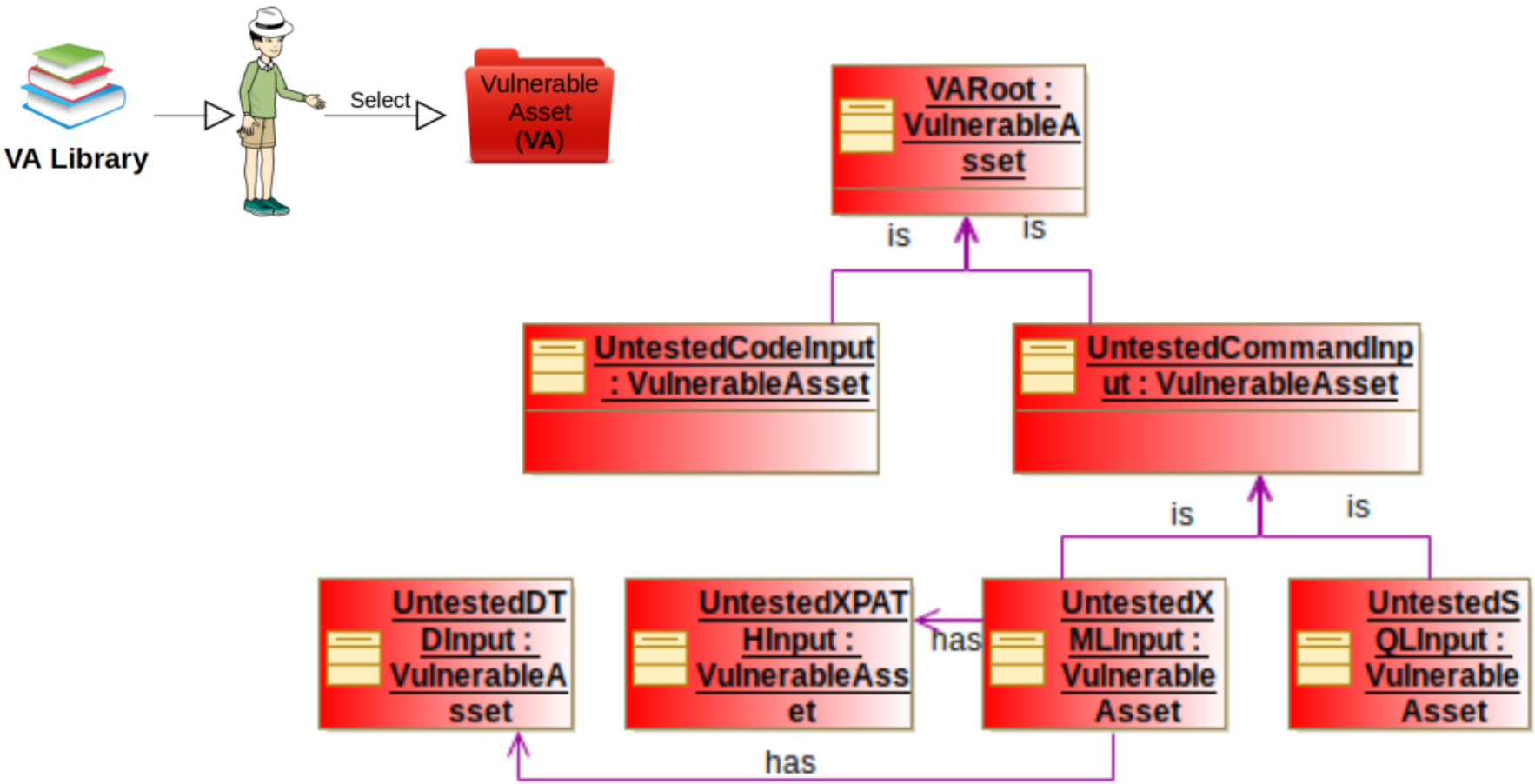
Microsoft SDL threat modeling tool [4]

4. https ://www.microsoft.com/en-us/download/details.aspx ?id=49168

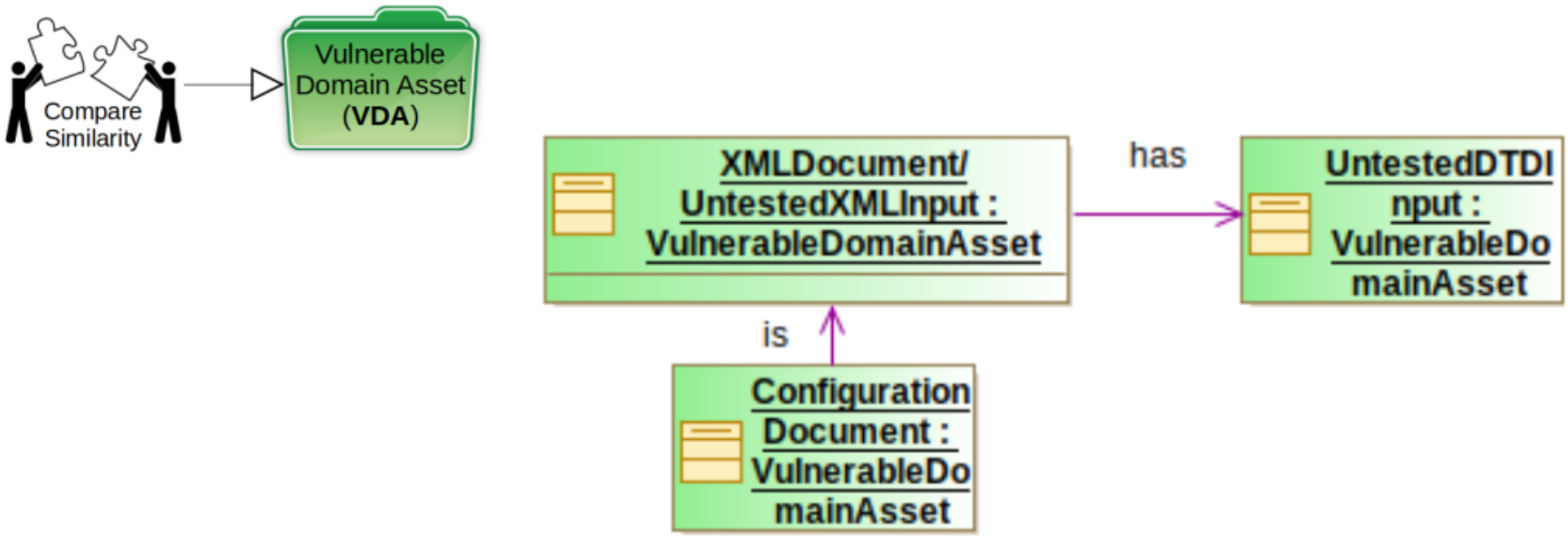
I. Integrating our process into Microsoft SDL threat modeling process – DA



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
(*XML Schema Poisoning, XML Ping of the Death, XML Entity Expansion, XML Entity Linking, Spoofing of UDDI/ebXML Messages, XML Routing Detour Attacks, XML External Entities Blowup, XML Attribute Blowup, XML Nested Payloads, XML Oversized Payloads, XML Injection, XML Quadratic Expansion, XML Flood, DTD Injection*).

A reusable BASH prototype for security experts

KEYWORD	VULNERABILITY_ASSET	CAPEC_ID
Manipulate	Registry Information	203
Manipulate	Human Behavior	416
Manipulate	Timing and State	172
Manipulate	Data Structures	255
Manipulate	System Resources	262
Leveraging	Race Conditions	26
Leveraging	Race Conditions via Symbolic Links	27

Figure – An excerpt of BASH application result

5

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

Plan

Conclusion

Structuring the threat modeling process :

- An asset-based referece 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