SSVC: Stakeholder-Specific Vulnerability Categorization

Art Manion
amanion@cert.org
@zmanion

FIRST PSIRT TC 2020

Photo by Brandon Green on Unsplash

- This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
- The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.
- References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.
- NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

- DM20-0207

SSVC: Stakeholder-Specific Vulnerability Categorization

	Input	Evaluation	Output
CVSS	Vectors	Byzantine math	Partial range 0-100 (reduced to 0-4)
SSVC	Decision points	Decision trees	Qualified priority

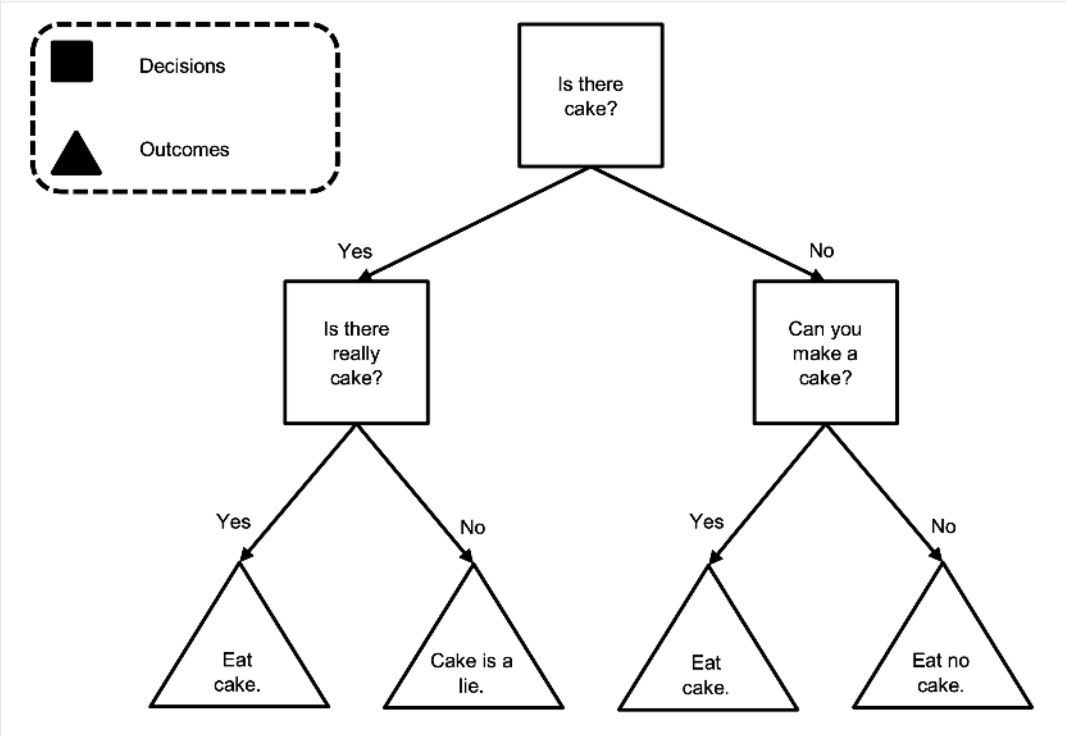
- Briefly known as TEMSL (Threat, Exposure, Mission, Safety, Loss) at S4x2019
  - ICS Security Patching: Never, Next, Now: https://bit.ly/2PDzsoM
- Goals
  - Better decision support, context, risk-orientation
  - Transparent, adjustable, adequate formalism
  - Automation, low evaluation cost per vulnerability
- Towards Improving CVSS: https://bit.ly/32So0LA
- SSVC: https://bit.ly/3ambIP4

Decision Tree

Photo by Faye Cornish on Unsplash

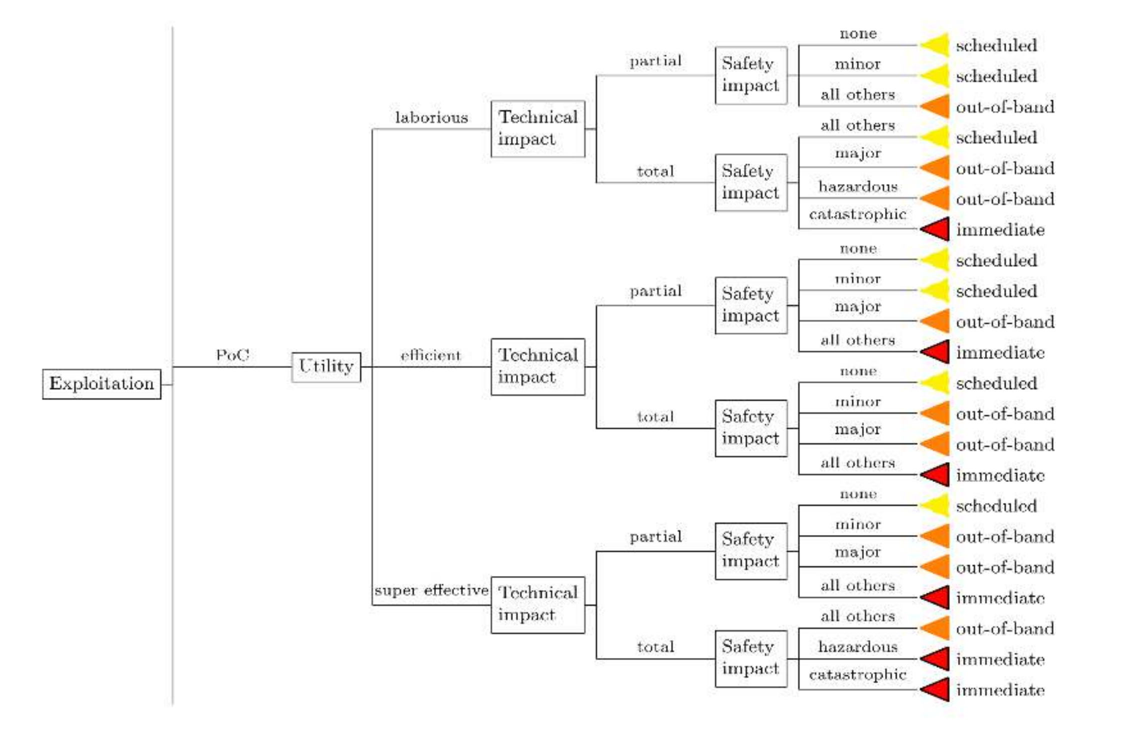
Decision trees

- “Decisions are not numbers. Decisions are qualitative actions that an organization can take.”
- Sets of decision point values mapped to response
- Two proposed trees
  - Patch developer (vendor)
  - Patch applier (asset owner)
  - More or different trees?



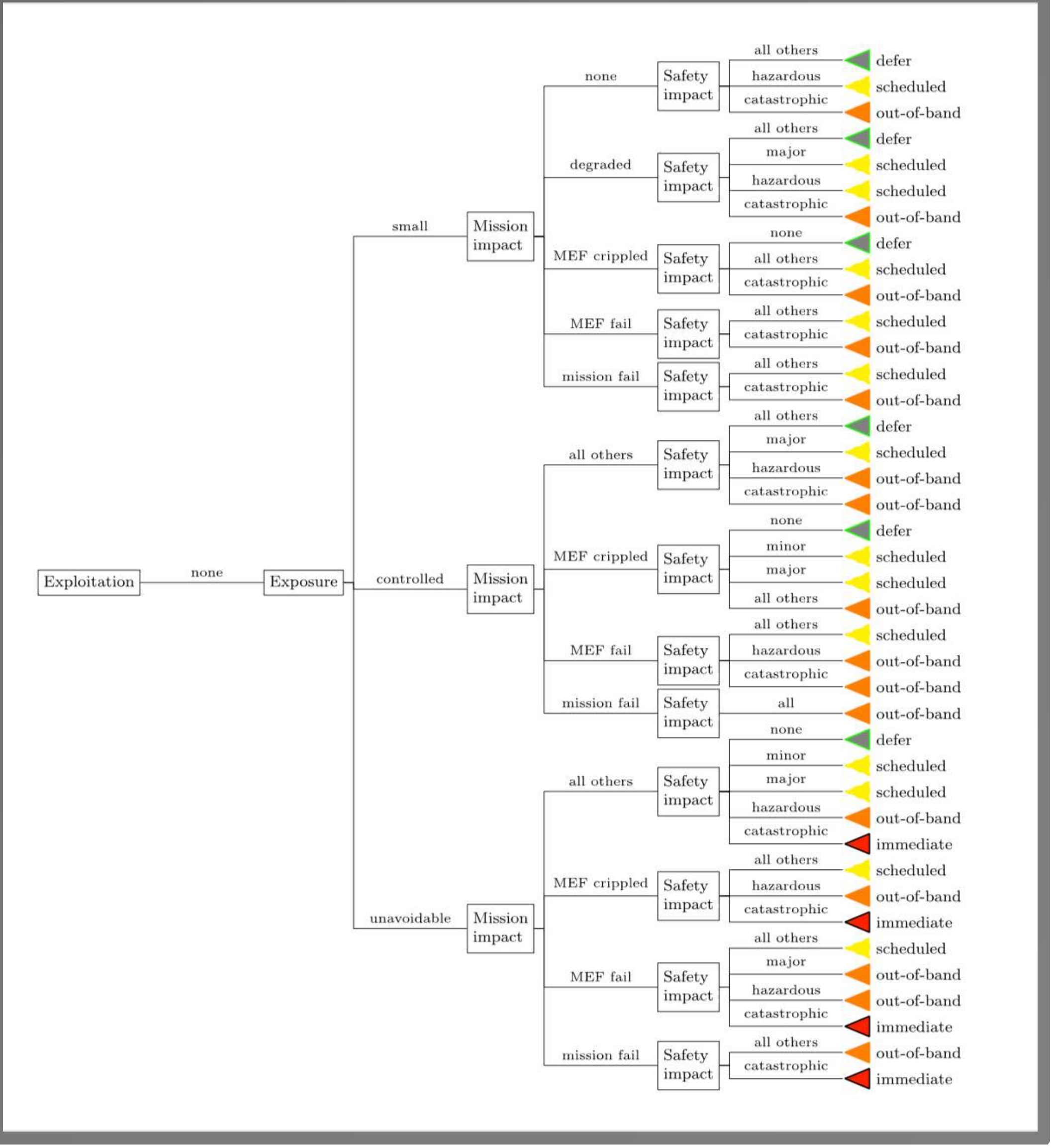
Decision trees

- “Decisions are not numbers. Decisions are qualitative actions that an organization can take.”
- Sets of decision point values mapped to response
- Two proposed trees
  - **Patch developer (vendor)**
  - Patch applier (asset owner)
  - More or different trees?



Decision trees

- “Decisions are not numbers. Decisions are qualitative actions that an organization can take.”
- Sets of decision point values mapped to response
- Two proposed trees
  - Patch developer (vendor)
  - **Patch applier (asset owner)**
  - More or different trees?



Decision trees

- “Decisions are not numbers. Decisions are qualitative actions that an organization can take.”
- Sets of decision point values mapped to response
- Two proposed trees
  - Patch developer (vendor)
  - Patch applier (asset owner)
  - **More or different trees?**

Decision trees

- “Decisions are not numbers. Decisions are qualitative actions that an organization can take.”
- Sets of decision point values mapped to response
- Two proposed trees
  - Patch developer (vendor)
  - Patch applier (asset owner)
  - **More or different trees?**

- Coordinators?
- Domain specific?
  - ICS/OT
  - Medical device
  - Consumer IoT
  - Critical infrastructure

When to patch

Priority	Description
Defer	Do not act at present
Scheduled	Act during regularly scheduled maintenance time
Out-of-band	Act more quickly than usual to apply the fix out-of-band, during the next available opportunity, working overtime if necessary
Immediate	Act immediately; focus all resources on applying the fix as quickly as possible, including, if necessary, pausing regular organization operations

How to decide

Decision Point	Description
Exploitation	Evidence of active exploitation
Technical Impact	Technical impact of exploitation (developer only)
Utility	Usefulness to adversary, virulence and value density (developer only)
Exposure	Accessible attack surface (applier only)
Mission Impact	Impact on mission essential functions (applier only, based on FEMA)
Safety Impact	Impact on safety, broadly defined (based on DO-187C)

How to decide (patch developer)

Decision Point	Description
Exploitation	Evidence of active exploitation
Technical Impact	Technical impact of exploitation (developer only)
Utility	Usefulness to adversary, virulence and value density (developer only)
Exposure	Accessible attack surface (applier only)
Mission Impact	Impact on mission essential functions (applier only, based on FEMA)
Safety Impact	Impact on safety, broadly defined (based on DO-187C)

How to decide (patch applier)

Decision Point	Description
Exploitation	Evidence of active exploitation
Technical Impact	Technical impact of exploitation (developer only)
Utility	Usefulness to adversary, virulence and value density (developer only)
Exposure	Accessible attack surface (applier only)
Mission Impact	Impact on mission essential functions (applier only, based on FEMA)
Safety Impact	Impact on safety, broadly defined (based on DO-187C)

Decision point values

Decision Point	Values
Exploitation	None, PoC, Active
Technical Impact	Partial, Total
Utility	Laborious, Efficient, Super Effective
Exposure	Small, Controlled, Unavoidable
Mission Impact	None, Non-Essential Degraded, MEF Support Crippled, MEF Failure, Mission Failure
Safety Impact	None, Minor, Major, Hazardous, Catastrophic

Decision point values (patch developer)

Decision Point	Values
Exploitation	None, PoC, Active
Technical Impact	Partial, Total
Utility	Laborious, Efficient, Super Effective
Exposure	Small, Controlled, Unavoidable
Mission Impact	None, Non-Essential Degraded, MEF Support Crippled, MEF Failure, Mission Failure
Safety Impact	None, Minor, Major, Hazardous, Catastrophic

Decision point values (patch applier)

Decision Point	Values
Exploitation	None, PoC, Active
Technical Impact	Partial, Total
Utility	Laborious, Efficient, Super Effective
Exposure	Small, Controlled, Unavoidable
Mission Impact	None, Non-Essential Degraded, MEF Support Crippled, MEF Failure, Mission Failure
Safety Impact	None, Minor, Major, Hazardous, Catastrophic

Data sources

Decision Point	Data Source
Exploitation	Threat feed (including public sources like Metasploit, Exploit Database)
Technical Impact	CVSS Base Scores?
Utility	Vendor, threat feed?
Exposure	Asset management (initial valuation, periodic review)
Mission Impact	
Safety Impact	

Data sources (patch developer)

Decision Point	Data Source
Exploitation	Threat feed (including public sources like Metasploit, Exploit Database)
Technical Impact	CVSS Base Scores?
Utility	Vendor, threat feed?
Exposure	Asset management (initial valuation, periodic review)
Mission Impact	
Safety Impact	

Data sources (patch applier)

Decision Point	Data Source
Exploitation	Threat feed (including public sources like Metasploit, Exploit Database)
Technical Impact	CVSS Base Scores
Utility	Vendor, threat feed
Exposure	Asset management (initial valuation, periodic review)
Mission Impact	
Safety Impact	

ICSA-19-113-01 Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers (patch developer)

Vulnerability	Decision Tree Path	Result
Open URL redirect (CVE-2019-10955)	Exploitation: PoC (trivial)	SSVC: Out-of-band
	Technical Impact: Partial	
	Utility: Efficient	CVSS: 7.1 (should be 4.7)
	Safety: Major	

- Out-of-band, WTF?

ICSA-19-113-01 Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers (patch developer), take 2

Vulnerability	Decision Tree Path	Result
Open URL redirect (CVE-2019-10955)	Exploitation: PoC (trivial)	SSVC: ~~Out-of-band~~ Scheduled
	Technical Impact: Partial	
	Utility: Efficient	CVSS: 7.1 (should be 4.7)
	Safety: ~~Major~~ None	

- Safety is an attribute of the asset, but safety impact of this vulnerability is effectively zero
- Scheduled seems too high, should be Defer?

ICSA-19-113-01 Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers (patch applier)

Vulnerability	Decision Tree Path	Result
Open URL redirect (CVE-2019-10955)	Exploitation: PoC (trivial)	SSVC: Scheduled
	Exposure: Small (OT network)	
	Mission: MEF Failure	CVSS: 7.1 (should be 4.7)
	Safety: Major	

- Scheduled, WTF?
- This tree does not consider Technical Impact, should it?

ICSA-19-113-01 Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers (patch applier), take 2

Vulnerability	Decision Tree Path	Result
Open URL redirect (CVE-2019-10955)	Exploitation: PoC (trivial)	SSVC: ~~Scheduled~~ Defer
	Exposure: Small (OT network)	
	Mission: ~~MEF Failure~~ None	CVSS: 7.1 (should be 4.7)
	Safety: ~~Major~~ None	

- Mission and Safety are attributes of the asset, but their impacts are effectively zero

ZyXEL ZyWALL 1100 pre-authentication command injection in weblogin.cgi (patch developer)

Vulnerability	Decision Tree Path	Result
Web interface command injection (CVE-2020-9054)	Exploitation: Active	SSVC: Out-of-band
	Technical Impact: Total	
	Utility: Efficient	CVSSv2: 10.0
	Safety: Minor	

- Summary: Internet-facing RCE via CGI and popen(), LPE via setuid binary, EoL, insecure updates

ZyXEL ZyWALL 1100 pre-authentication command injection in weblogin.cgi (patch applier 1)

Vulnerability	Decision Tree Path	Result
Web interface command injection (CVE-2020-9054)	Exploitation: Active	SSVC: Scheduled
	Exposure: Unavoidable	
	Mission: Non-Essential Degraded	CVSSv2: 10.0
	Safety: None	

- Patch applier 1 uses VPN for basic remote client access, can operate without VPN, staff can be physically present
- Scheduled seems low, should be Out-of-Band?

ZyXEL ZyWALL 1100 pre-authentication command injection in weblogin.cgi (patch applier 2)

Vulnerability	Decision Tree Path	Result
Web interface command injection (CVE-2020-9054)	Exploitation: Active	SSVC: Immediate
	Exposure: Unavoidable	
	Mission: MEF Failure	CVSSv2: 10.0
	Safety: Minor	

- Patch applier 2 can only operate with VPNs running between sites, considerable financial losses if VPNs are down

Photo by Jan Huber on Unsplash

Exploitation

Values	Description
None	There is no evidence of active exploitation and no public proof of concept (PoC) of how to exploit the vulnerability.
PoC (Proof of Concept)	One of the following cases is true: (1) private evidence of exploitation is attested but not shared; (2) widespread hearsay attests to exploitation; (3) typical public PoC in places such as Metasploit or ExploitDB; or (4) the vulnerability has a well-known method of exploitation. Some examples of condition (4) are open-source web proxies serve as the PoC code for how to exploit any vulnerability in the vein of improper validation of TLS certificates. As another example, Wireshark serves as a PoC for packet replay attacks on ethernet or WiFi networks.
Active	Shared, observable, reliable evidence that the exploit is being used in the wild by real attackers; there is credible public reporting.

Technical Impact (patch developer)

Values	Description
Partial	The exploit gives the adversary limited control over, or information exposure about, the behavior of the software that contains the vulnerability. Or the exploit gives the adversary an importantly low stochastic opportunity for total control. In this context, “low” means that the attacker cannot reasonably make enough attempts to overcome the low chance of each attempt not working. Denial of service is a form of limited control over the behavior of the vulnerable component.
Total	The exploit gives the adversary total control over the behavior of the software, or it gives total disclosure of all information on the system that contains the vulnerability

Utility (patch developer)

Values	Description
Laborious	Slow virulence and diffuse value
Efficient	{Rapid virulence and diffuse value} OR {Slow virulence and concentrated value}
Super Effective	Rapid virulence and concentrated value

Safety Impact

Values	Description
None	Dimensions: Physical harm, Operator resiliency, System resiliency, Environment, Financial, Psychological
Minor	
Major	
Hazardous	
Catastrophic	

Exposure

Values	Description
Small	Local service or program; highly controlled network
Controlled	Networked service with some access restrictions or mitigations already in place (whether locally or on the network). A successful mitigation must reliably interrupt the adversary’s attack, which requires the attack is detectable both reliably and quickly enough to respond. *Controlled* covers the situation in which a vulnerability can be exploited through chaining it with other vulnerabilities. The assumption is that the number of steps in the attack path is relatively low; if the path is long enough that it is implausible for an adversary to reliably execute it, then *exposure* should be *small*.
Unavoidable	Internet or another widely accessible network where access cannot plausibly be restricted or controlled (e.g., DNS servers, web servers, VOIP servers, email servers)

Mission Impact (patch applier)

Values	Description
None	Little to no impact
Non-Essential Degraded	Degradation of non-essential functions; chronic degradation would eventually harm essential functions
MEF Support Crippled	Activities that directly support essential functions are crippled; essential functions continue for a time
MEF Failure	Any one mission essential function fails for period of time longer than acceptable; overall mission of the organization degraded but can still be accomplished for a time
Mission Failure	Multiple or all mission essential functions fail; ability to recover those functions degraded; organization’s ability to deliver its overall mission fails