CWE/CAPEC User Experience Working Group

April 6, 2022

Agenda

- **Housekeeping**
- **Primary topics**
  - Begin drafting formal definitions for CWE/CAPEC User Personas
  - CWE/CAPEC Content Fields
  - Responsive Actions after the CAPEC Community Summit
- **Reminders**
- **Adjourn**

UEWG: Reminders

- **Mission:** Identifying areas where CWE/CAPEC content, rules, guidelines, and best practices must improve to better support stakeholder community, and work collaboratively to fix them
- **Periodic reporting of activities to CWE/CAPEC Board**
- **Please solicit participations from your contacts**
  - Contact: cwe@mitre.org & capec@mitre.org

Housekeeping

- **Monthly discussion has been informative**
- **We would like more community ownership by UEWG members**
  - Take a more active role
  - Help complete related tasks
- **Community member co-chair?**
- **Be aware: new meeting series invite is coming**
  - Forthcoming email to explain actions to take

Topic

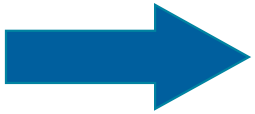
User Personas: Drafting formal definitions

Alec Summers

CWE/CAPEC Deputy Project Lead

CWE/CAPEC Personas

- **User Persona List (UEWG)**
  1. System Security Engineer
  2. OEM Software Developers
  3. Risk Assessors
  4. Audit / IV&V
  5. Penetration Testers
  6. Application/Product Security Engineer
  7. Data Scientist
  8. Technical Writer
  9. Educator
  10. Weakness Advocate
  11. Tool Vendors
  12. Assessment Customers
  13. Software customers
  14. Threat/Information Sharing Groups



- Those who:

1. Build systems
2. Use systems
3. Protect infrastructure around those systems

- **Educators**
- **Technical Writers**
- **Tool Developers**
- **Security Researchers**
- **Incident Response Teams**

AJS1

AJS0

Personas: Next Steps

- **Formally define each user persona**
  - Share with CWE/CAPEC Board
  - Once finalized, make public on our sites
  - Use that as a catalyst for modernizing presentation according to persona needs
- **"Development lifecycle"**
  - Those who build systems: [DEFINE]
  - Those who use systems: [DEFINE]
  - Those who protect infrastructure around those systems: [DEFINE]

AJS2

- **Educators:** Teachers, professors, or certification programs that educate developers and system designers how to develop more secure code, design more secure products, and/or how to find vulnerabilities.
- **Technical Writers:** Those who communicate advanced technical concepts as clearly, accurately, and comprehensively as possible to their intended audience (e.g., code analysis tool users or system designers)
- **Tool Developers:** Developers of code scanning products, services, and other types of automated techniques for finding weaknesses and attacking systems
- **Security Researchers:** Those who look for ways to attack a product by finding weaknesses using manual and/or automated techniques, then reporting the findings to the vendor and/or the general public
- **Incident Response Teams:** Those responsible for the preparation and reaction to any security event

Slide 7

AJS0 inclusive enough? security researchers / analysts
Alec J Summers, 2022-04-06T16:16:28.845

AJS1 within tool developers - there is an educational component that is relevant... as well as technical writer...
Alec J Summers, 2022-04-06T16:20:12.344

AJS2 supply chain team... threat modeling is potentially in that scope... where does this fit?
Alec J Summers, 2022-04-06T16:23:19.339

Topic

CAPEC Summit: Responsive Actions

Rich Piazza

CAPEC Task Lead

CAPEC Summit Informs Future Direction

Opportunities We Heard:

"Frameworks like CWE and CAPEC are significantly important for beginners in the cyber workforce."

"CWE/CAPEC content 'fields' vary in importance by user persona"

"A CWE/CAPEC REST API would be a valuable resource for the community"

Responsive Action:

- **Develop a curriculum for using CAPEC/CWE in the classroom or training setting**
  - Start with Pen Testing & Static Analysis
  - Support external PIs
- **Formally define personas & requirements**
- **REST API**
  - New working group launching!

AJS0

CWE/CAPEC REST API Working Group

- **Launching imminently – first meeting being scheduled for early next week!**
- **Activities:**
  - 1) Craft the RESTful API syntax and semantics which users will send to the CWE and CAPEC database web services;
  - 2) Determine which content and syntax the databases will use to deliver content back to the users;
  - 3) Determine if there are structures or content missing from these databases which would complete a link between this content and that required for tools and standards (such as the Accellera SA-EDI standard); and
  - 4) List any structure or content missing from these databases that would help with further automation (such as versioning, etc.).
- **Attendance at virtual meetings, once a week, likely through the end of 2022.**
- **At the end of this process, the Working Group will provide development and design support, and deliver a document and any other collateral that can be used by MITRE to craft the required infrastructure to support the RESTful API.**
- **Please reply to cwe@mitre.org, capec@mitre.org if you are interested in actively participating in this effort.**

Slide 10

AJS0 has there been any discussion on how orgs might transform and transfer CWE/CAPEC information in a standard format that is managed by mitre, or an open standard… e.g., SBOM development out of NTIA and now CISA. Encapsulating CWE info is left up to the vendors. How is that maintained and tracked over time when you are transferring information across or between organizations
Alec J Summers, 2022-04-06T16:36:14.941

AJS0 0 - chris (synopsys)
Alec J Summers, 2022-04-06T16:37:28.326

Topic

Continued Discussion:

CWE/CAPEC 'field' importance findings

Rich Piazza

CAPEC Task Lead

AJS6

Field Importance Findings

Field/Element	Past CAPEC Team Priority	UEWQ % Required	UEWG % Important	Summit % Required	Summit % Important	UEWG % (Req+Imp)	Summit % (Req+Imp)
Description	MUST	80	20	N/A	N/A	100	
Prerequisites	MUST	60	20	27	28	80	55
Related_Weaknesses	MUST	60	20	52	35	80	87
Taxonomy_Mappings	OPTIONAL	0	80	31	35	80	66
Indicators	OPTIONAL	40	20	21	24	60	45
Consequences	MUST	60	0	38	35	60	73
Mitigations	MUST	60	0	59	17	60	76
Related_Attack_Patterns	MUST	0	40	38	28	40	66
Execution_Flow	MUST	20	0	24	14	20	38
Skills_Required	MUST	0	40	7	27	40	34
Resources_Required	MUST	0	40	14	24	40	38
Likelihood_Of_Attack	MUST	20	0	27	28	20	55
Typical_Severity	MUST	20	0	21	28	20	49
Example_Instances	MUST	0	20	24	21	20	45
References	MUST	0	20	24	21	20	45

- Results relatively consistent
  - UEWG (over 50%) –
    Prerequisites, Related_Weaknesses, Taxonomy_Mappings, Indicators, Consequences, Mitigations
  - Summit (over 50%)
    Related_Weaknesses, Mitigations, Consequences, Taxonomy_Mappings, Related_Attack_Patterns, Prerequisites, Likelihood_Of_Attack
- Execution Flows and Example Instances rated near the bottom
  - Execution Flows only important for pen testing use case
  - Why aren't examples instances viewed as important?

Slide 12

AJS0 currently writing an STRC for a customer… request to have examples for python, go, etc. Going back to CVE to get examples there
Alec J Summers, 2022-04-06T16:46:15.213

AJS1 CWE examples are not good enough at this time to be useful. Perhaps use the CVE database more effectively to provide “examples”
Alec J Summers, 2022-04-06T16:47:25.865

AJS2 it would be nice to look at a cwe and be able to right-click to show all the cve data relevant to cwe data in python. human readable view.
Alec J Summers, 2022-04-06T16:49:10.642

AJS3 coverage is too patchy that it can’t be relied upon…
Alec J Summers, 2022-04-06T16:50:24.721

AJS4 cwe99 examples in cve on java
Alec J Summers, 2022-04-06T16:50:45.457

AJS5 “we are looking for examples in different languages of this cwe” cves is a second level… it would be helpful to see these examples in chronological order within CVE records
Alec J Summers, 2022-04-06T16:52:45.308

AJS6 filter option on severity ranking (cvss) … what are the cwes associated. cve data is so important because those that are not technical folks must make a decision. cve information is what is so important for them… they see a high visibility cve event… correlated CWE
Alec J Summers, 2022-04-06T16:56:15.030

Announcements and Reminders

- **CWE 4.7 Release – end of April**
- **Status attribute will no longer be displayed in CWE or CAPEC web pages**
  - Still included in XML data
  - Strictly for internal tracking
  - No schema or data changes planned until field completeness is finalized

Next Meeting – check your inbox soon ;-)

New meeting series invite coming!

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG **CAPEC@MITRE.ORG**