CWE/CAPEC User Experience Working Group

May 4 , 2022

Agenda

- **Housekeeping**
- **Primary topics**
  - CWE v4.7 Release
  - Continuing discussion of User Personas
    - Definitions
    - The “two-type” model proposal
- **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

- **We would like more community ownership by UEWG members**

- **Community member co-chair?**
  - Take a more active role in such things as:
    - Plan meeting agendas, identify opportunities for discussion/action, drive working group activities, etc.
    - Possible co-chair might periodically brief the CWE/CAPEC Board with me to update them on UEWG activities

Topic

Minor Release Overview: CWE v4.7

Steve Christey Coley

CWE/CAPEC Technical Lead

CWE 4.7 Release Highlights

- **Removed "Status" attribute from display**
- **New/updated individual entries**
  - Software: CWE-1385: Missing Origin Validation in WebSockets
  - Hardware: CWE-1384: Improper Handling of Extreme Physical Environment Conditions
  - HW/SW: CWE-1357: Reliance on Uncontrolled Component
  - Deprecated: CWE-365: Race Condition in Switch
- **144 entries changed**
  - Relationships (54), Related Attack Patterns (37), Research Gaps (27)
  - Issue: how best to describe what's changed? For which user personas?
  - https://cwe.mitre.org/data/reports/diff_reports/v4.6_v4.7.html

CWE 4.7 Release Highlights (2)

- **New expansion / coverage of ICS/OT**
  - New CWE/CAPEC ICS/OT SIG formed
- **New view: CWE-1358: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS**
  - Active development to take place in the coming months (in the SIG)
  - Many "scoping" challenges, e.g., human processes or practices
  - https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf

Update – External Submissions and Transparency

- **External submission server has received 3 new submissions**
  - One "good" one
  - One that's not a weakness, just a kind of technology where many weaknesses can occur
  - One that's not a weakness, just a specific CVE example. Are they asking us to add it as a demonstrative example? (The cited CWE isn't immediately relevant.)
- **Limitation: users can't submit Categories, or suggest modifications**
- **Still refining full process with better back-and-forth communication**
- **Still working on transparency (e.g., public GitHub server)**
  - Comments / change suggestions from community
  - Transparent shifts in submission status
- **Formally defining / documenting "scope" and inclusion/exclusion criteria**
- **This may be a "rich" area for UEWG input**

Topic

Continuing the Discussion: User Personas and CWE/CAPEC User Experience

Alec Summers

CWE/CAPEC Deputy Project Lead

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]
- **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, and reporting/educating on findings to users
- **Security Researchers/Analysts:** 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 (to include threat modeling, C-SCRM)
- **Incident Response Teams:** Those responsible for preparation and reaction to any security event

Use Case Scenarios → Content Presentation

- **CAPEC Existing functionality to filter content detail**
  - Basic, High-level, Mapping-friendly, Complete

CWE Content Filter			
BASIC	HIGH-LEVEL	MAPPING	COMPLETE
Description	Description	Description	Description
Applicable_Platforms	View_Audience	View_Audience	View_Audience
Common_Consequences	Alternate_Terms	Alternate_Terms	Alternate_Terms
Likelihood_of_Exploit	Time_of_Introduction	Terminology_Notes	Terminology_Notes
Demonstrative_Examples	Common_Consequences	Relationships	Applicable_Platforms
Potential_Mitigations	Relationships	Relationship_Notes	Modes_of_Introduction
Relationships	Content_History	Theoretical_Notes	Common_Consequences
Content_History		Related_Attack_Patterns	Likelihood_of_Exploit
		Content_History	Enabling_Factors_for_Exploitation
			Detection_Methods

and more…

Use Case Scenarios → Content Presentation

- **CAPEC Existing functionality to filter content detail**
  - Basic, Complete

CAPEC CONTENT	
BASIC	COMPLETE
Description	Description
Relationships	Relationships
Memberships	Memberships
Execution_Flow	Execution_Flow
Prerequisites	Prerequisites
Mitigations	Mitigations
Related_Weaknesses	Likelihood_Of_Attack
	Alternate_Terms
	Typical_Severity
	Skills_Required
	Resources_Required
	Indicators
	Consequences
	Example_Instances
	Related_Weaknesses
	Taxonomy_Mappings
	References
	Notes
	Content_History

Community Suggestion

- **Such granular definitions might not bring expected results**
  - might make wrong decisions based on such definitions and in the end make CWE/CAPEC data more complex than it is now
- **“Two-type” persona-defined presentation**
- **Current user personas definitions, there two major groups:**
  - ‘Theoretical’ users (Educators, Technical Writers, subset of Tool Developers)
  - ‘Advanced technical users’ (Advanced Tool Developers, Security Researchers, IR Teams, etc.
  - What are the needs of these of these “two types”?
    - e.g., timely CVE information

Next Meeting – June 1 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

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