CWE/CAPEC User Experience Working Group Meeting

February 8, 2023

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Agenda

This meeting is being recorded :-)

- **Purpose**
- **Housekeeping**
- **Primary topics**
  - User Story Development
  - Demo: CWE Custom Presentation Filters
  - Open Discussion
- **Reminders and Adjourn**

UEWG: Purpose

- **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**
  - (next quarterly Board meeting TBD Q1-2023)
- **Please solicit participations from your contacts**
  - Contact: cwe@mitre.org & capec@mitre.org

Housekeeping

- **We are working to identify further UEWG opportunities and priorities for FY23**
  - See open discussion / topic 3

Topic 1

User Story Development

Przemyslaw Roguski

Updates

- **We have four potential user stories and personas lined up:**
  - Milind Kulkarni – Security response teams using CWE in security bulletins and disclosures
  - John Keane - Management persona and how they “use/influence the use of” CWE/CAPEC
  - Kirsten Gantenbein – Technical writers
  - Jason Oberg - Hardware engineer and/or hardware verification engineer

CWE / CAPEC user stories

Created by Przemysław Roguski (aka Rogue) from Red Hat

WHY we need user stories?

First of all let's ask: What we as a UEWG want to improve?

Users can use CWE data to better understand how weaknesses lead to vulnerabilities. CWE data can be used to proactively identify how existing weakness in the software or hardware can lead to new vulnerabilities and exploits. Better knowledge of product weaknesses will improve the general security posture of the product. The CWE data is key information in the shift left security initiative.

The only problem is that **CWE users MUST KNOW** and **UNDERSTAND** what they can **ACHIEVE** by using CWE/CAPEC data.

WHAT we want to achieve by creating user stories?

Defining User Personas is not enough, because users don’t know which persona they are and what they can do with weaknesses data.

We should help users to identify themselves with specific user personas or groups and show them how to use CWE data in real user stories. People can learn much fuster what value is in the CWE / CAPEC data.

HOW do we want to present user stories?

A user story has three unique elements.
We will need a good, clear to everyone template.
Something like:

- Business Problem
  Understating the business problem.
- Level of responsibility
  The tasks the user is responsible for and cares about
- Outcome
  The results achieved by using CWE/CAPEC data.

Example user story - Security Architects

- Business Problem (Context): Security Architects are responsible for a secure design of application/hardware. They must take into consideration the whole product purpose, future deployment and usage, and make sure that all aspects of it are well designed and protected from the security point of view. The purpose of all this work is a very deep risk assessment process to ensure that the final product is secure. Using the CWE data can help significantly in the Security Architects work to better understand the nature of the weaknesses and at the end help to take the final decision about the remediation steps.

Example user story - Security Architects

- Level of responsibility (Story): Security Architect is going to review a new SaaS solution. During the risk assessment process it is necessary to verify findings from various security scanners (SAST and DAST) and threat modeling tools. The detected weaknesses can be verified with the CWE available data to better understand the nature of the weaknesses. User can see example usage of the particular weakness and possible mitigation steps. It is also possible to see correlation to other similar weaknesses from the specific weakness category that can help to avoid potential other issues and as a consequence vulnerabilities in the future. Security Architect can use the “Operational” view of the CWE data to see useful technical information about this specific weakness. For example if the CWE-23 Relative Path Traversal is reviewed, the Security Architect might recognize that this weakness is also mapped to the OWASP Broken Access Control risk, which is the top 1 of the web application security risks and take necessary steps for deeper verification.

Example user story - Security Architects

- Outcome:

All information available in the CWE program can help to perform more detailed risk assessment and provide more robust and less vulnerable final product. Using the CWE data can show the correlation between weaknesses and historical CVEs cause by the specific weakness. It can also help to proactively identify other similar weaknesses from the same type of weakness category that will improve the overall security posture of the reviewed service/application/hardware.

Example user story - different approach

The same user story can be presented as a comparison of two different approaches taken by different users based on their roles.

Each story element (Business Problem / Level of responsibility / Outcome) can describe then an approach taken by different users for the same issue.

For example, in the next slides there will be presented one and the same use case but from the perspective of different roles (different user stories depending on the roles).

Security Architects vs. Software Developers

- Business Problem (Context):

Security Architects

Security Architects are responsible for a secure design of application/hardware.
They must take into consideration the whole product purpose, future deployment and usage, and make sure that all aspects of it are well designed and protected from the security point of view. Using the CWE data can help significantly in the Security Architects work to better understand the nature of the weaknesses and at the end help to take the final decision about the remediation steps.

Software Developers

Software Developers are mostly focused on the creation/implementation phase of the software according to the instruction delivered by Project Managers and Design Architects including Security Architects. Using the CWE data can help Software Developers to better understand the possible mitigation steps for the detected weaknesses in the software.

Security Architects vs. Software Developers

- Level of responsibility (Story):

Security Architects

For a new SaaS solution implementation, verification of findings from various security scanners (SAST and DAST) must be performed. The detected weaknesses can be verified with the CWE available data to better understand the nature of the weaknesses. In the CWE data Operational view the Security Architect can see example usage of the particular weakness (Demonstrative Examples field) and correlation with other similar weaknesses (Relationships field). Can also see example CVEs caused by the specific weakness (Observed Examples field).
All this data helps with the risk assessment process and helps to decide next, necessary action steps.

Software Developers

During the new SaaS solution implementation phase Software Developers must mitigate all detected and reported by Project Owners or Security Architects potential weaknesses in the software. By using the CWE data like Demonstrative Examples and Potential Mitigations users can better understand the nature of the particular weakness and better prepare the mitigation/remediation plan.

Security Architects vs. Software Developers

- Outcome:

Security Architects

All information available in the CWE program helps Security Architects to provide more detailed risk assessment for the specific software or solution implementation.
That leads to a better, more focused on the right things implementation phase.

Software Developers

By using the information from the CWE program Software Developers can mitigate or remediate the weaknesses in a accurate way.

The overall outcome from cooperation of both above roles for the same use case is a more robust and less vulnerable final product. Additionally, continue cooperation and usage of the CWE data helps the to better handle the Secure Development Lifecycle (SDL) plan for the specific product/software and do more proactive steps in regards to the general product security posture.

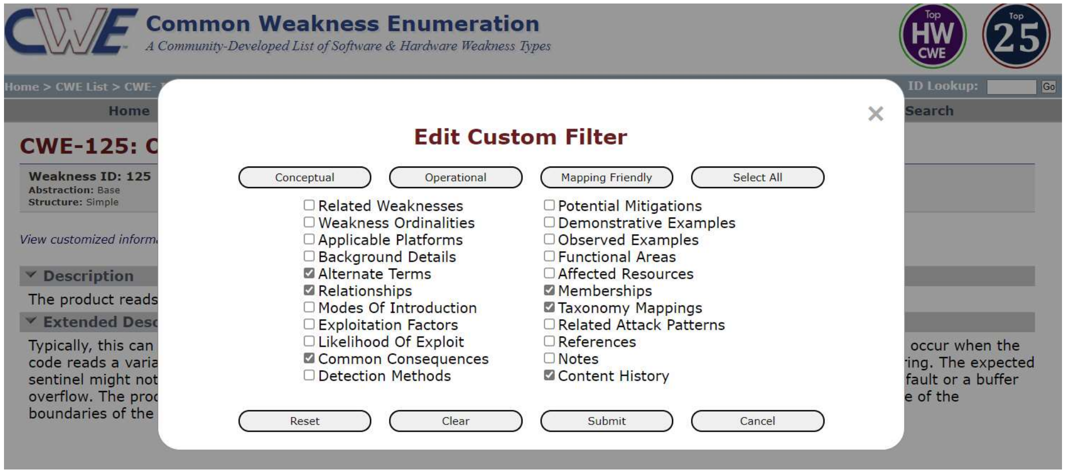
Topic 2

CWE/CAPEC Presentation Filters

David Rothenberg

Presentation Filters

- **Presentation filters on CWE site will allow users to select exactly what information they want to view within CWE records**
- **The custom filter allows users of the site to choose which data elements they wish to view for a CWE**



Edit Custom Filter

□ Related Weaknesses
□ Weakness Ordinalities
□ Applicable Platforms
□ Background Details
☑ Alternate Terms
☑ Relationships
□ Modes Of Introduction
□ Exploitation Factors
□ Likelihood Of Exploit
☑ Common Consequences
□ Detection Methods
□ Potential Mitigations
□ Demonstrative Examples
□ Observed Examples
□ Functional Areas
□ Affected Resources
☑ Memberships
☑ Taxonomy Mappings
□ Related Attack Patterns
□ References
□ Notes
☑ Content History

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Topic 3

Open Discussion

Topics?

- Ideas for UEWG priorities in 2023 and beyond?
- Is there anything we can do to help foster more participation? Questions you might have that are blockers?
- Any additional thoughts on pain points from previous discussion?
- Any additional ideas for communication strategies from previous discussion?
- Any other topics or thoughts?

Next Meeting – March 8 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

CAPEC@MITRE.ORG

Backups

CWE User Pain Points

- **Pain point topics that the group is aware of or would like to discuss**
- **For those on the call, what were your biggest questions or concerns when beginning to use CWE?**
- **Are there common questions that CWE users have that are not covered in the current FAQ?**

- **Other potential opportunities:**
  - Features we could expand or improve to make CWE consumption easier?
  - Maybe engage the community in one or more ways to solicit this kind of feedback (see topic #3)

- **Other thoughts?**

Community Engagement Strategy

- Develop a strategy for engaging the CWE user community for feedback
- What are the best methods to query the community on topics such as the pain points covered in topic #2
- What communication methods should be employed?
  - E.g., polls, emails, web, social media
- Should we target specific user types?
- Other thoughts?