CWE/CAPEC User Experience Working Group Meeting

Wednesday May 4@ 1200–1300 EST

Members in Attendance

Rich Piazza – MITRE CWE
Alec J Summers – MITRE CWE
Nick Tait – Red Hat
Steven M Christey – MITRE CWE
Przemyslaw Roguski – Red Hat
Yves Younan – Cisco Talos
Suzanna Schmeelk – St. John's University
Nick Tait – Red Hat
Altaz Valani – SecurityCompass
Farbod Foomany – SecurityCompass
Kirsten Gantenbein– ExtraHop
Shadya B. Maldonado Rosado – Sandia
Paul Wortman – Wells Fargo
Milind Kulkarni – NVIDIA
Matthew Coles – Dell
Ellie Soroush – SecurityCompass

General / Initial Discussion

• Community member discussion for user experiences

• Request for community volunteers for a co-chair role on the UEWG. An opportunity to share leadership, guide work, and drive meeting agendas.

CWE 4.7 Release

- Minor release published on April 28
- Removed the status attribute from the display of individual CWE entries
- Deprecation of CWE–365
- Added a small number of new entries to CWE 4.7
- Improving CWE coverage with respect to ICS and OT issues. New view has been created

Work Behind the Scenes

CWE/CAPEC Technical Lead: Steve Christey Coley

• Hardware team came up with a new entry

• Updated CAPEC attack patterns

• Building documents about what is and what is not within CWE scope

A member asked how to better incorporate personas more into different user experiences.

- The speaker replied that the CWE team is looking for insights and expertise helping in that respect.
- Submitted content would not necessarily be focused around a weakness
- An early–stage draft is being built for feedback

Attack surfaces

A member asked about characterizing attack surfaces to inform designs of systems and how to support

- The speaker replied that we may cover in more detail in the next month, which potentially could be useful for a broader range of activities

External submissions server (see https://cwe.mitre.org/community/submissions/guidelines.html)

• New Submissions server not fully promoted, but three new submissions were received

• Developing quality control and processes to ensure that we have better back and forth communication

• Vision is ultimately to have a public GitHub server where new external submissions are made available to the broader community for others to suggest changes, further develop, or make comments

• There will be user experience issues with the submission server as well

Member observes about the difference between vulnerability and weakness and the pros and cons of having a public GitHub server, as well as customer–level experiences

- The speaker replies about active development of weakness content and development of guidance material.
- Speaker also mentions focused training or explanatory material to distinguish between a vulnerability and a weakness

Member comments about terminology that is confusing and used incorrectly or differently

User personas and defining various user types as well as potential end–user customization

- **Discusses CWE and CAPEC for knowing the different types of user personas and their needs**

Member proposes limiting the number of user personas to perhaps two:
- theoretical users (Educators, Technical Writers, subset of Tool Developers)
- advanced technical users (Advanced Tool Developers, Security Researchers, IR Teams, ...)

Idea would be to consider the technical information the latter group may prefer to have clear/immediate access to (e.g., recent CVE data) which would be different from the primary data elements the former may be interested in

Second member also has concerns about making the user personas' various needs too simplistic or difficult for CWE to be consumed between different roles and personas