UEWG CWE/CAPEC Meeting

Wednesday, June 1 2022

Members in Attendance

Rich Piazza – MITRE CWE
Alec Summers – MITRE CWE
Chris Clark - Synopsys
Shadya Maldonado Rosado - Sandia
Przemyslaw Roguski - Red Hat (Guest)
Matthew Coles – Dell
Farbod Foomany – Security Compass
Ellie Soroush – Security Compass
Yves Younan - Cisco Talos
Milind Kulkarni- PSIRT
Doug Nichols - GE Aviation, US
Lokesh Balu - Dell
Paul Wortmann - UCONN
Joe Jarzombek (Guest)
Arif Dhanidina

Agenda – Alec Summers

- Definitions
  - Harmonizing common terms across CWE/CAPEC (CVE?)
  - Review proposed definitions and consider initial feedback
- Continue/Finalize persona definitions for publication
  - CWE v4.8 June 28
- 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
    - (next quarterly Board meeting June 3)

Housekeeping

- Shadya Maldonado Rosado, Sandia National Labs – new CWE/CAPEC UEWG Community Co-Chair
  - Plan meeting agendas, identify opportunities for discussion/action, drive working group activities, etc.
  - Help brief the CWE/CAPEC Board on UEWG activities

Definitions

- Common terms across CWE, CAPEC, and possibly CVE
- Vulnerability is defined three different ways between CVE, CWE, and CAPEC (historical reasons)
  - State of practice search shows almost 10 different definitions across eight organizations
- Weakness definitions shows five different findings across four organizations
- Attack patterns show six different findings across four organizations

Caller Matthew Coles comments that unified definitions would be preferred. Also mentions that vulnerabilities that are not only a security impact, but also privacy and safety.

Steve Christey Coley comments that wrestling with definitions has been going on for “years and years” but definitions that are too broad can have a negative impact.

Caller Shadya Maldonado Rosado comments that building a conceptual model to help abstract the concept of attack surfaces may be helpful.

Caller Chris Clark comments that unifying descriptions would be “great” but also extremely challenging

Caller Shadya Maldonado Rosado comments that she will take defining an “attack surface” as an action item.

Alec Summers comments that user education would be easier if certain items were more formalized.

Caller Chris Clark comments that unifying definitions between MITRE and NIST may be a future goal.

Board Member Feedback

- Logic model as a flow for stepping stone patterns

User Personas and Experiences

- Personas based on self-identification (builders, users, protectors)
- Educators, technical writers, tool developers, researchers/analysts, incident response teams
- “Two-type” model for CWE presentation (theoretical and technical)

Caller Matthew Coles comments that solution architects are not really educators and should be listed as technical. Caller Przemyslaw Roguski agrees.

- Proposed data elements for use case scenarios and content presentation, lifecycle phasing

Rich Piazza comments that collapsing some elements in filters may be useful.

Caller Joe Jarzombek comments about maintaining the relationships between CAPEC, CWE, and CVE entries.

Alec Summers replies that filtering may be different per user.

Caller Przemyslaw Roguski comments expanding filter options would be good, but does not have to be a default view.

Caller Joe Jarzombek agrees that a solutions architect role is different than that of an educator.

Alec Summers replies that it’s not always clear what filter names mean and asks if there are other user groups that wouldn’t fit into either theoretical or technical and other possible options.

Caller Lokesh asks about risk-based decisions for theoretical or technical "buckets" for personas.

Alec Summers replies that we want to include elements that allow people to make risk decisions.

Next meeting is June 29, 2022 at 12:00pm Eastern