CWE/CAPEC User Experience Working Group

Friday, July 27, 20222

Member in Attendance

Alec J Summers - MITRE

Christopher Sundberg

John Keane - Guest

Yves Younan - Cisco

Paul Wortman – Wells Fargo

Shadya Beatriz Maldonado Rosado - Sandia

Jay Jacobs - Guest

John Keane - Guest

Farbod Fooman – Security Compass

Steven M Christey - MITRE

Nick - Red Hat

Matthew Coles - Dell

Rich Piazza - MITRE

Velian - Guest

Milind Kulkarni - Nvidia

Bob Natale – MITRE

General/Initial Discussion

MITRE CWE: Alec Somers

- There's been a lot of feedback on the idea of harmonizing our definitions across the CWE/CAPEC and possibly CVE.
- Looking to close Personas on the sites and discuss implementing presentation filters based on persona
- Discussion on purposes of the User Experience Working Group
- Next meeting TBD Sept/Oct
- Want to improve ability for members to work in the content space collaboratively. We are looking for solutions

Co-Chair: Shadya Maldonado Rosado

- Working to identify opportunities and priorities for FY23
- Looking for any feedback
- *A member recommends going to NIST or DHS as approving authorities to assist in creating a common language. ISO 5055 has a definition of weakness that may have been derived from MITRE CWE, but the definition is not being used by CWE.*

Definitions! Harmonizing common terms across CWE/CAPEC - Shadya Maldonado Rosado

- Recap: There are inconsistencies or multiple definitions of vulnerability and weakness across CISA, NIST, ISO Standards, etc
- Today is a talk about the definition of weakness
- Steven Christey – *In viewing in the email discussion the definition has become more and more general/generic, almost to the point of being meaningless*
    - A definition of weakness should exclude things that do not have computing logic and/or have security implications
    - Software is too specific as the scope also encompasses hardware
    - APES test discussion:
        - **An acceptable definition for "weakness" should, on its surface, exclude the following:**
            - **Aspirin. Aspirin bottles and other medication containers that are expected to have child-proof caps and/or anti-tamper mechanisms.**
                - Example: the Chicago Tylenol murders of 1982
                - Rationale: These have no computing logic in them.
            - **Physical padlocks that are only opened by a physical key or physical combination.**
                - Example: Master Lock Keyed Padlock as used for school lockers, etc. (Model #5KADPF is an example)
                - Rationale: while related to security, these have no computing logic in them
            - **Extension cord with insufficient strain relief.**
                - Example: OSHA requirements for flexible cords, https://www.osha.gov/electrical/hazards/flexible-cords
                - Rationale: no computing logic and no security implications
            - **Spelling error in informational message from web application**
                - Example: web form with tip that says "Do not include dashes when you enter your phone number”
                - Rationale: no security implications
                - Counter-argument: "sometimes spelling errors have security implications."

- Current state of vulnerability, weakness, and attack pattern were shared with community 7/13/2022

Vulnerability	A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components (from CVE®)
Weakness	A type of flaw or defect inserted during a product lifecycle that, under the right conditions, could contribute to the introduction of vulnerabilities in a range of products made by different vendors
Attack Pattern	The common approach and attributes related to the exploitation of a weakness, usually in cyber-enabled capabilities

  -
  - Is weakness and exploitable element?
- *A member states that weaknesses that are included in the CWE are ones that can potentially have a security implication. That statement can really clarify or helps clarify the scope of the CWE. I'm just not sure how we would necessarily present it in the definition of weakness so that that's clear to everyone who comes to this resource that perhaps isn't already in that mindset.*
  - *A member replies Binding it only to security is a bit limiting. Obviously, that's the core focus of both CVE and CWE have been focused on primarily security, but with the notion that privacy and safety are becoming more prevalent and more of an interest to organizations.*
  - *Member continues with the idea that if something is exploitable, it is exposed in the attack surface. If something is just a weakness it may not be exposed. In fact, if it is a weakness and it is not exploitable, its therefore not a vulnerability.*
- Three schools of thought reviewed
  - Hierarchy of attack surface with parent child relationships
  - Is a weakness on the same level as a vulnerability, or a child attribute of a vulnerability?
- Discussion over making definitions readable to non-technical persons

Continuing the Discussion: User personas and CWE/CAPEC Presentation Filters – Alec Summers

- Looking at defining different types of users/personas
  - Formal definitions complete and will go up on site
  - Types of proposed filters
    - Theoretical
    - Technical
    - Mapping friendly (existing)
    - Complete (existing)
- Improve filter awareness
  - Better how-to documentation across CWE