HW CWE SIG Meeting
Friday, May 12, 2023

Members in Attendance

Gananand G Kini
Allen Krell
Gage Hackford
Bob Heinemann
Alec J Summers
Dr. Michael J Smith
Don Davidson
Joe Jarzombek
Rich Piazza
Manna, Parbati K
Ahmed, Faheem
Swami, Shivam
Steve Christey Coley
Alric Althoff
James Pangburn
Lyndon Fawcett
Coles, Matthew
Milind Kulkarni
Jason Oberg
Shafqat Ullah
Abraham Fernandez Rubio
Fung, Jason M
Das, Amitabh
Mohan Lal
Bormann, Joerg
Rafael Dos Santos
Nicole Fern
Wortman, Paul
Sebastian Fischmeister
Hallman, John
Carlos Moreno
Evan Bryers
Andy Meza
Devraj, Keerthi
Luke W Malinowski
Sanaka, Naveen
Heebink, Joel
Daniel DiMase
Raghudeep

Agenda

- Housekeeping and Announcements
- Working Items for this Meeting
    - 4.11 Release Announcement
    - D3FEND and CWE Mention
    - CWE Key Concepts – Selection from HOST Presentation
    - SAE G-32 Call for Participation in HwA Standard
    - Side Channels vs Covert Channels.
      NOTE: This topic was not covered in the meeting due to lack of time.

Housekeeping

- Next meeting: June 9, 12:30 – 1:30 PM EDT (16:30 – 17:30 UTC)
- MS Teams
- Contact: cwe@mitre.org
- Mailing list: hw-cwe-special-interest-group-sig-list@mitre.org
- Minutes from previous meetings: https://github.com/CWE-CAPEC/hw-cwe-sig

Announcements

- Reminder: April SIG was cancelled. Welcome back.

- CWE 4.11 Released April 27
- CWE/CAPEC Board Meeting Occurred on Feb 15
- D3FEND / CWE Integration Presentation Next Month

4.11 Release Announcement (Steve Christey Coley)

- Usability improvement was made with the implementation of custom filtering to help users find records/data of interest and applicability to their needs. This is in addition to the original set of preset profiles/filters.
- Created a new list of 23 categories for the software assurance trends view. One category is memory safety, and we hope that this will help to spark some community wide discussion and potentially be useful for certain kinds of research. Worked closely with CSA and with CISA's awareness, not done in isolation.
    - Categories are a result of a request to track vulnerabilities across different buckets analogous to memory safety because memory safety is a strategic initiative to get people to switch to.
    - Also wanted to look at data trends around the percentage of data in NVD that is the result of things that could have been avoided by using such languages.
    - Comment that just because a language allows you to implement a buffer overrun doesn't mean you shouldn't use that language.
- Made significant updates to the software development view, and the view about weaknesses introduced during design (this view is now more usable and accessible, and challenges the assumption that CWE is only about implementation issues).
- Continued to update content based on work from the ICS OT SIG, especially in terms of mappings to secure-design-oriented 62443.
- Modernized memory safety-related mitigations based on D3FEND as part of our collaboration with them.
- Started adding mapping notes to categories of CWEs telling the public to not map vulnerabilities to these CWEs because they're categories, not actual weaknesses.

D3FEND and CWE Mention (Mike Smith)

- Doing something similar to MITRE's ATT&CK, but we're taking the counterpart and articulating defensive tactics and techniques.
- With support from NSA, created a tactics and techniques matrix. It's expressed in industry standard formats, and vendor-agnostic semantic representations.
- There is ongoing discussion about connection to CWE and CAPEC.
- Next SIG meeting there will be a deeper discussion about D3FEND.

CWE Key Concepts – Selection from HOST Presentation (Bob Heinemann)

- Jason Oberg and Bob Heinemann presented a CWE tutorial at IEEE HOST recently to help people understand how to use CWE. Presented at the SIG as useful refresher material for the HW SIG.
- A weakness is a condition in a software, firmware, hardware, or service component that, under certain circumstances, *could contribute* to the introduction of *vulnerabilities*. The condition is described in terms of one or more of the following dimensions: behavior, property, resource, technology, or language.

- A vulnerability is 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.
- Discussion about CWE weakness abstraction levels.
    - Weaknesses are hierarchically organized from high-low abstraction, using Pillars, Classes, Bases and Variants.
    - The difference is the level of specificity in a weakness description. Pillars are the highest level of abstraction and Variants are the lowest. Depends on how many of the dimensions are captured in the description of the weakness.
    - Try to work at the lowest level you can.
    - A common question is what's the difference between a pillar and a category? A pillar is a weakness, and a category is not. A category is a collection of convenience based on a common characteristic.

SAE G-32 Call for Participation in HwA Standard (Joel Heebink)

- The G-32 Committee is a cyber physical Systems Security Committee within SAE to develop standards for cyber physical systems. Overview provided on mission, key staff and standards in progress.
- An overview of G-32 conceptual framework was provided. Consists of a system level and a component level below that. Also has domains of consideration for risk mitigation, e.g., information sharing, issue and event management, data security and electronic and physical security, etc.
- Example about the Microelectronics Threat Landscape – An Enormous Attack Surface…and traceability.
- The real risk mitigation for microelectronics is not in the operations and maintenance phase, it's all the stuff that precedes it.
- The G32 Hardware Assurance Subgroup goals were presented.

Side Channels vs Covert Channels (if time allows)

Out of time.