HW CWE SIG Meeting
Friday, June 9, 2023

Members in Attendance

Gananand G Kini
Allen Krell
Gage Hackford
Peter E Kaloroumakis
Bob Heinemann
Alec J Summers
James Pangburn
Dr. Michael J Smith
Ashrafi Gulam Mohammed
Ryan Xu
Mike Borza
Evan Bryers
Abraham Fernandez Rubio
John Hallman
Joerg Bormann
Jason Fung
Thomas Ford
Remy V. Stolworthy
Rafi Kaplan
Lyndon Fawcett
Shafqat Ullah
Lang Lin
Khaled Karray
Arun Kanuparthi
Farbod Foomany
Erwann Chevallier
Daniel DiMase
Rafael Dos Santos
Domenic J Forte
Keerthi Devraj
Patrick Lejoly
Luke W Malinowski
Sohrab Aftabjahani
Kris Britton
Bruce Monroe
Rich Piazza
Faheem Ahmed
Shivam Swami
Steve Christey Coley
Alric Althoff
Mohan Lal
Nicole Fern
Raghudeep Kannavara

Agenda

- D3FEND and Hardware Coverage
- CVE Quality Working Group Hardware and Software Tagging
- HW CWE DEMOXs from Student Competitions
- Becoming a CNA (if time permits)

Housekeeping

- Next meeting: July 14, 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

- Top 25 Release is scheduled for June 13.
- CWE/CAPEC Board Meeting occurred on June 2.
- Tentative: CISA strategy around Secure by Design/Secure by Default for July SIG.

D3FEND and Hardware Coverage (Peter Kaloroumakis)

- D3FEND has been released for two years (end of this month) and is funded by NSA.
- What we're trying to do is improve the language and the way that we talk about cyber security countermeasures, things you do in response to adversary activity.
- Very complex space for a security architect to navigate (thousands of vendors/products) to put together a portfolio of capabilities that address a problem.
- In addition to security technology, there is also policy that is applied to IT infrastructure to make it harder to attack. We wanted to build a functional model of both the cyber security technology side and the policy space to unify these domains, and make it easier to understand from an engineering perspective.
- D3FEND provides a succinct taxonomy of cyber security countermeasures.

- Think about defending from two angles. One is trying to get practitioners to have more of an engineering mindset when it comes to their cyber security capabilities and architectures. The other is a formal model for systems engineering applications to help develop better systems in the design phase rather than bolting things on after the fact.
- D3FEND is being used by government in reporting about problems in threat reports and how to address them with specific D3FEND techniques. It is also used by vendors to describe their capabilities, and by commercial companies and the DoD to understand their posture.
- Just launched our first integration with CWE (top 25 CWEs inside of D3FEND). When we modeled the top 25, we focused on the weakness and where it would live in our ontology. Does not include mitigations against the weaknesses, but will soon.
- There's a hardware device taxonomy on the website which is the beginnings of what we're thinking for a hardware ontology. Hardware includes both hardware systems and microelectronic parts.

CVE Quality Working Group Hardware and Software Tagging (Jason Fung)

- Many CVEs are filed every year, but there is not an easy way to find CVEs with a hardware root cause (CWE). A proposal is to start tagging CVE records with a root cause (hardware or software) to allow an easy way to query.
- Would like to see the next generation of the most important hardware weaknesses list be based on data/results from CVE records, rather than voting.
- The CVE QWG agreed to create a record-level experimental tag for root cause, and later promote to an official tag based on usage and feedback. It will allow both tags in cases where applicable.
- A topic for discussion is how to distinguish between hardware and software root causes. Several suggestions were presented to the group for feedback, e.g., by position in the compute stack, ease of patching, or security implication. It was decided to use the CVE GitHub as a place for further discussion. Link is in the meeting chat.

HW CWE DEMOXs from Student Competitions (Jason Fung)

- We have an idea to help improve the contents of CWE with demonstrative examples. Not many HW CWEs include examples.
- Have been working with two universities for the past 6 years, and the idea is to use buggy code from past university student competitions to serve as demonstrative examples for HW CWEs. Two examples were shown, one for CWE 1281 and one for CWE 1260.

Becoming a CNA

- Out of time.