HW CWE SIG Meeting

Friday, May 13 2022

Members in Attendance

Sohrab Aftabjahani – Intel
Matt Bascom (Guest)
Jeremy Bellay
Evan Bryers
Steve Carlson
Matthew Coles – Dell
Steve Christey Coley - MITRE CWE
Amitabh Das – AMD
Iain Deason
Daniel DiMase - Aerocyonics
Nicole Fern - Riscure
Sebastian Fischmeister
Thomas Ford – Dell
Domenic J Forte
Jason Fung – Intel
Kathy Herring Hayashi
Bob Heinemann – MITRE CWE
Arun Jain
Shahram Jamshidi
Joe Jarzombek – Synoposys
Arun Kanuparthi – Intel
Hareesh Khattri
Gananand Kini - MITRE CWE
Allen Krell
Vikas Kumar
Lang Lin – Ansys
Mohan Lal – NVIDIA
Parbati K Manna
Bruce Monroe – Intel
Carlos Moreno
Luke Malinowski – MITRE CWE
Kumar Mangipudi – Lattice Semiconductor
Jason Oberg – Tortuga Logic
Michael Pak - Cloudflare (Guest)
Sathyamurthi Sadhasivan
Naveen Sanaka – Dell
Brent M. Sherman
Alec Summers - MITRE (HW CWE SIG Moderator)
Charles Timko – Red Hat
Robert Van Spyk
Paul Wortman - Wells Fargo

General/Initial Discussion

MITRE CWE: Gananand G Kini

• Next meeting is scheduled for June 10, 2022 12:30-1:30pm EST
• Mailing list discussion - removal of the IP phrase
• Update about scope exclusions for CWE
• Presentation on new categories

New Categories

MITRE CWE: Bob Heinemann, Paul Wortman, Jason Fung

• Use of work streams for updating and making CWE more accessible and usable

• Overlaps between environmental system issues and physical attacks

- "Missing/Improper Protection against Physical Attacks" (Jason F)
- "Environmental System Issues", "Hardware Trojans", "Untrusted Manufacturing", and "Reverse Engineering" (Paul W)

A member comments about classifying between a weakness and an attack point.

A member comments about having a good utility between end users and suppliers regarding environmental conditions.

• Discussion about creating new categories and then either moving or linking existing entries into the new categories.

A member asks how the cross-linking might work under the proposal. Steve Christey Coley replies that CWE wants to make information browsable and accessible and understandable to people who are doing hardware design and implementation.

• Speaker replies that there should be a separate category we do not have all of the entries related to power management security in there yet

• Additional discussion about thermal, physical, power, and clock reset weaknesses for potential category distinctions

CWE 4.7 released

CWE/CAPEC Technical Lead: Steve Christey Coley

• ICS/OT related submissions

• ICS/OT Special Interest Group kickoff coming soon (DOE Working Group)

• Working on insufficient technical documentation

• Reminder: CWE/CAPEC REST API Working Group is in progress now

• Dependencies on software libraries and how applications and open-source components may be handled

• Potentially changing certain technology names to account for applicability to hardware

• Scope exclusions have been discussed with the ICS SIG, and also regarding hardware

A member comments about a data memory dependent prefetcher that may have an associated CWE or CVE record.

• Speaker replies that it is under research as a potentially new weakness.

[End of meeting]