HW CWE SIG Meeting
Friday, September 9, 2022

Member in Attendance

Name	Company
DiMase, Daniel	Aerocyonics Inc
Walters, Steven	Aerocyonics Inc
Bryers, Evan	Aerospace Corporation
Wesselkamper, Jim	AMD
Lin, Lang	Ansys
Pangburn, James	Cadence
Pak, Michael	Cloudflare
Oberg, Jason	Cycuity
Ford, Thomas	Dell
Matthew, Coles,	Dell
Sanaka, Naveen	Dell
Schweiger, Andreas	Gast
Constable, Scott	Intel
Fung, Jason	Intel
Iyer, Priya	Intel
Kanuparthi, Arun	Intel
Khattri, Hareesh	Intel
Kumar, Vikas	Intel
Manna, Parbati	Intel
Ramesh, Sayee Santhosh	Intel
Krell, Allen	Invariant Corporation
Barry, Jim Jr.	MITRE
Christey, Steven	MITRE
Heinemann, Bob	MITRE
Kini, Gananand	MITRE
Malinowski, Luke	MITRE
Mullaly, Connor	MITRE
Piazza, Rich	MITRE
Summers, Alec	MITRE
Kulkarni, Milind	Nvidia
Lal, Mohan	Nvidia
Moreno, Carlos	Palitronica
Foomany, Farbod	SecurityCompass
Fischmeister, Sebastian	University of Waterloo
Wortman, Paul	Wells Fargo

Meeting Kick Off and Administration

Housekeeping:

- Next Meeting – October 14, 2022, 12:30 – 1:30 PM EST (16:30 – 17:30 UTC)
- Contact: cwe@mitre.org
- Mailing List: hw-cwe-special-interest-group-sig-list@mitre.org
    - All mailing list items are archived publicly at: https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/
- Minutes from previous meetings: https://github.com/CWE-CAPEC/hw-cwe-sig

Announcements:

- CAPEC content freeze is scheduled for September 22, 2022.
- CAPEC release is scheduled for September 29, 2022.
- CWE content freeze is scheduled for October 5, 2022.
- CWE 4.9 release is scheduled for October 13, 2022.

Topics for this meeting:

- CAPEC/CWE HW Mapping Example
- HCWE109 Submission
- Existing CWEs that may map to microarchitectural attacks

CAPEC/CWE HW Mapping Example – Connor Mullaly (MITRE)

- A weakness (CWE) may lead to an attack pattern (CAPEC)
- For example, CAPEC-682: Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities was motivated by the following two HW CWE entries:
    - CWE-1277: Firmware not Updateable
    - CWE-1310: Missing Ability to Patch ROM Code
- Looking for SIG feedback and knowledge in the hardware field to help make CAPEC entries better.
- Shared pre-publication screenshots of the CAPEC entry for the Exploitation of Firmware example. Provided information about the attributes (fields) in the entry and current text in the fields (see meeting slides).
    - Special attention was called to the Execution Flows section, which describe a step-by-step pattern of attack. This allows readers to get an idea how the adversary may be carrying out an attack.
    - Attention was also called to the Example Instances field, which describes a scenario of what could happen with the attack “in the wild.”

HCWE109 Submission – Scott D Constable (Intel)

- Discussion about Intel's experience with CWEs, particularly those that relate to transient execution. This refers to instructions that execute on a CPU, but do not retire so they are not committed to architectural state.

- There are three existing CWEs (CWE-1037, CWE-1264, CWE-1303) that at least reference or mention Spectre and are generally the best candidates with transient execution issues (see meeting slides). But these three do not really capture the root cause.
- To close the gap, HCWE109 was submitted: “Hardware features (e.g., branch predictors) can violate the expected behavior of a program.”
- Description of Non-transparent Behavior of Architectural Features: “modern processors use techniques such as out of order execution, speculation, and prefetching to increase performance, and this can create problems when the programmer writes code with the expectation it's going to behave in a certain way, and it does behave in a certain way at the architectural level, but does not behave in the same way at the microarchitectural level and that can provide an opportunity for an exploit.”
- An alternative to adding new CWEs may be to revise existing CWEs to address any omissions. It would be difficult but could be done.
- Approval of the new CWE will wait for at least another version. Quality is important and more review is needed, e.g., minimizing or eliminating overlap with existing CWEs.

Existing CWEs that may Map to Microarchitectural Attacks – Ganu Kini (MITRE)

- Slide presentation of some of the issues that exist in CWE:
    - Improper handling of transient state (improper clean up etc.)
    - Consistency of the behavior of transient operations to developers
    - Transparency of the behavior of transient operations to developers
    - Leakage of the transient state into the cache
    - Covert timing channels in caches
- Additional discussion on the HW SIG mailing list.