HW CWE SIG Meeting

Friday, September 8, 2023

Members in Attendance

Gananand G Kini	Nicole Fern	Luke W Malinowski
Milind Kulkarni	Fung, Jason M	Jiang Fu (Guest)
Gage Hackford	Mike Borza	Bormann, Joerg (DI SW ICS DVT RD CSF FS)
Bob Heinemann	Constable, Scott D	Sanaka, Naveen
Jiang Fu (Guest)	Manna, Parbati K	Aftabjahani, Sohrab
Monroe, Bruce	Carlos Moreno (Guest)	Raghudeep (Guest)
Steve Christey Coley	Evan Bryers	Devraj, Keerthi (DI SW ICS DVT RD CSF FS)
Ahmed, Faheem	Abraham Fernandez Rubio	Soheil Salehi Mobarakeh
Hallman, John (DI SW ICS DVT SM)	Rafael dos Santos	Das, Amitabh
James Pangburn	Allen Krell (Guest)	Wortman, Paul (OSRT) (Guest)
Mohan Lal	Jason Oberg (Cycuity) (Guest)	Kris Britton
Ford, Thomas	Alec J Summers	

Agenda

- Housekeeping and Announcements
- CWE Nit Bits
- Call For Help: HW CWEs Missing DEMOXs, OBEXs and Mitigations
- Resonant and Harmonic Based Weaknesses
- Weaknesses Dealing with HW Initialization (Nordic APPROTECT)

Housekeeping

- Next meeting: October 13, 12:30 – 1:30 PM EDT (16:30 – 17:30 UTC) on 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

- Tentative: CISA strategy around Secure by Design/Secure by Default for October SIG.
- HW CWE Spotlight: SIG Member to present internal tool developed that utilizes HW CWE.

CWE Nit Bits (Gananand Kini)

- Release 4.11 included a new custom filter that allows users to select a subset of fields they are interested in.
- There is also now a “Custom” view option that shows relationships and attack patterns to help a user map a CVE to a CWE entry.
- Question: When selecting filter options from the Custom screen, what is the meaning of the filter “Weakness Ordinalities?”
    - Answer: Question was not answered. There was discussion about improving CWE usability in future releases for a broader audience.

Commented [SMC1]: This option has existed for years. Maybe it's talking about "Custom" ?

Commented [SMC2]: I need to look into the transcript - I would/should have answered but maybe the topic strayed

Call for Help: HW CWEs Missing DEMOXs, OBEXs and Mitigations (Steve Christey Coley)

- The program wants CWE entries to be as complete as possible. There are 20 different fields/data elements in a CWE record.
- For HW CWEs, a Mitigation is missing for four percent, a Demonstrative Example (DEMOX) is missing for 16%, and an Observed Example (OBEX) is missing for 64%.
- The program requests the assistance of the SIG (and their SME contacts) to help populate this missing information.
- The HW CWE’s with these missing elements will be posted to the program’s public GitHub where issue trackers can be shared for consideration.
- Question: When a CVE is assigned/published, is there an automated method that asks the user to also identify the associated CWE?
    - Answer: No, a CNA is not required to enter a CWE mapping when publishing a CVE. Some CNAs may have some insight to the root weakness, and they are encouraged to enter a mapping. The program is going to be working actively with the CNAs to try to improve the quality and completeness of mappings.
- Suggestion was made to include Demonstrative examples for both hardware and software.
- Comment was made that CWE supports incorporating images into demonstrative examples.

Commented [SMC3]: Maybe rephrase to issues / issue trackers?

Commented [SMC4]: Need to look - what examples? Demox or obex

Resonant and Harmonic Based Weaknesses (Gage Hackford)

- CVE-2022-38392 is the vulnerability where playing Janet Jackson's Rhythm Nation on certain laptop speakers can cause the laptop to crash. This is due to the resonant frequency (a type of harmonic frequency) of the music causing the hard disk to vibrate at a frequency that causes the OS to fail.
- Studies have found examples of how hardware/system issues or problems can be introduced by exposure to resonant frequencies.
- Are resonant frequencies a topic that should be covered by CWE? And if so, what would the weakness be? A suggestion is: CWE-1384: Improper Handling of Physical or Environmental Conditions.

- Comment: I think it makes sense to include these as a child node under 1384.
- Comment: To me, it seems natural to add this under the same umbrella of improper protection (CWE-1384). Could be another way to introduce fault injection.
- Question: If people want to get involved in this issue, is it going to be put on GitHub? Answer: No, but it’s a good idea, and in the meantime, we can use the email list.

Weaknesses Dealing with HW Initialization (Nordic APPROTECT) (Gananand Kini)

- Does the program have adequate coverage for incorrect initializations in the HW View?
- An example is CVE-2020-27211 (“Nordic Semiconductor nRF52840 devices through 2020-10-19 have improper protection against physical side channels. The flash read-out protection (APPROTECT) can be bypassed by injecting a fault during the boot phase.”). This CVE refers to physical side channels and is mapped to CWE-203, but that isn’t the best mapping.
- Other entries that might be a better fit are: CWE-1188: Insecure Default Initialization of Resource and CWE-1221: Incorrect Register Defaults or Module Parameters.
- Are there other scenarios in HW design where there are initialization mistakes that aren’t registers or module parameters? Is this something we should add to the HW View?
- Comment: CWE-1271 maybe relevant here which is uninitialized value and reset for registers holding security settings. The CVE description says reset, but really in this case its power on. There is also a requirement for a fault injection. The attacker needs two things happen, default state needs to be wrong and then they also need a weakness of being able to inject a fault.

Commented [SMC5]: @Gananand G Kini I think these bullets touch on some important points but are far too detailed for a "minutes" report. I'm not sure how to handle this, though.

- Comment: The root cause here actually is improper protection against fault injection attacks. Because what happened here was that the AP protect bit was configured correctly in flash, but then it had to be copied from flash over to the debug access port when the product was being initialized and attack not dependent on default value.
- Comment: Root cause is actually that they didn't do any countermeasures like double checking, reading it out twice from flash, seeing if the values are consistent with each other, or were the standard mechanisms you would use to kind of protect security critical configuration bits being read out.
- Comment: MITRE is going to create a new CWE for incorrect initialization of resources. Other parts of CWE distinguish “missing” activity versus an “incorrect” activity or behavior. There is already a CWE for missing initialization but not one for incorrect initialization. And this is certainly applicable on the software side as well. We welcome feedback from the hardware people so that we can be sure that this new entry also appropriately covers hardware.
- Comment: For the initialization discussion, the differentiation of 1221 vs. 1271 is the former is the static (design-time) vs. the latter is dynamic (run-time). Both are common design issues. Some targets such as registers are relevant under both static and dynamic scenarios, while some other targets such as design parameters and fuse are

more design-time specific. Memory will be run-time mostly. CWE-1188 seems to tie more with CWE-1221 conceptually.