HW CWE SIG Meeting

Friday, October 13, 2023

Members in Attendance

Gananand G Kini	Frost, Sandy	Swami, Shivam
Allen Krell	Manna, Parbati K	Milind Kulkarni
Alec J Summers	Das, Amitabh	Hallman, John
Bob Heinemann	Nicole Fern	Rafael dos Santos
Monroe, Bruce	James Pangburn	Khattri, Hareesh
Ahmed, Faheem	Rich Piazza	Kanuparthi, Arun
Forbes, Justin	Ford, Thomas	Jiang Fu
Alric Althoff	Steve Christey Coley	Luke W Malinowski
Kepa, Krzysztof	Aftabjahani, Sohrab	Wortman, Paul
Gage Hackford	Mohan Lal	

Agenda

- Housekeeping and Announcements
- CWE Nit Bits: Observed Examples
- Missing Initialization Weakness Sneak Preview (Discussion)
- Inclusive Language and HW CWEs
- Community Items

Housekeeping

- Next meeting: November 10 (US federal holiday), 12:30 – 1:30 PM EST (16:30 – 17:30 UTC). May be rescheduled to November 3. MS Teams. The following meeting is December 8.
- 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

- The new CWE Content Development Repository (CDR) is in a pilot stage; access is by invitation only. Hoping to use this to collaborate with the Community in real time on CWE submissions. Scheduled for public release in November.
- CWE 4.13 is scheduled for release October 26. A content freeze goes into effect on October 20th.
- The presentation on the CISA strategy around secure by design, secure by default is still tentative.

- The presentation from the HW SIG member (about the internal tool developed that utilizes HW CWE) is on hold until further notice.

CWE Nit Bits: Observed Examples (Bob Heinemann)

- Observed examples (OBEXs) are entries in CWEs of publicly reported vulnerabilities in real world products that exhibit the weakness. An OBEX should contain a brief description of the weakness seen in the example, and preferably include a CVE Reference(s).
- Each CVE record ideally should have at least one OBEX, and a link to the source example(s).
- As observed examples age over time, we like to refresh whenever possible.
- Two CWE examples with OBEXs were presented. (1) CWE 1300 is about not having sufficient side channel protection and includes several references that provide a lot of insight into what is meant by the weakness. (2) CWE 1191 is an example that includes a single CVE reference associated with multiple CWEs (1191 and 362). This is known as a weakness chain.

Missing Initialization Weakness Sneak Preview (Discussion) (Steve Christey Coley)

- Research into the NORDIC APPROTECT (CVE-2020-27211) issue discussed at the last HW CWE SIG highlighted a gap in CWE. The issue is about incorrect initialization but was not related to default initialization.
- When we were figuring out where to place this CVE as an OBEX, all we really could place it under was the high-level class (improper initialization) CWE 665, but this is a pretty specific weakness.
- For CWE 4.13, a new entry has been created that is about incorrect initialization of a resource. This has been given the entry ID of CWE-1419. The MITRE team asked the HW SIG participants to provide any feedback to help improve the quality of CWE 1419 before it is published on October 26. For example, should it be added to the HW view? What entry elements can be enhanced, e.g., modes of introduction, potential mitigations?
- Regarding where a weakness can originate, we should include more information in the CWE entry about reset values, and how turning on a system may include hardware initialization events.
- Our continuing program research leads to adding intermediate nodes within CWEs hierarchy that better ties-in high level concepts with lower-level variants or bases, and that's what we're seeing in this case.
- For demonstrative examples, the program will create an entry in GitHub (https://github.com/CWE-CAPEC/hw-cwe-sig/issues/106) that people can use to submit any comments/suggestions, or an email can be sent.
- Mohan provided 3 scenarios where fuses can be incorrectly initialized by HW:

    - The fuse is set correctly but the fuse line is broken.
    - The fuse is set incorrectly.
    - The fuse is set correctly but some extra HW on the fuse line modifies the fuse value.
    - This is in the context of defining the protection level of a specific product. This is typically done using fuses. Level 0 means not protected which is meant for internal use only, e.g., engineering, QA, or developer only hardware. This is not for public use. Level 3 means fully protected and for field use.
- Arun Kanuparthi provided the following comments:
    - A concern worth mentioning in the extended description is that of reset values. It is possible to have incorrect reset values set by HW that default to a non-secure mode or something like that.
    - When the system comes out of reset, like from a cold boot or power-on-reset (POR), there is a little bit of initialization that is performed by the hardware itself to initialize some resources to an initial state (e.g., like what value certain registers should be). Then there is some sort of firmware/software that comes in then programs them to a different value. Typically, the firmware will reduce the security level from secure to non-secure and then goes on. So, the very first step, before any kind of software or hardware is doing some sort of hardware initialization. It is this HW initialization, reset values, that can be incorrect."

Inclusive Language and HW CWEs (Steve Christey Coley)

- Inclusive language has been a concern since the beginning of CWE with the use of gender-neutral pronouns.
- As the program grew, more formalization of policy was needed, as well as branching out to more inclusive language of diversity, equity and inclusion that has been going on in recent years.
- In the past few years, there have been several efforts in the software community around inclusive language, e.g., IETF draft "Terminology, Power, and Inclusive Language in Internet-Drafts and RFCs."
- In the semiconductor industry, there are examples (Arm, Xilinx, Intel) of organizations with policies and initiatives to update language as needed.
- Looking for help from the HW SIG community to identify instances of non-inclusive language in CWEs and provide recommended new language. Email CWE@mitre.org.

Community Items (Bob Heinemann)

- Since the last meeting, one new OBEX and one demonstrated example (DEMOX) were added by the community.
- HW CWE entries are missing 4 mitigations, 16 DEMOXs, and 66 OBEXs.