HW CWE SIG Meeting
Friday, May 10, 2024

Members in Attendance

Abraham Fernandez	Monroe, Bruce
Bob Heinemann	Mell, Peter M. (Fed)
Alec J Summers	Constable, Scott D
Steven Christey Coley	Bojanova, Irena V. (Fed)
Gage Hackford	Mohan Lal
Nicole Fern	Ahmed, Faheem
Hallman, John (DI SW ICS DVT SM)	Ford, Thomas
Kepa, Krzysztof	
Masike, Takunda	
Mohan Lal	
Manna, Parbati K	

Agenda

- Search for a HW SIG Co-Chair
- Comparing the Hardware and Software/Vulnerability Management Infrastructure
- HW Covert Channels Discussion

Housekeeping

- Next meeting: June 14th, 12:30 – 1:30 PM EST (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

- April meeting was cancelled.
- CDR update: Closed pilot phase is complete, and it is now open by request – email Github user ID for access.
- Next release scheduled for June/July timeframe.

Search for a HW SIG Co-Chair

- A note was disseminated on HW side regarding the need for a HW SIG Co-Chair.

- Looking to bring someone external to MITRE on who has been active within HW SIG community, with some contributions to CWE. Looking for help in the following areas:
    - Strategic and leadership role
    - Membership engagement
    - Gathering thoughts, highlight priorities
    - Determine focus areas
    - Assist with future technical discussions
    - General topic submissions for upcoming meetings
    - Help form ad hoc working groups
- Nominations close on Friday, May 17th
    - Self-nominations will be accepted
    - Email Bob
    - Short discussions will be held with nominees and co-chair will be selected in-time for June meeting.

Your Hardware Has Bugs – Comparing HW and SW Vulnerability Management Infrastructures

Peter Mell
Bio:

- Senior scientist at NIST
- Started the national vulnerability database.
- Worked as technical lead on two common vulnerability scoring systems.

Presentation:

- Historically HW was viewed as an immutable root-of-trust.
- "Hardware is software – because it is made with code – it should have software like flaws" is the assumption.
- Hardware has unique physical characteristics that give it unique vulnerabilities or weaknesses – but are we missing something?
- Anytime we increase functionality in our IT products, we increase instability and insecurity.

Software Vulnerability Landscape

- For 1,000 lines of delivered code, there are 15 to 50 bugs – some effect security.
- 2023 28,000 security vulnerabilities published publicly.
- Bart Momolade security has the known exploited vulnerabilities that they know are being exploited.
- Lots of resources and programs help the community handle vulnerabilities
- CVE is primarily SW vulnerabilities.
    - 130 CWE weakness types
    - Weakness types cover 94% of the vulnerabilities.

    - 108 hardware weakness types
    - Only half have observed examples.
    - 131 hardware vulnerabilities – of these, only three of them overlapped with software vulnerabilities.
    - Those vulnerabilities cannot just be covered by three software weaknesses.
    - Are we missing something?
- 13 Hardware Weakness categories
- How was this determined?
    - Took the CWE research review CWE 1000 and added a handful of missing edges from hardware view.
    - Put hardware CWEs in graphs.
    - Used research view to look at parents of those and included non-hardware CWEs that were parents to get to top level pillars.
        - Not all top-level pillars apply to hardware – only 7 do.

Hardware Weakness Hierarchies Chart

Looking toward the Future

- Software vulnerability management infrastructure is being re-done to incorporate hardware, historically it has just been software.
- Hardware should share more than three weaknesses with software.

Questions:

1. Is the goal to figure out how much SW and HW share and figure out if they are really distinct?

   Yes, not all of the software weaknesses apply, some apply to things that are absolutely not considered hardware. I encourage you to figure out which CWEs overall apply to hardware.

2. Is your goal to try to help the corpus be more clean in case where there is a common root cause between software and hardware, they should be represented in one CWE entry, not two?

   Yes. I would be disappointed to find the SIG created CWEs for hardware, when really they could have just used an existing software CWE.

3. 1194 is almost entirely hardware specific. Is this a reasonable time to revisit the notion of these more generally applicable hybrid CWE that could apply to software or hardware?

Covert Channel Coverage in CWE

- CWE 514

    - Has relationships and children.
    - Timing channels, storage channels
    - Can follow observable behavioral discrepancies.
- Description: can be used to transfer information away, not intended by the system designers.
- No coverage around other physical characteristics that may be used as a communications medium.

Questions:

1. Should we add it to the hardware view or is it too generic?
2. What would hardware-centric concerns be?
3. Is 514 really a weakness?
4. Should we have coverage in the hardware view?

Covert Channels vs Side Channels Notes

- *Covert Channels*- Intentional transmissions, an adversary controls input and output, a method of using the same HW features to intentionally transfer information.
- *Side Channels* – accidental transmissions, adversary can only read output, typically refers to an implementation artifact of an algorithm, such that when it executes it unintentionally exposes data through a feature in the hardware whose design is incidental to its use.
- We go after the underlying cause vs trying to address the channels themselves.
- There is a single feature that could be used as a side channel or used as a covert channel.
- In a HW feature that can be used to transmit or encode information, but that use is incidental to its intended purpose.