HW CWE SIG Meeting

Friday, July 15, 20222

Member in Attendance

Bob Heinemann - MITRE

Luke W Malinowski - MITRE

Allen Krell (Guest)

Milind Kulkarni (PSIRT) - Nvidia

Steven M Christey - MITRE

Ford, Thomas - Dell

Wortman, Paul – Wells Fargo

Khattri, Hareesh - Intel

Michael Pak (Guest)

Alec J Summers - MITRE

Kumar, Vikas - Intel

Connor Mullaly - MITRE

Mohan Lal - Nvidia

Coles, Matthew - Dell

Rich Piazza - MITRE

Jason Oberg (Guest)

Sanaka, Naveen - Dell

Jim Barry Jr. - MITRE

Ramesh, Sayee Santhosh - Intel

DiMase, Daniel - Aerocyonics Inc

Walters, Steven - Aerocyonics Inc

Sebastian Fischmeister - University of Waterloo

Evan Bryers

James Pangburn - Cadence

Lang Lin - Ansys

Wesselkamper, Jim - AMD

Farbod Foomany - SecurityCompass

Andreas Schweiger - Gast

Carlos Moreno – Palitronica

General/Initial Discussion

MITRE CWE: Bob Heinemann

- Meeting intro covering the days topics
    - New Category proposals
    - 4.8 release on June 28 – prioritization for 4.9 (target date September or October ’22)
    - CWE Scope Exclusions
- Next meeting – August 5, 2022 12:30 – 1:30 EST (1630 – 1730 UTC)
- Mailing list items are archived at https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org
- Discrepancy between mailing list and invitees to meeting. Working solution. Expect new invite series
- Top 25 release June 28
- ICS/OT Working group is under way

New Category Proposal – Dr. Paul Wortman

- Untrusted manufacturing
    - 2 Categories untrusted manufacturing and hardware trojans
    - Untrusted manufacturing is potential introduction of weaknesses
        - Introduction of additional logic or other components that alter system behavior
    - Solutions
        - Split up design, add logic locking to protect IP
    - Fit into CWE?
        - Entries into existing categories such as manufacturing
        - Similar with environmental protection that can be considered its own category
        - *So part of the reasoning for having this category of untrusted manufacturing is that it really starts to assuage concerns over either untrustworthy or malicious, or otherwise counterfeit integrated circuits where again, we've got a lot of these mitigations that are clearly present and defining the weaknesses themselves, I think is where a lot more of the work is going to come from.*
- Hardware Trojans
    - Not seen as express weakness, but category that includes exploitation of hardware trojan vulnerabilities
    - Could be related to design: *A good example of how I tried to frame it is that you can have a hardware Trojan present within your design, and the presence of that hardware Trojan is a weakness that perhaps would not necessarily be triggered either because the triggering command is not received or the Trojan is placed in the design in such a way it’s nothing malicious.*
    - *I think the weaknesses that allow for the presence of hardware Trojans are enough in the CWE that we can at least present the initial category and fill them*
- Questions/Discussion:

- *A member asks So are you proposing like a new category for manufacturing? Because there is a category for issues related to manufacturing in life cycle management*
    - **Speaker answers there was the discussion about whether or not untrusted manufacturing would work as a form of a subset or as part of 1195. I would say that the counterargument for that is that the manufacturing and lifecycle management concerns are a far more wide-reaching set of category entries, because it's not only looking at just the manufacturing stage, but also the entirety of the device's lifecycle or components lifecycle.**

- *A member I'm just I'm wondering. I'm just and then related to untrusted manufacturing too. I'm trying to get my head wrapped around whether we want to have weaknesses and process and rather than weaknesses in the design itself. I'm not sure where to draw the line that makes sense.*
    - **Speaker answers that same question comes to mind is how much of weakness is in process. Do we want to place under here to your point of the hardware Trojan, I agree that the hardware Trojan itself is not the weakness, which is why I was proposing it as sort of a category name, but perhaps a hardware Trojan is just more of a buzzword intention here, in which case there might be a better name that we can give to the category, but I believe you understood the intent, which is yes, we're mainly concerned about listing out those introductions of weaknesses through these design changes or components or ways in which all of this is put together.**
    - *Member replies: pinpoint the actual weakness, then a deficiency in organizational process is probably where we want to go*

- *Member comments so the manufacturing process could inject new firmware or make modifications to configuration, for instance, that are not strictly hardware*
    - **Speaker replies I would say the reason I propose it here was when I was looking at these, I was really looking at the hardware and was very hardware focused. But I do agree that there there's a lot of software consideration to it and in one case of say just like manufacturing and fabrication, the scope can very easily balloon out because if you start looking at not only just the hardware that is being produced but the software that's running all the fabrication, the net files that are used for incorporating the designs into a means that can be manufactured, all those steps along the line, you're right. They absolutely do count, and I would even argue that what we really have to look at to have more of a holistic view here is to look at software, hardware and even a social aspect to it.**
- Further discussion of CWE covering hardware vs CVE for specific hardware vulnerabilities and how to work the reporting of hardware vulnerabilities in the CWE space

Scope Exclusion Update - Steven M Christey

- *There are almost fully documented, and I've been working on beefing them up. They have new symbolic identifiers. Really breaking out the rationale for why the exclusion exists. Giving some examples based on a lot of feedback from you all and using a lot of your examples.*
- First draft will be pushed to the Sigs and working groups
- Still working the process related to the CWE research list and how final decision will be made