HW CWE SIG Board Meeting #3

Friday January 22 @ 1230-1330 EST

Members in Attendance*

Sohrab Aftabjhani – Intel
Steven Christey
Mike Borza - Synopsis
Erik Costlow – Contrast Security
Nusrat Farzana Dipu – University of Florida
Farbod Foormany – Security Compass
Jason Fung – Intel
Lang Lin - Ansys
Pabrati Manna – Intel
Mohan Lal – NVIDIA
Jason Oberg – Tortuga Logic
Alec Summers – MITRE (HW CWE SIG Moderator)

**This is only a partial capture based on the information available via recording*

Housekeeping – Community Expansion

Reviewed by the moderator

- Are there other communities with which you engage that the HW CWE SIG could interact with?
- Are there upcoming events or issues with your organization to discuss?
- As the SIG grows, the number of representatives from a single organization may be capped (haven't reached threshold yet)
- Point other potential participants to cwe@mitre.org

OWASP IoT Project

A member shared that he was in search of reviewers for a new initiative (relating to IoT verification standards) which incorporates some of the hardware requirements from the Hardware Design CWE page.

ACTION: Moderator will send more information.

Detecting Hardware Weaknesses with Radix

Presented by Jason Oberg of Tortuga Logic
Additional details are available on accompanying deck.

I. Company Introduction
   a. Focused on mostly logical or architectural weaknesses (vs. physical)
II. Asset-based Threat Modeling
   a. The presenter shared how information around how using CWE as a central taxonomy is an approach that was helpful for customers. Looking specifically at what assets need

protection in relation to the associated attack vectors can help bring more focus since not all CWEs are relevant for every customer's design.

b. Next, common weaknesses at various levels of a system-on-chip were shared. This includes Individual Blocks, CPUs, Hardware Roots of Trust, and SOC Systems.
c. The presenter then walked through the process of conducting threat modeling based on which assets need protection beginning with security requirements from the architecture. ROM (eFuse) was used as the example asset.
    i. *Moderator asked a question regarding whether customers use CWE site filters to search through hardware design content and specific consequences (getting to ease of use). The presented said that the current format was helpful as an initial guideline. However, some of the CWEs can get very specific making it more difficult to map to their specific use model. Following this asset-based approach can make the process less overwhelming.*
    ii. *A member asked if there was a process or tool for the hardware team to identify assets in the design. The presenter said that within larger organizations (which have distinct security architectures among them), there should be someone aware of the security architecture who can prioritize and share the most important assets. Providing full automation can be challenging. The member and presented also discussed how adding the domain (HW, SW, etc.) can be helpful for mitigation.*
d. The presenter explained how selecting relevant CWEs can be automated by choosing the appropriate keywords for queries.
e. Finally, steps for creating a Radix Security Rules from CWEs were covered. Security rule templates are available for CWEs from the latest version.

III. Introduction to Radix (example usage for CWE)

a. The presenter discusses how Tortuga's Radix-S (simulation) and Radix-M (emulation) can be utilized for a more streamlined hardware security development lifecycle in addition to which design environments, security rules, etc. the tools work with best.
b. Additional details on the security rules, which are the foundation of Radix and connect well with confidentiality and integrity requirements, were shared. This is run within design flow and doesn't require a tool change to see if rules are being violated.
    i. *A member asked if there is a standard for security rule definitions. The presenter said that there is not one currently.*
c. Information Flow Analysis: Information flow (not values-based) is tracked through the design which is important especially in regards to hardware.
    i. *A member asked whether the no flow operator was the syntax developed for Radix. The presented confirmed that it was developed for Radix. He went on to explain how the user writes the rules in a separate file, which is loaded in with an organization's design and generates checkers that run the design environment.*
d. Details of the user flow for how to deploy Radix were shared. The existing/functional verification environment is leveraged to deploy the checkers into your simulation flow.
    i. *A member asks whether the security rules are in natural languages and then being translating them into some assertions. The presenter said yes, but at a*

higher level because the security rules aren't just being translated to SD Texas umbrella assertions, for example, because those are all value-based. Instead, the movement of information is tracked while the user runs the simulation emulation. The presenter acknowledged that there are analysis views to help users look at the results and look at the details of the specific run to understand where assets have gone – not presented on the slide.

e. The presenter concludes with information on detecting vulnerabilities as design evolves
    i. A member asked whether Radix notifies designers of whether a rule has been violated. The presenter said that that countermeasure recommendations aren't automatically provided but that the different analysis view would help users understand where the assets went and whether they were mismanaged.

At the conclusion of the presentation, the presenter clarifies that the deck was not intended to be confidential and proprietary as originally stated on the slides. The moderator shares that he will distribution the deck when received.

Potential Topics for Next Meeting

- Upcoming HW CWE Release 3/2021
    - Content suggestions for CWE or CAPEC
- A perspective from your organization
    - Leveraging HW CWE in your organization and/or operations
- Academic engagement

Next meeting is scheduled for 2/19.

The moderator asked if anyone had additional thoughts on these topics. A member responded that for the last 3 years his organization has hosted competitions (e.g. Hardware Capture the Flag) and made appearance at conferences with academic partners like Texas A&M. The purpose is to create awareness around high risk security issues being found in designs. Vendors, industry teams, and students come together. The moderator shared similar experiences that he has seen within MITRE.