HW CWE SIG Meeting

Friday, August 9, 2024

Members in Attendance

Gananand G Kini	Monroe, Bruce	Hallman, John
Alec J Summers	Mell, Peter M.	Charles Timko
Steven Christey Coley	Constable, Scott D	Evan Bryers
Gage Hackford	Bojanova, Irena V.	Jason Oberg
Nicole Fern	Frost, Sandy	Mohan Lal
James Pangburn	Ahmed, Faheem	Swami, Shivam
Mike Borza	Ford, Thomas	Das, Amitabh
Forbes, Justin	Rich Piazza	Iyer, Priya B
Sathyamurthi Sadhasivan	Kepa, Krzysztof	Salehi, Soheil
Manna, Parbati K, Co-Chair	Masike, Takunda	Krell, Allen
Keerthi Devraj	Milind Kulkarni	Robet Van Spyke
Mohan Lal	Joe Resienger	
Steven M Christey		

Agenda

- **Covert Channels Discussion Close Out**
- **SystemVerilog vs Verilog Discussion**
- **Useability Updates and HW CWEs Discussion**

Housekeeping

- Next meeting: September 13th, 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

- CWE 4.15 release was released on July 16th
- CWE Content Development pilot is now on GitHub
- We are seeking any interesting topics for the next SIG in September.

Previous Meeting Recap

- Dan Dimase mentioned weekly Articles of Security Interest during the last HW SIG.
    - A few articles deal with hardware security.
    - There is a need to determine a hardware angle that is not currently being covered by the HWE CWE.
    - **Call for reviewer volunteers**: We are looking for someone to scour the table of contents for entries and determine what is important or not. It will require going to the page and determining if it looks interesting.

- Hareesh discussed a new way that CWE is already making an impact in the security world. He shared an academic work that uses CWE content and LLMs to automate the generation of security assertions.
    - Name of paper – DIVAS: An LLM-based End-to- End Framework for SoC Security Analysis and Policy-Based Protection.

Call for topics for next meeting: None submitted.

Covert Channels Discussion Summary

- **Member Comments**
    - Covert channels should have coverage in the HW view – *Jason Oberg*
    - Covert channels should be in the hardware categories Security Flow Issues, General Circuit and Logic Design Concerns, or Debug and Test problems – *Paul Wortman*
    - CWE-514 as currently written, is specific to software and would need to be tweaked – *Bruce Monroe*
- **May/June HW SIG Meeting**
    - Bob/Manna presented current CWE coverage on covert channels.
    - **Call for comments**: Today, last call for comments on Covert Channels are being sought. After today, Chair and Co-Chair will consider comments and develop a proposal for the HW SIG consideration.
    - **No comments submitted**.

SystemVerilog

- When code examples are created, they are being specified as SystemVerilog code, the schema does not contain an entry for SystemVerilog.

Questions:

1. What is the difference between SystemVerilog and Verilog?
2. Is that difference significant enough that we should add SystemVerilog to the schema enumeration?

Andreas: Do some research and come back with briefing next meeting

Robert: I believe there is a bit of a difference between the two. Especially if someone is using automated tools.

Nicole: Agreed. SystemVerilog is different from Verilog. It is similar to C++. Verilog and VHDL are designed to describe the hardware that you are making. SystemVerilog is a superset of Verilog. It has types and lists built in.

Gage: There are certainly instances where we code examples that are technically SystemVerilog, but there isn't anything particularly unique to SystemVerilog that is used in the code. We could get in touch with the authors of those HACK@DAC code examples and see if they could categorize them as just Verilog.

Steven Christey: This would not be a significant schema change, so the overhead would be minimal to none. Supporting SystemVerilog is a very easy lift. There are two places where the language enumeration is used:

1. Used in the demonstrative examples where we write code snippets and then say what language the code snippet is in.
2. In applicable platforms.

It is something we can accomplish in CW 4.16 in October.

Manna: The other angle is to change the schema. The cost is minimal, but the implications are not. If someone is looking at a basic code in SystemVerilog, they could potentially enter that code and put in the entry to the CWE as either Verilog or as a SystemVerilog. If we have two entries later, they would have to query both Verilog and SystemVerilog.

Nicole: We could change everything to SystemVerilog since Verilog is a subset of SystemVerilog it would still be correct.

Useability Updates and HW CWEs Discussion

Goals:

- Put all important information above the fold, at the top.
- Make it easily digestible.
- Create a visual aide.
- Describe the weakness condition and some context.
- No more than 3-4 sentences.

Changes have been applied to a few CWE entries in 4.15.

Thomas: I plan to meet with my hardware designers next week and I can ask them which of the CWEs seems to be the most confusing and get back to the group.