HW CWE SIG Meeting

Friday, November 18, 2022

Members in Attendance

Aftabjahani,Sohrab
Bryers, Evan
Christey, Steven
Coffin, Chris
Coles, Matthew
Constable, Scott
Das, Amitabh
Fern, Nicole
Ford, Thomas
Hackford, Gage
Heinemann, Bob
Iyer, Priya B
Kaplan, David
Khattri, Hareesh
Kini, Gananand
Krell, Allen
Kumar, Vikas
Lal, Mohan
Malinowski, Luke
Manna, Parbati
Monroe, Bruce
Mullaly, Connor
Oberg, Jason
Pak, Michael
Pangburn, James
Piazza, Rich
Summers, Alec
Taggart, Philip
Timko, Charles
Wortman, Paul

Introduction, Announcements, and Agenda

MITRE CWE: Gananand Kini

- Topics: Scope Exclusions, Hardware items in 4.10 release, Hardware root of trust.
- Next meeting rescheduled for December 16th, 1230-1330 EST (1630-1730 UTC).
- CWE 4.10 targeted for January 2023.
- New ICS/OT SIG Working Groups launched – Boosting CWE Content.
- Scope Exclusions and Submission Problems to be posted for public review.

Scope Exclusions

MITRE CWE: Steve Christey Coley

- As CWE opens to allow outside entities to submit CWEs, it needs to be more precise on scope definitions.
- Exclusions – What people think CWE should cover but does not. See slides for structure/types of exclusions.
- Version almost ready to publish for comment.
- Need to be clear about what constitutes a weakness.
- Needs more examples.
- Publish on the CWE website by the end of the month (hopefully).

HW Items in 4.10 Release

MITRE CWE: Bob Heinemann

- Items being worked (51 total) / working queue topics description (see slides).

Discussing Improper Protection of Intermediate Cryptographic State/Results

Cycuity: Jason Oberg

- Background.

    - Security of cryptographic algorithms relies on intermediate states being unobservable, but there are hardware channels that can provide observability.
- Presentation of OpenTitan's OTP controller.
    - See slides.
    - Analysis via Radix found leaks of intermediate states.
        - CWE submitted.
- Discussion over this being a widespread issue, software versus hardware.
- A member asked, "why does observable behavior discrepancy not fit, and what is the new proposition?"
    - **Response**: there is a distinction between information that is explicitly copied to (or left uncleared in) an area where it can be accessed by attackers, and the inability to indirectly observe discrepancies in behavior. The former is not an observable discrepancy.
- Discussion over best practices in hardware regarding exposing data as observable at an intermediate state.

Closing

- What topics to consider for the next meeting.
- If you would like to present, please let the team know.