HW CWE SIG Board Meeting #2

Friday December 18 @ 1230-1330 EST

Members in Attendance*

Sohrab Aftabjahani – Intel
Patrick Bailey – Microchip
John Bell – iRobot
Matthew Coles – Bose Corporation
Steve Christey - MITRE
Farbod Foormany – Security Compass
Arun Kanuparthi – Intel
Bruce Monroe – Intel
Jason Oberg – Tortuga Logic
Kerry Crouse – MITRE
Rich Piazza – MITRE
Andreas Schweiger – Airbus
Alec Summers – MITRE (HW CWE SIG Moderator)

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

CAPEC Introduction Presentation

- Background and history (see slides for more information)
- Use Cases for CAPEC
    - Application Testing – Red Teaming
    - Analysis
    - Threat Modeling
    - Requirements
    - Evaluations
    - Reporting
    - Training/Education
    - Prioritization
- The Relationship Between CWE and CAPEC
    - Hardware CWEs inform a CAPEC entry
    - Some of what users submit for CWE might be more appropriate for CAPEC.
    - Looking at how to describe the submission as a CAPEC can help determine the underlying weakness

A member asked if there is requirement that CAPECs link to a CWEs (more specifically, would the CWE describe the weakness and the CAPEC would have to link to that weakness?) The moderator shared that CAPEC does cover items like social engineering (an example area where there are no associated weaknesses) so generally there isn't a requirement. The presenter explained that there is interest in

establishing a link and that with the expansion of the domain NWCE their could be plans to make this happen in the future.

Another member asked if there was a one-to-one mapping or one to many in addition to asking if CAPEC handles chains of attacks. The presenter shared that the relationship between CWE and CAPEC is many to many. In regards to the second question, the labels "can proceed" and "can follow" are used to specify chains although this process isn't complete.

The group also discussed the connection between hardware, firmware, and software weaknesses and the impact they can have on each other. Determining whether a CWE has a root cause in hardware or software because of the vague nature of some weaknesses (e.g. access control) had been a focus area of the CWE board. The presenter encouraged the group to use the existing chaining relationships to link different weaknesses together when developing submissions.

CAPEC Introduction Presentation (cont'd)

- Differences between CAPEC and ATT&CK (both are community-based programs; managed by MITRE)
    - CAPEC – based on weaknesses; aimed at "getting ahead of boom"
    - ATT&CK – based on they types of things out in the real world that you would need to protect and defend against
    - Both tools address similar problems but with different approaches

The new version of CAPEC (3.4) was released on 12/17.
Questions about the CAPEC project – CAPEC@mitre.org

CWE New Minor Release – v 4.3

The presenter shared that almost all of the 20 new hardware weakness came from community submissions (one was internally developed). There are now close to 100 new weaknesses in total. Peripherals, On-Chip Fabric and Interface/IO Problems – (1203) was a category that grew significantly.

ACTION: Members should review these new weaknesses and share feedback.

Hardware Relevant Consequences

The upcoming hardware consequences are a bit different than what is currently in the schema. The presenter describes what has not been previously covered (e.g. physical damage and safety hazards) and how even the current "regular" software weaknesses can impact hardware. Weak authentication in medical devices (pacemakers mistakenly sending out shocks to patients) was mentioned as a real-life example.

The presenter then asks the group whether they think it is important for CWE to cover "safety hazard." He then invites the representatives from Intel to share their thoughts since the group had participated in previous related discussions.

A representative from Intel shares that there are (4) different levels to denial-of-service attacks and suggests incorporating some of the terminology and discuss the different types of impact they could have. Another Intel representative agrees with including the information, emphasizing that IoT will be a focal point. He also shares that the new CVSS 4.0 will incorporate some of this thinking.

The moderator asks for clarification on whether the intent is to add the information in the event that an adversary can cause a safety hazard, noting that the concept could get into quality and could move away from adversarial focus.

The first Intel representative responded with a recommendation to not speak from an impact angle, but a root cause perspective. In this case, the impact is the functional task. He said that we should limit ourselves to the security vulnerabilities that can be exploited to cause a safety issue.

Another question that came up from the Intel team, specifically for MITRE staff, regarding what to do in when a safety hazard occurs in isolated environments but not across the board.

The presenter explained that the current schema within Common Consequences can indicate how often a technical impact occurs although there may be room to modify the current setup.

The discussion continues with drawing a distinction between safety hazards from a device versus application of the device. Other members of the group agree. The idea of the same components being used across different types of devices was also brought up for consideration. Looking at relevant regulatory material to see how the topic should connect with CWE was another suggestion.

Next Meeting (1/22)

- Tortuga Logic Presentation – Identifying HW CWEs
- Future Volunteer Presenters – Share thoughts on leveraging HW CWE in your organization and/or operations