HW CWE SIG Meeting

Friday, March 10, 2023

Members in Attendance

Bob Heinemann
Bruce Monroe
Gananand G Kini
Joerg Bormann (DI SW ICS ICV OS)
Rich Piazza
Shafqat Ullah
Paul Wortman
Jason Fung
John Hallman (DI SW ICS ICV OS)
Luke W Malinowski
Amitabh Das
Mohan Lal
Parbati K Manna
Thomas Ford
Jason Oberg (Cycuity) (Guest)
Alec J Summers
Arun Kanuparthi
Nicole Fern
Shivam Swami
Steven M Christey
James Pangburn
Brian M Vohaska
Soheil Salehi (ECE, U of Arizona) (Guest)
Donald Davidson
Naveen Sanaka
Milind Kulkarni
Bronn Pav
Carlos Moreno
Andy Meza (UCSD) (Guest)
Mike Borza
Scott Constable
Matthew Coles
Gage Hackford

Agenda

- Housekeeping and Announcements
- Working Items for this Meeting
  - Crypto HW Weaknesses Community Discussion
  - Scope Exclusions and Updates on Submissions Process
  - Feedback on our Current Use of GitHub (if time permits)

Housekeeping

- Next meeting: April 14, 12:30 – 1:30 PM EDT (16:30 – 17:30 UTC). Virtual meeting using 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 4.11 targeted for release in May 2023. Might be moved to late April.
- CAPEC announcement (Alec Summers)
  - Over the past year, have tried to promote wider CAPEC adoption and coverage from the community. Limited success. Very few new submissions or edits to existing entries. Program team has done most of the content updates.
  - CAPEC will be a low priority going forward, and the CWE/CAPEC Board is considering options about how to proceed, including:
    - Continue to host CAPEC site on a server (definite) with a potential banner about halted maintenance and development.
    - Move maintenance and development to open source.

        - Transition CAPEC to a willing organization for maintenance and development.
    - Survey open (available on any CAPEC web page) through today for the community to provide their feedback.
    - Board is having an out of cycle meeting on this subject March 17.

Crypto HW Weaknesses Community Discussion (Luke Malinowski)

- Investigating CWE for gaps in cryptography, and potential gaps relate to hardware.
- Key observations:
    - Secure key management concerns from an Ops perspective. Are critical keys stored in an HSM? Don't fully believe CWE is capturing the usage of an HSM as a mitigation, and capturing the fact that using HSM is different than other normal software-based mitigations.
    - Little mention of cryptographic hardware in CWE.
    - Not much discussion of hardware in relation to PKI or web of trust systems.
    - Discussion of key management in hardware is lacking.
- Want to ensure the advantages provided by hardware for cryptographic applications like TLS are properly captured in CWE.
- Fundamentally, we think there are gaps in hardware cryptography, and we want discussion with you about whether you agree or think it's currently adequately covered.
- The motivating example of not storing critical keys in an HSM (hardware security module) was presented, using selected CWE records.
- Question to the group: Do you feel that CWE covers weaknesses, in terms of the use of cryptography and in hardware? And if not, what are the gaps? What improvements can be made?
    - Don't think the current state of CWE covers very clearly the difference between HW and SW keys.
    - Question: Does CWE capture the concept about not reusing a key for multiple purposes? We should have a key hierarchy to use for very specific purposes. Answer: Don't think so. Will look into this to verify.
    - Review CWEs in the areas of data clearing, side channels, timing, faulting. Maybe there needs to be some additional examples that are crypto focused.
    - May be helpful to list out weaknesses we have in the hardware view that are specific to this topic, and determine whether they are sufficient.

Scope Exclusions and Updates on Submissions Process (Steve Christey Coley)

- Scope exclusion discussions have been on-going. Getting close to publishing list of scope exclusions and opening up to broader community discussion.
- Why define scope exclusions instead of just defining scope?
    - Scope has been defined, but the community still puts in requests for out-of-scope entries.

    - Scope exclusions attempt to formalize decisions about what can or cannot be included in CWE. They are explicit statements that say which things would not fall under CWE scope and why.
- Expect to publish the suggested list of exclusions in the next few weeks, and allow a period of time for the community to review and comment (suggested adds, deletes, modifications).
- The current list of 10 suggested exclusions was presented. The meeting slide deck includes details for all 10 exclusions and will be made available to members.
- A scope exclusion has: ID, Name, Description, Rationale, Examples, Resolution, Debate, and Status.
- The details for three exclusions were shown:
    - SCOPE.NOMITS (no actionable mitigations)
    - SCOPE.CUSTREL (not customer-relevant)
    - SCOPE.CONFLICT (conflict/contradiction with other weaknesses)

Feedback on our Current Use of GitHub (Bob Heinemann)

- Have been testing different ways to facilitate collaboration and discussion items, rather than relying on email/mailing list.
- Put a couple tracker items on the public GitHub to see how it works in terms of getting more participation. GitHub provides transparency to the broader user community and serves as a repository of actions and decisions related to issues.
- Also trying to use GitHub to facilitate document collaboration.
- Please visit the GitHub site and provide feedback on its usefulness.
- Today’s meeting slides will be posted to GitHub.