Hardware CWE™ Special Interest Group (SIG)

Bob Heinemann, Gage Hackford, Steve Christey Coley, Alec Summers

MITRE

March 8, 2024

Agenda

REMINDER: This meeting is being recorded.

1	µArchitecture Weaknesses Deep Dive	Scott Constable	40 min
2	Inclusive Language	Steve Christey Coley	10 min

Housekeeping

- **Schedule:**
  - **Next Meeting: April 12**
    - **12:30 – 1:30 PM EST (16:30 – 17:30 UTC)**
    - **Microsoft Teams**
- **Contact: cwe@mitre.org**
- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
- **Minutes from previous meetings available on our GitHub site:**
  - **https://github.com/CWE-CAPEC/hw-cwe-sig**

Announcements

- **CWE Content Development Repository (CDR) pilot now on GitHub! Currently invite only. Potential public release in early 2024.**

- **CWE 4.14 Released on February 29.**
  - 4 New Weakness Entries Related to Transient Execution
    - Thank you, Intel, AMD, ARM, Cycuity and Riscure
  - 10 Demonstrative Examples from HACK@DAC
    - Thank you Mohamadreza and team

- **CWE 4.15 release will be around June/July**

Transient Execution Weaknesses Media

Chips & Salsa: Industry Collaboration for New Hardware CWEs | Intel

- https://youtu.be/am-36eiETyg

Intel Corporation Blog Post About Transient Execution Weaknesses

- https://community.intel.com/t5/Blogs/Products-and-Solutions/Security/Chips-Salsa-Industry-Collaboration-for-new-Hardware-CWEs/post/1575521

Cycuity Blog: Microarchitecture Vulnerabilities: Uncovering the Root Cause Weaknesses

- https://cycuity.com/type/blog/microarchitecture-vulnerabilities-uncovering-troot-cause-weaknesses/

Dark Reading Article

- https://www.darkreading.com/endpoint-security/four-new-cwes-released-for-microprocessor-architectures

Overview of Recently Released Microarchitectural Weaknesses

Scott Constable (Intel)

Inclusive Language and HW CWEs (Inclusive Terminology)

Inclusive Language in CWE

- **In October 2023's HW-SIG meeting, we talked about CWE's evolving use of inclusive language since 2006**
- **2020 to today: software/standards community efforts**
  - IETF draft "Terminology, Power, and Inclusive Language in Internet-Drafts and RFCs"
  - NISTIR 8366 - Guidance for NIST Staff on Using Inclusive Language in Documentary Standards
  - ACM: "Words Matter - Alternatives for Charged Terminology in the Computing Profession"
  - Semiconductor industry adoption (details in next slide)
- **For CWE 4.15, we want to address the use of "master"/"slave" in some hardware-related CWEs**

Inclusive Language in Semiconductor Industry

- Arm’s “Inclusive Language Commitment: Arm is committed to making the language we use inclusive, meaningful, and respectful. Our goal is to remove and replace non-inclusive language from our vocabulary to reflect our values and represent our global ecosystem.”[1]

- Xilinx has their Inclusive Naming Initiative[2]

- Numerous examples of Intel updating documentation to use inclusive terminology[3]

1. https://www.arm.com/en/company/sustainability/business-practices
2. https://www.amd.com/content/dam/amd/en/documents/corporate/cr/Inclusive-terminology.pdf
3. https://www.intel.com/content/www/us/en/docs/programmable/683609/21-3/creating-a-system-with-revision-history.html

Example Usage of “Master”/”Slave” in CWE

- **9 CWEs use “master,” “slave,” or both**
- **Demonstrative examples**
  - CWE-1311 demox: “One of the masters to this NoC... and another master”
  - CWE-1267, CWE-1290, CWE-1318 demox: center around “bus masters”
  - CWE-1264: demox uses “bus masters”. Alt term? “first-party DMA” ?
  - CWE-1318: “bus master” in both demox
- **Extended description**
  - CWE-1317: “a bridge… forwards transactions to the slave without checking the privilege level of the master”
  - CWE-1193: “master transactions on the hardware bus”
  - CWE-1318: “bus master… master to slave”
- **Other**
  - CWE-1274: a detection method focuses on “fabric master agents”
  - CWE-1394: obex for “master encryption key”

Options for Changing Non-Inclusive Language

- **Consider alternate terms (mostly from IETF draft version 15)**
  - Primary-secondary based on authority
  - Primary-replica based on originality
  - Active-standby based on state
  - Writer-reader based on function
  - For “bus master” - “first-party DMA” ?
- **If a standard specification or architecture used master/slave but changed to other terms, then use the new terms of that standard**
- **Ensure that the meaning remains clear and limits the amount of “cognitive load” on the reader (i.e., avoid being awkward or vague)**

How to Decide on Changes to Inclusive Language for HW CWEs?

- **Where to discuss and decide?**
  - HW-SIG mailing list
  - HW-SIG GitHub repository issue?
  - (maybe too soon) Content Development Repository (CDR) on GitHub
- **Some demox's submitted before October 2023 were able to use alternate terminology**
- **Please email cwe@mitre.org any standards or references for alternate terminology for hardware.**

- **UEFI Industry Guidance: https://uefi.org/sites/default/files/resources/UEFI_Inclusive%20Language.pdf**

Next Meeting (April 12)

CWE@MITRE.ORG

- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
  - ***NOTE: All mailing list items are archived publicly at:***
    - *https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/*
- **What would members of this body like to see for the next HW SIG agenda?**
- **Questions, Requests to present? Please let us know.**

Backup

Addressing Observed Example Gaps for HW CWE

OBEX Gaps Agenda

- Current Need
- OBEX Challenges
- Participation and Organizing Work
- How you can help

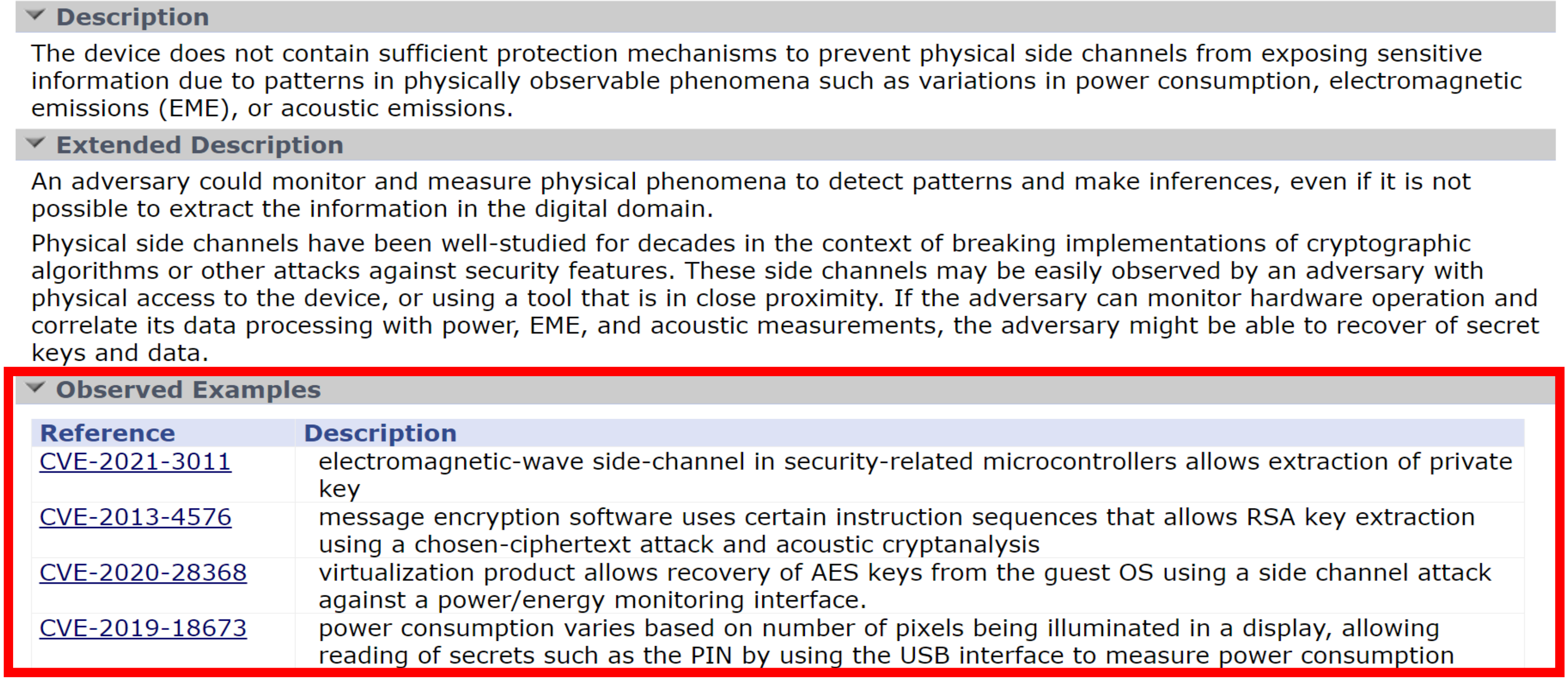
Observed Examples Working Group

- **Goal:** Ensure every HW CWE has at least one OBEX.
  - The OBEX element is important in that it links real-world examples to weaknesses.
  - 61 (52%) of HW CWEs lack observed examples.
  - Your contribution can reduce this gap.

- **Timeframe and Commitment:** Next release cycle, approx., March through June.
  - We value your time and expertise, so would like to structure the workgroup so that participation can be flexible and asynchronous.
  - Target generating OBEXs for 10% - 20% of the HW CWEs missing OBEXs for this release.

- **Recognition:** All contributors will be acknowledged for their valuable input.
  - This is a great opportunity to gain recognition within the community and add a contribution to your professional portfolio.

CWE-1300:
Improper Protection of Physical Side Channels



Description

The device does not contain sufficient protection mechanisms to prevent physical side channels from exposing sensitive information due to patterns in physically observable phenomena such as variations in power consumption, electromagnetic emissions (EME), or acoustic emissions.

Extended Description

An adversary could monitor and measure physical phenomena to detect patterns and make inferences, even if it is not possible to extract the information in the digital domain.

Physical side channels have been well-studied for decades in the context of breaking implementations of cryptographic algorithms or other attacks against security features. These side channels may be easily observed by an adversary with physical access to the device, or using a tool that is in close proximity. If the adversary can monitor hardware operation and correlate its data processing with power, EME, and acoustic measurements, the adversary might be able to recover of secret keys and data.

Observed Examples

Reference	Description
CVE-2021-3011	electromagnetic-wave side-channel in security-related microcontrollers allows extraction of private key
CVE-2013-4576	message encryption software uses certain instruction sequences that allows RSA key extraction using a chosen-ciphertext attack and acoustic cryptanalysis
CVE-2020-28368	virtualization product allows recovery of AES keys from the guest OS using a side channel attack against a power/energy monitoring interface.
CVE-2019-18673	power consumption varies based on number of pixels being illuminated in a display, allowing reading of secrets such as the PIN by using the USB interface to measure power consumption

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

OBEX Challenge #1 – Specific to HW CWE

- **CVE has limited coverage for hardware specific vulnerabilities**
- **Examples:**
  - **Did not find a CVE that could be mapped to the above CWEs**
    - CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments did not turn up any results
    - CWE-1338: Improper Protections Against Hardware Overheating
    - CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy
  - **Found CVE that may map but not enough details to be sure**
    - CWE-1328: Security Version Number Mutable to Older Versions
  - **Found CVE that map**
    - CWE-1326:Missing Immutable Root of Trust in Hardware
    - CVE-2022-38773, CVE-2022-28383, CVE-2023-22955

How to help: HW Vulnerability Sources

- **Since CVE has limited coverage for hardware vulnerabilities, we need to consult other sources for observed examples.**
- **We like to tap into the collective knowledge and expertise of this group.**
- **Please provide sources other than CVE that we could use to pull observed examples from for HW CWEs.**
- **Preferably site that aggregate vulnerability reports.**
- **[WORKING ITEM] Sources for Hardware Vulnerability Reports**
  - https://github.com/CWE-CAPEC/hw-cwe-sig/issues/109

Observed Example Element

- Contains one or more publicly reported vulnerabilities in real-world products that exhibit the weakness.

- **<u>Sub-Elements</u>**
  - **Reference**: This contains ~~the CVE Identifier, e.g., CVE-2005-1951~~ a vulnerability identifier.
  - **Description**: Clear, simple, and concise summary of ~~CVE~~ vulnerability report that focuses on the link between the ~~CVE~~ report and weakness. Exclude product name, attack vectors and other irrelevant details.
  - **Link**: URL Link to ~~CVE~~ vulnerability report. ~~Preferably from https://www.cve.org/.~~

OBEX Challenge #2 – General CWE Challenge

- **Vulnerability reports are not written from a weakness aspect**
  - The original weakness is not always covered.
  - From a vulnerability management perspective, the underlying weakness may not actually be important to the organization.
  - Reports emphasize product impact, product versions affected, and how easy it is for an attacker to exploit.
  - Routinely we see that many of the vulnerability descriptions do not have enough information to determine what the underlying weakness is.
  - For OBEXs we cannot infer the weakness, the vulnerability report must specifically describe the weakness.

How to help: Submitting an OBEX

1. **Find HW CWE(s) you would like to contribute an OBEX.**
   - There is a list maintained on our GitHub.
   - There is an issue per HW CWE that is missing an OBEX.
   - NVD Data may be a help here
2. **Assign yourself to the GitHub Issue.**
3. **In the Issue comments, provide a CVE Number, URL, description, and how you would like to be cited for the contribution.**
   - Preferred Name and organization.

Issues are here:

https://github.com/CWE-CAPEC/hw-cwe-sig/labels/Missing%20OBEX

Note: We are planning to release a OBEX Style guide soon

Summary

Our ask

1. **Commit to supporting the working group.**
   - Send an email to cwe@mitre.org, subject: OBEX WG.

2. **Provide additional HW Vulnerability Sources.**
   - https://github.com/CWE-CAPEC/hw-cwe-sig/issues/109

3. **Generate 1 OBEX or many OBEXs.**
   - https://github.com/CWE-CAPEC/hw-cwe-sig/labels/Missing%20OBEX

Open *Community Items*

HW CWE's With Missing:
DEMOX's, OBEX's and Mitigations

- **Missing Mitigations**
  - 4 HW CWEs are missing mitigations (No change)
- **Missing Detection Methods**
  - How many do we have? CREATE A TRACKER
- **Missing demonstrative examples (DEMOX)**
  - 15 HW CWEs missing demonstrative examples (down 1)
    - 1 added from Hack@DAC, CWE-440
    - Note: there are other DEMOXs from Hack@DAC but now adding DEMOXs to entries that have an existing DEMOX
  - How many DEMOX's are not code based? CREATE A TRACKER

https://github.com/CWE-CAPEC/hw-cwe-sig/issues

Discussion Items on GitHub

Resonant frequency weakness, proposal (Topic Lead: OPEN)	• https://github.com/CWE-CAPEC/hw-cwe-sig/issues/105
Covert Channel Coverage in HW View (Topic Lead: OPEN)	• https://github.com/CWE-CAPEC/hw-cwe-sig/issues/108
CWE Coverage of HW Cryptography (Topic Lead: OPEN)	• https://github.com/CWE-CAPEC/hw-cwe-sig/issues/7
Lifecycle-stage classification for HW CWEs –Dan DiMase (Topic Lead: OPEN)	• https://github.com/CWE-CAPEC/hw-cwe-sig/issues/4

Covert Channel Coverage in CWE

COVID-Bit Research Item[1][2]

- **In 2022, researchers at Ben Gurion University in Israel developed a new data exfiltration method for air-gapped systems called COVID-bit.**
- **Malware generates electromagnetic radiation in the 0-60 kHz frequency band (assumes Malware got there somehow).**
- **EM emissions are generated by manipulating the workload of the CPU. Claims of indirect control SMPS.**
- **The electromagnetic radiation generated by this intentional process can be received from a distance using appropriate antennas.**

1. *https://thehackernews.com/2022/12/covid-bit-new-covert-channel-to.html?m=1*
2. *https://arxiv.org/abs/2212.03520*

Covert Channels and Side Channels

- Initial thought was that COVID-Bit could be a DEMOX for CWE-1300: Improper Protection of Physical Side Channels
- As HW SIG Members had correctly pointed out, COVID-Bit is about Covert Channels and NOT Side Channels
- Covert Channel (CC) / Side Channel (SC)
    - Intentional transmission (CC). Accidental transmission (SC) – *Ross Anderson* [1]
    - Adversary controls input and output (CC). Adversary can only read output (SC) – *Intel* [2]
    - Not an intended resource but exists due the application's behaviors. –*CWE-514 Notes* [3]
- If not CWE-1300 (SC), where would something like this map to in HW view?
- Closest we have is CWE-514: Covert Channels

1. *https://www.cl.cam.ac.uk/~rja14/Papers/SEv3-ch19-7sep.pdf*
2. *https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/best-practices/refined-speculative-execution-terminology.html*
3. *https://cwe.mitre.org/data/definitions/514.html*

CWE-514: Covert Channel

https://cwe.mitre.org/data/definitions/514.html

Abstraction: Class

Description: A covert channel is a path that can be used to transfer information in a way not intended by the system's designers.

Extended Description: Typically the system has not given authorization for the transmission and has no knowledge of its occurrence.

Relationships:

ChildOf	CWE-1229:Creation of Emergent Resource
ParentOf	CWE-385:Covert Timing Channel
ParentOf	CWE-515: Covert Storage Channel
CanFollow	CWE-205: Observable Behavioral Discrepancy

Vulnerability Mapping Notes:

Usage: Allowed-with-Review; **Reason:** Abstraction

Rationale: This CWE entry is a Class and might have Base-level children that would be more appropriate; **Comments:** Examine children of this entry to see if there is a better fit.

NOTE: Nothing about EM based Covert Channels, nor HW cause, e.g., SMPS

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Discussion

Questions:

- Should we place CWE-514 in the HW View?
- Do we need to modify CWE-514 to be less software centric?
- Or create a base of CWE-514 and put that into the HW view?

Previous HW SIG Member Comments:

- Covert Channels should have coverage in the hardware view *–Jason Oberg*
- Covert Channels should be in the HW categories Security Flow Issues, General Circuit and Logic Design Concerns, or Debug and Test Problems. *– Paul Wortman*

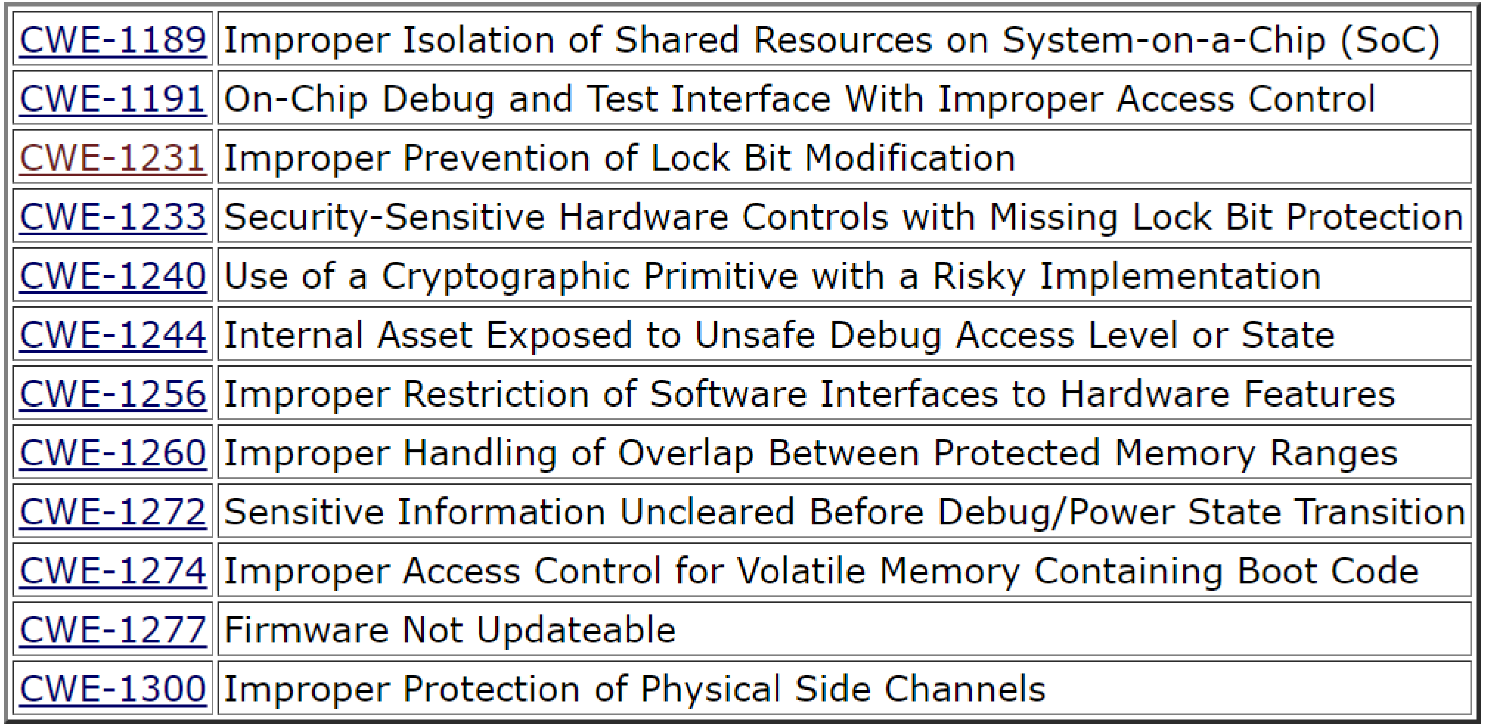
Most Important Hardware Weaknesses Refresh

Bob H

Most Important Hardware Weaknesses (MIHW)

- **Is this something worth revisiting?**
- **Part of CWE 4.6 Release, October 28, 2021**
- **Have there been substantial developments since the last release of MIHW?**
- **Would those affect the rankings and inclusions of the list in any meaningful way?**

Current MIHW



CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

New HW CWEs Since MIHW

- **CWE-1342: Information Exposure through Microarchitectural State after Transient Execution**
- **CWE-1357: Reliance on Insufficiently Trustworthy Component**
- **CWE-1384: Improper Handling of Physical or Environmental Conditions**
- **CWE-1388: Physical Access Issues and Concerns**

Discussion

- **Have there been substantial developments since the last release of MIHW?**
- **Would those affect the rankings and inclusions of the list in any meaningful way?**
- **Are there observational trends that would change the current list in any significant and meaningful way?**

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

OBEX WG Formation

- **Purpose:** Populating missing observed examples (OBEXs) in HW CWEs.
  - Your expertise can make a difference!
- **Challenge:** 61 (52%) of HW CWEs lack observed examples.
  - Your contribution can significantly reduce this gap.
- **Goal:** Ensure every HW CWE has at least one OBEX
  - You can help enhance the quality and comprehensiveness CWE.
- **Motivation:** The OBEX element is important for new users
  - Your input will directly impact the ease of use
- **Timeframe and Commitment:** March through June. Participation is flexible and asynchronous, allowing you to contribute when it suits you best.
  - We value your time and expertise.
- **Recognition:** All contributors will be acknowledged for their valuable input.
  - This is a great opportunity to gain recognition within the community and add a significant contribution to your professional portfolio.