CWE-CAPEC ICS/OT Special Interest Group

Co-Chair: Greg Shannon
Co-Chair: Alec Summers

- Kickoff Meeting Minutes -

Wednesday May 18, 2022 | 3:00 pm – 4:30 pm ET

Housekeeping

Next Meeting – *Wednesday, June 29, 2022 from 3:00 to 4:30 pm ET*

Minutes from previous meetings available at: https://github.com/CWE-CAPEC/ICS-OT_SIG

To join the listserv, email: cwe@mitre.org

Opening Remarks

After reviewing the meeting's purpose and agenda, ICS/OT Special Interest Group (SIG) co-chairs and representatives from government provided introductions.

- **Alec Summers**, Principal Cybersecurity Engineer & Group Lead, the MITRE Corporation
- **Greg Shannon**, Chief Cybersecurity Scientist, Cybersecurity Manufacturing Innovation Institute (CyManII)
- **Lindsey Cerkovnik**, U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)
- **Cheri Caddy**, Senior Advisor, U.S. Department of Energy (DOE), Cybersecurity, Energy Security, and Emergency Response (CESER)

Presentations

Representatives from MITRE and CyManII discussed the formation of the ICS/OT SIG, background and related efforts, and a work plan for the upcoming year.

Kickoff meeting slides are available at: https://github.com/CWE-CAPEC/ICS-OT_SIG

How We Got Here

SIG leadership provided background on the DOE CESER's Securing Energy Infrastructure Executive Task Force (SEI ETF) that produced 20 categories of security vulnerabilities in ICS/OT systems at the direction of Congress, as well as alignment with the CWE and CAPEC programs. Leveraging this work from the SEI ETF, CWE and CAPEC formed a Special Interest Group (SIG) open to the public to explore updating and expanding the scope of these programs to cover weaknesses arising in ICS/OT systems.

One participant recommended the SIG identify champions in the group early on to move work forward and coordinate messaging.

Where We Are Today

SIG leadership discussed highlights from the CWE 4.7 update released in June, which included updates to the CWE database drawn from four of the SEI ETF's security vulnerability categories, and previewed the remaining work to be done around expanding CWE-CAPEC scope to ICS/OT systems to capture more of the SEI ETF categories.

One participant asked about the connection between CWEs and security controls that can be used to mitigate weaknesses and a representative from MITRE noted that CWEs include potential mitigations. A recommendation was made to map CWE mitigations to existing security control standards or guidelines like ISA 62443 or NIST CSF.

Another participant asked if we can link this activity to the term KEV - Known Exploitable Vulnerability.

Several participants emphasized the need to further clarify the problem that is trying to be solved, as well as use a common set of definitions for the terms being used. These participants also emphasized the need to explore how to better leverage/communicate CWE-CAPEC findings to the broadest possible audience. Many resources exist within the current group of participants to make that happen.

Related Activities

Representatives from CyManII discussed related activities, including the institute's Coordinated Vulnerability Awareness (CVA) program to build awareness and well-informed means of responding to reported vulnerabilities for a cyber-proactive manufacturing community.

A representative from DOE CESER discussed the upcoming release of its National Cyber-Informed Engineering Strategy, which is now available here: https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document

Where We Want to Go This Year

SIG leadership reviewed a notional work plan to cover in the SIG this year:

1. Review NCSV TPT work and prioritize/edit categories for incorporation into future CWE and CAPEC updates
2. Collaborate with MITRE to meet content submission requirements
3. Explore 2 categories/weaknesses for broader advisories/publications
4. Explore further avenues for dissemination/communication around weaknesses
5. Define current CWE/CAPEC scope
6. Identify challenges for expanding CWE/CAPEC scope

SIG leadership also noted the June CWE/CAPEC board meeting on June 3, 2022, as well as the next major update for CWE/CAPEC weakness in the Fall of 2022.