CWE-CAPEC ICS/OT Special Interest Group

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

- Meeting Minutes -

Wednesday July 27, 2022 | 3:00 pm – 4:30 pm ET

Housekeeping

Next Meeting – *Wednesday, August 31, 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 provided updates on the National Cyber-Informed Engineering (CIE) Strategy and the recent Cybersecurity and Infrastructure Security Agency (CISA) security advisories.

- **Alec Summers**, Principal Cybersecurity Engineer & Group Lead, the MITRE Corporation
- **Greg Shannon**, Chief Cybersecurity Scientist, Cybersecurity Manufacturing Innovation Institute (CyManII)

Presentation

Representatives from MITRE and CyManII discussed the purpose and scope of the Common Weakness Enumeration (CWE) framework as well as challenges that users face when applying it to ICS/OT systems.

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

Existing Applications for CWE in ICS/OT

SIG leadership provided background on how sister programs similar to MITRE ATT&CK, all curate cyber information, but they all do different things as related to detecting vulnerabilities, and from different points of view. SIG leadership described how CAPEC, ATT&CK, and D3FEND each provide a unique approach to enumeration.

CAPEC focuses on how an adversary exploits a weakness, while ATT&CK identifies taking advantage of a design feature for nefarious purposes and enumerates a process an adversary goes through to attribute an attack on a network, as opposed to identifying weaknesses.

D3FEND is about a knowledge graph of countermeasures and focuses on the different ways these types of attacks can be countered.

SIG leadership went on to say it is understood that each of these programs have clear delineations that can, oftentimes, seem arbitrary or hard to discern, but it is on us to improve our community engagement. We are also looking at other possibilities to provide value to the community.

Gaps for CWE to Address/Priority Gaps in Classifying ICS/OT Weaknesses

SIG leadership shared five key points that participants should consider when classifying ICS/OT weaknesses and asked the candidates if the weaknesses resonated as strong examples to them.

Classifying ICS/OT Weaknesses:

1. Emerging tech
2. Cloud driven software development
3. OT devices are not built for the load
4. Weaknesses inherent w architectural patterns
5. Security concerns

A participant, and CWE technical lead, shared that they are independently looking at cloud related weaknesses and have started this as a sub-project of CWE. They further stated that at least some of the work will come for free because of other ongoing work that is not solely applicable to ICS/OT, such as identifying architectural weaknesses.

Another participant stated that looking at traditional ICS/OT, the lack of V&V for conducting updates – you don't want automatic updates because systems are so critical. However, with updates, you don't have good assurance that it won't break anything; there is innovation to be had there in the future.

Properties of Weaknesses

- Utilization
- Identification
- Standardization of terminology
- Limited framing of weaknesses
- ICS
- Develop hands-on training materials/field guide

The facilitator opened a discussion regarding the properties of the weaknesses. A participant asked, as related to normalization, if that aligns with the REST API Working Group. Another participant stated that within the National Vulnerability Database, individual CVEs are mapped to CWEs. All the ICS CERT advisories include one or more CVEs. Trend analysis, as part of the annual software Top 25, started looking at large scale analysis of ICS CERT advisories and started showing some interesting results. These results were different than overall CVE database.

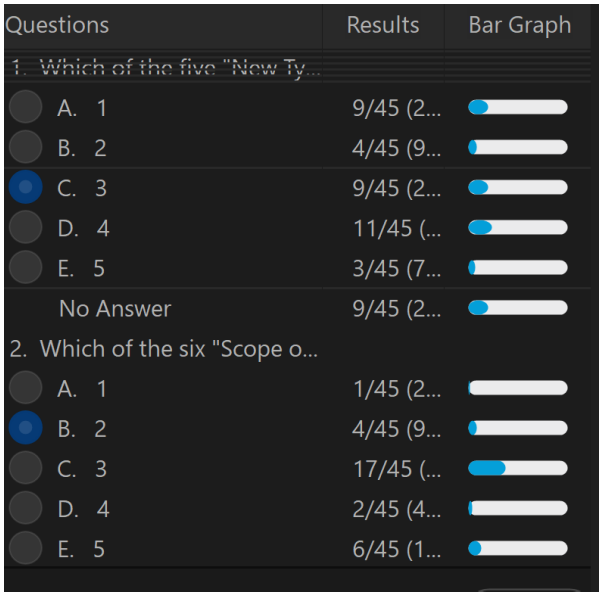
To the point of normalization, one challenge is faced: we will be working with vendors and other CVE publishing authorities to include quality and mapping of their individual CVEs. Their quality working group is making improvements to schema for sharing CVE data, including better ways to reference CWE identifiers. That's one area with significant progress on area of normalization.

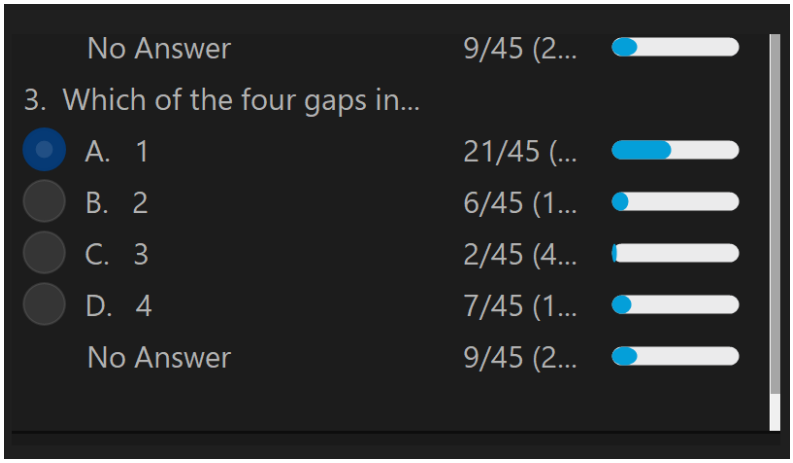
Polling

SIG attendees participated in in three polls to prioritize gaps in classifying, scoping, or communicating ICS/OT weaknesses. See slides 14, 15, and 16 from the last meeting in the Github repository.

Questions:

1. Which of the five "New Types of Weaknesses" gaps should be our highest priority?
2. Which of the six "Scope of CWE-CAPEC" gaps should be our first priority?
3. Which of the four gaps in communication ICS/OT weaknesses should be our first priority?




No Answer 9/45 (2...
3. Which of the four gaps in...
A. 1 21/45 (...
B. 2 6/45 (1...
C. 3 2/45 (4...
D. 4 7/45 (1...
No Answer 9/45 (2...

Participants

1. Abdelrahman Elsanose, *Freelance*
2. Ahmad Sharafi, *Allied Arabian Maintenance & Trade Co. (AAMCO)*
3. Anton Shipulin, *Nozomi Networks*
4. Ashley McGlone, *Tanium*
5. Beverly Novak, *INL*
6. Bill Aubin, *Nozomi Networks*
7. Bryan Owen, *Aveva*
8. Chris Humphrey, *Boeing*
9. CJ Harvey, *MITRE*
10. Cynthia Hsu, *DOE*
11. Evgeni Sabev, SAP
12. Howard Grimes, *CyManII*
13. Iain Deason, *DHS CISA*
14. Ismael Garcia, *NRC*
15. Joe Agres, *West Yost*
16. Jon Terrell, *Hitachi Energy*
17. Jose Jimenez, *Sothis*
18. Joseph Januszewski, *E-ISAC*
19. Jude Desti, *Boeing*
20. Junya Fujita, *Hitachi America*
21. Matthew Knoll, *ArcelorMittal*
22. Marc Sachs, *Auburn University*
23. Martin Scheu, *Switch*
24. Melissa Vice, *Air Force*
25. Michael Chaney, *CyManII*
26. Monika Akbar, *UTEP & CyManII*
27. Paul Martyak, *EPRI*
28. Paul Peix, *Headmind*
29. Rex Wempen, *DOE*
30. Rich Piazza, *MITRE*
31. Richard Robinson, *Cynalytica*
32. Rita Ann Foster, *Idaho National Laboratory*
33. Roger Johnson, *Novelis*
34. Shadya Maldonado, *INL*
35. Sharin Crane, *Boeing*
36. Steve Granda, *NREL*
37. Stephen Trachian, *Hitachi Energy*
38. Susan Farrell, *Object Security*
39. Timothy Isaacs, *NuScale Power*

Leadership/Meeting Support

1. Aeriel Lane, *Nexight Group*
2. Alec Summers, *MITRE*
3. Steve Christey Coley, *MITRE*
4. Greg Shannon, *CyManII*

5. Jeff Hahn, *INL*

6. Stephen Bolotin, *Nexight Group*

7. Greg Kerr, *Nexight Group*

8. Greg Shannon, *CyManII*