CWE-CAPEC ICS/OT Special Interest Group

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

- Meeting Minutes -

Wednesday June 29, 2022 | 3:00 pm – 4:30 pm ET

Housekeeping

Next Meeting – *Wednesday, July 27, 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 vulnerabilities and design-related issues in ICS/OT systems that CWE already covers. SIG leadership then discussed why CWE is not widely used by ICS/OT cybersecurity professionals. Potential users in this space are often not fully aware of or familiar with the CWE framework.

An example of this can be seen in the recent Forescout publication covering 56 vulnerabilities in various vendor products. Although this paper included several vulnerabilities that could be mapped to existing CWE IDs, it did not mention any of the relevant CWE IDs.

Relevant vulnerability-CWE mappings:

- Hardcoded credentials (CWE-798)
- Hardcoded crypto key (CWE-321)
- Plaintext transmission (CWE-319)
- Weak encryption (CWE-327)
- No authentication (CWE-306)

Gaps That CWE Should Grow to Address

SIG leadership shared questions that participants should consider when thinking about the future of CWE and how to apply it to ICS/OT systems.

Questions to consider:

- What are some opportunities to make CWE more useful for those who care about ICS/OT vulnerabilities?
- Which of the NCSV TPT categories includes gaps for CWE to address?
- Which gaps are related to other stages of the secure development lifecycle?

One participant then shared an example of how CWE-319 could be updated to be more applicable to Modbus and other ICS protocols.

Expanding the Scope and Focus of CWE

SIG leadership communicated goals and guidance for formally expanding the scope of CWE to be more applicable to ICS/OT systems. SIG leadership then discussed the focus of CWE on mistakes. Several participants expressed their confusion around the term “mistake” and the general lack of standardized, industry-recognized terms in ICS/OT cybersecurity.

SIG leadership further clarified the definition of mistake and discussed the difficulties of characterizing particular issues like counterfeit components. In this example, CWE focuses on the weaknesses introduced by a counterfeit component rather than the counterfeit component itself; however, CWE may also recognize additional flaws at the process/institution level that allowed the introduction of the counterfeit component.

SIG leadership and participants then discussed the ways in which a lack of standard, industry-recognized terms is an obstacle preventing many potential users from applying CWE to ICS/OT systems. For example, it is often difficult for new users to differentiate between weaknesses, vulnerabilities, and attack surfaces, or between risk mitigation and avoidance.

CWE as a Community-Driven Framework

SIG leadership reviewed the purpose of this SIG and explained how they would like to engage the ICS/OT cybersecurity community to help improve existing CWEs, propose new content for CWEs, and drive the modernization of the CWE program itself. SIG leadership then discussed the ways in which community involvement could change MITRE's approach to CWE for ICS/OT systems as well as specific goals for the community to help define specific activities and decision-making mechanisms to ensure the success of CWE in solving the needs of its ICS/OT users.

Several participants then shared their experiences working in the ICS/OT cybersecurity space and their thoughts on the future of CWEs and how to integrate them with other relevant cybersecurity frameworks.

Breakout Sessions

SIG attendees participated in breakout sessions aiming to brainstorm ideas are two topics:

1. Defining the set of stakeholders that should participate in the SIG
2. Identifying gaps participants think would be useful for this working group to address

Participants

1. Abdelrahman Elsanose, *Freelance*
2. Ahmad Sharafi, *Allied Arabian Maintenance & Trade Co. (AAMCO)*
3. Anton Shipulin, *Nozomi Networks*
4. Ashley McGlone, *Tanium*
5. Ayman Alissa, *Mckinsey*
6. Beverly Novak, *INL*
7. Bill Aubin, *Nozomi Networks*
8. Bill Kintz, *Invictus*
9. Bradley Nickens, *GE*
10. Bryan Owen, *Aveva*
11. Christopher Sundberg, *Woodward*
12. Chris Humphrey, *Boeing*
13. Cynthia Hsu, *DOE*
14. Evgeni Sabev, *SAP*
15. Hadeli Hadeli, *Hitachi Energy*
16. Howard Grimes, *CyManII*
17. Iain Deason, *DHS CISA*
18. Ismael Garcia, *NRC*
19. Jace Powell, *Fortress*
20. Jen Walker, *Water ISAC*
21. Joe Agres, *West Yost*
22. Kerry Stuver, *GE*
23. Khalid Ansari, *FM Approvals*
24. Kimberly Denbow, *American Gas Association (AGA)*
26. Marc Sachs, *Auburn University*

27. John Parmley, *Zuuliot*

28. Jon Terrell, *Hitachi Energy*

29. Jon White, *NREL*

30. Jordon Sims, *Imperium Global Advisors*

31. Jose Jimenez, *Sothis*

32. Joseph Januszewski, *E-ISAC*

33. Matthew Knoll, *ArcelorMittal*

34. Max Wandera, *Eaton*

35. Michael Chaney, *CyManII*

36. Monika Akbar, *UTEP & CyManII*

37. Oystein Brekk-Saunderud, *Norma Cyber*

38. Peter Pongracz

39. Renan Xavier, *Novo Nordisk*

40. Rex Wempen, *DOE*

41. Rich Piazza, *MITRE*

42. Richard Robinson, *Cynalytica*

43. Rita Ann Foster, *Idaho National Laboratory*

44. Robert Heinemann, *MITRE*

45. Rob Garry, *General Electric*

46. Roger Johnson, *Novelis*

47. Ryan Bays, *PNNL*

48. Saravanakumar "Kumar" G, *Transport for NSW*

49. Saleh Almaghrabi, *Schneider Electric*

50. Shadya Maldonado, *INL*

51. Sharin Crane, *Boeing*

52. Steve Granda, *NREL*

53. Stephen Trachian, *Hitachi Energy*

54. Susan Farrell, *Object Security*

55. Timothy Isaacs, *NuScale Power*

56. Wayne Austad, *CyManII*

57. William Kintz, *Invictus International Consulting, LLC*

Leadership/Meeting Support

1. Alec Summers, *MITRE*

2. Andrew Kresses, *Nexight Group*

3. Daisyareli Martin, *Nexight Group*

4. Greg Kerr, Nexight *Group*

5. Greg Shannon, *CyManII*

6. Jennifer Ekperigin, *Nexight Group*

7. Katie Baker, *Nexight Group*

8. Stephen Bolotin, *Nexight Group*

9. Steve Christey, *MITRE*