CWE-CAPEC ICS/OT Special Interest Group

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

- Meeting Minutes -

Wednesday August 31, 2022 | 3:00 pm – 4:30 pm ET

Housekeeping

Next Meeting – *Wednesday, September 28, 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, the ICS/OT Special Interest Group (SIG) co-chairs provided opening remarks, thanking attendees for their participation and written comment provided. The meeting host reviewed meeting objectives and material covered during the prior session.

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

CWE Discussion

How do you and your organization use CWE today?

After reviewing a sample of questionnaire responses, participants further discussed how they and their organizations use CWE **today**:

- To enable comparison of security product capabilities
- To help with development
- Conducting larger scale analysis and trend analysis
- To "get in front of the problem" rather than waiting to respond to vulnerability discovery in OT systems

One participant express interest in how future iterations will provide insight on applications in distributed control systems (DCS). A MITRE representative responded that there are upcoming efforts to annotate existing CWEs as affected by or related to DCS and to identify gaps to recognize or explain weaknesses as they are recognizable to ICS/OT users.

How would you and your organization like to use CWE in the future?

After reviewing a sample of questionnaire responses, participants further discussed how they and their organizations would like to use CWE in the **future**:

- To support/incorporate Cyber Informed Engineering (CIE) from the original Securing Energy Infrastructure Executive Task Force
- To prioritize response to threat intel given limited resources
- To enable proactive guidance on where vulnerabilities may be
- To map against risk scoring and quantify presence of risk
- To prioritize and improve efficacy of mitigations
    - MITRE identified this as a longer-term goal for both CWE and CAPEC
- To improve efficiency in mitigation, prevention, and response to threats

Sub-Working Group Charters

Link to Charters

Participants reviewed the list of volunteers, potential leaders, charter, and work plan for each proposed sub-working group. Participants further discussed ideas for activities/contributions to each sub-working group.

Note that volunteers for sub-working group leadership will receive support from chairs, MITRE, and Nexight for facilitation, project planning, and documentation.

A call for participation will be sent to the mailing list once a working group is kicked off. Participants who expressed interest during this meeting were added to the slides accordingly.

Boosting CWE Content

- A lead for this group will have to tackle the challenge of effectively educating on what the CWE mindset is and how we create new content. A leader should help manage some content and have a good understanding of the CWE mindset, being able to distinguish between weaknesses and vulnerabilities.
- Need for steady progression towards goals. Due to abundance of content enhancing opportunity, prioritization is needed. Leads will define milestones and help reduce uncertainty while making steady progress.
- This working group will work very closely with folks like **Steve** and **Alec.**

Education and Awareness of CWE and ICS/OT weaknesses

- This group will move more quickly due to easier ramp-up on technical details. Existing participant social and network connections provides opportunity to hit the ground running, proselytizing and connecting with contacts individually and in small groups.

Participants discussed additional ideas for boosting CWE content:

- 62443 as lingua franca
- Opportunity to coordinate with CVE CNAs to drive consistent use of CWE categories mapped from CVEs. Coordinate with CVE board to potentially require CWE mapping to fulfill "vulnerability type." While CWE is a part of that in the sense that there is a small list from years ago, "vulnerability type"
- Mapping to CAPEC and vice versa
    - Also applies to sub-group #1.
- Increasing awareness of CWE that differ between IT and OT

Mapping to 62443

Participants discussed additional ideas for mapping to 62443:

- Cross-references within definitions for CWEs using taxonomy mapping
  - MITRE expressed that this recommendation is highly feasible, with support developing the list of mappings between CWEs and 62443

Launching Sub-Working groups

- **Sub-working groups 1 and 3** will be launched first. **Action item** to schedule follow-up discussions with lead volunteers.

Enumerate SIG Stakeholders (Org and Representative Types)

Review Questionnaire and breakout session results from prior meetings

Participants reviewed the draft list of SIG stakeholders and provided recommendations for additions, which were captured directly in the slide deck (available via Github).

Identify any gaps in current set of SIG participants

Overview of the current set of SIG participants provided:

- Total of 241 individuals either participating or registered to the listserv.
- Total of 162 people who have participated in one or more meetings, including participants from IT, OT, or cybersecurity services, manufacturers, research and academia, government, associations, and asset owners and operators.
- **Action item:** Please reach out to MITRE or Nexight if you are not registered for the listserv/are joining from a forwarded invite.

Wrap-Up

Closing remarks and meeting conclusion.

Participants

- Ahmad Sharafi
- Anjel Jimenez
- Anton Shipulin
- Beverly Novak, INL
- Bryan Owen, Aveva
- Christopher Sundberg, Woodward
- Chris Humphrey, Boeing
- Curtis Taylor, CyManII
- Cynthia Hsu, DOE
- Edward Liebig
- Howard Grimes, CyManII
- Ismael Garcia, NRC
- Joe Agres, West Yost
- Jon White, NREL
- Jose Jimenez, Sothis
- Joseph Januszewski, E-ISAC
- Junya Fujita
- Ken Cole, Entergy
- Khalid Ansari, FM Approvals
- Kyle Hussey
- Matt Sexton, Hexagon
- Max Wandera, Eaton
- Michael Chaney, CyManII
- Paul Martyak, EPRI
- Renan
- Rich Piazza
- Rita Ann Foster
- Ryan Bays, PNNL
- Samuel Chanoski, INL
- Shadya Maldonado, Sandia
- Steve Granda, NREL
- Susan Farrel, ObjectSecurity
- Timothy Isaacs, NuScale Power
- Wayne Austad, CyManII

Leadership and Support Staff

- Alec Summers, MITRE
- Greg Kerr, Nexight Group
- Greg Shannon, CyManII
- Jeff Hahn, INL
- KatherineAnne Baker, Nexight Group
- Stephen Bolotin, Nexight Group
- Steve Christey, MITRE