CWE-CAPEC ICS/OT Special Interest Group

Co-Chairs

Greg Shannon, *Chief Science Officer, Cybersecurity Manufacturing Innovation Institute (CyManII)*
Alec Summers, *Principal Cybersecurity Engineer, MITRE Corporation*

Introduction

The Common Weakness Enumeration (CWE)/Common Attack Pattern Enumeration and Classification (CAPEC) program – in partnership with the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER) and operated by the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) Homeland Security Systems Engineering and Development Institute (HSSEDI) – is pleased to announce a new special interest group focusing on security weaknesses in industrial control systems (ICS) and operational technology (OT).

Background

The CWE-CAPEC ICS/OT Special Interest Group (SIG) offers a forum for researchers and technical representatives from organizations operating in ICS and OT design, manufacturing, and security to interact, share opinions and expertise, and leverage each other's experiences in supporting the continued growth and adoption of CWE as a common language for defining ICS/OT security weaknesses. While Information Technology (IT) has an extant body of work related to identify and classifying security weaknesses, IT and ICS/OT are different, and existing IT classifications are not always useful in describing and managing security weaknesses in ICS/OT systems. Addressing this gap will help all stakeholders communicate more efficiently and effectively and promote a unity of effort in identifying and mitigating ICS/OT security weaknesses, especially in critical infrastructure. The CWE-CAPEC ICS/OT SIG began in May 2022. Additional information is available at the ICS/OT SIG's GitHub repository.

Objectives

The ICS/OT SIG aims to achieve the following objectives:

1. Address gaps in describing and managing security weaknesses in ICS/OT systems
2. Establish a stakeholder community for discussing ICS/OT CWE content
3. Explore cross-organizational collaboration opportunities
4. Provide critical input regarding CWE domain coverage and hierarchical structure

October 2022

Intended Participants

The following stakeholder categories are invited to participate in the ICS/OT SIG:

1. Owners and operators
2. Manufacturers/vendors/system integrators
3. Government and policy subject matter experts
4. National Laboratories
5. Research and academic institutions
6. IT, OT, or cyber service providers or security professionals

Sub-Working Groups

The ICS/OT SIG's co-chairs are standing up three sub-working groups to achieve these objectives:

1. "Boosting CWE Content" Sub-Working Group

Launch Date: Wednesday 10/12 from 10:30 to 11:30 am ET (then meeting biweekly)

- Howard Grimes, *Chief Executive Officer, CyManII* (co-chair)
- John Kingsley, *Senior Cybersecurity Engineer, Hitachi Energy* (co-chair)
- Steve Christey Coley, *Principal Information Security Engineer, MITRE* (CWE-CAPEC Program Rep)

This sub-working group will engage stakeholders in boosting CWE content for ICS/OT, including expanding content when applicable by adding new entries or enhancing existing entries. The effort will identify gaps in the current ICS/OT CWE view and analyze the scope and nature of those gaps, as well as add appropriate weaknesses to categories without any weaknesses, where supported by CWE's established scope. Additionally, the subgroup will analyze the 20 categories of security vulnerabilities identified by SEI ETF and contribute to public discussions of potential changes to CWE's scope that may benefit the ICS/OT community.

2. "Mapping CWE to ISA/IEC 62443" Sub-Working Group

Launch Date: Tuesday 10/11 from 1:00 to 2:00 pm ET (then meeting biweekly)

- Bryan Owen, *Head of Product Security, Aveva* (co-chair)
- Khalid Ansari, *Senior Engineer of Industrial Control Cybersecurity, FM Approvals* (co-chair)
- Alec Summers, *Principal Cybersecurity Engineer, MITRE* (CWE-CAPEC Program Rep)

The sub-working group will produce a documented association of the CWE list of software and hardware weakness types to the current ISA/IEC 62443 cybersecurity standards in ICS/OT. If there are no restrictions imposed by ISA or other parties, then CWE will capture these associations using "Taxonomy Mappings" elements within the relevant CWE weaknesses. The effort will also contribute to public discussions of potential changes to CWE's scope that may benefit the ICS/OT community.

3. "Communicating ICS/OT Weaknesses" Sub-Working Group

Launch Date: Early 2023

The goal of this sub-working group is to develop a plan of action for making all ICS/OT stakeholders aware of the weaknesses and the impacts they can have on their safety and business operations. This effort will also disseminate the findings and deliverables from the first two subgroups.