CWE-CAPEC ICS/OT Special Interest Group

"Boosting CWE Content" Sub-Working Group Charter

Co-Chairs

Howard Grimes, *Chief Executive Officer, CyManII*
John Kingsley, *Senior Cybersecurity Engineer, Hitachi Energy*

CWE-CAPEC Program Rep

Steve Christey Coley, *Principal Information Security Engineer, MITRE Corporation*

Introduction

The CWE-CAPEC Industrial Control Systems (ICS)/Operational Technology (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. The objective of the CWE-CAPEC ICS/OT SIG is to establish a stakeholder community for discussing ICS/OT-related content in CWE/CAPEC and explore further cross-organizational collaboration opportunities. Members of the ICS/OT SIG work with each other through open and collaborative discussions to provide critical input regarding domain coverage, coverage goals, and content hierarchical structure.

Purpose

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. The effort will also add appropriate weaknesses to categories without any weaknesses, where supported by CWE's established scope. The group will also contribute to public discussions of potential changes to CWE's scope that may benefit the ICS/OT community. Boosting may include the identification of sub-domains of weaknesses.

Work Plan

1. Define the problem space and identify the stakeholders that need to be involved
2. Reach consensus on how to move the state of the practice forward
3. Establish project plan including key tasks, subtasks, and milestones
    a. Expand participants with outreach to manufacturers

b. Review of SEI ETF 20 Categories of Security Vulnerabilities in ICS/OT and conduct a deeper analysis than MITRE had done. ICS/OT experts will provide input and insights into whether these are appropriate mappings.
c. Nominate existing CVEs for ICS/OT issues that CWE does not have coverage for.
d. Examine common architectural weaknesses in ICS/OT/SCADA (including connections to Cyber-Informed Engineering).
e. Examine OT:ICEFALL vulnerabilities and determine if CWEs exist but may not be findable/understandable for ICS/OT. This activity may involve additional content in CWEs and/or explicitly labeling for ICS/OT.
f. Wrestle with scope questions. It may be important or useful to expand CWE's scope to include additional types of weaknesses. Previous tasks may produce certain proposals for the expansion of CWE's scope. For important findings outside of CWE's scope, explore how to represent them in ways that make them more accessible to ICS manufacturers and practitioners.

4. Execute on the project schedule, reporting out progress to the ICS/OT SIG at key milestones
5. Review final deliverables and identify additional channels of dissemination