CWE-CAPEC ICS/OT Special Interest Group

Wednesday, November 30, 2022

THIS MEETING IS BEING RECORDED

ICS/OT Special Interest Group Participants

1. **Aagam Shah**
2. **Aamir Khan,** Tata Power
3. **Abdelrahman Elsanose**
4. **Adam Hahn**
5. **Adrian Crespo-Ortiz,** Capgemni
6. **Ahmad Sharafi,**
7. **Albert Vartic,** OMV Petrom
8. **Alex Rodriguez**, PG&E
9. **Alfinie Bullock,**
10. **Amanda Kraus**
11. **Andres Fuentes-Fernandez,** Inetum
12. **Andrew Kling**, Schneider Electric
13. **Andy Kling,** Schneider Electric
14. **Anjel Jimenez**
15. **Anton Shipulin**
16. **Armada Sramek**
17. **Ashley McGlone,** Tanium
18. **Aw Landgraaf,**
19. **Ayman Alissa**, Mckinsey
20. **Barry Greene**, Senki
21. **Bayard Johnson**
22. **Bill Newhouse**
23. **Brandon Carter**,
24. **Ben Deering,** ODNI
25. **Ben Sooter**, EPRI
26. **Beverly Novak**, INL
27. **Bill Aubin,** Nozomi Networks
28. **Bill Kintz**, Invictus
29. **Bill Newhouse**
30. **Bob Hanson,** LLNL
31. **Bob Heinemann**,
32. **Bob Radvanovsky**
33. **Bradley Nickens**, GE
34. **Bryan Beckman,** INL
35. **Bryan Owen**, Aveva
36. **Cameron Burden,**
37. **Carl Mccants,** ODNI

ICS/OT Special Interest Group Participants

38. **Carmen Zapata**, DHS
39. **Chris Charpentier**, GE
40. **Christopher Havey,** Applied Cybersecurity Engineering
41. **Christopher Sundberg**, Woodward
42. **Chris Humphrey,** Boeing
43. **Chris Levendis**,
44. **CJ Harvey,**
45. **Cody Kieltyka**,
46. **Craig Barrett,** Kinder Morgan
47. **Curtis Taylor**, CyManII
48. **Curt Wiggins**
49. **Cynthia Hsu,** DOE
50. **Dana Thomas**
51. **Dan Bennett,** NREL
52. **Dan Ehrenreich,** SCCE
53. **Danielle Jablanski**,
54. **Daniel Santos**, Forescout
55. **Daniel Stachan**
56. **Daryl Haegley**
57. **Dave Halla**
58. **Dave Keppler**
59. **David Hernandez**
60. **David Nicol**, UIUC & CyManII
61. **David Simpson**
62. **Deborah Kobza,** IACI
63. **Derek Hart**
64. **Dimple Shah**
65. **Dylan Sundy**
66. **Ed Hicks**
67. **Edward Liebig**
68. **Eric Cosman**
69. **Eric Mitchell,** NSA
70. **Eric Strief,** John Deere
71. **Erik Hrin**
72. **Espen Endal,** KraftCERT
73. **Evgeni Sabev**
74. **Gabriela Ciocarlie,** CyManII (new)
75. **Gananand G Kini**
76. **Greg Ahira,** GE
77. **Greg Bastien**

ICS/OT Special Interest Group Participants

78. **Greg Sanchez**
79. **Gus Serino**
80. **Hadeli Hadeli,** Hitachi Energy
81. **Haritha Srinivasan,** FM Global
82. **Harry Perper,** Cyber Architecture and Resiliency
83. **Howard Grimes,** CyManII
84. **Iain Deason,** DHS CISA
85. **Ismael Garcia,** NRC
86. **Jace Powell,** Fortress
87. **Jarvis Robinson**
88. **Jason Li,** TrustedST
89. **Jason Plant**
90. **Jason Robbins,** AT&T
91. **Jay Gazlay,** DHS CISA
92. **Jen Walker,** Water ISAC
93. **Jennifer Pedersen**
94. **Jeremy Mckeown**
95. **Jesper Johansson,** Nouryon
96. **Jess Smith,** PNNL
97. **Jodi Jensen**
98. **Joe Agres,** West Yost
99. **Joe McCormick**
100. **Joe Weiss**
101. **John Almlof**
102. **John Kingsley**
103. **John Repici**
104. **John Schneider**
105. **John Parmley,** Zuuliot
106. **John Ransom**
107. **Jon Terrell,** Hitachi Energy
108. **Jon White,** NREL
109. **Jonti Talukdar,** Duke
110. **Jordon Sims**
111. **Jose Jimenez,** Sothis
112. **Jose Perez,** Tenable
113. **Joseph Cummings,** NYPA
114. **Joseph Januszewski,** E-Isac
115. **Joseph Matthews**

ICS/OT Special Interest Group Participants

117. **Jude Desti,** Boeing
118. **Junya Fujita**,
119. **Justin Cain**
120. **Karen Wetzel**
121. **Ken Wang,** DOD
122. **Ken Cole**, Entergy
123. **Kerry Stuver,** GE
124. **Khalid Ansari,** FM Approvals
125. **Kimberly Denbow,**
126. **Krystel Castillo**
127. **Kumar**
128. **Kyle Hussey**
129. **Kyle Johnson,** GSOC
130. **Lee Szilagyi**, MITRE (new)
131. **Lindsey Cerkovnik,** DHS CISA
132. **Manoj Balachandran**
133. **Marc Sachs,** Auburn University
134. **Marco Ayala**
135. **Mark Sullivan,** NSA
136. **Martijn Jansen,** Taqa
137. **Martin Kihiko**
138. **Martin Ring,** Bosch
139. **Martin Scheu,** Switch
140. **Marty Edwards**
141. **Matt Bishop,** UC Davis & CyManII
142. **Matt Sexton,** Hexagon
143. **Marie Stanley Collins**
144. **Matthew Bohne**
145. **Matthew Knoll,** ArcelorMittal
146. **Max Wandera,** Eaton
147. **Megan Samford**
148. **Melissa Vice,** Air Force
149. **Michael Chaney,** CyManII
150. **Michael Hok,** Hitachi Energy
151. **Michael Toecker**
152. **Michalis Pavlidis,** University of Brighton
153. **Mike Cohen** (new)
154. **Mina Todorova**
155. **Monika Akbar,** UTEP & CyManII
156. **Muhammed Shaban**
157. **Nik Urlaub,** MITRE

ICS/OT Special Interest Group Participants

158. **Niyu Ogunniyi,** Corteva
159. **Oystein Brekk-Saunderud,** Norma Cyber
160. **Patrick Dale**
161. **Patrick Obruba**
162. **Patti Escatel,** DHS CISA
163. **Paul Martyak,** EPRI
164. **Paul Peix,** Headmind
165. **Paul Zawada**
166. **Pete Tseronis**
167. **Peter Colombo**
168. **Peter Jackson,** SGS
169. **Peter Pongracz,** MOL
170. **Philip Huff, UALR**
171. **Pierre Janse van Rensburg,** BBA
172. **Piotr Pedziwiatr,** Arcelor Mittal
173. **Ralph Ley**
174. **Raymond Savarda**
175. **Renan**
176. **Rex Wempen,** DOE
177. **Rezaur Rahman**
178. **Rich Piazza,** MITRE
179. **Richard Robinson,** Cynalytica
180. **Rita Ann Foster**
181. **Robert Garry,** GE Gas Power
182. **Robert Heinemann**, MITRE
183. **Robert Murphy**
184. **Roger Johnson,** Novelis
185. **Ronald Atwater**
186. **Ryan Bays,** PNNL
187. **Ryan Gagliastre,** HF Sinclair
188. **Sabri Khemissa**
189. **Sachin Shah,** Armis
190. **Saleh Almaghrabi**
191. **Salman Salman,** Aerospace Corporation
192. **Sam Thom**
193. **Samuel Chanoski,** INL

ICS/OT Special Interest Group Participants

194. **Sandeep Shukla,** Virginia Tech
195. **Sarah Fluchs,** Admeritia
196. **Shane Stailey**
197. **Shannon Hughes**
198. **Shadya Maldonado,** Sandia
199. **Sharin Crane,** Boeing
200. **Sharla Artz**
201. **Sherry Hunyadi**
202. **Steve Battista**
203. **Steve Chapin**
204. **Steve Granda,** NREL
205. **Stephanie Saravia**
206. **Stephen Trachian,** Hitachi Energy
207. **Susan Farrell**, ObjectSecurity
208. **Ted Wittmer**
209. **Thomas Ruoff,** DHS CISA
210. **Timothy Isaacs,** NuScale Power
211. **Todd Riley, Goodyear**
212. **Tom McGoogan**
213. **Tony Turner,** Fortress
214. **Tonya Riley,** Cyberscoop
215. **Tracy Briggs,** CyManII
216. **Travis Ashley,** PNNL
217. **Vivek Ponnada**
218. **Wayne Austad,** CyManII
219. **Wayne Cantrell**
220. **William Kintz** (Added)
221. **William Welch**
222. **Yasoda Ramchune,** Chevron
223. **Zachary Rogan,** Xage

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

ICS/OT Special Interest Group Leadership and Support

1. **Aeriel Lane,** Nexight Group
2. **Alec Summers,** MITRE
3. **Andrew Kresses,** Nexight Group
4. **Cheri Caddy,** DOE-CESER
5. **Daisyareli Martin,** Nexight Group
6. **Greg Kerr,** Nexight Group
7. **Greg Shannon,** CyManII
8. **Ginger Wright,** INL
9. **Jeff Hahn,** INL
10. **Jeff Mitchell,** INL
11. **Jennifer Ekperigin,** Nexight Group
12. **Katie Baker,** Nexight Group
13. **Karsten Daponte,** Nexight Group
14. **Lindsay Kishter,** Nexight Group
15. **Stephen Bolotin,** Nexight Group
16. **Steve Christey,** MITRE

Agenda

Eastern Time	Activity
3:00 – 3:05 pm	**Login and Roll Call**
3:05 – 3:10 pm	**Opening Remarks** • Review meeting objectives • Review material covered in last meeting
3:10 – 3:15 pm	**Updated Definition of a Weakness from MITRE**
3:15 – 3:35 pm	**CWE and CAPEC Updates Related to ICS/OT Weaknesses** • CWE 4.9 updates from Oct 2022 • CAPEC 3.8 updates from Sep 2022 • Scope exclusions
3:35 – 4:25 pm	**Progress Updates from SIG Sub-Working Groups** • “Boosting CWE Content” subgroup update by co-chairs Howard Grimes and John Kingsley • “Mapping CWE to 62443” subgroup update by co-chairs Khalid Ansari and Bryan Owen • Solicit additional volunteers • Open Q&A
4:25 – 4:30 pm	**Wrap-Up** • Closing remarks • Major milestones • Next SIG meeting – Wed 1/25 @ 3pm ET • Action Items
4:30 pm	**Meeting Ends**

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Opening Remarks

Opening Remarks

Meeting Objectives

1. Review updated definition of a weakness
2. Review CWE 4.9 and CAPEC 3.8 updates
3. Share progress updates from SIG sub-working groups

Review of Last Meeting 8/31

- Previewed upcoming CWE/CAPEC releases for Fall 2022
- Gathered volunteers for the launch of our first two sub-working groups
    1. “Boosting CWE Content”
    2. “Mapping CWE to 62443”
- Deferred launch of third working group on “Awareness and Education” to 2023
- Requested support for outreach to additional volunteers

Updated Definition of a Weakness from MITRE

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Modernizing Definitions on CWE/CAPEC Sites

Term	Definition	Authority	Authorities Doc
Vulnerability	A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components	CVE	website
Weakness	A condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities	n/a	edited from previous definition on CWE website
Attack Pattern	The common approach and attributes related to the exploitation of a weakness in a software, firmware, hardware, or service component.	n/a	edited from previous definition on CAPEC website

CWE and CAPEC Updates Related to ICS/OT Weaknesses

Background: Identify New Classes of Security Vulnerabilities (NCSV) Technical Project Team (TPT)

KEY DELIVERABLE:

Categories of Security Vulnerabilities in ICS

- Identified **20 Categories of Security Vulnerabilities** that are distinct from those already documented in information technology (IT), go beyond vulnerabilities arising from the implementation of ICS systems, and include those arising from design, architectural, operational, and human factors.
- Now exploring the inclusion of these categories in the Common Weakness Enumeration (CWE) database from the MITRE Corporation.

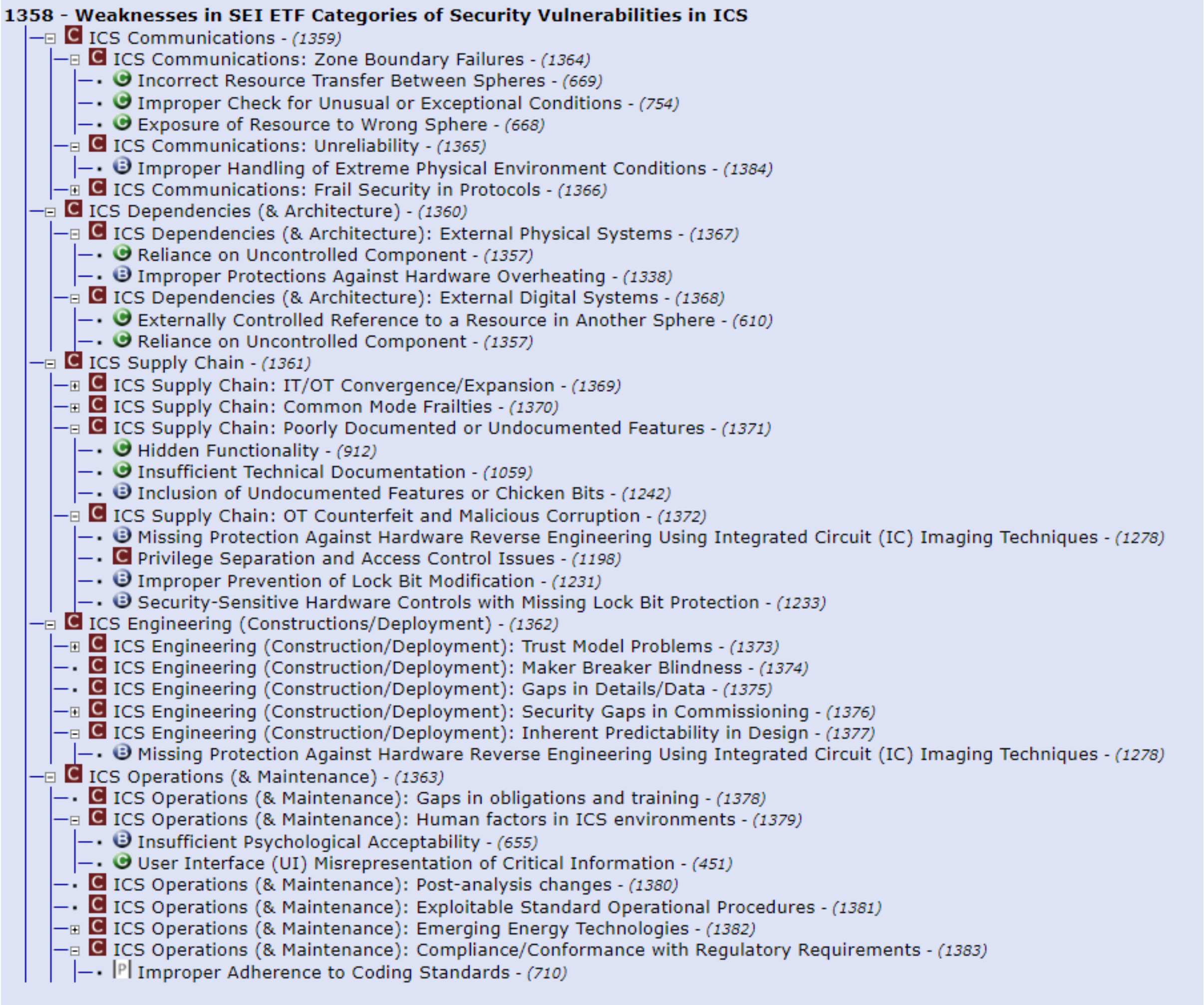
Examples

1. ICS Communications
   - **Unreliability:** Vulnerabilities arise in reaction to disruptions in the physical layer (e.g., creating electrical noise) used to carry the traffic.
2. ICS Dependencies (& Architecture)
   - **External Physical Systems:** Due to the highly interconnected technologies in use, an external dependency on another physical system could cause an availability interruption for the protected system.
3. ICS Supply Chain
   - **Common Mode Frailties:** At the component level, most ICS systems are assembled from common parts made by other companies. One or more of these common parts might contain a vulnerability that could result in a wide-spread incident.
4. ICS Engineering (Constructions/Deployment)
   - **Maker Breaker Blindness:** Lack of awareness of deliberate attack techniques by people (vs. failure modes from natural causes like weather or metal fatigue) may lead to insufficient security controls being built into ICS systems.
5. ICS Operations (& Maintenance)
   - **Post-Analysis Changes:** Changes made to a previously analyzed and approved ICS environment can introduce new security vulnerabilities (as opposed to safety).

CWE 4.7 (Apr 2022) - Published SEI ETF view

- **New view: CWE-1358: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS**
  - https://cwe.mitre.org/data/definitions/1358.html
  - 3-level hierarchy (“super-categories”, categories, weaknesses)
  - Currently includes all TPT-recommended mappings and MITRE’s recommended mappings
  - Many “scoping” challenges, e.g., human processes or practices
- **Signalled new expansion / coverage of ICS/OT**
  - Possible overlap with hardware CWE, Top 20 Secure PLC Coding Practices

ICS/OT View – Sample Visualization



1358 - Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS

- C ICS Communications - *(1359)*
  - C ICS Communications: Zone Boundary Failures - *(1364)*
    - C Incorrect Resource Transfer Between Spheres - *(669)*
    - C Improper Check for Unusual or Exceptional Conditions - *(754)*
    - C Exposure of Resource to Wrong Sphere - *(668)*
  - C ICS Communications: Unreliability - *(1365)*
    - B Improper Handling of Extreme Physical Environment Conditions - *(1384)*
  - C ICS Communications: Frail Security in Protocols - *(1366)*
- C ICS Dependencies (& Architecture) - *(1360)*
  - C ICS Dependencies (& Architecture): External Physical Systems - *(1367)*
    - C Reliance on Uncontrolled Component - *(1357)*
    - B Improper Protections Against Hardware Overheating - *(1338)*
  - C ICS Dependencies (& Architecture): External Digital Systems - *(1368)*
    - C Externally Controlled Reference to a Resource in Another Sphere - *(610)*
    - C Reliance on Uncontrolled Component - *(1357)*
- C ICS Supply Chain - *(1361)*
  - C ICS Supply Chain: IT/OT Convergence/Expansion - *(1369)*
  - C ICS Supply Chain: Common Mode Frailties - *(1370)*
  - C ICS Supply Chain: Poorly Documented or Undocumented Features - *(1371)*
    - C Hidden Functionality - *(912)*
    - C Insufficient Technical Documentation - *(1059)*
    - B Inclusion of Undocumented Features or Chicken Bits - *(1242)*
  - C ICS Supply Chain: OT Counterfeit and Malicious Corruption - *(1372)*
    - B Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques - *(1278)*
    - C Privilege Separation and Access Control Issues - *(1198)*
    - B Improper Prevention of Lock Bit Modification - *(1231)*
    - B Security-Sensitive Hardware Controls with Missing Lock Bit Protection - *(1233)*
- C ICS Engineering (Constructions/Deployment) - *(1362)*
  - C ICS Engineering (Construction/Deployment): Trust Model Problems - *(1373)*
  - C ICS Engineering (Construction/Deployment): Maker Breaker Blindness - *(1374)*
  - C ICS Engineering (Construction/Deployment): Gaps in Details/Data - *(1375)*
  - C ICS Engineering (Construction/Deployment): Security Gaps in Commissioning - *(1376)*
  - C ICS Engineering (Construction/Deployment): Inherent Predictability in Design - *(1377)*
    - B Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques - *(1278)*
- C ICS Operations (& Maintenance) - *(1363)*
  - C ICS Operations (& Maintenance): Gaps in obligations and training - *(1378)*
  - C ICS Operations (& Maintenance): Human factors in ICS environments - *(1379)*
    - B Insufficient Psychological Acceptability - *(655)*
    - C User Interface (UI) Misrepresentation of Critical Information - *(451)*
  - C ICS Operations (& Maintenance): Post-analysis changes - *(1380)*
  - C ICS Operations (& Maintenance): Exploitable Standard Operational Procedures - *(1381)*
  - C ICS Operations (& Maintenance): Emerging Energy Technologies - *(1382)*
  - C ICS Operations (& Maintenance): Compliance/Conformance with Regulatory Requirements - *(1383)*
    - P Improper Adherence to Coding Standards - *(710)*

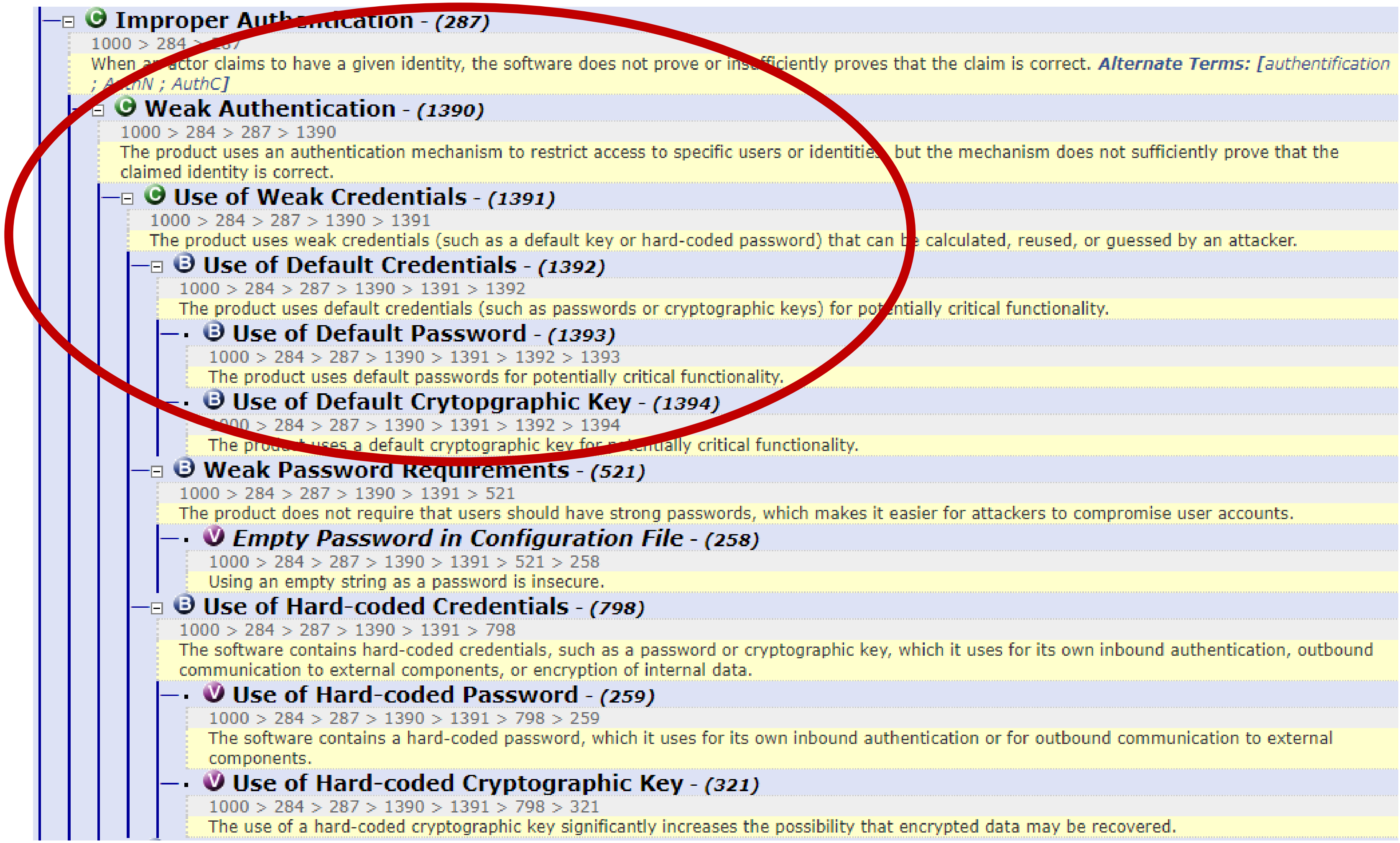
- This screenshot is partially expanded
- Red “C” icon = CWE Category
- Green “C” / Blue “B” icons – Class/Base level weaknesses
- Categories without member weaknesses have a dot to the left of their icon
- Go to individual web page for CWE-1358
- Click “Expand All”

https://cwe.mitre.org/data/definitions/1358.html

CWE 4.7 – Other Highlights Related to ICS/OT

- **Some content changes influenced by SEI ETF Categories document**
- **(New) CWE-1384: Improper Handling of Extreme Physical Environment Conditions**
  - NCSV 11. Maker Breaker Blindness
  - NCSV 16. Human factors in ICS environments
  - Parent of some existing CWEs
- **(Modified) CWE-1059: Insufficient Technical Documentation**
  - NCSV 8. Poorly documented or Undocumented features
  - Includes "gold standard"
  - Parent of some existing CWEs
- **(New) CWE-1357: Reliance on Uncontrolled Component**
  - NCSV 7. Common mode frailties
  - Parent of some existing CWEs
  - Criticism: "every product has uncontrolled components"

CWE 4.9 (Oct 2022) Access Control Enhancements – Weak Authentication



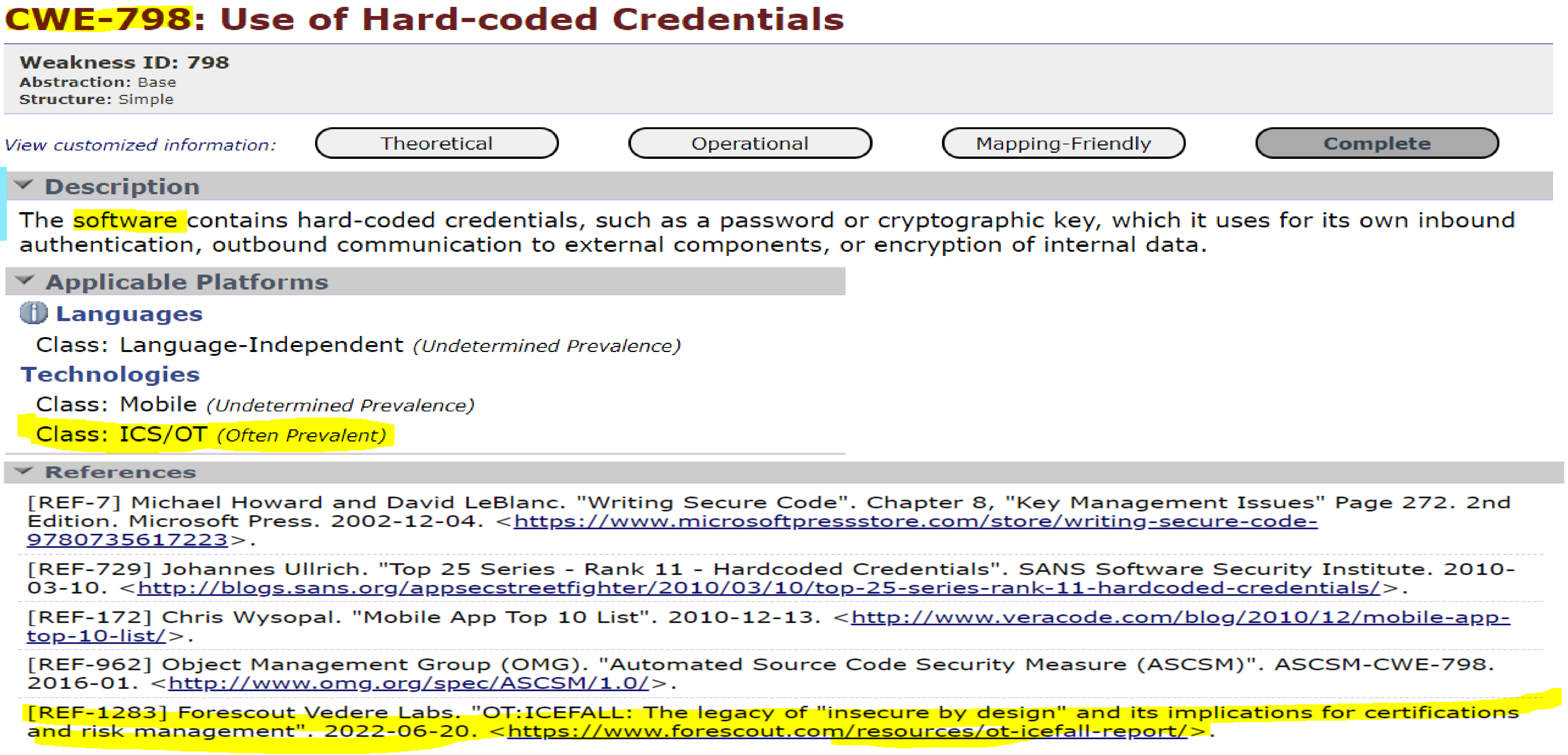
- Improper Authentication - *(287)*
  1000 > 284 > 287
  When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. ***Alternate Terms:*** *[authentification ; AuthN ; AuthC]*
  - Weak Authentication - *(1390)*
    1000 > 284 > 287 > 1390
    The product uses an authentication mechanism to restrict access to specific users or identities, but the mechanism does not sufficiently prove that the claimed identity is correct.
    - Use of Weak Credentials - *(1391)*
      1000 > 284 > 287 > 1390 > 1391
      The product uses weak credentials (such as a default key or hard-coded password) that can be calculated, reused, or guessed by an attacker.
      - Use of Default Credentials - *(1392)*
        1000 > 284 > 287 > 1390 > 1391 > 1392
        The product uses default credentials (such as passwords or cryptographic keys) for potentially critical functionality.
        - Use of Default Password - *(1393)*
          1000 > 284 > 287 > 1390 > 1391 > 1392 > 1393
          The product uses default passwords for potentially critical functionality.
        - Use of Default Crytopgraphic Key - *(1394)*
          1000 > 284 > 287 > 1390 > 1391 > 1392 > 1394
          The product uses a default cryptographic key for potentially critical functionality.
      - Weak Password Requirements - *(521)*
        1000 > 284 > 287 > 1390 > 1391 > 521
        The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.
        - *Empty Password in Configuration File* - *(258)*
          1000 > 284 > 287 > 1390 > 1391 > 521 > 258
          Using an empty string as a password is insecure.
      - Use of Hard-coded Credentials - *(798)*
        1000 > 284 > 287 > 1390 > 1391 > 798
        The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.
        - Use of Hard-coded Password - *(259)*
          1000 > 284 > 287 > 1390 > 1391 > 798 > 259
          The software contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.
        - Use of Hard-coded Cryptographic Key - *(321)*
          1000 > 284 > 287 > 1390 > 1391 > 798 > 321
          The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered.

- “Improper” -> “Missing” or “Incorrect” (Weak)
- “Incorrect AuthN” could only use more-general CWE-287
- Others like authZ have had this distinction for a long time
- Use of Weak Credentials (CWE-1391) is a key breakdown from other authN issues
- Entries are incomplete (to address in 4.10)
- “software” -> “product”

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

CWE 4.9 Example ICS/OT Change – CWE-798: Hard-Coded Credentials

change →



CWE-798: Use of Hard-coded Credentials

Weakness ID: 798
Abstraction: Base
Structure: Simple

View customized information:

Description

The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.

Applicable Platforms

Languages

Class: Language-Independent *(Undetermined Prevalence)*

Technologies

Class: Mobile *(Undetermined Prevalence)*

Class: ICS/OT *(Often Prevalent)*

References

[REF-7] Michael Howard and David LeBlanc. "Writing Secure Code". Chapter 8, "Key Management Issues" Page 272. 2nd Edition. Microsoft Press. 2002-12-04. <https://www.microsoftpressstore.com/store/writing-secure-code-9780735617223>.

[REF-729] Johannes Ullrich. "Top 25 Series - Rank 11 - Hardcoded Credentials". SANS Software Security Institute. 2010-03-10. <http://blogs.sans.org/appsecstreetfighter/2010/03/10/top-25-series-rank-11-hardcoded-credentials/>.

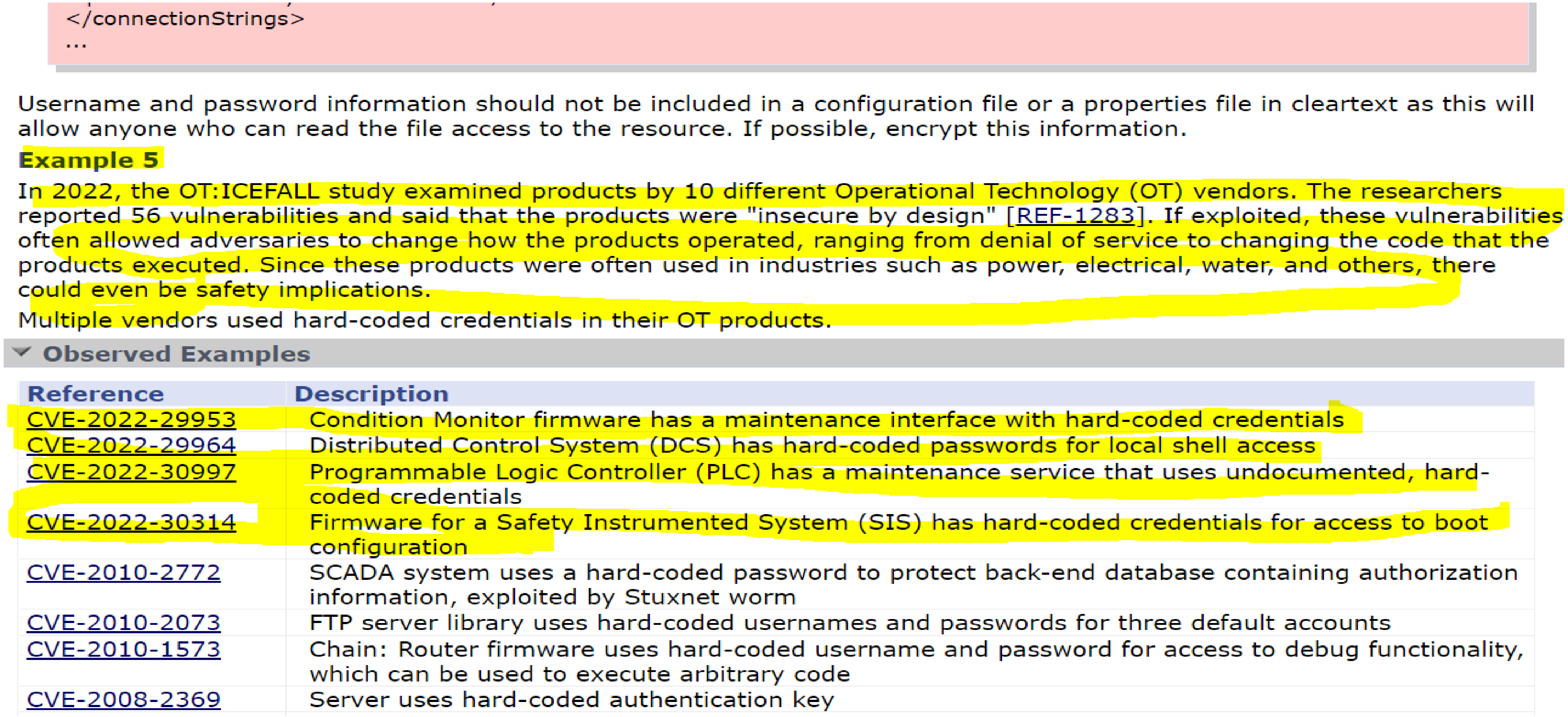
[REF-172] Chris Wysopal. "Mobile App Top 10 List". 2010-12-13. <http://www.veracode.com/blog/2010/12/mobile-app-top-10-list/>.

[REF-962] Object Management Group (OMG). "Automated Source Code Security Measure (ASCSM)". ASCSM-CWE-798. 2016-01. <http://www.omg.org/spec/ASCSM/1.0/>.

[REF-1283] Forescout Vedere Labs. "OT:ICEFALL: The legacy of "insecure by design" and its implications for certifications and risk management". 2022-06-20. <https://www.forescout.com/resources/ot-icefall-report/>.

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

CWE 4.9 Example ICS/OT Change (2) – CWE-798: Hard-Coded Credentials



```
</connectionStrings>
...
```

Username and password information should not be included in a configuration file or a properties file in cleartext as this will allow anyone who can read the file access to the resource. If possible, encrypt this information.

Example 5

In 2022, the OT:ICEFALL study examined products by 10 different Operational Technology (OT) vendors. The researchers reported 56 vulnerabilities and said that the products were "insecure by design" [REF-1283]. If exploited, these vulnerabilities often allowed adversaries to change how the products operated, ranging from denial of service to changing the code that the products executed. Since these products were often used in industries such as power, electrical, water, and others, there could even be safety implications.

Multiple vendors used hard-coded credentials in their OT products.

Observed Examples

Reference	Description
CVE-2022-29953	Condition Monitor firmware has a maintenance interface with hard-coded credentials
CVE-2022-29964	Distributed Control System (DCS) has hard-coded passwords for local shell access
CVE-2022-30997	Programmable Logic Controller (PLC) has a maintenance service that uses undocumented, hard-coded credentials
CVE-2022-30314	Firmware for a Safety Instrumented System (SIS) has hard-coded credentials for access to boot configuration
CVE-2010-2772	SCADA system uses a hard-coded password to protect back-end database containing authorization information, exploited by Stuxnet worm
CVE-2010-2073	FTP server library uses hard-coded usernames and passwords for three default accounts
CVE-2010-1573	Chain: Router firmware uses hard-coded username and password for access to debug functionality, which can be used to execute arbitrary code
CVE-2008-2369	Server uses hard-coded authentication key

CAPEC v3.8

- **Created the new view of Supply Chain CAPEC entries based on the CISA supply chain life cycle**
- **New CAPECs for Supply Chain domain**:
  - CAPEC-690: Metadata Spoofing, CAPEC-691: Spoof Open-Source Software Metadata,CAPEC-692: Spoof Version Control System Commit Metadata,CAPEC-693: StarJacking, CAPEC-695: RepoJacking
- **New CAPECs for Hardware domain**:
  - CAPEC-682: Exploitation of firmware or ROM code with un-patchable vulnerabilities
  - CAPEC-696: Load Value Injection
- **Other new CAPECs**:
  - CAPEC-694: System Location Discovery
  - CAPEC-697: DHCP Spoofing
- **Updated CAPEC to ATT&CK mapping**

Expanding CWE-CAPEC Scope to ICS/OT Systems – From Low-Hanging Fruit to Pie in the Sky

- **Some concerns are more easily expressed as attacks (CAPEC) than weaknesses (CWEs)**
- **Many technical weaknesses fit within CWE/CAPEC's current scope**
  - CWE has known gaps related to architecture, systems-of-systems, and operations/configuration
  - Clarifying problems like Access Control can be difficult because of the variety of models and terms in use
  - Unclear when to create new entries for a technology type or function, versus adding ICS-specific details to existing higher-level entries
  - Supply chain has been difficult to integrate into CWE and CAPEC
- **Scope "exclusions" try to clarify issues with submissions (proposed weaknesses)**

Expanding CWE-CAPEC scope to ICS/OT systems (2)

- **CWE does not (yet) have formal definitions for its scope**
- **The formal weakness definition helps but is insufficient**
- **Primary scope: "mistakes/defects in behavior of software or other electronic logic that has been shown - or can be reasonably expected – to contribute to real-world vulnerabilities"**
- **Focus: any measurable or analyzable artifact related to design, architecture, or other phase that (1) enables the introduction or (2) prevents the detection of weaknesses**
- **Scope expansion might require public debate**
  - CWE/CAPEC Board
  - SIGs (HW-SIG, ICS/OT SIG)
  - Other stakeholders (e.g., CWE-Research "power users," sponsor)

Example Exclusion: SCOPE.HUMANPROC (Human/organizational process)

- **Exclude any human or organizational process or policy that is not measurable and does not produce clear artifacts that identify weaknesses (BSIMM, NIST Secure Software Framework cover these)**
  - 13. Security Gaps in Commissioning: *"As a large system is brought online components of the system may remain vulnerable until the entire system is operating and functional and security controls are put in place. This creates a window of opportunity for an adversary during the commissioning process."*
  - 15. Gaps in obligations and training: *"OT ownership and responsibility for identifying and mitigating vulnerabilities are not clearly defined or communicated within an organization, leaving environments unpatched, exploitable, and with a broader attack surface."*

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Example Exclusion: SCOPE.SITUATIONS (Focus on situations in which weaknesses may appear)

- **Exclude conditions or situations in which weaknesses are more likely to appear**
  - 19. Emerging Energy Technologies: *"With the rapid evolution of the energy system accelerated by the emergence of new technologies such as DERs, electric vehicles, advanced communications (5G+), novel and diverse challenges arise for secure and resilient operation of the system."*

- **Draft scope exclusions to be published ASAP (early December 2022?)**
- **ICS/OT SIG will be notified and consulted**

Progress Updates from SIG Sub-Working Groups

“Boosting CWE Content” Subgroup

Boosting CWE Content Group Participants

1. **Howard Grimes**, CyManII (co-chair)
2. **John Kingsley**, Hitachi (co-chair)
3. **Steven Christey Coley**, MITRE
4. **Adrian Crespo-Ortiz**, Capgemini
5. **Alec Summers**, MITRE
6. **Beverly Novak**, INL
7. **Bryan Owen**, Aveva
8. **Chris Coffin**, MITRE
9. **Curtis Taylor**, CyManII
10. **Daniel Ehrenreich**
11. **David Hernandez**, Takeda
12. **Edward Liebig**, Hexagon
13. **Evgeni Sabev**, SAP
14. **Gabreila Ciocarlie**, CyManII
15. **Greg Shannon,** CyManII
16. **Gus Serino**, Dragos
17. **Haritha Srinivasan,** FM Global
18. **Iain Deason**, DHS
19. **Ismael Garcia**, NRC
20. **John Repici, DoD**
20. **Joseph Giampapa**, Arm Institute
21. **Joseph Januszewski**, E-ISAC
22. **Junya Fujita**, Hitachi
23. **Kyle Hussey**, TDI
24. **Marco Ayala**, 1898
25. **Melissa Vice**, Air Force
26. **Michael Chaney**, INL
27. **Monica Akbar**, CyManII
28. **Oystein Brekke-Saunderud**, Norma Cyber
29. **Paul Peix**, HeadMind
30. **Ryan Bays, PNNL**
31. **Sean Gordon** LLNL
32. **Steven Grzesiak**, Lift
33. **Wayne Austad**, CyManII

34. **Aeriel Lane**, Nexight Group
35. **Greg Kerr**, Nexight Group
36. **Katie Baker**, Nexight Group
37. **Stephen Bolotin**, Nexight Group

Work Plan From Subgroup Charter

✓ **1. Define the problem space and identify the stakeholders that need to be involved**

- What is the problem we are trying to solve?
- What is the value proposition for this effort?

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 event appropriate mappings.

c. Examine common architectural weaknesses in ICS/OT/SCADA (including connections to Cyber-Informed Engineering).

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Work Plan From Subgroup Charter

3. **Establish project plan including key tasks, subtasks, and milestones**
   d. 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

   e. 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.

   f. Nominate existing CVEs for ICS/OT issues that CWE does not have coverage for.

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**

Boosting CWE Content Meetings

- **10.12.2002**
  - Reviewed subgroup charter
  - Determined priority to review 20 SEI ETF categories of security vulnerabilities in ICS/OT
  - Decided to group tasking based on 5 super categories
- **10.26.2002**
  - Reviewed questionnaire for feedback regarding
    - Defining problem space
    - Articulating value proposition
  - Formed task groups
- **11.9.2022**
  - Reviewed/edited problem space and value proposition paragraphs
  - Developed plan and criteria to review SEI ETF categories and to identify gaps

Defining Problem Space

Common Weakness Enumeration (CWE) is the currently the best repository of weaknesses, but there are sizable gaps with respect to the ICS/OT space. There are gaps in identifying and categorizing weaknesses and gaps in the current content of recognized weaknesses. Boosting the CWE content is important because CWE provides an ecosystem and a common language for the ICS/OT community to better understand issues they may encounter and to understand whether to accept risk. Understanding and identifying the issues should help prevent or mitigate cyber events, which ultimately can be a matter of national security.

Value Proposition

The group will identify and quantify gaps in the current ICS/OT CWE content and develop a path forward. Boosting CWE content will establish a framework to illustrate risk, will create a unified weakness language within the ICS/OT community, and enable the ICS/OT community to better understand the significance of the CWE system. Ultimately, the group will deliver actionable content to appropriate audiences. This will allow ICS/OT systems to be secured during the design phase, decreasing the chances of cyber events.

Task Group Volunteers

ICS Communications

- Ian Deason
- Kyle Hussey
- Oystein Brekke-Sanderud

ICS Dependencies

- Iain Deason
- John Kingsley
- Kyle Hussey
- Haritha Srinivasan

ICS Supply Chain

- Ismael Garcia
- John Repici
- Melissa Vice
- Joseph Giampapa

ICS Engineering

- Monika Akbar
- Gabreila Ciocarlie
- Curtis Taylor

ICS Operations

- Beverly Novak
- John Kingsley
- Kyle Hussey
- Michael Chaney
- Oystein Brekke-Sanderud
- Ed Liebig
- Haritha Srinivasan

Boosting CWE Content Meetings

- **11.16.2022 – 11.29.2022**
  - Each task group met twice to discuss one category
    - ICS Supply Chain: OT Counterfeit and Malicious Corruption (CWE-1372)
    - ICS Engineering: Trust Model Problems (CWE-1373)
    - ICS Operations: Emerging Energy Technologies (CWE-1382)
    - ICS Dependencies: External Digital Systems (CWE-1368)
    - ICS Communications: Frail Security in Protocols (CWE-1366)
- **11.30.2022**
  - Discussed findings of task groups
  - Determined next steps: continue review of categories

“Mapping CWE to 62443” Subgroup

“Mapping” Subgroup Participants

1. **Bryan Owen**, AVEVA (co-chair)
2. **Khalid Ansari**, FM Approvals (co-chair)
3. **Alec Summers**, MITRE (CWE-CAPEC program rep)
4. **Michael Thompson**, MITRE
5. **Dave Morse**, MITRE
6. **Philip Taggart**, MITRE
7. **Steve Christey Coley**, MITRE
8. **Oystein Brekke-Sanderud**, NORMA Cyber
9. **Paul Peix**, HeadMind Partners
10. **Marco Ayala**, 1898 & Co.
11. **Martin Scheu**, SWITCH
12. **Matt Knoll**, ArcelorMittal
13. **Junya Fujita**, Hitachi Energy
14. **Stephen Trachian**, Hitachi Energy
15. **John Kingsley**, Hitachi Energy
16. **Kyle Hussey**, TDI Technologies
17. **Edward Liebig**, Hexagon
18. **Sam Chanoski**, INL
19. **Beverly Novak**, INL
20. **Jose Luis Jimenez Izquierdo**, SOTHIS
21. **Jose Miguel Perez Vergara**, SOTHIS
22. **Ruben Aguilar Rives**, SOTHIS
23. **Susan Farrell**, ObjectSecurity
24. **Melissa Vice**, DoD Cyber Crime Center (DC3)
25. **John Repici**, DoD Cyber Crime Center (DC3)
26. **Ismael Garcia**, NRC
27. **Christopher Sundberg**, Woodward, Inc.
28. **Curtis Taylor**, CyManII
29. **Mike Chaney**, CyManII
30. **Greg Shannon**, CyManII
31. **Mina Todorova**, ITARICON GmbH
32. **Adrian Crespo**, Capgemini
33. **Daniel Ehrenreich**, Secure Communications and Control Experts
34. **Richard Robinson**, Cynalytica
35. **Joseph Bessette**, Cynalytica
36. **Sean Gordon**, LLNL
37. **James “Jake” Jones**
38. **Tony Turner,** Fortress
39. **Chris Coffin,** MITRE
40. **Stephen Bolotin**, Nexight Group
41. **KatherineAnne Baker**, Nexight Group
42. **Greg Kerr,** Nexight Group
43. **Aeriel Lane**, Nexight Group

Defining the Problem Space & Value Proposition

- **Defining the Problem Space**
  - There is not a direct relationship between current CWEs associated with OT vulnerabilities and 62443 security requirement (both product and system requirements/enhancements). Further, there is a need to design-out weaknesses in products, but this is hampered by a gap in terminology between CWE and 62443.
- **Articulating the Value Proposition**
  - Help organization in their application of standards by outlining how CWEs can be addressed, especially in terms of improving design quality of products commonly used in critical infrastructure.

Work Plan from Subgroup Charter

- **Tasking & Major Milestones**
  1. Identify failure examples to be referenced in applicable CWEs (and SEI ETF 20 categories of security vulnerabilities with CWE updates)
     - ➢ 1st Month Milestone: Determine top-10 CWEs (most exploited) in ICS/OT ✓
     - ➢ 2nd Month Milestone: Determine top CWEs for subsequent rounds of mapping (potentially 2-4 more)
     - ➢ 3rd Month Milestone: Identify gaps in CWE relevant to ICS/OT for the "Boosting" subgroup to consider
  2. Tier ISA/IEC 62443 requirements (must have, nice to have, if there is time) as candidates to enrich CWE
     - ➢ 1st Month Milestone: Determine top 62443 security requirement **parts** (must haves) ✓
     - ➢ 2nd Month Milestone: Map top-10 CWEs to specific requirements of 62443 (e.g., 62443-4-2 CR 2.1)
     - ➢ 3rd Month Milestone: Map remaining CWEs to 62443, and identify areas where 62443 does not address top weaknesses in ICS/OT
  3. Provide recommendations to CWE to add cross references to ISA/IEC 62443 requirements/guidance based including the example case(s)
- **Accessing ISA/IEC 62443 requirements**
  - – ISA-99 committee has provided the following 62443 sections for this mapping exercise: 1-1, 2-1, 2-2, 2-4, 3-2, 3-3, 4-1, 4-2, TR99
- **Additional Suggested Tasking**
  - – Identifying a comprehensive list of threats beyond threats currently listed in 62443
  - – Consider reaching out to other Standards Development Organizations (e.g., IEEE) based on the outcome of this effort

Criteria for Selecting Top-*N* CWEs

- **What criteria should we consider for selecting the top-10 CWEs?**
  - Relevance to ICS/OT
  - Criticality – result of exploitation
  - Likelihood of exploit
  - Existence and impact to critical infrastructure
    - Applicability across multiple industry verticals (e.g. same controller put in different environments may have different configurations and therefore different weaknesses)
  - Mitigation guidance that differs from IT assets
  - Applicability to lower architecture level OT communications (0-3)
  - Mapped CVE frequency and severity
  - Applicability to most common MITRE ICS ATT&CK techniques or tactics
  - Include at least one hardware example i.e. CWE-1266
  - Included in (or relevant to) SEI ETF 20
- **What characteristics of a CWE would lead us to *NOT* prioritize it for mapping?**
  - Too IT-centric
  - Easily mitigated
  - Already covered in CWE Top 25?

Example Mapping

- **Example Mapping of CWE-862:**
  - CWE-862 is *Missing Authorization* and its description states: “The software does not perform an authorization check when an actor attempts to access a resource or perform an action.”
  - Requirement CR 2.1 of 62443-4-2 states: “Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.”
  - 62443-4-2 CR 2.1 → CWE-862

Small Group Pairings, CWE Assignments & Instructions

1. Beverly Novak, Stephen Trachian, Sandeep Kumar Shukla, Sean Gordon
   - **CWE-287:** ***Improper Authentication***
2. Ismael Garcia, Tony Turner, Junya Fujita, John Kingsley
   - **CWE-321:** ***Use of Hard-coded Cryptographic Keys***
3. Mike Chaney, Mina Todorova, Ruben Aguilar Rives, Martin Scheu
   - **CWE-657:** ***Violation of Secure Design Principles (parent of CWE-636)***
4. Susan Farrell, Edward Liebig, James "Jake" Jones, Jose Miguel Perez Vergara, Daniel Ehrenreich
   - **CWE-798:** ***Use of Hard-coded Credentials***
5. John Repici, Joseph Bessette, Jose Luis Jimenez, Richard Robinson, Monika Akbar
   - **CWE-319:** ***Cleartext Transmission of Sensitive Information***
6. Michael Thompson, Curtis Taylor, Oystein Brekke-Sanderud, Marco Ayala, Paul Peix
   - **CWE-327:** ***Use of a Broken or Risky Cryptographic Algorithm***
7. Sam Chanoski, Matt Knoll, Iain Deason, Kyle Hussey, Christopher Sundberg
   - **CWE-400:** ***Uncontrolled Resource Consumption***

- **Meet in small groups of 4-5**
- **Ensure all participants can access the 62443 sections in Google Spaces**
- **Determine if you are at the right level of abstraction for CWE**
- **Complete your CWE mapping to a section of 62443, as specifically as possible, before next meeting Tue 12/20**

Wrap-Up

Milestones

- **Sub-Working Groups meet bi-weekly**
  - Mapping to 62443 Tuesday 12/20 from 1:00 to 2:00pm ET
  - Boosting CWE Content Wednesday 12/21 from 10:30 to 11:30am ET
- **ICS/OT SIG meets bimonthly going forward**
  - Next meeting Wednesday 1/25 from 3:00 to 4:30pm ET
- **CWE/CAPEC publish content on quarterly basis**
  - Next major update for CWE 4.10 – Jan 2023
  - Next major update for CAPEC 3.9 – Jan 2023

Action Items

1. **Insert Text**

MITRE

MITRE’s mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org