CWE-CAPEC ICS/OT Special Interest Group

Wednesday, August 31, 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

19. **Barry Greene**, Senki
20. **Bayard Johnson**
21. **Bill Newhouse**
22. **Brandon Carter**,
23. **Ben Deering,** ODNI
24. **Ben Sooter**, EPRI
25. **Beverly Novak**, INL
26. **Bill Aubin,** Nozomi Networks
27. **Bill Kintz**, Invictus
28. **Bill Newhouse**
29. **Bob Hanson,** LLNL
30. **Bob Heinemann,**
31. **Bob Radvanovsky**
32. **Bradley Nickens**, GE
33. **Bryan Beckman,** INL
34. **Bryan Owen**, Aveva
35. **Cameron Burden,**
36. **Carl Mccants,** ODNI

ICS/OT Special Interest Group Participants

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

ICS/OT Special Interest Group Participants

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

ICS/OT Special Interest Group Participants

113. **Karen Wetzel**
114. **Ken Wang,** DOD
115. **Ken Cole**, Entergy
116. **Kerry Stuver,** GE
117. **Khalid Ansari**, FM Approvals
118. **Kimberly Denbow,**
119. **Krystel Castillo**
120. **Kumar**
121. **Kyle Hussey**
122. **Kyle Johnson,** GSOC
123. **Lindsey Cerkovnik,** DHS CISA
124. **Marc Sachs,** Auburn University
125. **Mark Sullivan,** NSA
126. **Martijn Jansen,** Taqa
127. **Martin Kihiko**
128. **Martin Ring,** Bosch
129. **Martin Scheu,** Switch
130. **Marty Edwards**
131. **Matt Bishop,** UC Davis & CyManII
132. **Matt Sexton**, Hexagon
133. **Marie Stanley Collins**
134. **Matthew Bohne**

132. **Matthew Knoll,** ArcelorMittal
133. **Max Wandera**, Eaton
134. **Megan Samford**
135. **Melissa Vice,** Air Force
136. **Michael Chaney**, CyManII
137. **Michael Hok,** Hitachi Energy
138. **Michael Toecker**
139. **Michalis Pavlidis,** University of Brighton
140. **Mina Todorova**
141. **Monika Akbar,** UTEP & CyManII
142. **Muhammed Shaban**
143. **Nik Urlaub**
144. **Niyu Ogunniyi,** Corteva
145. **Oystein Brekk-Saunderud,** Norma Cyber
146. **Patrick Dale**
147. **Patrick Obruba**
148. **Patti Escatel,** DHS CISA
149. **Paul Martyak**, EPRI
150. **Paul Peix,** Headmind

ICS/OT Special Interest Group Participants

151. **Paul Zawada**
152. **Pete Tseronis**
153. **Peter Colombo**
154. **Peter Jackson,** SGS
155. **Peter Pongracz** (Added)
156. **Philip Huff, UALR**
157. **Pierre Janse van Rensburg,** BBA
158. **Piotr Pedziwiatr,** Arcelor Mittal
159. **Ralph Ley**
160. **Raymond Savarda**
161. **Renan**
162. **Rex Wempen,** DOE
163. **Rezaur Rahman**
164. **Rich Piazza**
165. **Richard Robinson,** Cynalytica
166. **Rita Ann Foster**
167. **Robert Garry,** GE Gas Power
168. **Robert Heinemann**, MITRE
169. **Robert Murphy**
170. **"Rob"** (Added – Unsure which of the above)
171. **Roger Johnson,** Novelis
172. **Ronald Atwater**
173. **Ryan Bays**, PNNL
171. **Ryan Gagliastre,** HF Sinclair
172. **Sabri Khemissa**
173. **Sachin Shah,** Armis
174. **Saleh Almaghrabi**
175. **Salman Salman,** Aerospace Corporation
176. **Sam Blackfell**
177. **Samuel Chanoski**, INL
178. **Sandeep Shukla,** Virginia Tech
179. **Sarah Fluchs,** Admeritia
180. **Shane Stailey**
181. **Shannon Hughes**
182. **Shadya Maldonado**, Sandia
183. **Sharin Crane,** Boeing
184. **Sharla Artz**
185. **Sherry Hunyadi**

ICS/OT Special Interest Group Participants

186. Steve Battista
187. Steve Chapin
188. Steve Granda, NREL
189. Stephanie Saravia
190. Stephen Trachian, Hitachi Energy
191. Susan Farrell, ObjectSecurity
192. Ted Wittmer
193. Thomas Ruoff, DHS CISA
194. Timothy Isaacs, NuScale Power
195. Todd Riley, Goodyear
196. Tom McGoogan
197. Tony Turner, Fortress
198. Tonya Riley, Cyberscoop
199. Tracy Briggs, CyManII
200. Travis Ashley, PNNL
201. Vivek Ponnada
202. Wayne Austad, CyManII
203. Wayne Cantrell
204. William Kintz (Added)
205. William Welch
206. Yasoda Ramchune, Chevron
207. Zachary Rogan, Xage

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 – 3:30 pm	**CWE Discussion** • Review questionnaire results • How do you and your organization use CWE today? • How would you and your organization like to use CWE in the future?
3:30 – 3:55 pm	**Sub-Working Group Charters** • Discuss charters • Seek volunteers and identify chairs • Plan sub-working launch

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

Agenda

Eastern Time	Activity
3:55 – 4:25 pm	**Enumerate SIG Stakeholders (Org and Representative Types)** • Review questionnaire and breakout session results from prior meetings • Identify any gaps in current set of SIG participants • Plan for additional outreach to fill gaps
4:25 – 4:30pm	**Wrap-Up** • Closing remarks • Next SIG meeting – Wed 9/29 @ 3pm • Action Items
4:30 pm	**Meeting Ends**

Opening Remarks

Opening Remarks

- **Review meeting objectives**
  1. Gather feedback on aspirations for CWE
  2. Identify, structure, and stand-up at least one sub-working group
  3. Enumerate the set of stakeholders that need to be involved in the SIG
- **Review material covered in last meeting**
  - Differentiated CWE, CAPEC, D3FEND, and ATT&CK at MITRE
  - Discussed questionnaire and breakout session results around priority gaps in classifying, communicating, or the scope of ICS/OT weaknesses in CWE
    - Priority gap in classifying: Weaknesses inherent in architectural patterns
      - Emerging tech challenging existing legacy understand of and approach to data
      - OT devices not built for load now expected to carry
    - Priority gap in scope: Standardization of terminology and methods
    - Priority gap in communicating: Involve ICS/OT vendors
  - Reached consensus on preparing charters for each target sub-working group (shared as read-aheads prior to this meeting)

CWE Discussion

How do you and your organization use CWE today?

- **Sample of questionnaire responses *(36 complete, 32 incomplete)***
  - Six respondents indicated their org does not currently use CWE
  - Looking for software quality issues
  - Machine learning in analyzing vulnerabilities
  - Identify what security controls to mitigate vulnerabilities in ICS, OT, and IoT products and services
  - Our product development processes are held to minimum standards which address CWE
  - Threat research; identify common weaknesses; compatible tools
  - Coordinate multi-party vulnerability disclosure
  - For effective communication in cyber vulnerability management and cyber education domains
  - Classify weaknesses in wind turbine SCADA systems
  - Design secure architecture (i.e., Cyber-Informed Engineering)

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

- **Sample of questionnaire responses**
  - Use CWEs to tag vulnerabilities
  - Automate vulnerability mitigation decision making
  - Helpful if CWEs were mapped to 4-2 and 3-3 parts of 62443
  - Baseline for weakness identification, mitigation, and prevention efforts
  - Address all current and emerging technology domains
  - Use CWEs to design new security concepts/solutions
  - ***More quantitative understanding of where the most urgent threats are***

Sub-Working Group Charters

#1 - Boosting CWE Content

VOLUNTEERS	
LEAD	**12.** Bryan Owen
1. Howard Grimes	**13.** Gus Serino
2. John Kingsley	**14.** Beverly Novak
3. Adrian Crespo	**15.** Joseph Januszewski
	16. Ryan Bays
	17. Wayne Austad
PARTICIPATE	**18.** Monika Akbar
1. Evgeni Sabev	
2. Oystein Brekke-Sanderud	
3. Paul Peix	
4. Ian Deason	
5. Marco Ayala	
6. Melissa Vice	
7. Junya Fujita	
8. Kyle Hussey	
9. Edward Liebig	
10. Ismael Garcia	
11. Mike Chaney	

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. Validate first set of mappings from SEI ETF 20 categories to CWE
   b. Identify where new content can be developed from the SEI ETF 20 categories
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

SIG Participant Suggestions

A. Expand participants to include ICS security researchers
B. Explore handling of vulns that are “hidden” in COTS systems for which asset owners may have limited options to respond
C. Examine common architectural weaknesses in ICS/OT/SCADA
D. Streamline collection and normalize distribution of newly found issues
E. CWEs may need to be mapped to potential matches within the VRMN database

#2 – Education and Awareness of CWE and ICS/OT Weaknesses

VOLUNTEERS	
LEAD	**12.** Kyle Hussey
1. Evgeni Sabev	**13.** Edward Liebig
2. Philip Huff	**14.** Ismael Garcia
	15. Sam Chanoski
	16. Mike Chaney
PARTICIPATE	**17.** John Kingsley
1. Howard Grimes	**18.** Ahmad Sharafi
2. Martjn Jansen	**19.** Bryan Beckman
3. Oystein Brekke-Sanderud	**20.** Adrian Crespo
4. Paul Peix	**21.** Khalid Ansari
5. Mina Todorova	**22.** Christopher Sundberg
6. Ian Deason	**23.** Beverly Novak
7. Marco Ayala	**24.** Joseph Januszewski
8. Martin Scheu	**25.** Max Wandera
9. Melissa Vice	**26.**
10. Matt Knoll	**27.**
11. Junya Fujita	

Work Plan

1. Define the problem space
2. Identify the stakeholders that need to be involved and solicit their participation
3. Establish a set of topical areas for which educational materials and training can be created
4. Reach consensus on how to move the state of the practice forward
5. Create a project schedule including key tasks, subtasks, and milestones
6. Execute on the project schedule, reporting out progress to the ICS/OT SIG at key milestones
7. Review final deliverables and identify additional channels of dissemination

SIG Participant Suggestions

A. Should 62443 mapping efforts come as a pre-requisite to this sub-group?

B. Coordinate with CVE Number Authorities (CNAs) to consistently report the new CWE categories

C. Create monthly and on-demand educational offerings

D. Create awareness initiatives highlighting where CWE can “cut the chaff”

E. Create educational blog posts on how to use and integrate CWE into an organization

F. Conduct a needs analysis on what our target audience(s) need from CWE

G. Combine CWE with CSAF

#3 – Mapping CWE to 62443

VOLUNTEERS	
LEAD	**8.** Kyle Hussey
1. Mina Todorova	**9.** Edward Liebig
2. Mike Chaney	**10.** Ismael Garcia
3. Bryan Owen	**11.** Sam Chanoski
4. John Kingsley	**12.** Susan Farrell
5. Adrian Crespo	**13.** Stephen Trachian
6. Khalid Ansari	**14.** Christopher Sundberg
	15. Beverly Novak
	16. Jose Luis Jimenez
PARTICIPATE	**17.** Curtis Taylor
1. Oystein Brekke-Sanderud	**18.**
2. Paul Peix	**19.**
3. Marco Ayala	
4. Martin Scheu	
5. Melissa Vice	
6. Matt Knoll	
7. Junya Fujita	

Work Plan

1. Define the problem space
2. Identify the stakeholders that need to be involved and solicit their participation
3. Reach consensus on how to move the state of the practice forward
4. Establish project schedule including key tasks, subtasks, and milestones
    a. Document a comparison of standards that address each CWE
    b. Compare and document whether each CWE is addressed by existing ISA/IEC 62443
    c. Provide recommendations to ISA/IEC 62443 committees to develop additional standards to address CWE’s that are not currently addressed
5. Reporting out progress to the ICS/OT SIG at key milestones
6. Review final deliverables and identify additional channels of dissemination

SIG Participant Suggestions

A. Mapping should be integrated into the definition of CWE instead of having a separate reference tool.
B. Prepare effective communications for when mapping is complete
C. Create automation options for updating both CWE and ISA 62443 iterations
D. Focus on: Hardware root of trust, Software/firmware updates, Trusted computing base, Purdue model 4Rs (Response time, Resolution, Reliability, Repairability), PKI related weaknesses (TR62443-3-3-1)

Launching Sub-Working Groups

- **Are we ready to launch the first sub-working group in September?**
- **Which sub-working group should start first?**
- **Can all three sub-working groups start at the same time? Or should they be sequenced, say, kicking off one month apart?**

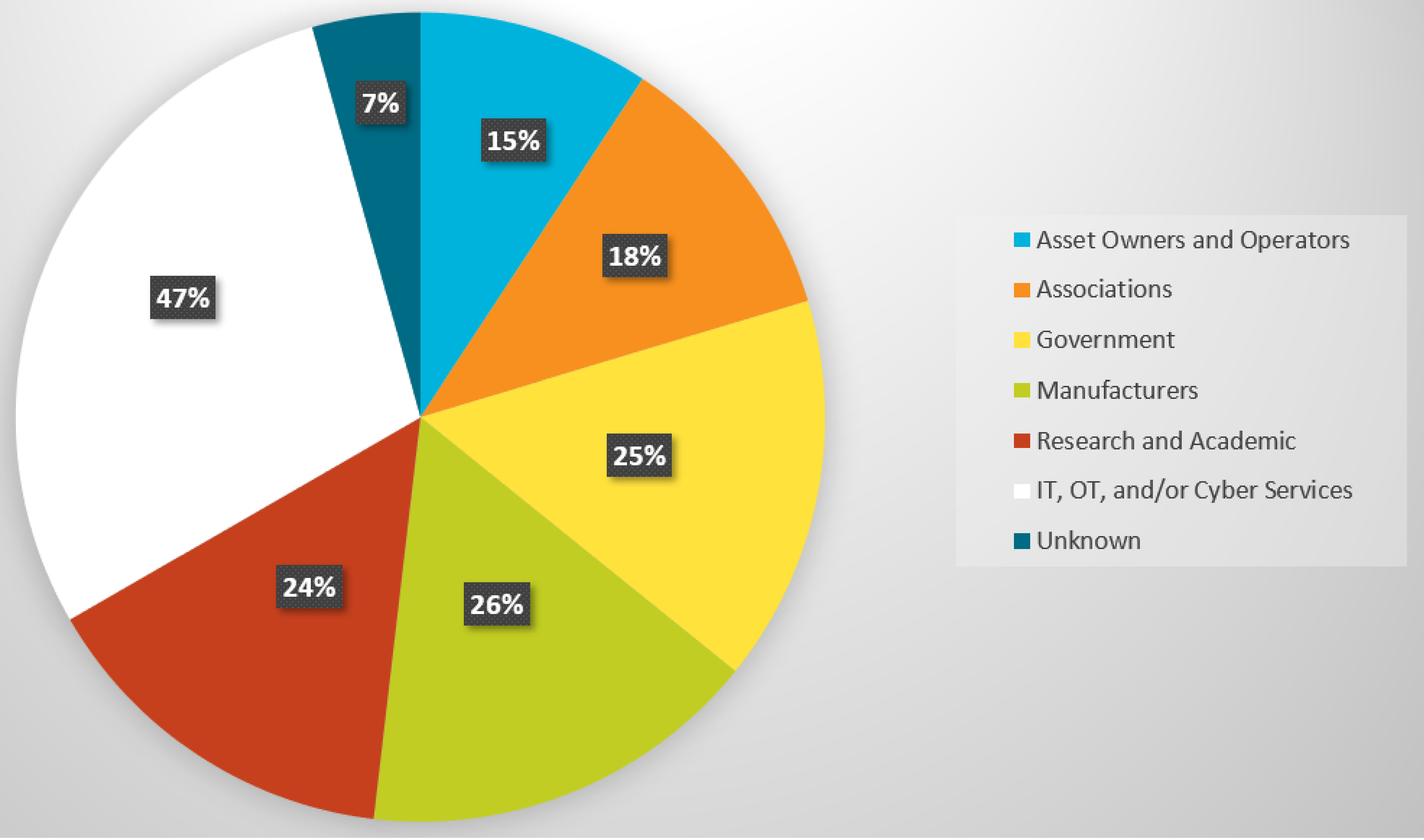
- **Nexight Group** is available to assist sub-working group leads with project planning, meeting facilitation, and technical document writing.

Enumerate SIG Stakeholders

Organization Types

- **Developers and Vendors**
  - Security vendors (involved in ISA 62443, IEC, CISA [ICS-CERT, US-CERT], NIST)
  - Equipment vendors and system integrators
  - Research groups and third-party cybersecurity companies (Dragos, Honeywell, Schneider, Claroty, Bechtel, GE, Nozomi, Schweitzer, Siemens, Xylem, Rockwell, Johnson Controls, CyPhy, Nova, Munio)
- **Manufacturers**
  - Including electrical, ONG, and water
  - Software security tool manufacturers
  - Manufacturers of discrete components
- **Research and Academic Community**
  - Security researchers
  - Academic affiliations (esp. those with a lab that can help process data)
  - Market analyst community
  - Certification labs (non-academic)
- **End Users**
  - Utilities
  - AOOs within each CI sector
- ***Policymakers (local reps, legal and insurance communities, ISAC reps)***
- ***OSS Community***
- ***Other OT SIGs (ISA, CS2AI, etc)***

SIG Participants



Representative Types

- **Engineering**
  - Chief Engineers
  - Integrators
  - Engineers
  - Safety/Protection Engineer
- **OT Staff**
  - Operators
  - Technical managers
  - Plant managers
- **All Levels of Management**
  - General vulnerability/risk management
  - CTOs
- **Support Staff**
  - Consultants - form trust relationships and need configuration
  - Policy/Legal professionals
  - Procurement/Acquisition specialist – to ensure proper terminology
  - Supply chain for manufacturers (such as for chips and software)
  - Lifecycle specialists
  - Auditors/assessors ISSOs ISSMs

- **IT Cybersecurity**
  - Security architects
  - Security engineers tasked with implementation
  - System/software developers
  - CSO
  - Researcher/threat analyst
  - Security analysts/researchers
  - Red team and pen testers
- ***Software quality assurance***
- ***Firmware developers x2***
- ***SBOM/HBOM specialists***
- ***DevSecOps***
- ***Infrastructure security specialists***
- ***Academia***
  - *Researchers*
  - *Professors*
  - *Writers*
  - *Industry Lab people*
  - *Students*

Wrap-Up

Wrap-Up

- **Closing remarks**
- **Next SIG meeting – Wed 9/28 @ 3pm**
- **Action items**

Major Milestones

- **ICS/OT SIG meets monthly**
  - Next meeting Wednesday 9/28 from 3:00 to 4:30pm ET
- **CWE/CAPEC publish content on quarterly basis**
  - Next board meeting [being scheduled soon; 15th, 19th, 20th or 21st], occurring quarterly
  - Next major update for CWE/CAPEC weakness Fall 2022

Action Items

1. **Setup follow-up discussion with sub-working group leads**

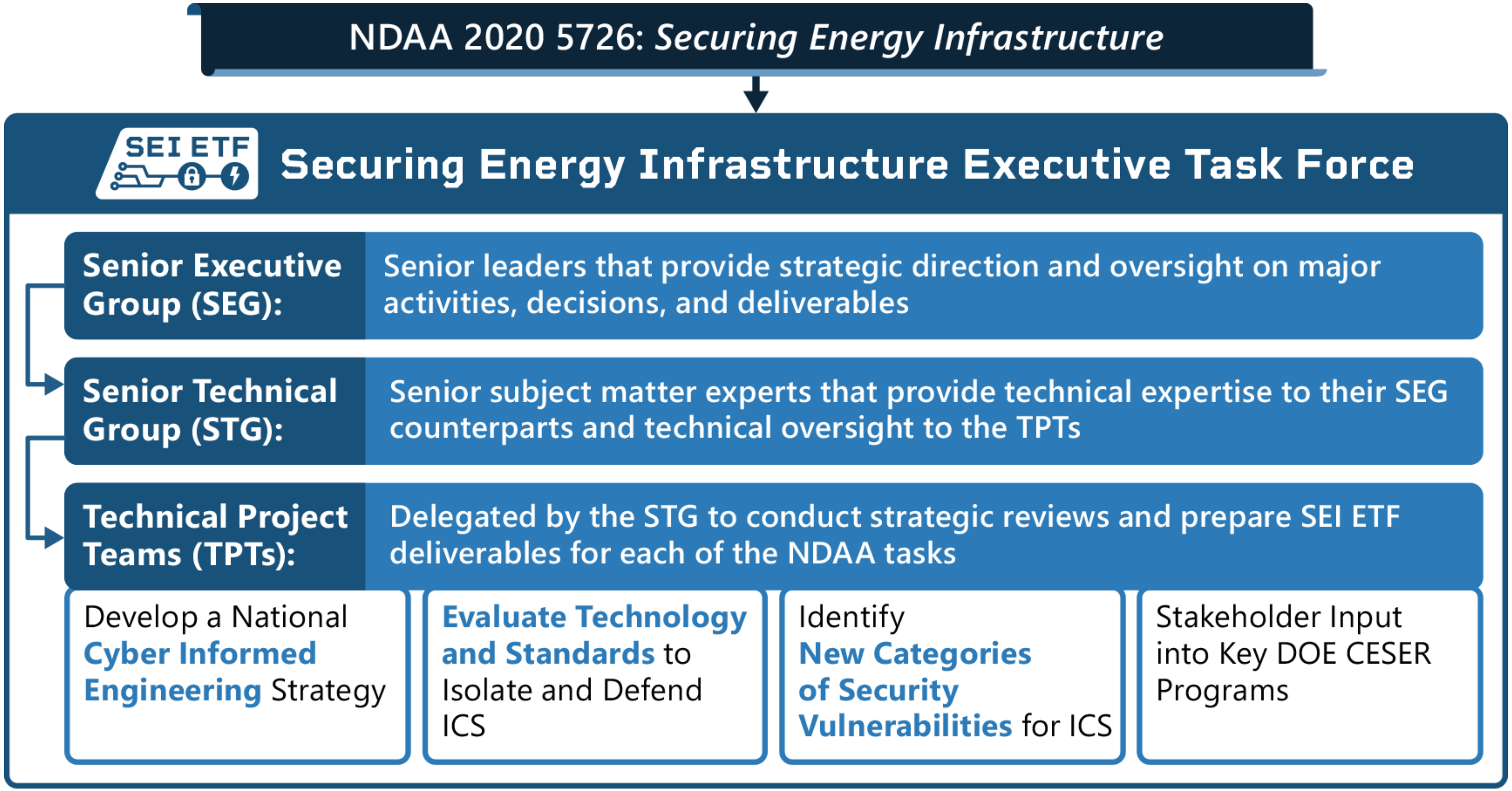
MITRE

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

Additional Program Background

BACKGROUND: Securing Energy Infrastructure Executive Task Force (SEI ETF)



NDAA 2020 5726: *Securing Energy Infrastructure*

SEI ETF

Securing Energy Infrastructure Executive Task Force

Senior Executive Group (SEG): Senior leaders that provide strategic direction and oversight on major activities, decisions, and deliverables

Senior Technical Group (STG): Senior subject matter experts that provide technical expertise to their SEG counterparts and technical oversight to the TPTs

Technical Project Teams (TPTs): Delegated by the STG to conduct strategic reviews and prepare SEI ETF deliverables for each of the NDAA tasks

- Develop a National **Cyber Informed Engineering** Strategy
- **Evaluate Technology and Standards** to Isolate and Defend ICS
- Identify **New Categories of Security Vulnerabilities** for ICS
- Stakeholder Input into Key DOE CESER Programs

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

KEY DELIVERABLE:

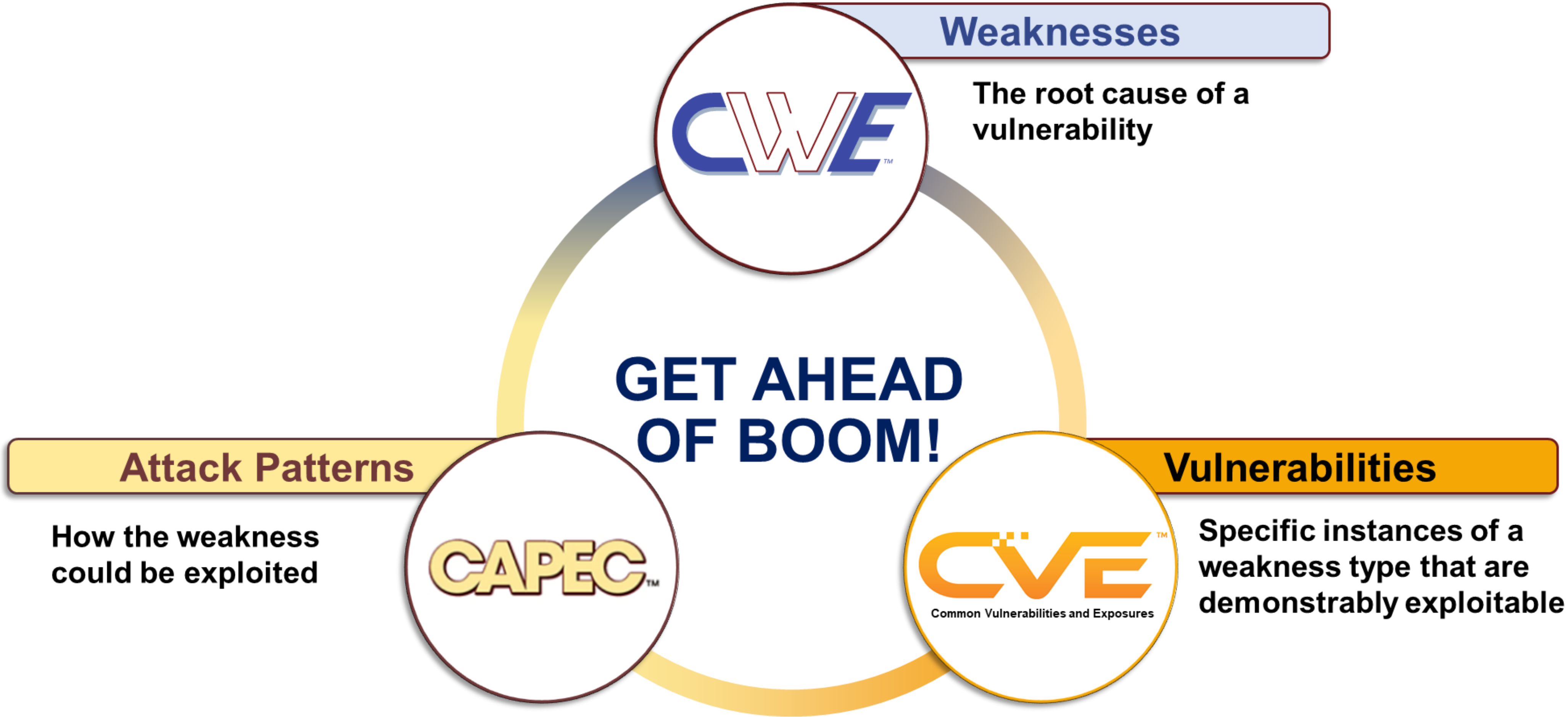
Categories of Security Vulnerabilities in ICS

- 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

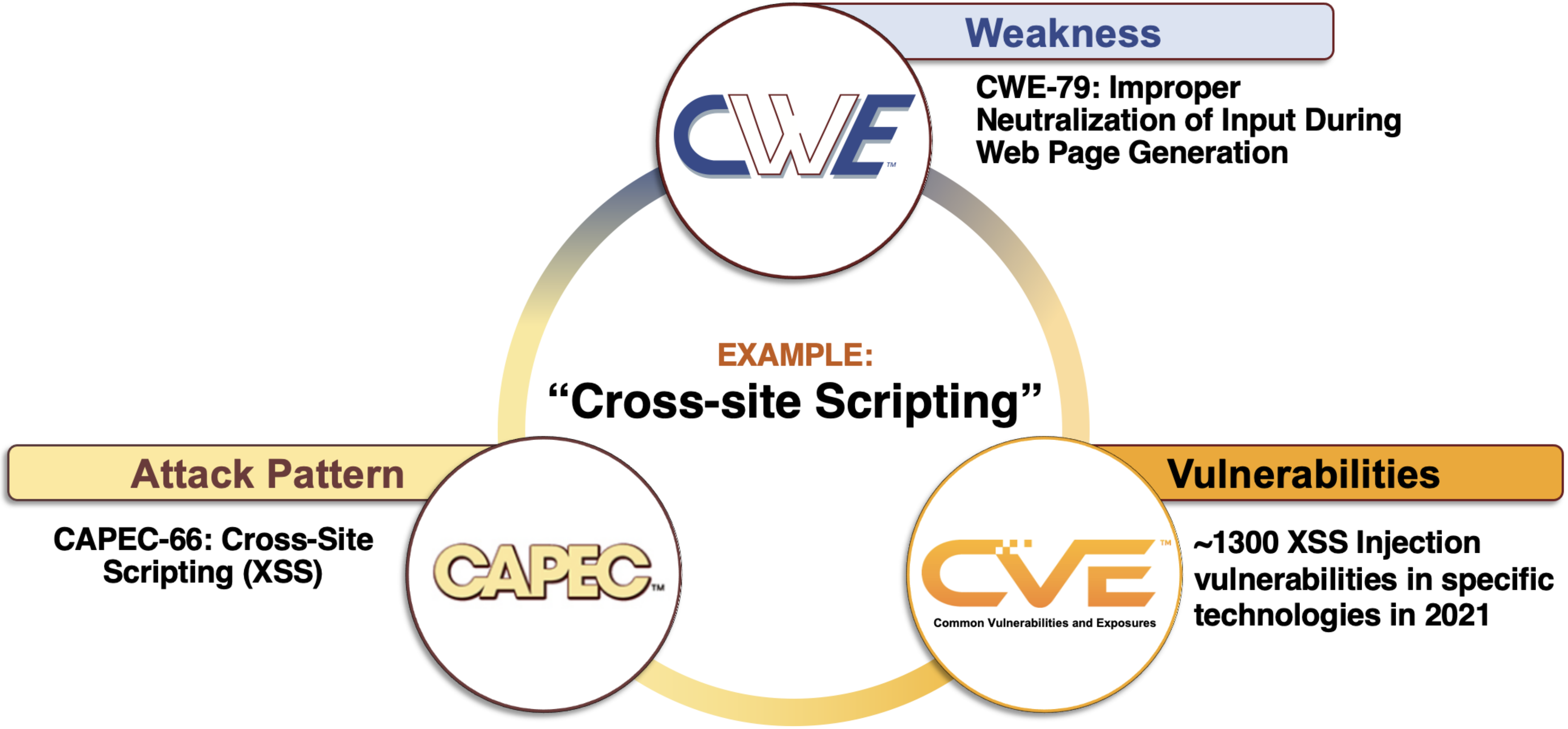
1. ICS Communications
   - **Unreliability:** Vulnerabilities arise in reaction to disruptions in the physical layer (e.g., creating electrical noise) used to carry the traffic.
2. ICS Dependencies (& Architecture)
   - **External Physical Systems:** Due to the highly interconnected technologies in use, 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).

‘Get Ahead of Boom’ Landscape



Weaknesses
CWE
The root cause of a vulnerability
GET AHEAD OF BOOM!
Attack Patterns
CAPEC
How the weakness could be exploited
Vulnerabilities
CVE
Common Vulnerabilities and Exposures
Specific instances of a weakness type that are demonstrably exploitable

‘Get Ahead of Boom’ Landscape



Weakness

CWE-79: Improper Neutralization of Input During Web Page Generation

EXAMPLE:

“Cross-site Scripting”

Attack Pattern

CAPEC-66: Cross-Site Scripting (XSS)

Vulnerabilities

~1300 XSS Injection vulnerabilities in specific technologies in 2021

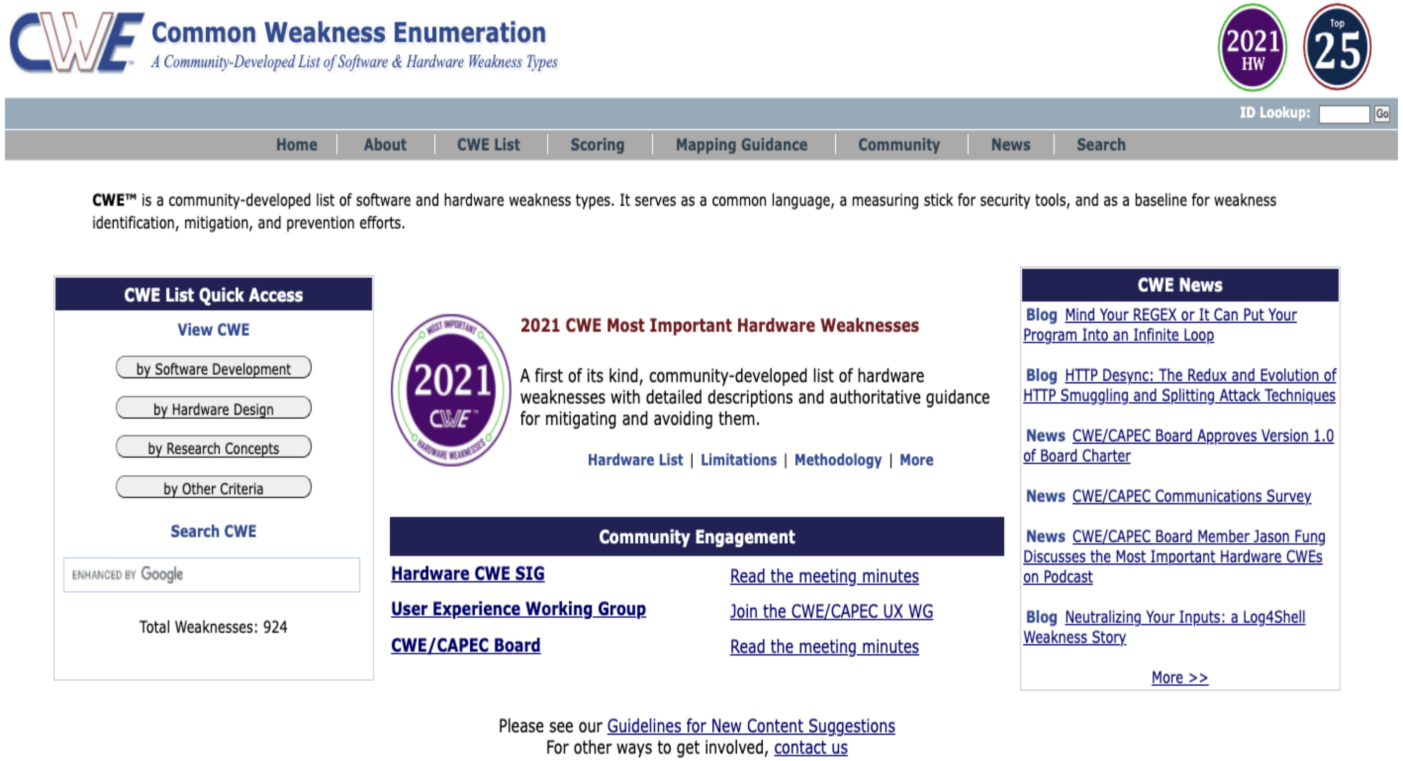
CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

CWE is…

CWE™ is a community-developed list of common software and hardware security weaknesses – mistakes that, in proper conditions, could contribute to the introduction of vulnerabilities.

- View all weaknesses related to a category
- Search for a specific weakness type
- Find mapping to other information lists

Vision: CWE informs development, acquisition, and operational efforts resulting in more secure information technology capabilities at lower costs.



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

CWE List Quick Access

View CWE

Search CWE

Total Weaknesses: 924

2021 CWE Most Important Hardware Weaknesses

A first of its kind, community-developed list of hardware weaknesses with detailed descriptions and authoritative guidance for mitigating and avoiding them.

Hardware List | Limitations | Methodology | More

Community Engagement

Hardware CWE SIG	Read the meeting minutes
User Experience Working Group	Join the CWE/CAPEC UX WG
CWE/CAPEC Board	Read the meeting minutes

CWE News

Blog Mind Your REGEX or It Can Put Your Program Into an Infinite Loop

Blog HTTP Desync: The Redux and Evolution of HTTP Smuggling and Splitting Attack Techniques

News CWE/CAPEC Board Approves Version 1.0 of Board Charter

News CWE/CAPEC Communications Survey

News CWE/CAPEC Board Member Jason Fung Discusses the Most Important Hardware CWEs on Podcast

Blog Neutralizing Your Inputs: a Log4Shell Weakness Story

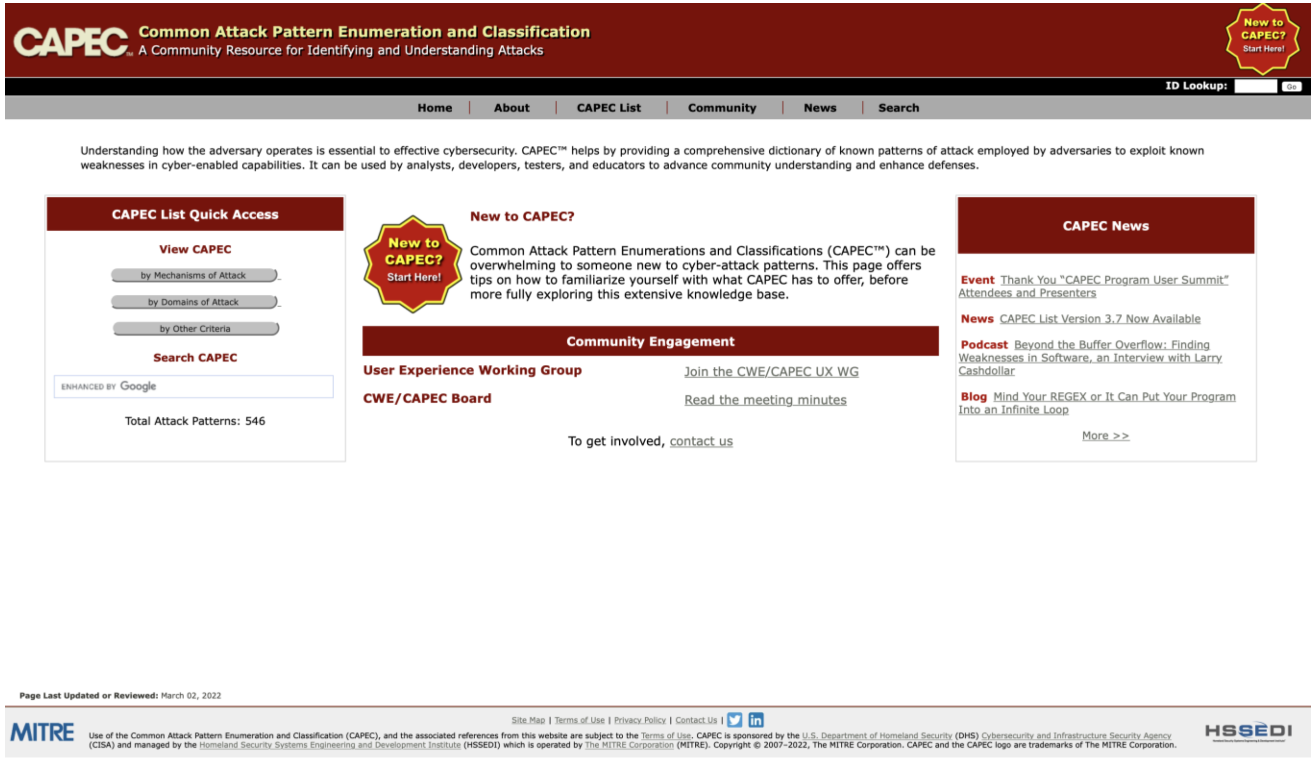
More >>

Please see our Guidelines for New Content Suggestions
For other ways to get involved, contact us

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

CAPEC is…

- **A comprehensive dictionary of attack patterns employed by adversaries to exploit known weaknesses in cyber-enabled capabilities**
- **Built on software ‘design patterns’**
  - Paradigms for solving common software design issues
- **‘Attack patterns’ are ‘design patterns’ for cyber attackers aimed at exploiting a weakness (CWE)**



CAPEC™ Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

New to CAPEC? Start Here!
ID Lookup: Go
Home | About | CAPEC List | Community | News | Search

Understanding how the adversary operates is essential to effective cybersecurity. CAPEC™ helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.

CAPEC List Quick Access

View CAPEC

Search CAPEC

Total Attack Patterns: 546

New to CAPEC?

Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.

Community Engagement

User Experience Working Group Join the CWE/CAPEC UX WG

CWE/CAPEC Board Read the meeting minutes

To get involved, contact us

CAPEC News

Event Thank You "CAPEC Program User Summit" Attendees and Presenters

News CAPEC List Version 3.7 Now Available

Podcast Beyond the Buffer Overflow: Finding Weaknesses in Software, an Interview with Larry Cashdollar

Blog Mind Your REGEX or It Can Put Your Program Into an Infinite Loop

More >>

Page Last Updated or Reviewed: March 02, 2022

Site Map | Terms of Use | Privacy Policy | Contact Us |

Use of the Common Attack Pattern Enumeration and Classification (CAPEC), and the associated references from this website are subject to the Terms of Use. CAPEC is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation (MITRE). Copyright © 2007–2022, The MITRE Corporation. CAPEC and the CAPEC logo are trademarks of The MITRE Corporation.

Helping Improve Security Pre-Compromise

CWE/CAPEC Helps Organizations “Shift Left”

- **Enables better security earlier in the development lifecycle by enumerating the weaknesses and related attack patterns to avoid**
  - System designers/developers can be informed about risk from the beginning
  - Product security teams can focus on the weaknesses that they produce
- **Helps make tools easier to use by creating a common language across all tools (e.g., static analysis, dynamic analysis)**
- **Helps users better understand different types of mistakes by providing detailed information about individual weakness types**