CWE-CAPEC ICS/OT Special Interest Group

Wednesday, July 27, 2022

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. **Anton Shipulin**
15. **Armada Sramek**
16. **Ashley McGlone**, Tanium
17. **Aw Landgraaf,**
18. **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. **Eric Cosman**
66. **Eric Mitchell,** NSA
67. **Eric Strief,** John Deere
68. **Erik Hrin**
69. **Espen Endal,** KraftCERT
70. **Evgeni Sabev**
71. **Gananand G Kini**
72. **Greg Ahira,** GE
73. **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. **Kerry Stuver,** GE
116. **Khalid Ansari,** FM Approvals
117. **Kimberly Denbow,**
118. **Krystel Castillo**
119. **Kumar**
120. **Kyle Johnson,** GSOC
121. **Lindsey Cerkovnik,** DHS CISA
122. **Marc Sachs,** Auburn University
123. **Mark Sullivan,** NSA
124. **Martijn Jansen,** Taqa
125. **Martin Kihiko**
126. **Martin Ring,** Bosch
127. **Martin Scheu,** Switch
128. **Marty Edwards**
129. **Matt Bishop,** UC Davis & CyManII
130. **Marie Stanley Collins**
131. **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 – 3:15 pm	**Opening Remarks** • Review meeting objectives • Solicit questions around and confirm the purpose of the ICS/OT SIG
3:15 – 4:10 pm	**Priority Gaps in Classifying ICS/OT Weaknesses** • Review breakout session and survey results • Solicit any additional feedback or insights • Prioritize what this group wants to tackle
4:10 – 4:25 pm	**Sub-Working Group Topics** • Review short list of topics for a sub-working group under the ICS/OT SIG • Define structure and cadence • Identify chair(s) and participants
4:25 – 4:30 pm	**Wrap-Up** • Closing remarks • Next SIG meeting – Wed 8/31 @ 3pm • Action Items
4:30 pm	**Meeting Ends**

Opening Remarks

Opening Remarks

- **Meeting Objectives**
- **Purpose of the ICS/OT SIG**

Differentiating CWE/CAPEC, MITRE ATT&CK, etc.

- **MITRE manages both CWE/ CAPEC, ATT&CK, and D3FEND although all are community-based programs**
- **Both curate cyber-attack knowledge, but from *different points of view***
  - CAPEC details how an adversary can exploit a weakness (i.e., a CWE)
  - ATT&CK is more oriented towards understanding known attack techniques “from the wild” to detect/prevent adversary actions (includes malicious use of a common application or utility, i.e., not necessarily exploiting a weakness)
  - D3FEND is a knowledge graph of defensive cybersecurity countermeasures which address attack types against specific weaknesses
- **Going forward:**
  - Continued improvements in mappings between the entries in each corpus
  - Explore further collaborative opportunities aimed at optimizing each respective program

Gaps in Classifying/Communicating ICS/OT Weaknesses

Gaps in Classifying ICS/OT Weaknesses – In Scope

New Types of Weaknesses

1. **Emerging tech is challenging the existing legacy understanding of and approach to the data** and we need to know how to utilize the new technology available in a meaningful way (which is why including academia and incoming talent is vital)
   - Including weaknesses due to the legacy nature of ICS communication protocols (e.g., Modbus, etc.)
2. **Rapid, cloud-driven software development** and how this changes the mindset
3. **OT devices were not built for the load they are expected to now carry.** Updates not only need to be accessible to the industry, but someone needs to actively push those updates on the industry to make them aware of their importance.
4. **Weaknesses inherent with architectural patterns** (e.g., ICS protocol requires weakest device/chipset to open a network listener)
   - Embedded ICS/OT systems does not allow the use of several types and brands of security tool
5. **Security concerns even in air gapped ICS/OT systems**

Gaps in Classifying ICS/OT Weaknesses – In Scope

Scope of CWE-CAPEC

1. **Utilization of CWE/normalization of data** (data is elusive and we need to compare apples to apples, by putting it into terms we can all understand)
2. **Identifying the overlap of newly discovered CWEs with existing CWEs**
3. **Standardization of terminology and methods** such that ICS/OT and IT integration/convergence creates less uncertainty and work
   - Develop a central/common language
4. **Limited framing of weakness as part of whole system life cycle** for considering and mitigating security challenges efficiently
5. **ICS/OT top n (3, 5, 10, etc.) list(s)** to focus on to move the state of the practice forward instead of taking on too much. This will also help practitioner focus
   - Basic minimum which should be mandatory/most important. This may stem from a database of cybersecurity incidents like that of the Chemical Safety Board.
   - Reduce "noise" of too many CWEs to remediate
6. **Develop hands-on training materials/field guide for technicians** e.g. a virtual lab to practice ICS/OT cybersecurity; blue and red team exercises

Gaps in Classifying ICS/OT Weaknesses – Out of Scope

New Types of Weaknesses

1. **Weaknesses that usually go unaddressed due to operational priorities** (e.g., many control rooms do not implement account-lockout after incorrect password attempts)
   - *Falls into a proposed scope exclusion*: Any human or organizational process or policy that is not measurable and does not produce clear artifacts that identify weaknesses

Scope of CWE-CAPEC

1. **Mapping weaknesses to MITRE ATT&CK framework**
   - Develop a repository of TTPs of cyber attacks on the ICS/OT environment
2. **Exploitability** e.g., high (only remote access needed), to low (several vulns need to be chained)
3. **Security testing tools and procedures for ICS/OT products**
4. **Create metrics/baselines/benchmarks for given set of criteria or best practices across sectors** for incremental and future analysis. Potentially like a census with resources to track and analyze progress over time, with forms for daily usage.

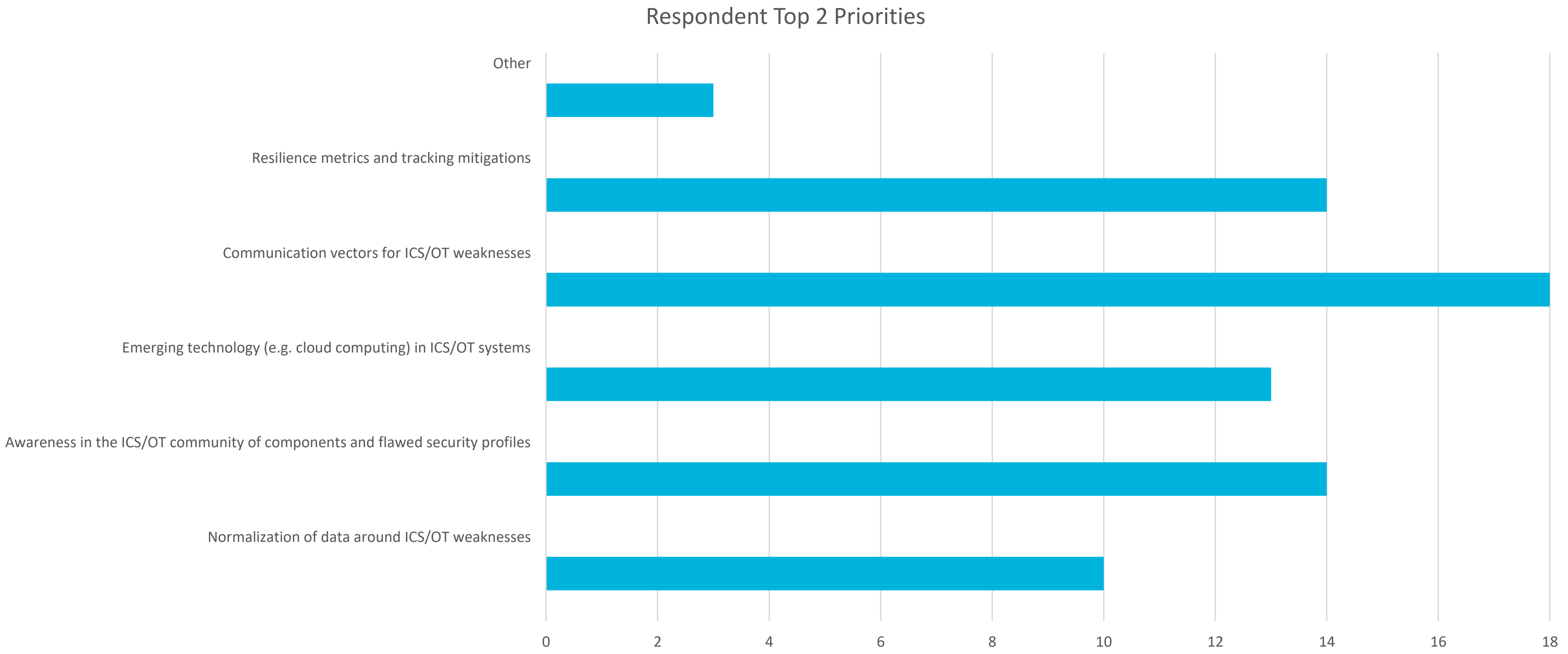
Gaps in Communicating ICS/OT Weaknesses – In Scope

1. **Involve the ICS/OT vendors** and have a joint community with them where the state of practice can be shared with a broader (maybe already existing in the vendors networks) community
2. **Create a community similar to OWASP Chapters** but related to ICS/OT cybersecurity challenges. There the researchers will be able to start gathering and exchange experience and SIG can be the core team from that community
   - There is IT communication vectors, but we don't know what the right ICS/OT communication vectors are for disseminating information
3. **Leverage the WFD work at CyManII** to a) promote knowledge of weaknesses and b) 'what to do'
4. **What are the barriers the receiving audience is facing** that either is resistance or reluctant or unable to receive the information?

Gaps in Communicating ICS/OT Weaknesses – Out of Scope

1. **Interagency information sharing in a formalized capacity**. So far it has been ad hoc.
2. **Ensure equities of all critical infrastructure sectors are considered.** Ensure costs associated with OT vulnerability discovery and mitigation are effectively communicated with the business side of the organization.
3. **Sharing actual cases of attacks on ICS/OT systems**

Respondent Top 2 Priorities



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

Sub-Working Group Topics

Sub-Working Groups Topics

Generated by the SIG Co-Chairs

1. Education and Awareness of CWE
2. Boosting CWE Content
3. Mapping CWE to ISA 62443 Security Control

Generated by SIG Participants

1. Creating an ICS/OT community of device manufacturers and an open testbed that replicates the Purdue Model for vulnerability analysis, reporting, and remediation (much like the 5G vendor community has established)
2. Creating CWE "How to" guide for ICS/OT audiences. Consider ICS/OT audience needs/use cases for CWE are diverse across extended product lifecycles
3. Consider conducting a baseline benchmark on the focus areas for OT/ICS in its current state (CWE: awareness, content and coverage, framework alignment with 62443, etc.). Use benchmark to make focused on improvements in specific areas
4. Providing 'formal' descriptions of weaknesses so users of CWE can more readily reason about/across weaknesses and vulnerabilities

Volunteering for a Sub-Working Group

	Education and Awareness of CWE	Boosting CWE Content	Mapping CWE to ISA 62443 Security control
1	Ahmad Sharafi	Ahmad Sharafi	Sandeep Shukla
2	Danielle Jablanski	Danielle Jablanski	Aagam Shah
3	Greg Ahira	Evgeni Sabev	Danielle Jablanski
4	William Kintz	Ismael Garcia	Renan Xavier
5	John Kingsley		Greg Ahira
6	Howard Grimes		William Kintz
7	Bryan Owen		Khalid Ansari
8	DC3 participant		John Kingsley
9	Mike Chaney		Mina Todorova
10	Jose Luis Jimenez		DC3 participant
11			Mike Chaney
12			Susan Farrel
13			Jose Luis Jimenez
14			
15			
16			
17			
18			
19			
20			

Structuring Sub-Working Groups

Define structure and cadence

- Which sub-working group should be spun up first?
- How frequently will it meet?
- What forums for collaboration should we use?

Identify chair(s)

1. Boosting CWE Content
2. Education and Awareness of CWE

Wrap-Up

Closing Remarks

- **SIG Priorities**
  - Emerging consensus of participant priorities
  - Standing-up sub-working groups
  - Defining deliverables
- **Housekeeping**
  - Objections to sharing the full questionnaire results without attribution?

Major Milestones

- **ICS/OT SIG meets monthly**
  - Next meeting Wednesday 8/31 from 3:00 to 4:30pm ET
- **CWE/CAPEC publish content on quarterly basis**
  - Next board meeting [TBD, sometime in end of September/early October], occurring quarterly
  - Next major update for CWE/CAPEC weakness Fall 2022

Action Items

1. **Request access to the public & private Github repositories for the ICS/OT SIG**
2. **Review the 20 categories of security vulnerabilities identified in the SEI ETF: https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf**
3. **Please review the three sub-working group charter documents and volunteer to participate**

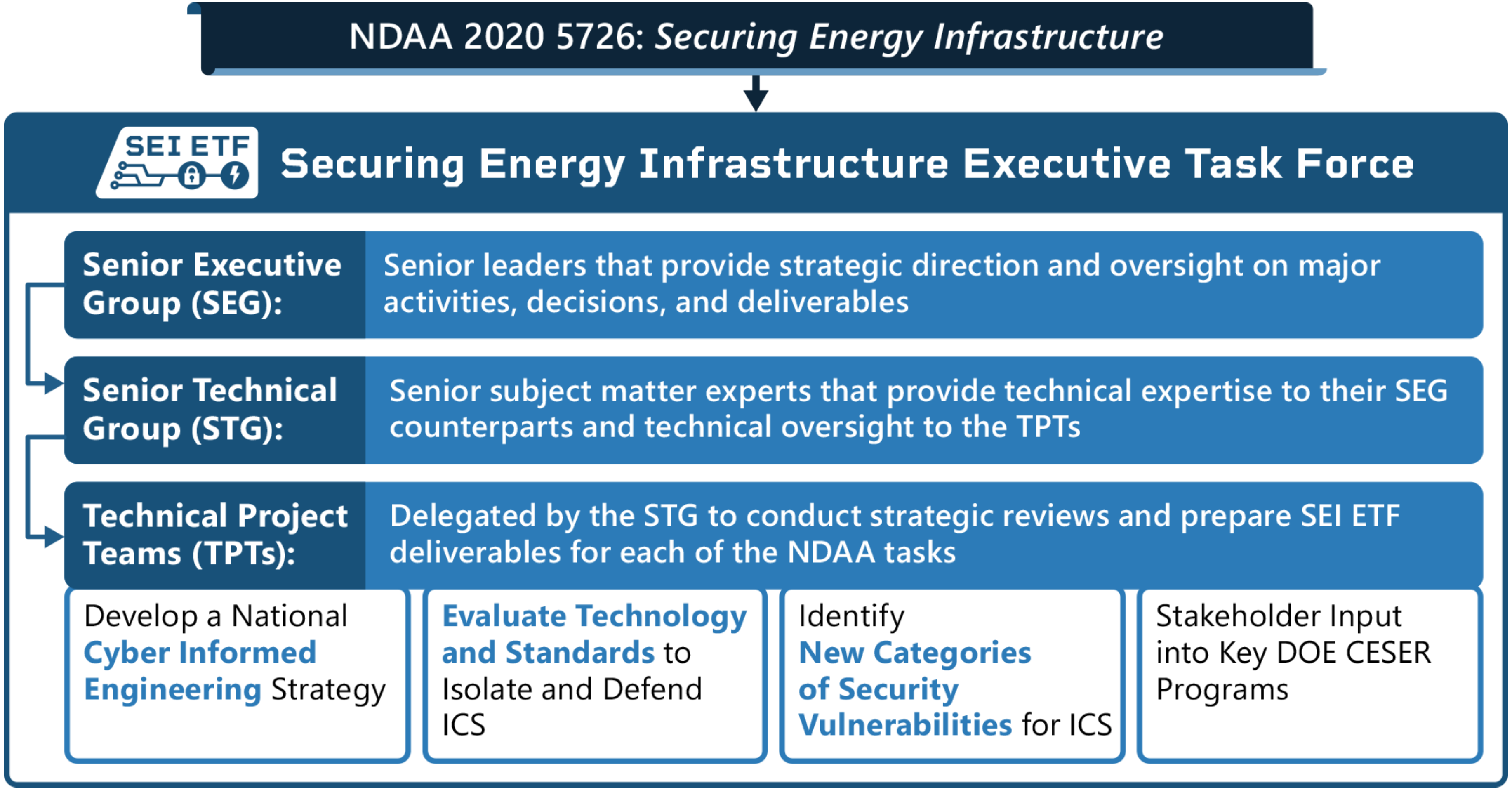
MITRE

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:

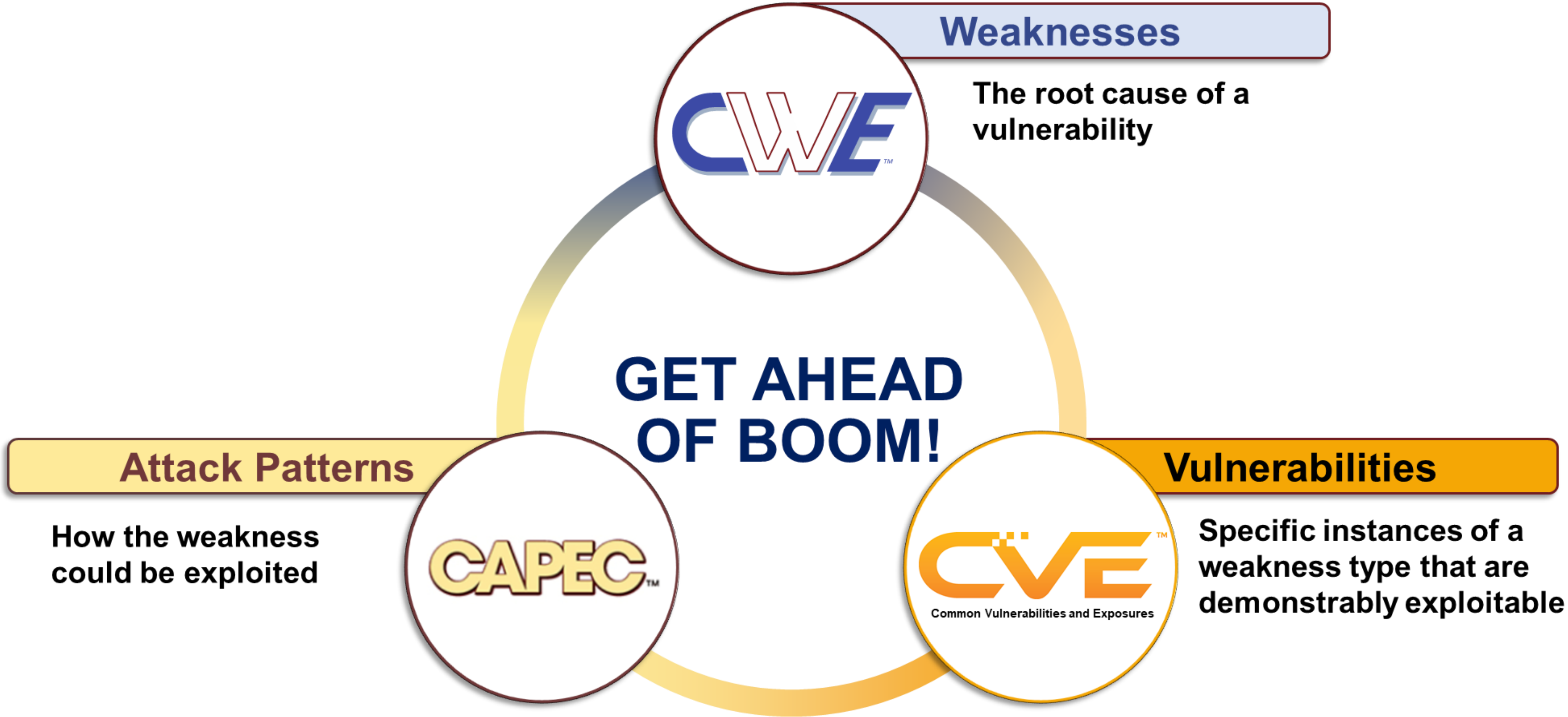
Categories of Security Vulnerabilities in ICS

- 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).

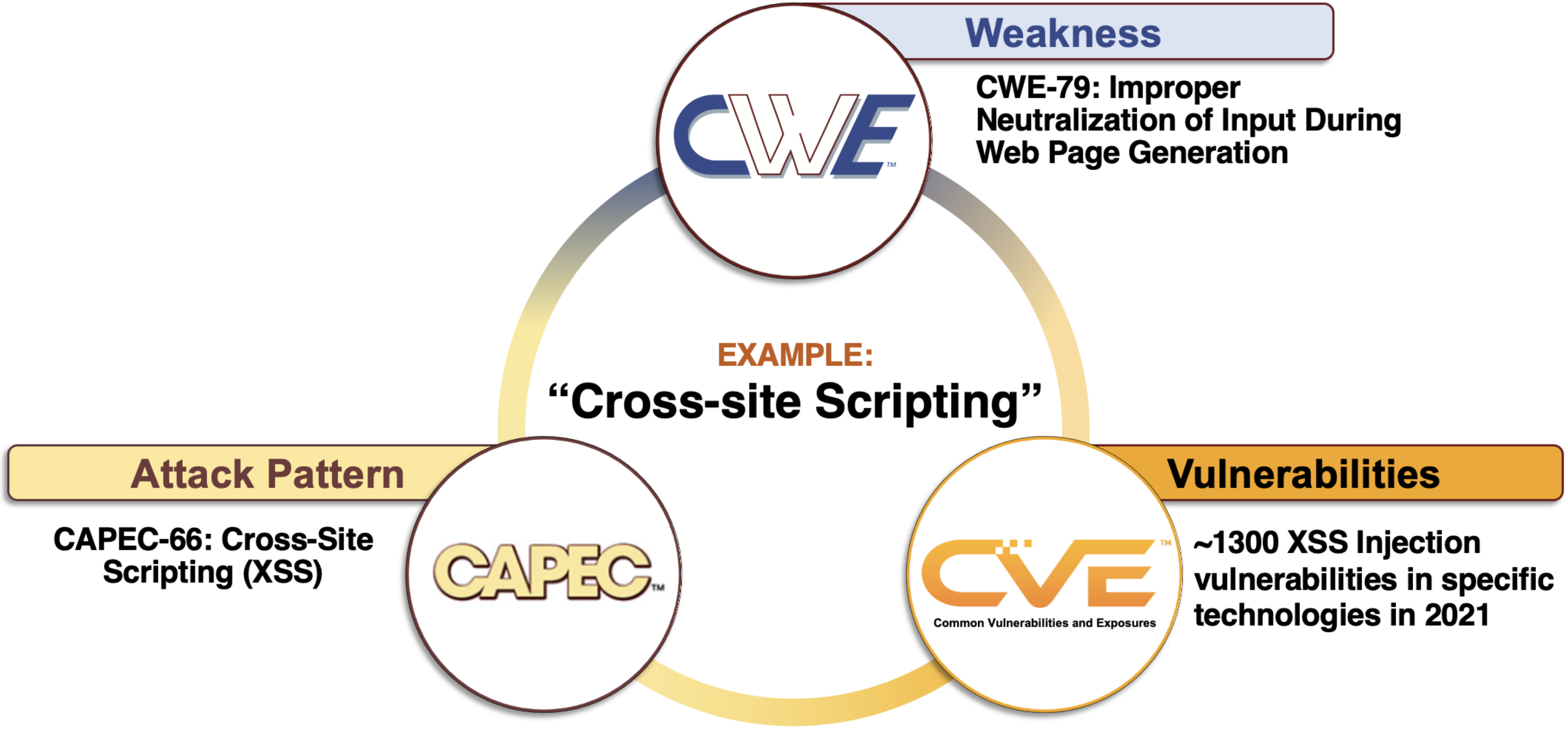
‘Get Ahead of Boom’ Landscape



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

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

‘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

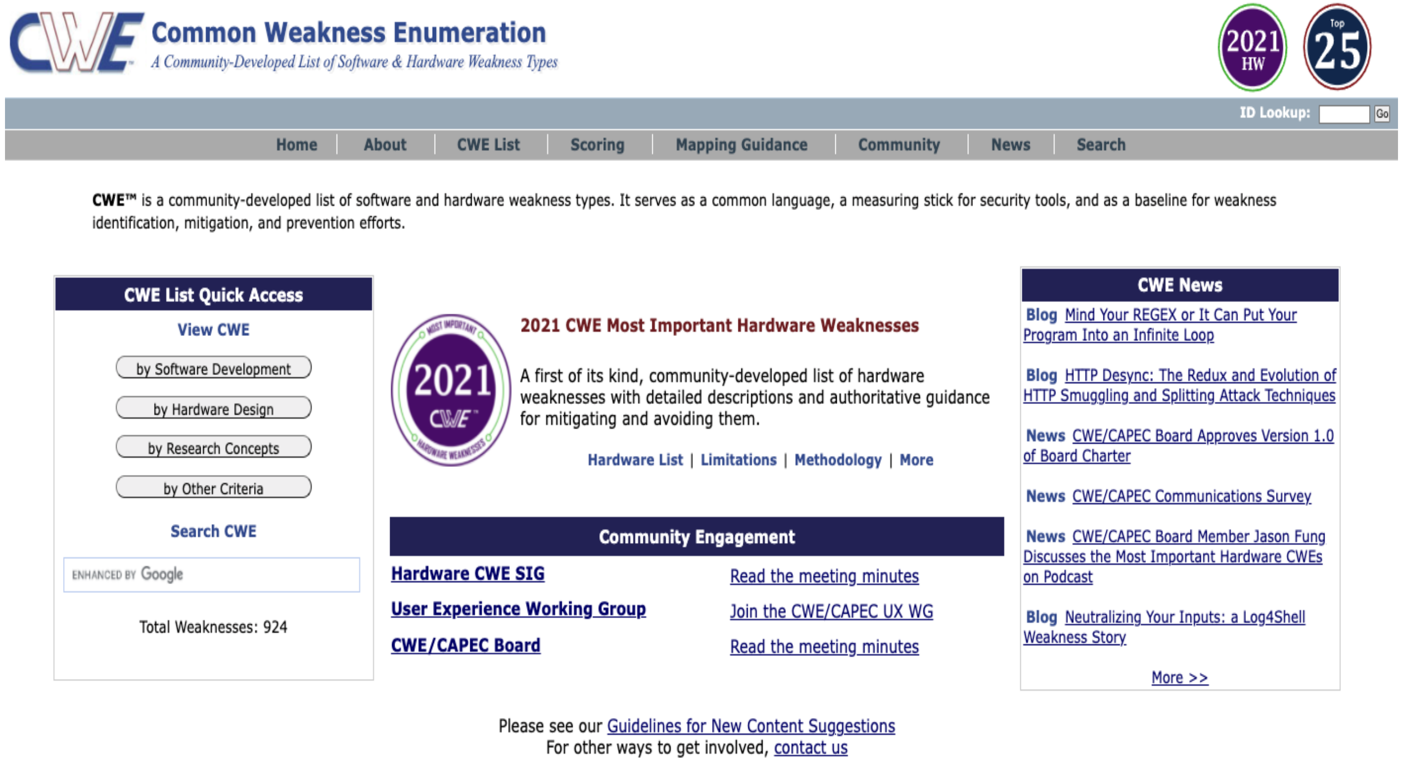
~1300 XSS Injection vulnerabilities in specific technologies in 2021

CWE 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

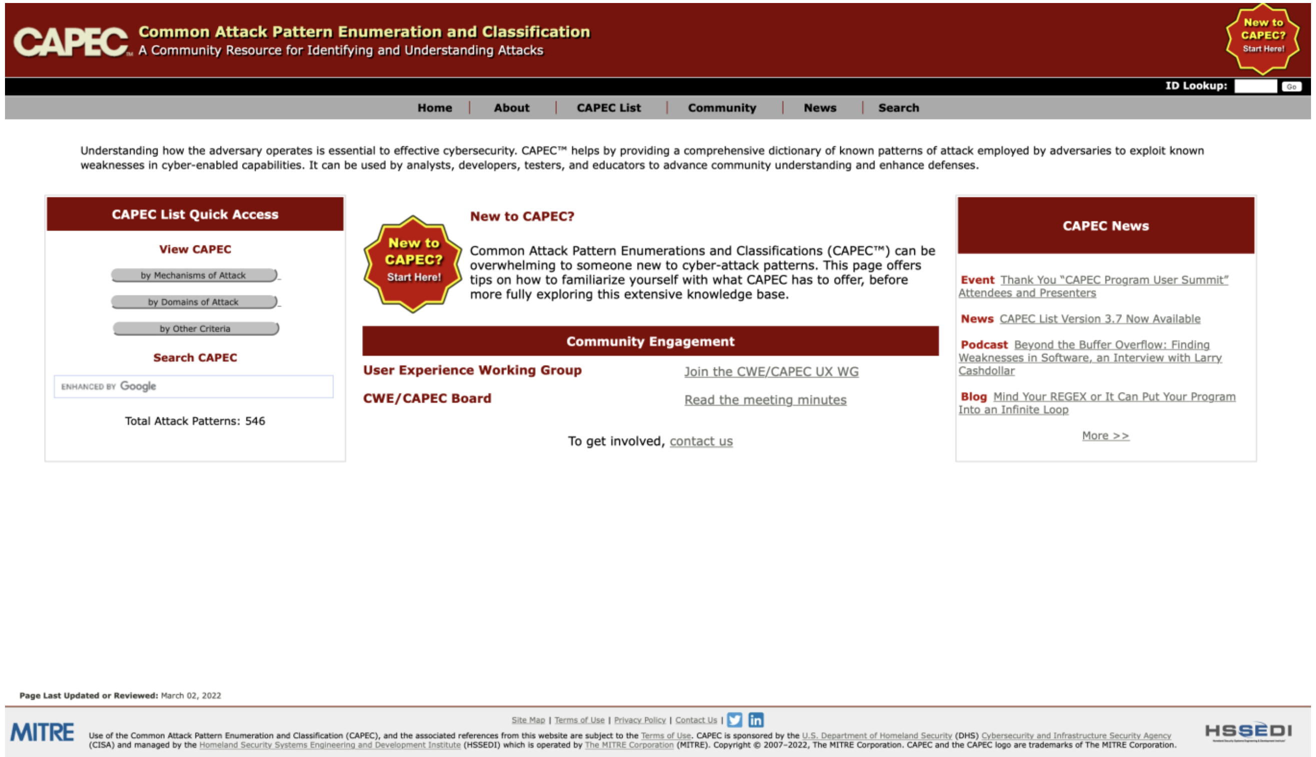
Blog Neutralizing Your Inputs: a Log4Shell Weakness Story

More >>

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

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**