

# CWE\_CAPEC User Experience Working Group

Wednesday, December 14, 2022

## Members in Attendance

Ahmed, Faheem  
Alexander, Erin  
Christey, Steven  
Coffin, Chris  
Coles, Matthew  
Foomany, Farbod

Gantenbein, Kirsten  
Keane, John  
Maldonado, Rosado  
Nichols, Doug  
Piazza, Rich  
Rothenberg, David

Schweiger, Andreas  
Summers, Alec  
Sundberg, Christopher  
Taggart, Philip  
Turkevich, Julia  
Whitmore, Jim

## Introduction, Announcements, and Agenda

*MITRE CWE: Alec Summers*

- Topics:
  - A Different View of CWE/CAPEC – Security Workbench
  - CAPEC Content Presentation Filters Proposal
  - Looking ahead - User Stories to come (January)
- Last meeting of the year
- Next quarterly board meeting TBD Q1-2023
- Looking to identify further UEWG opportunities
- CAPEC minor release 3.9 Jan 24, CWE minor release 4.10 Jan 31
- Q1/Q2 Efforts
  - User Persona -> User Stories
  - Determine best way to communicate user stories with community
  - CWE/CAPACE content development/collaboration space (underway)

## Security Workbench

*Dickinson College: Jim Whitmore*

- Discussion of the importance of security engineering
  - Starts with Cyber Thinking (“triad of security engineering”)
    - Threats, weaknesses, & vulnerabilities
  - Problem Statement
    - The volume and format of security information is an obstacle for learning and applied security analysis
- SE-Workbench
  - Goal to inject security into agile/devops
  - **Security Control Explorer (SCE)**. This tool organizes and displays the security and privacy controls from NIST SP800-53, their connections with ISO27001 along with the security capabilities from the NIST Cybersecurity Framework and links to authoritative security reference documents.
  - **Security Vulnerability Explorer (SVE)**. This tool organizes and displays security weaknesses and vulnerabilities from MITRE Common Weakness Enumeration (CWE),

relationship to published lists such as OWASP, connections to NIST Vulnerability Database (NVD), along with analytical insights and correlation from other information sources.

- **Security Attack Explorer (SAE).** This tool organizes and displays security attack patterns from MITRE Common Attack Pattern Enumeration and Classification (CAPEC), along with connections to MITRE Common Weaknesses (CWE), exploitation techniques from MITRE ATT&CK, recommended test and assurance strategies.
- <https://www.researchgate.net/project/Security-Engineering-Workbench>
- Discussion regarding licensing and project being open source. Is not open source and the repo requires permissions to access
- Overview of displays, user interface, and output formats

## CAPEC Content Filters

CAPEC: Rich Piazza

- Porting of CWE Presentation filters to CAPEC

CURRENT		PROPOSED			
BASIC	COMPLETE	CONCEPTUAL	OPERATIONAL	MAPPING-FRIENDLY	COMPLETE
Description	Description	Description	Description	Description	Description
Extended_Description	Extended_Description	Extended_Description	Extended_Description	Extended_Description	Extended_Description
Related_Attack_Patterns	Related_Attack_Patterns	Alternate_Terms	Alternate_Terms	Alternate_Terms	Related_Attack_Patterns
Execution_Flow	Execution_Flow	Taxonomy_Mappings	Related_Attack_Patterns	Related_Attack_Patterns	Execution_Flow
Prerequisites	Prerequisites	Consequences	Execution_Flow	Taxonomy_Mappings	Prerequisites
Mitigations	Mitigations		Prerequisites	Related_Weaknesses	Mitigations
Related_Weaknesses	Related_Weaknesses		Mitigations	Notes - Relationship	Related_Weaknesses
	Likelihood_Of_Attack		Related_Weaknesses	Notes - Terminology	Likelihood_Of_Attack
	Alternate_Terms				Alternate_Terms
	Typical_Severity				Typical_Severity
	Skills_Required				Skills_Required
	Resources_Required				Resources_Required
	Indicators				Indicators
	Consequences				Consequences
	Example_Instances				Example_Instances
	Taxonomy_Mappings				Taxonomy_Mappings
	References				References
	Notes				Notes
	Content_History				Content_History

- Emphasize customizing of what you want to see
- Tool tips when mousing over buttons

## Closing Discussion

- Discussion of better educating people on CAPEC and CWE
  - Meeting with academics and getting information out for classes and tutorials
- Still working out method for User Stories Collaboration/Development
  - Google docs?
- Need more user stories across each persona
- Happy Holidays and Happy New Year!