CWE/CAPEC User Experience Working Group Meeting

July 27, 2022

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

Agenda

- **This meeting is being recorded :-)**
- **Housekeeping**
- **Primary topics**
  - Definitions!
    - *Harmonizing common terms across CWE/CAPEC (CVE?)*
    - *Review proposed definitions and review the next round of feedback*
  - Personas and Presentation Filters
    - *Finalizing and Next Steps*
  - Reminders
- **Adjourn**

UEWG: Reminders

- **Mission:** Identifying areas where CWE/CAPEC content, rules, guidelines, and best practices must improve to better support stakeholder community, and work collaboratively to fix them
- **Periodic reporting of activities to CWE/CAPEC Board**
  - (next quarterly Board meeting TBD Sept/Oct)
- **Please solicit participations from your contacts**
  - Contact: cwe@mitre.org & capec@mitre.org

Housekeeping

Community member co-chair

- We are working to identify ongoing opportunities and priorities for FY23
- This discussion/action, drive working group activities, etc.

Focus Areas	Internal WG Member Efforts	Externally facing Efforts	Enhance User Experience
Goal #1 – Virtual collaboration space			
Goal #2 – Provide users technical reach back			
Goal #3 – Inform next version of the website			
Goal #4 - Socialization Strategy			

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

Topic

Definitions!

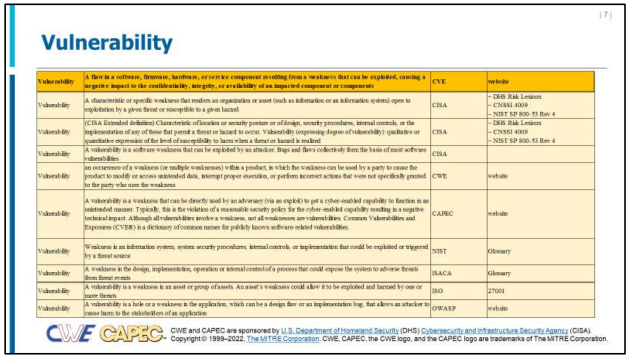
Harmonizing common terms across CWE/CAPEC

Shadya Maldonado Rosado

UEWG Co-Chair

CWE / CAPEC Terminology

- **Authoritative sources for cybersecurity terminology define terms differently – including CWE/CAPEC!**
  - Vulnerability is defined *three* different ways between CVE, CWE, and CAPEC ☹
- **Vulnerability, Weakness, and Attack Patterns have multiple definitions across CISA, NIST, ISO Standards, etc.**

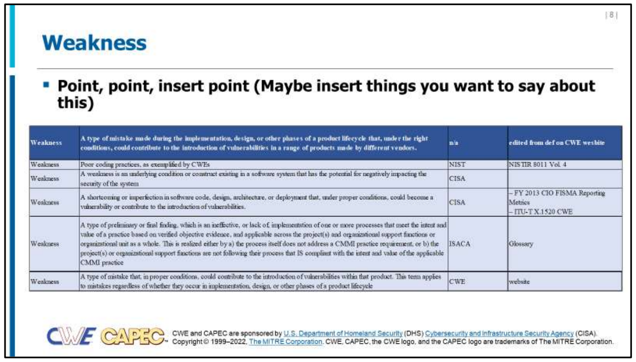


| 7 |

Vulnerability

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
Vulnerability	A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard	CISA	– DHS Risk Lexicon – CNSSI 4009 – NIST SP 800-53 Rev 4
Vulnerability	(CISA Extended definition) Characteristic of location or security posture or of design, security procedures, internal controls, or the implementation of any of these that permit a threat or hazard to occur. Vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized	CISA	– DHS Risk Lexicon – CNSSI 4009 – NIST SP 800-53 Rev 4
Vulnerability	A vulnerability is a software weakness that can be exploited by an attacker. Bugs and flaws collectively form the basis of most software vulnerabilities	CISA	
Vulnerability	an occurrence of a weakness (or multiple weaknesses) within a product, in which the weakness can be used by a party to cause the product to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness	CWE	website
Vulnerability	A vulnerability is a weakness that can be directly used by an adversary (via an exploit) to get a cyber-enabled capability to function in an unintended manner. Typically, this is the violation of a reasonable security policy for the cyber-enabled capability resulting in a negative technical impact. Although all vulnerabilities involve a weakness, not all weaknesses are vulnerabilities. Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names for publicly known software-related vulnerabilities.	CAPEC	website
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source	NIST	Glossary
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events	ISACA	Glossary
Vulnerability	A vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats	ISO	27001
Vulnerability	A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application	OWASP	website

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).
Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.



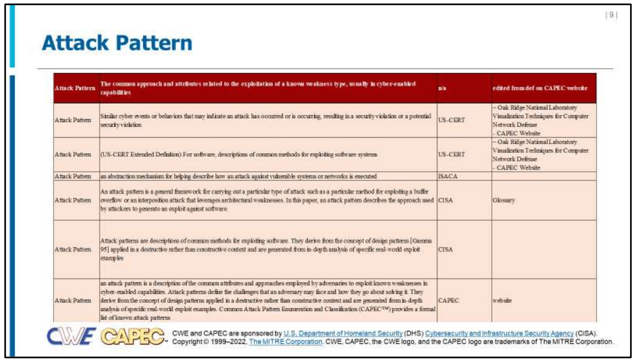
| 8 |

Weakness

- **Point, point, insert point (Maybe insert things you want to say about this)**

Weakness	A type of mistake made during the implementation, design, or other phases of a product lifecycle that, under the right conditions, could contribute to the introduction of vulnerabilities in a range of products made by different vendors.	n/a	edited from def on CWE wesbite
Weakness	Poor coding practices, as exemplified by CWEs	NIST	NISTIR 8011 Vol. 4
Weakness	A weakness is an underlying condition or construct existing in a software system that has the potential for negatively impacting the security of the system	CISA	
Weakness	A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities.	CISA	– FY 2013 CIO FISMA Reporting Metrics – ITU-T X.1520 CWE
Weakness	A type of preliminary or final finding, which is an ineffective, or lack of, implementation of one or more processes that meet the intent and value of a practice based on verified objective evidence, and applicable across the project(s) and organizational support functions or organizational unit as a whole. This is realized either by a) the process itself does not address a CMMI practice requirement, or b) the project(s) or organizational support functions are not following their process that IS compliant with the intent and value of the applicable CMMI practice	ISACA	Glossary
Weakness	A type of mistake that, in proper conditions, could contribute to the introduction of vulnerabilities within that product. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of a product lifecycle	CWE	website

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).
Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.



| 9 |

Attack Pattern

Attack Pattern	The common approach and attributes related to the exploitation of a known weakness type, usually in cyber-enabled capabilities	n/a	edited from def on CAPEC website
Attack Pattern	Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation	US-CERT	– Oak Ridge National Laboratory Visualization Techniques for Computer Network Defense - CAPEC Website
Attack Pattern	(US-CERT Extended Definition) For software, descriptions of common methods for exploiting software systems	US-CERT	– Oak Ridge National Laboratory Visualization Techniques for Computer Network Defense - CAPEC Website
Attack Pattern	an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed	ISACA	
Attack Pattern	An attack pattern is a general framework for carrying out a particular type of attack such as a particular method for exploiting a buffer overflow or an interposition attack that leverages architectural weaknesses. In this paper, an attack pattern describes the approach used by attackers to generate an exploit against software.	CISA	Glossary
Attack Pattern	Attack patterns are descriptions of common methods for exploiting software. They derive from the concept of design patterns [Gamma 95] applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples	CISA	
Attack Pattern	an attack pattern is a description of the common attributes and approaches employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. Attack patterns define the challenges that an adversary may face and how they go about solving it. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. Common Attack Pattern Enumeration and Classification (CAPEC™) provides a formal list of known attack patterns	CAPEC	website

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).
Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

‘APES’ Test (developed by Steve Christey Coley)

- **An acceptable definition for "weakness" should, on its surface, exclude the following:**
- **Aspirin. Aspirin bottles and other medication containers that are expected to have child-proof caps and/or anti-tamper mechanisms.**
  - Example: the Chicago Tylenol murders of 1982
  - Rationale: These have no computing logic in them.
- **Physical padlocks that are only opened by a physical key or physical combination.**
  - Example: Master Lock Keyed Padlock as used for school lockers, etc. (Model #5KADPF is an example)
  - Rationale: while related to security, these have no computing logic in them
- **Extension cord with insufficient strain relief.**
  - Example: OSHA requirements for flexible cords, https://www.osha.gov/electrical/hazards/flexible-cords
  - Rationale: no computing logic and no security implications
- **Spelling error in informational message from web application**
  - Example: web form with tip that says "Do not incccluuuddee dashes when you enter you're phone number”
  - Rationale: no security implications
  - Counter-argument: "sometimes spelling errors have security implications."

Current State (shared w/community 7/13)

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 (from CVE®)
Weakness	A type of flaw or defect inserted during a product lifecycle that, under the right conditions, could contribute to the introduction of vulnerabilities in a range of products made by different vendors
Attack Pattern	The common approach and attributes related to the exploitation of a weakness, usually in cyber-enabled capabilities

Key Question: Is a Weakness an exploitable element?

AJS0

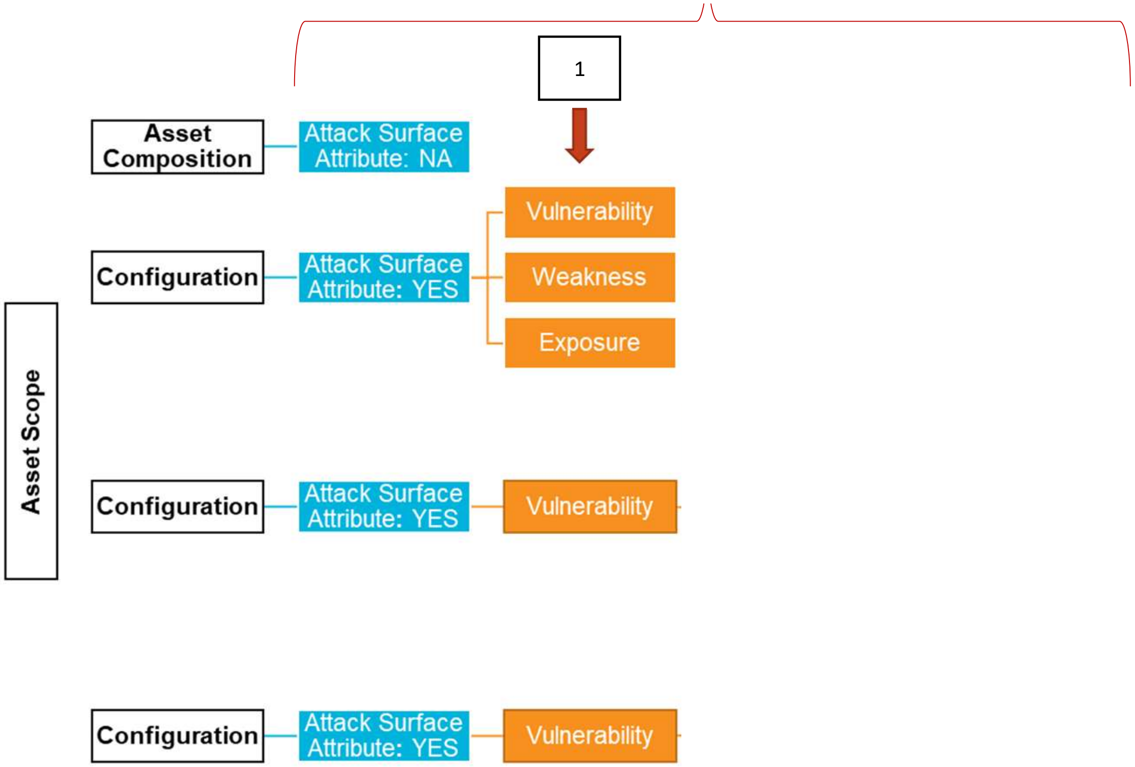
Big Picture Consensus

- **Three general schools of thought**

- **Definition of 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 (from CVE®)

Conceptual examples of an attack surface based on the feedback



Slide 9

AJS0 Take CVE def, per PaulW, add “firmware, or service” for CWE def, and then CAPEC similarly
Alec J Summers, 2022-07-27T16:37:46.888

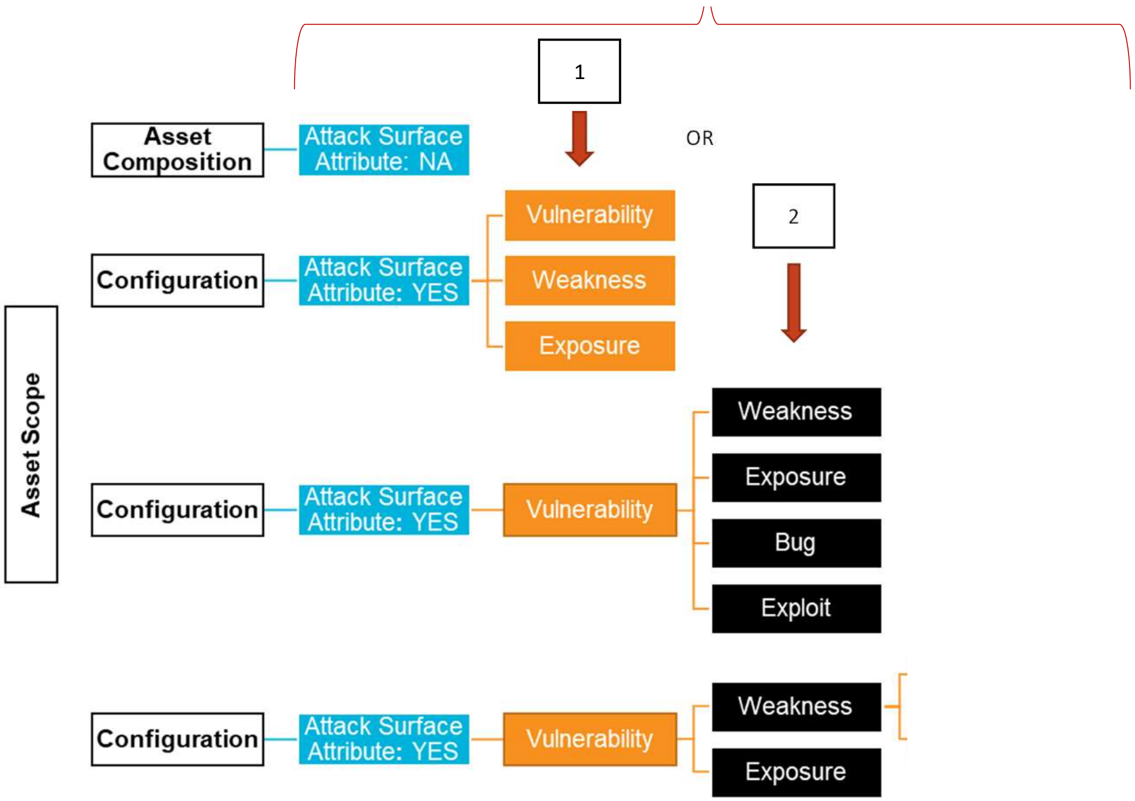
Big Picture Consensus

- **Three general schools of thought**

- **Definition of 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 (from CVE®)

Conceptual examples of an attack surface based on the feedback



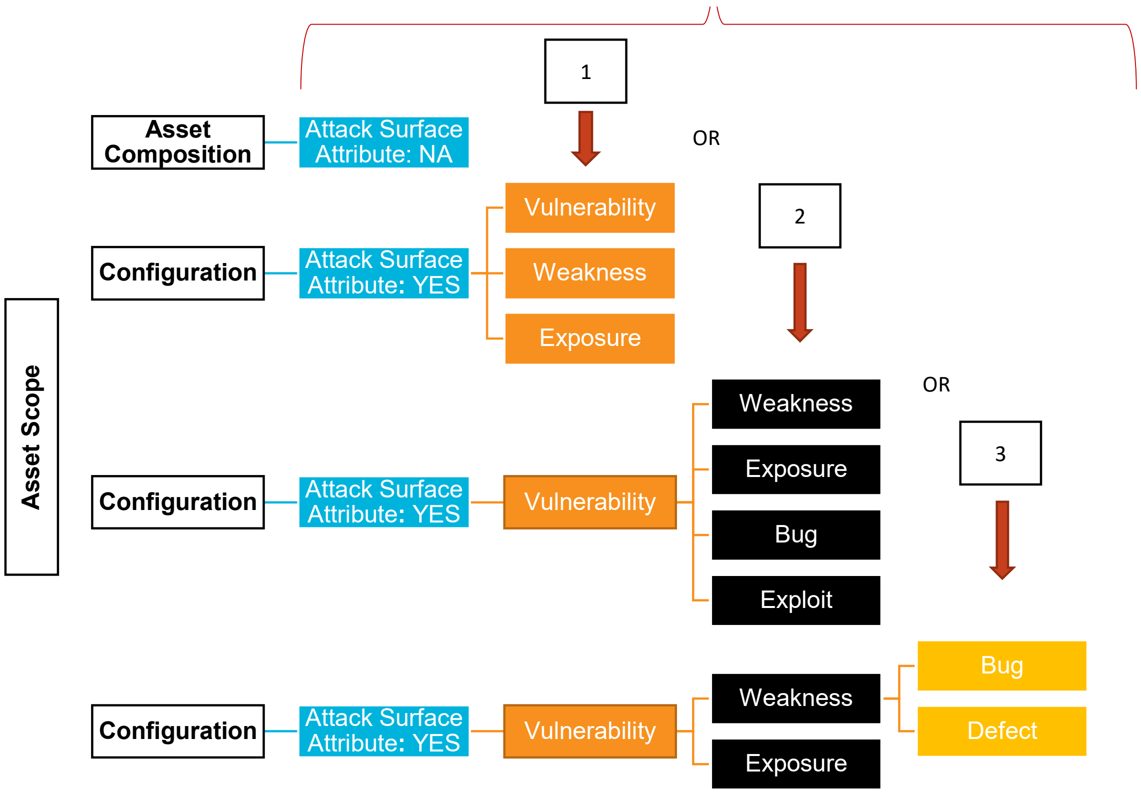
Big Picture Consensus

- **Three general schools of thought**

- **Definition of 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 (from CVE®)

Conceptual examples of an attack surface based on the feedback



Other Considerations

- **An “exploit” vs something that is “exploitable”**

- **Conditions are important**

- **A type of condition or mistake made during the implementation, design, or other phases of a product lifecycle could contribute to the introduction of vulnerabilities or other exploitable element in a range of products made by different vendors.**

Proposed Definitions

- **TBD based on feedback in this session**
- **Should we consider "attack surface attributes" within definition of attack pattern?**

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		n/a	edited from def on CWE website
Attack Pattern	The common approach and attributes related to the exploitation of a known weakness type, usually in cyber-enabled capabilities	n/a	edited from def on CAPEC website

Topic

Continuing the Discussion: User Personas and CWE/CAPEC Presentation Filters

Alec Summers

CWE/CAPEC Deputy Project Lead

Personas: Finalizing

- ~~Formally define each user persona~~
- ~~Share with CWE/CAPEC Board~~
- Once finalized, make public on our sites
- Use that as a catalyst for modernizing presentation according to persona needs

- **"Development lifecycle"**
  - Those who build, use, and protect infrastructure around information systems
- **Educators:** Teachers, professors, or certification programs that educate developers and system designers how to develop more secure code, design more secure products, and/or how to find vulnerabilities.
- **Technical Writers:** Those who communicate advanced technical concepts as clearly, accurately, and comprehensively as possible to their intended audience (e.g., code analysis tool users or system designers)
- **Tool Developers:** Developers of code scanning products, services, and other types of automated techniques for finding weaknesses and attacking systems, and reporting/educating on findings to users
- **Security Researchers/Analysts:** Those who look for ways to attack a product by finding weaknesses using manual and/or automated techniques, then reporting the findings to the vendor and/or the general public (to include threat modeling, C-SCRM)
- **Incident Response Teams:** Those responsible for preparation and reaction to any security event ??

Adjusting our Presentation Filters

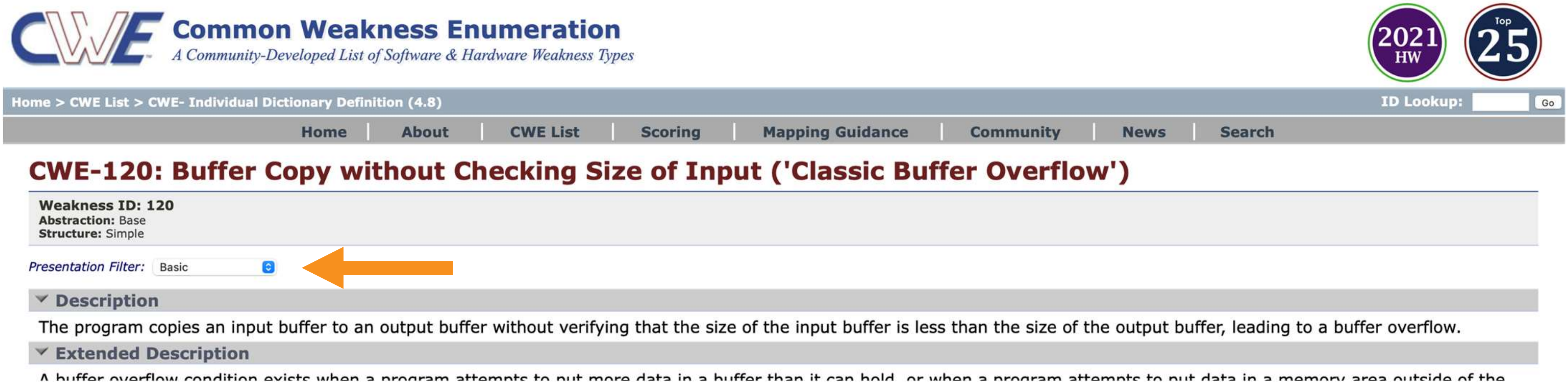
- **“Two-Types” Proposal by Premyslaw Roguski (Red Hat)**

1. Theoretical: users who are more focused on the theoretical aspects of the weaknesses
    - Educators (teachers, professors, solution architects who design the systems' requirements)
    - Technical Writers (people responsible for security content, security blogs and articles)
    - Project and Program Managers who need some level of understanding about security and weaknesses
2. Technical: users who are managing the security issues and need more details about the nature of the weakness and how to prevent this from happening
    - Tool Developers, Security Researchers, Pentesters, Incident Response Analysts
3. (existing) Mapping-Friendly: users who…
4. (existing) Complete:

Proposed Data Elements for Each Group

- **Theoretical:**
  - Description, Extended Description, Alternate Terms, Common Consequences
- **Technical:**
  - Description, Extended Description, Alternate Terms, Modes of Introduction, Demonstrative Examples, Observed Examples, Potential Mitigations, Relationships
- **Mapping-Friendly:**
  - Description, Extended Description, Alternate Terms, Modes of Introduction, Likelihood of Exploitation, Memberships, Notes
- **Complete:**
  - all

How Can we Improve Presentation Filter Awareness?


Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
2021 HW
Top 25
Home > CWE List > CWE- Individual Dictionary Definition (4.8)
ID Lookup:
Go
Home
About
CWE List
Scoring
Mapping Guidance
Community
News
Search

CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Weakness ID: 120
Abstraction: Base
Structure: Simple

Presentation Filter: Basic

Description

The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.

Extended Description

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the

- **Do people know it's there on each entry?**
- **Where else could we draw attention to it (e.g., landing page, how-to/guidance material?)**

Next Meeting – August 24 @ 12pm

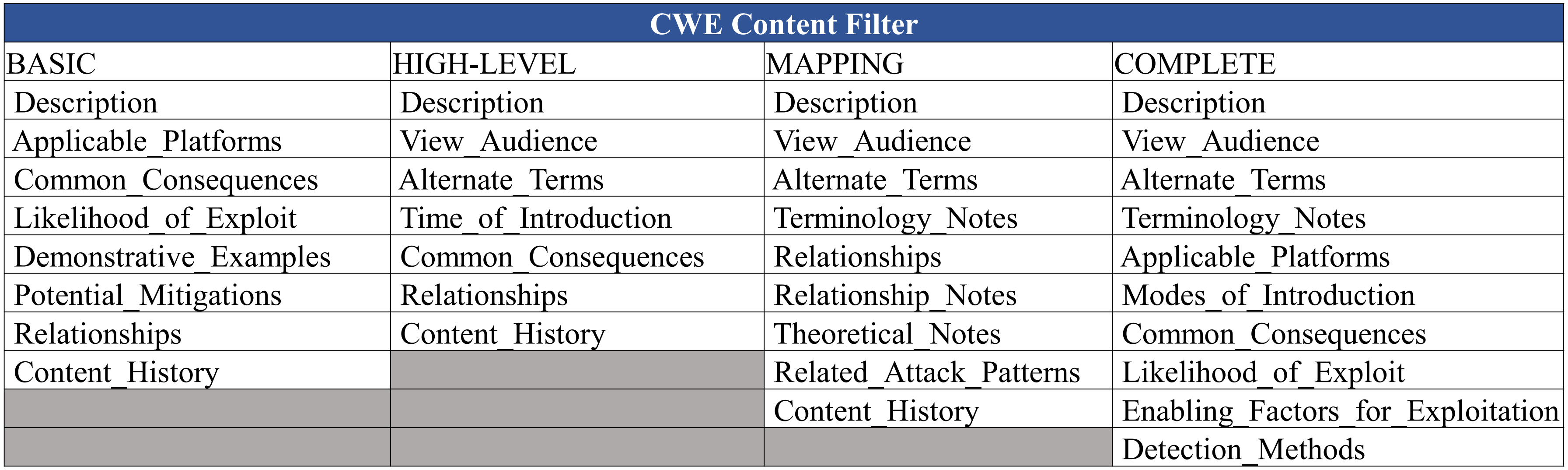
PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

CAPEC@MITRE.ORG

Use Case Scenarios → Content Presentation

- **CAPEC Existing functionality to filter content detail**
  - Basic, High-level, Mapping-friendly, Complete



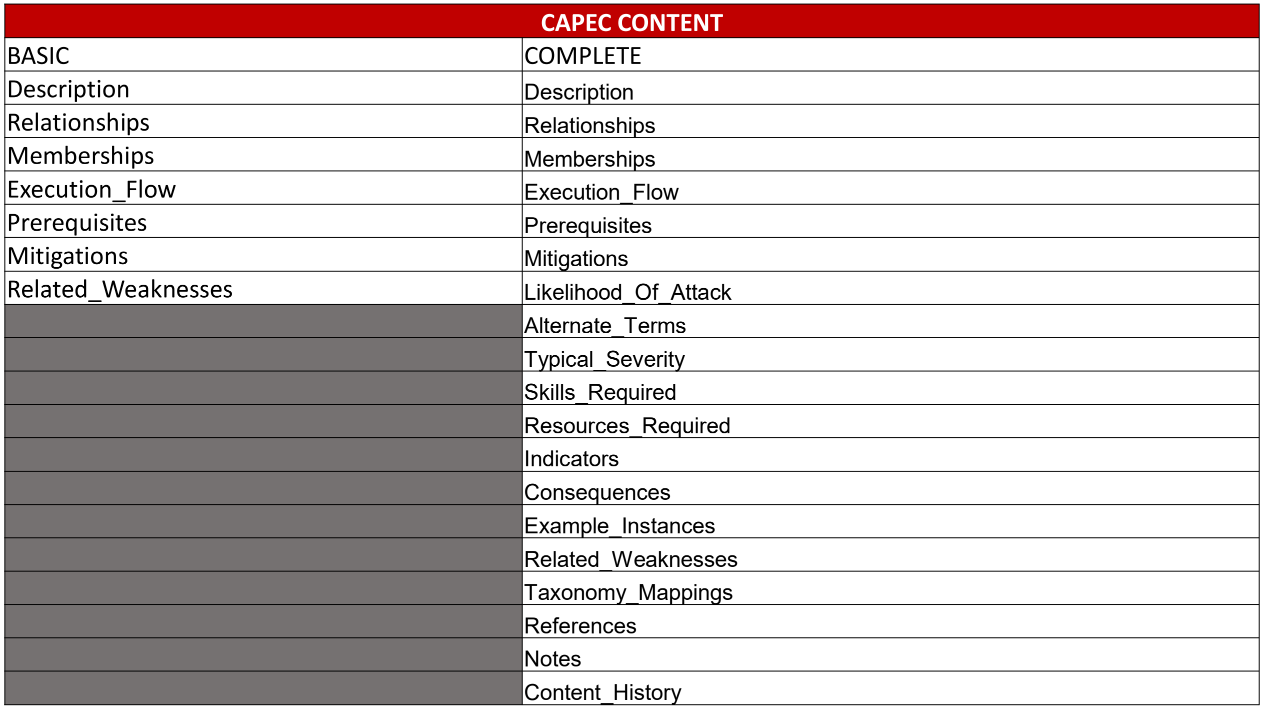
CWE Content Filter			
BASIC	HIGH-LEVEL	MAPPING	COMPLETE
Description	Description	Description	Description
Applicable_Platforms	View_Audience	View_Audience	View_Audience
Common_Consequences	Alternate_Terms	Alternate_Terms	Alternate_Terms
Likelihood_of_Exploit	Time_of_Introduction	Terminology_Notes	Terminology_Notes
Demonstrative_Examples	Common_Consequences	Relationships	Applicable_Platforms
Potential_Mitigations	Relationships	Relationship_Notes	Modes_of_Introduction
Relationships	Content_History	Theoretical_Notes	Common_Consequences
Content_History		Related_Attack_Patterns	Likelihood_of_Exploit
		Content_History	Enabling_Factors_for_Exploitation
			Detection_Methods

and more…

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

Use Case Scenarios → Content Presentation

- **CAPEC Existing functionality to filter content detail**
  - Basic, Complete



CAPEC CONTENT	
BASIC	COMPLETE
Description	Description
Relationships	Relationships
Memberships	Memberships
Execution_Flow	Execution_Flow
Prerequisites	Prerequisites
Mitigations	Mitigations
Related_Weaknesses	Likelihood_Of_Attack
	Alternate_Terms
	Typical_Severity
	Skills_Required
	Resources_Required
	Indicators
	Consequences
	Example_Instances
	Related_Weaknesses
	Taxonomy_Mappings
	References
	Notes
	Content_History