CWE/CAPEC
User Experience Working Group (UEWG)

January 12, 2022

Agenda

- **Housekeeping**
- **Primary Topic:**
  - Status Attributes, "Completeness," and "Qualiteh" in CWE and CAPEC
  - Steve Christey Coley, CWE/CAPEC Technical Lead
- **Question from the Community**
  - CVE data in CWE entries
- **Announcements and Reminders**
- **Adjourn**

Primary Topic

Status Attributes, "Completeness," and "Qualiteh" in CWE and CAPEC

Steve Christey Coley

CWE/CAPEC Technical Lead

The “Status” attribute in CWE and CAPEC

- **Each entry in CAPEC and CWE has a “Status” attribute**
- **Defined in the schema – but how many people know this and look?**
  - Incomplete
  - Draft
  - Stable
  - Usable
  - Obsolete
  - Deprecated
- **Prominently located in individual entry pages (upper right)**
- **Affects public perception of each entry’s “maturity” and “quality”**

Issues with Status

- **Current words can be misinterpreted by consumers**
  - Incomplete – "doesn't give enough information, don't bother"
  - Draft – "still subject to lots of change, don't reference it"
  - Stable – ???
- **As defined since ~2008-2010, Status combines two complementary characteristics:**
  - Completeness: "This entry has a broad range of important information in it"
  - Quality: "All provided information is correct and timely"
- **Reality**
  - Entries don't get a CAPEC or CWE ID unless they're already "pretty good" (usable to many users)
  - Almost everything is Draft or Incomplete
  - Every entry needs regular periodic review, change, and update
  - Status is not regularly reviewed or updated
  - "Quality" is difficult to evaluate

“Required” Elements to Establish Completeness

- UEWG members helped to identify which elements for CWE and CAPEC were most important
- Frequent disconnect with MITRE-determined priorities
- Combining UEWG and MITRE priorities roughly implies “80% of all possible elements are required”
- Insufficient consultation with broader audience

- … CWE and CAPEC seem to have done well, even when most entries don’t have all “high-priority” elements

Currently-Defined "Required" Elements for CWE

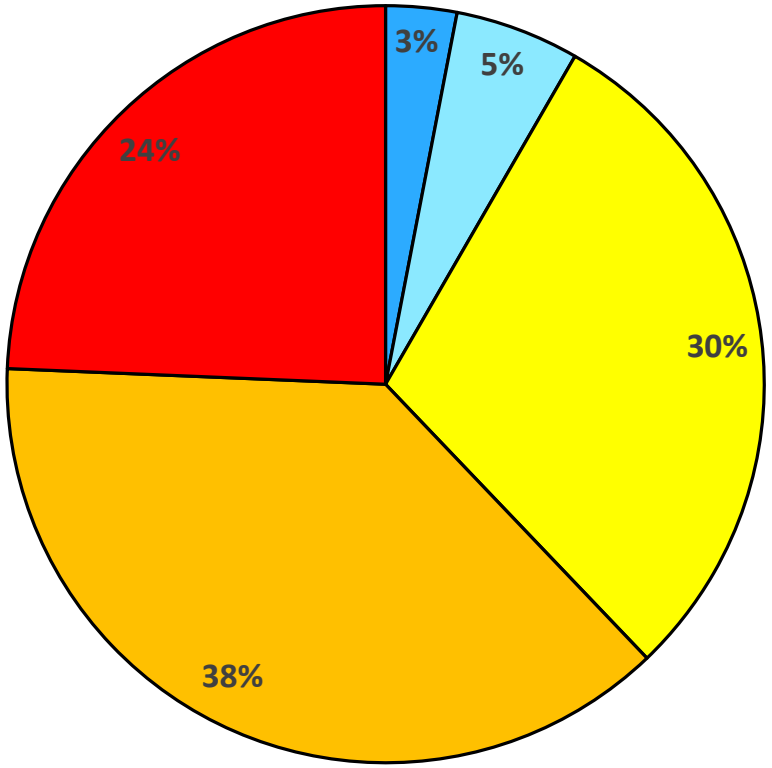
- **WHO**
  - Name (enforced by schema)
- **WHAT**
  - *Summary (enforced by schema – not included in stats in this presentation)*
  - Extended Desc
  - Observed Examples
  - Demonstrative Examples
- **WHEN (see "how")**
- **WHERE**
  - Relationships
  - *Ordinality (primary/resultant – plans to remove; unlikely use except 5+ years in future)*
  - Applicable Platforms
- **WHY**
  - Common Consequences
- **HOW**
  - Detection Methods
  - Potential Mitigations
  - Attack Patterns

(DEMO) Spreadsheet Comparing UEWG and MITRE Priorities

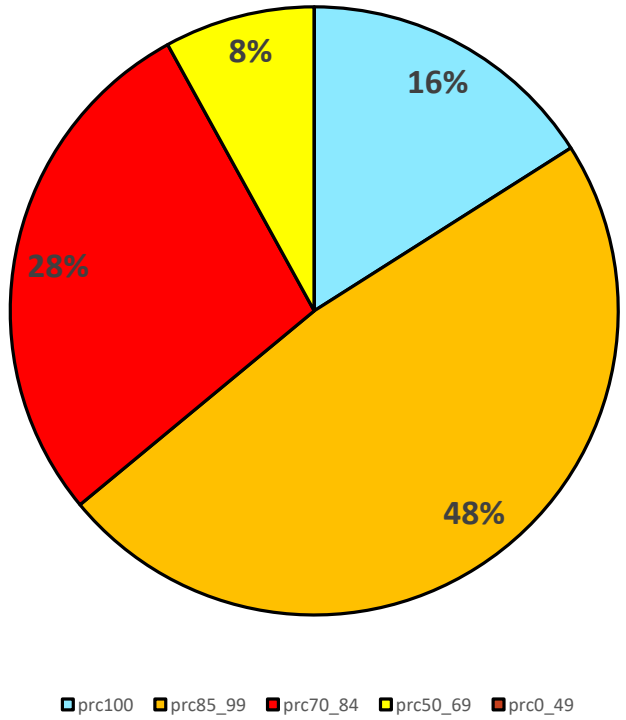
- ***over to excel…***

Completeness Percentage for All Weaknesses in CWE 4.6 (924 entries, 11 "Required" Elements)

- **24% of entries contain between 0 and 49% of required elements**
- **probably mostly quality-related (CWE) entries and MITRE-created classification nodes**

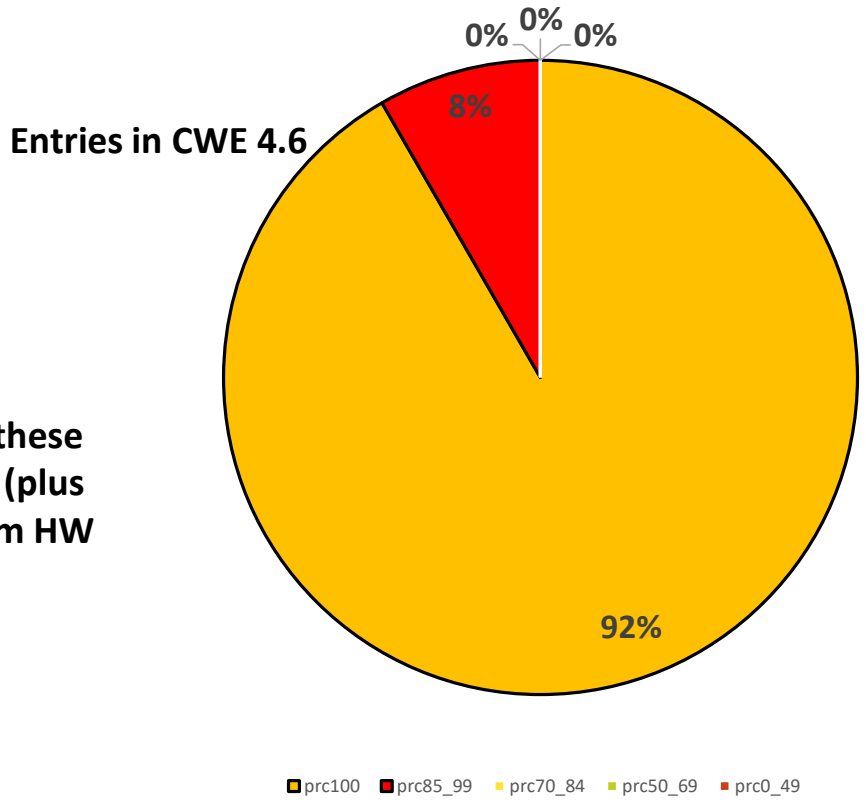


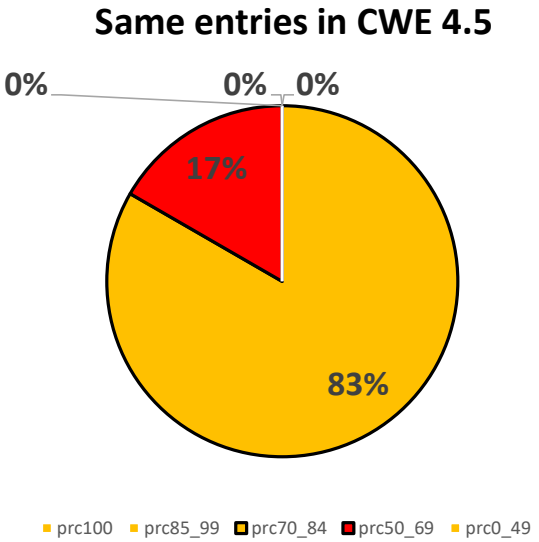
2021 Top 25 Completeness (as of CWE 4.6)



2021 CWE Most Important Hardware Weaknesses (12 entries)

- **Significant focus on these 12 hardware entries (plus Cusp) with input from HW SIG contributors**





Other Potential Changes re: Status

- **Keep primarily for “internal use only”**
  - Remove from individual web pages
  - Keep in raw CWE data for hardcore users
- **Deprioritize in visual display**
  - Move to content history / bottom of page?
- **Change to just numeric “stage” / “maturity” values?**

Proposed Status Name Changes

- **1. Initial / Preliminary (was: Incomplete)**
  - does NOT have all "required" elements
  - might not have perfect desc / name
  - by virtue of having an ID: seems useful/important to CAPEC/CWE teams
- **2. Established (was: Draft - any other words?)**
  - has at least 70% of all "required" elements
  - has desc / name with clearly-defined weakness
  - has no obvious overlap/duplication
  - has no significant maintenance notes
- **3. Stable (no change)**
  - no significant changes expected for the future
  - has all high-priority required elements
  - has well-defined desc / name
  - has zero overlap/duplication
  - has all additional preferred and optional elements (when possible)
  - all elements have undergone defined quality review from CWE leads and/or external community
- **Remove "Usable" (0 entries in CWE, 2 in CAPEC)**
- **Keep Obsolete / Deprecated**

Future Planning: Federated Submission/Publication Modes

- The CWE team is getting more external submissions, of different ranges of “completeness,” “quality,” and “scope”
- The volume could increase significantly as the submission process is simplified
- Experience of CVE (and many other public knowledge bases) shows consistent battles with initial contribution “quality”

Question from the Community

Can you explain the rationale behind which CVEs are used as "Observed Examples" in CWE entries?

Observed Examples in CVE

- Many CWE entries contain old CVEs as observed examples:
  - CWE-79 (one from the Top 25 CWEs) https://cwe.mitre.org/data/definitions/79.html
  - The newest example CVE is from 2017, most examples are from 2006-2007!
- Many CVEs - even if old - were chosen "by hand" because they had well-written references, were the canonical examples, etc.
- CVEs are also often listed in a particular order from easy-to-difficult
- We intend to try and strengthen CWEs with improved CVE examples, where possible. We encourage specific recommendations from the community!
- Possible change: add a doc string to the individual web page to make it clear that these were intentionally chosen

Announcements and Reminders

Announcements and Reminders (1 of 2)

- **CAPEC Community Summit**
  - February 23, 2022
  - Focus: Program improvements, education and awareness, and modernization.
  - Participate in discussions around:
    - Assessing CAPEC offerings
    - User perceptions
    - Mitigating supply chain attacks with CAPEC
    - Using CAPEC's execution flows (steps to perform an attack) as a playbook for pen testing
    - Vision shaping for the future of the program
    - Other topics suggested by attendees

Announcements and Reminders (2 of 2)

- **CWE/CAPEC Feedback Request**
  - Short survey
  - What do you think about the topics being covered through our blog and podcast, Out-of-Bounds Read? Did you know we had them??
  - Is there anything else that you want to see or learn more about? We invite you to take a few minutes to share your thoughts today!

Next Meeting (Wednesday, February 9)

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG **CAPEC@MITRE.ORG**