CPE – Common Platform Enumeration
CWE – Common Weakness Enumeration
CVE – Common Vulnerability Enumeration

Mapping a CPE to the UCKG would involve linking various entities such as software, hardware, and vulnerabilities in a structured and interconnected manner. As such, it is important to incorporate CWEs and CVEs to establish links and represent specific instances of vulnerabilities. A CPE outlines the

Below are a few steps to help elucidate the process of establishing links between these entities:

1. Define Entities: Identify the key entities in the knowledge graph such as software, hardware, vulnerabilities, and weaknesses. In a paper – "UCO: A Unified Cybersecurity Ontology[1]" the researchers mention that the CPE was not yet incorporated into the ontology since the data regarding CPEs was not publicly available.

2. Link CPEs to Entities: CPEs enable powerful querying based on their structures (CPEnameIDs…). Use CPE identifiers to represent software and hardware entities. Each CPE entry contains information about a specific platform, including vendor, product, and version information. In the case of our UCKG**, I propose we add a new node called ucoCPE that is a subclass of ucoPlatform which are both subclasses of existing node ucoUCOThing**. This mirrors how the CWE, CCE, and CVE nodes exist within the UCKG.

3. Link CWEs to Entities: Use CWE identifiers to represent specific types of weaknesses that may exist in software or hardware entities. Each CWE entry describes a common type of software or hardware weakness.

4. Link CVEs to Entities: Use CVE identifiers to represent specific instances of vulnerabilities that have been discovered in software or hardware entities. Each CVE entry provides details about a particular vulnerability, including affected versions and potential impact.

5. Establish Relationships: Establish relationships between entities based on known associations. We can link CVEs to the affected CPEs and CWEs to describe the specific weaknesses exploited by those vulnerabilities.

These steps can ease the integration of the CPE type into the UCKG, the integration of this data can further the goal of supplementing information about a platform/version/release of a certain hardware or software.

References

1. (PDF) UCO: A unified cybersecurity ontology. (n.d.). https://www.researchgate.net/publication/287195565_UCO_A_Unified_Cybersecurity_Ontology