Tactics to Technical Impacts Mapping Rationale

In order to connect mitre’s 11 attack tactics to Common Weakness Enumerations (CWEs), it is necessary to find a common link between the consequences of CWEs and what the tactics are attempting to exploit in a software system. This mapping explores which attack tactics can be used to exploit the 8 technical impacts caused by CWEs detectable using static analysis, which includes 18 different CWEs. Traversing between attack tactics and technical impacts provides a way to connect the tactics to the CWEs.

This mapping was created by analyzing mitre’s definition of each attack tactic and which techniques fall under each tactic (https://attack.mitre.org/wiki/Main\_Page) against examples of CWEs that result in each of the 8 technical impacts (<https://cwe.mitre.org/community/swa/detection_methods.html)>. CWEs list a number of code examples that result in the weakness arising as well as their scope, such as Access Control, Authentication, or other aspects of Security. Using this evidence along with intuition enabled an initial mapping to be drawn between the tactics and technical impacts.

Future work could investigate how these mappings may change or develop over time as more examples of attack tactics are witnessed in conjunction with exploited CWEs. For instance, it may be found that the tactic Credential Access is often used to exploit CWEs causing the technical impact Bypass Protection Mechanism, and in this case, an edge should be added in the mapping to link these two vertices.