Analyzing Cyber Threats Using Graph Database Technology

Using the ATT&CK Matrix and CWE/SANS to Identify and Analyze Software Weaknesses

Alejandro Zeno-Miranda & Daylyn Hoxie | REU Mentor – Dr. Clemente Izurieta | August 2019

Introduction

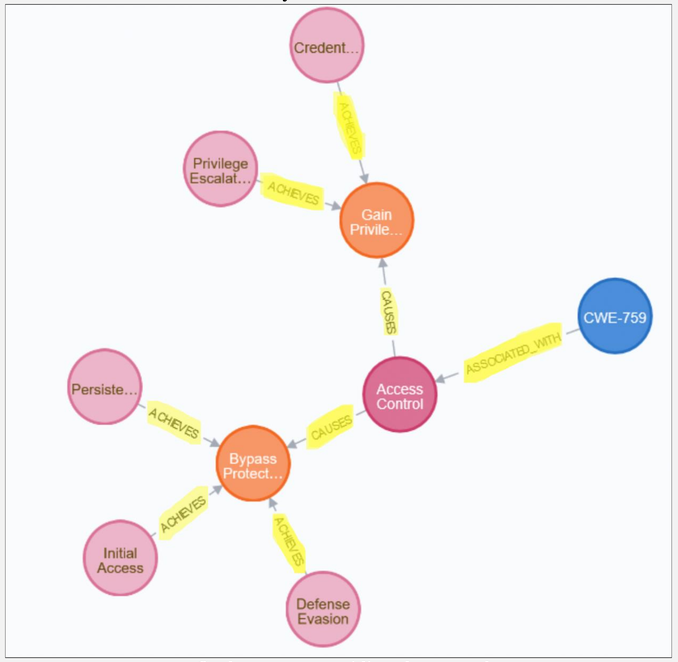
- Cyber adversaries use many different behaviors when compromising target enterprises.
- The MITRE ATT&CK Matrix [1] further divides these behaviors as techniques that may be used to achieve a tactic.
- The 2011 CWE/SANS Top 25 Most Dangerous Software Errors [2] identifies common and widespread software security weaknesses.
- Connecting an ATT&CK tactic to a CWE through the technical impacts caused by CWEs allows for cause-and-effect analysis of an attack, gives insight into the goals of an attacker's exploit, and allows for improved prioritization of software weaknesses requiring attention.

Keywords

- CWE(Common Weakness Enumeration): a community-developed list describing common software security weaknesses.
- ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge): MITRE's knowledge base of threat tactics and techniques used by cyber adversaries.
- Technical Impacts: consequences of CWEs that describe resources or information an attacker may exploit.
- Technical Debt: the implied cost of the choice of an expedient solution in the short term that may cause difficulty in future changes.

Graphing Tactics to CWE

- Using the Neo4j graph database management system [4], relationships between CWEs and attack tactics can be found in a meaningful and easy-to-read model.
- The mapping of attacker tactics to CWE impacts [3] provides a connection between attack tactics and technical impacts, allowing for a mapping from attack tactics to CWEs using the Cypher [4] query language.
- Relationships between CWEs provide insight to similar weaknesses a user may want to examine.



Cypher query providing above result:
MATCH (t:Tactic)-[:ACHIEVES]->(i:Impact)<-[:CAUSES]-(c:Consequence)<-[:ASSOCIATED_WITH]-(w:CWE) WHERE w.id = "CWE-759" RETURN t, i, c, w

Future Work

- Integrate livestream data to update database
- Technical debt quantification from attack behaviors
- Prioritization of CWEs based on ease of exploitation
- Integrate database with Java for ease of use

Proof of Concept

- A sample database was created to associate all 12 tactics and 244 techniques from ATT&CK Enterprise with the CWE/SANS Top 25 most common CWEs [3].
- Connections between the Top 25 CWEs and their related CWEs were created using the ChildOf, CanAlsoBe, ParentOf, MemberOf, CanPrecede, CanFollow, and PeerOf relationships listed [2] on MITRE's website.
- The sample database can be expanded upon to contain all CWEs listed on MITRE and update with MITRE's updates of CWE and ATT&CK listings.

Conclusion

- Attack tactics can be linked to exploitable CWEs by way of technical impacts.
- The mapping of attack tactics to weaknesses within a graph database provides easy interpretation of cause-and-effect relationships from both developer and operational responder (SecDevOps) perspectives.
- Providing connections between attack tactics and weaknesses within a graph database allows for better management of technical debt and prioritization of refactors.

References

[1] MITRE ATT&CK. The MITRE Corporation, 25 April, 2019, https://attack.mitre.org.
[2] CWE - Common Weakness Enumeration. The MITRE Corporation, 20 June, 2019, https://cwe.mitre.org.
[3] C. Izurieta, M. Prouty, "Leveraging SecDevOps to Tackle the Technical Debt Associated with Cybersecurity Attack Tactics", TechDebt'19. Montreal, Canada, May 2019.
[4] Neo4j Graph Platform. Neo4j Inc., 2019, https://neo4j.com.

softwarefactory
NSF
MONTANA STATE UNIVERSITY