Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting

Cameron Noakes

November 2021

1 Sentence Overview

This paper attempts to link MITRE ATT&CK, NIST CWEs, CVEs and CAPEC together. This paper takes five browsers and compares their severity ratings of CVEs to determine motives behind attacks and how attacks will be executed.

The researchers data mined datasets to expand on defense utilities.

2 Introduction - Notes

In this paper the researchers data mine a set of information sources (datasets) to expand on defense utilities for threat hunting and pursuing APTs.

The researchers combine the information sources with a graph framework of 'BRON', which provides the convenience of unification because the sources are independent but have relational links between them. These links improve technical efficiency when scripting queries and running on the graph.

3 Data Sources - Notes

General definitions of CVE, CWE, Mitre and NVD, my paper assumes the reader is familiar with these concepts already so no need to take notes on.

The motive and reasoning behind the paper:

"Attack Patterns often lack links to either a Weakness or a Technique." which concludes an explanation of why the researchers propose a link between CVEs,CWEs, Mitre Attack and alike.

4 BRON - Notes

BRON is a graphing system discussed by the researchers but is not a lot of information regarding it on Google.

BRON is a relational graphing system which represents the entries of its information sources as specific types of nodes. BRON is populated by downloading data from the information sources. BRON is said to expand on the capabilities of Mitre Attack to aid threat hunting. Further information outlining how BRON works is given but out of scope.

5 Exploring BRON for Security Insights

Brief explanation of how threat hunters methodology is ascertained and their thought process when infrastructure is under attack by APTs.

6 Threat Tactics and Affected Products

Examples of Mitre Attack techniques and subtechniques are given to provide clarity to how attacker steps and methodology can be different.

Various explanations of why outdated software is bad for security and how administrators should be alerted whenever this is the case.

This section did not have much else apart from the above.

OPINION: This paper is not very advanced, formatting issues are present and a lot of explanations of things that can be easily googled like Mitre Attack techniques, CVEs, and explanations of CWE top 25 lists.

7 Web Browser threat analysis

"We then examined their security scores across all the occasions they were referenced as an affected product configuration of a Vulnerability (CVE)"
they didn't say how they assessed the scores, doesn't make much sense to me.

The BRON model traces back CVEs to its weaknesses (but you don't need a model for this as the CVEs outline where they are present.)

8 US-CERT Alerts

Some good rhetorical questions are outlined:

"what Tactics and Techniques drive them and what Attack Patterns feature the abstract Weaknesses they instantiate?"

BRON finds the weaknesses associated with each CVE which can result in concluding attack patterns and then from there traces the technique to a specific tactic outlined in the Mitre Attack matrix. Acknowledgement is given of how every weakness cannot be linked to an attack pattern.

9 ANALYZING BRON'S SOURCES

The researchers analysed the BRON data to explore how connected and comprehensive the entries are and how the data has changed over time. The researchers exclaimed how they start by aggregating the number of entries and investigating the connectivity between them to be able to observe 'floating entries' or ones that are isolated.

The number of affected product configurations decreased by approximately 80 percent with the use of BRON, with regards to attack patterns, there are

519 attack patterns in total, 25 percent of which are Floating Entries.

The large portion of floating vulnerabilities indicates a gap between the data and informing its users of the vulnerability.

The mean number of links from a Tactic to a Technique is 28.4, and the mean number of Weakness links is 8.16.

10 Related Work

The researchers compared the BRON model for graphing to that of various other systems, they studied and analyzed NVD and pointed out several limitations which proposed the reasoning behind using BRON.

Details how there are various multiple threat modelling methods and goes to list some examples:
STRIDE, PASTA, LINDDUN.

BRON uses a single graph to connect entries from sources ranging from tactics to vulnerable software versions.

BRON could enhance some example approaches such as including more than the Mitre Attack and unify inter-source linking.

11 Future Work

In the future researchers outline how they plan to analyse and to align comparisons along a date or age of product. We have not studied data source entity similarity (connections), only similarity between data sources, if in the future this work was to be revisited entity similarity would be studied.

Performance of the BRON graphing system is mentioned to become better and more efficient with future work.

12 Research Gaps and Questions

more research and explanations for the BRON system are required for the reader of the paper.

What are the applications of BRON? Is it only threat modelling?

13 What problem does this solve?

This paper attempts to link , NIST CWEs, CVEs and CAPEC together. One way they do this is to compare vulnerability severity ratings of browsers to one another. A system is used known as BRON which provides the convenience of unification because the sources are independent but have relational links between them.

14 How do they solve it?

They solve the current problem by providing a solution of linking all the topics and regions together through a graph mapping node system a.k.a BRON.

15 How do they assess it?

the researchers did not say how they would assess the BRON model in order to determine key features and extract information in order to create a real world change.

16 Conclusion - Notes

no conclusion.