Interactive Visualization Dashboard for Common Attack Pattern Enumeration Classification

ICSEA 2022 Conference

By: Joi Bennett, Mounika Vanamala, Walter Smith and Xiaohong Yuan

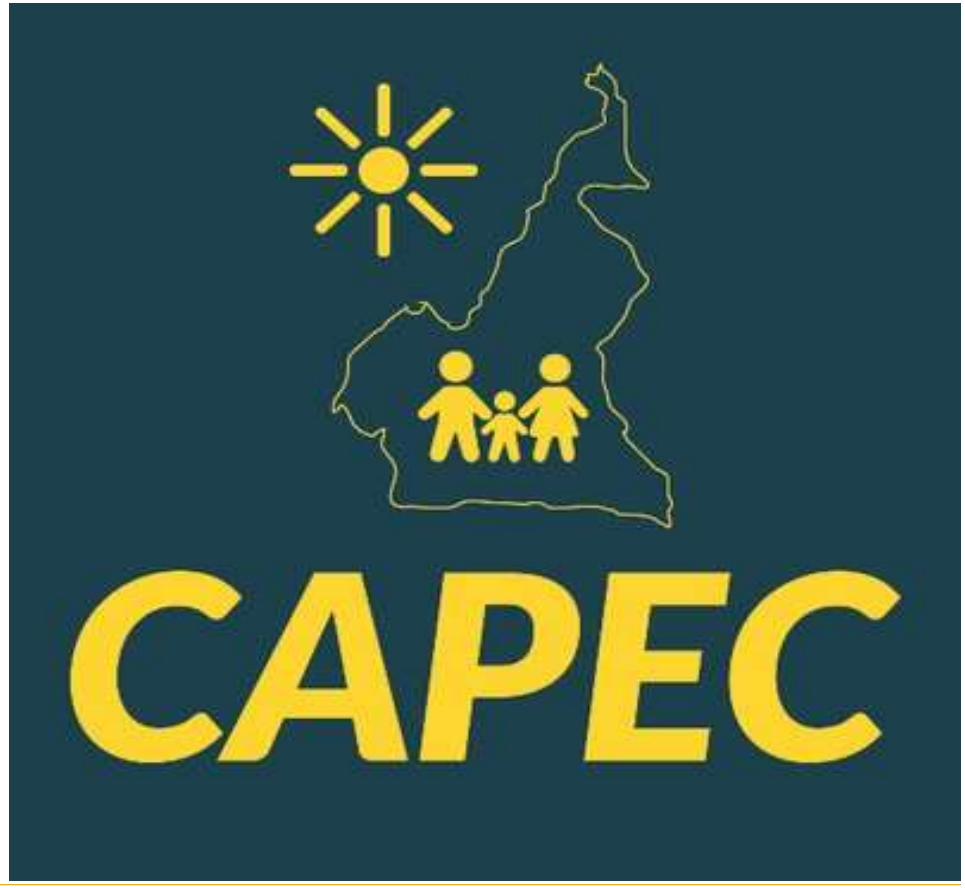
North Carolina Agricultural and Technical State University

OUTLINE

I. Introduction
II. Background
III. The CAPEC Visualization Dashboard
IV. Related Work
V. Conclusion and Future Work
VI. References

Introduction

- The current CAPEC release includes a list of 572 specific attack patterns.
- The goal of this research is to improve usability and provide a range of new capabilities for understanding and interacting with the rich content and relationships in CAPEC.
- Navigation of CAPEC web content relies on following parent-child hyperlinks in textual content.

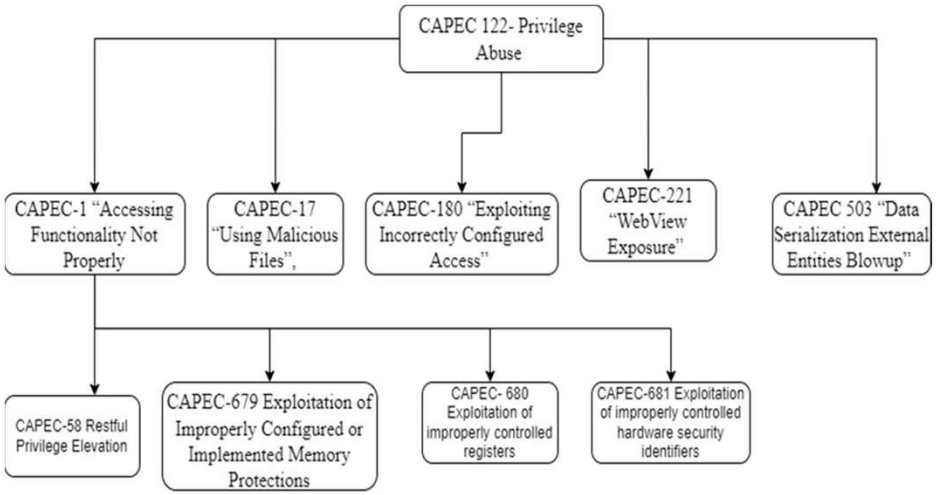


Background

CAPEC

- CAPEC attack patterns
- CAPEC attack are organized with parent and child hierarchy.

CAPEC-1, CAPEC 122, CAPEC-17, CAPEC-180, CAPEC-221.CAPEC-58,CAPEC-679,CAPEC-680,CAPEC-681



Background

Tree Map

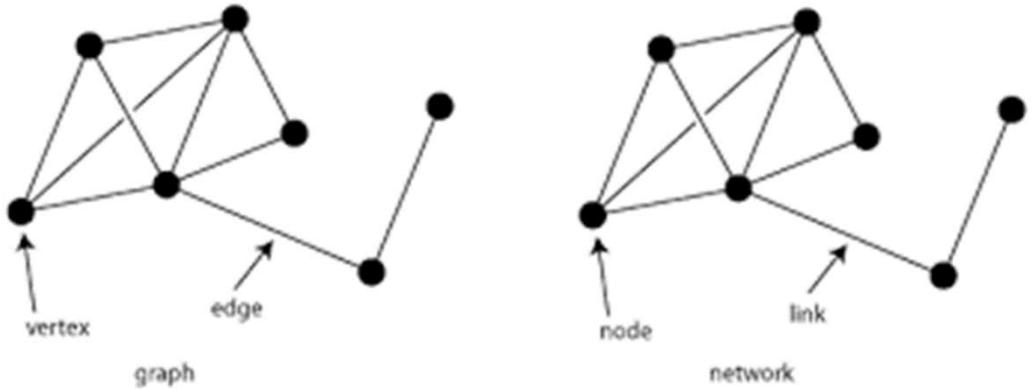
- Tree maps use rectangular space-filling layout.
- Rectangular and radial layout
- Basic tree map

Background

Network Graph

- Node-link diagram is the most common representation.
- visualize tree or hierarchical relationship.
- Not all of the nodes and links are created equally

Example of network graph



Background

Dash

- Plotly's dash library
- Dash-html components
- Interactivity is implemented with callbacks.

The CAPEC Visualization Dashboard

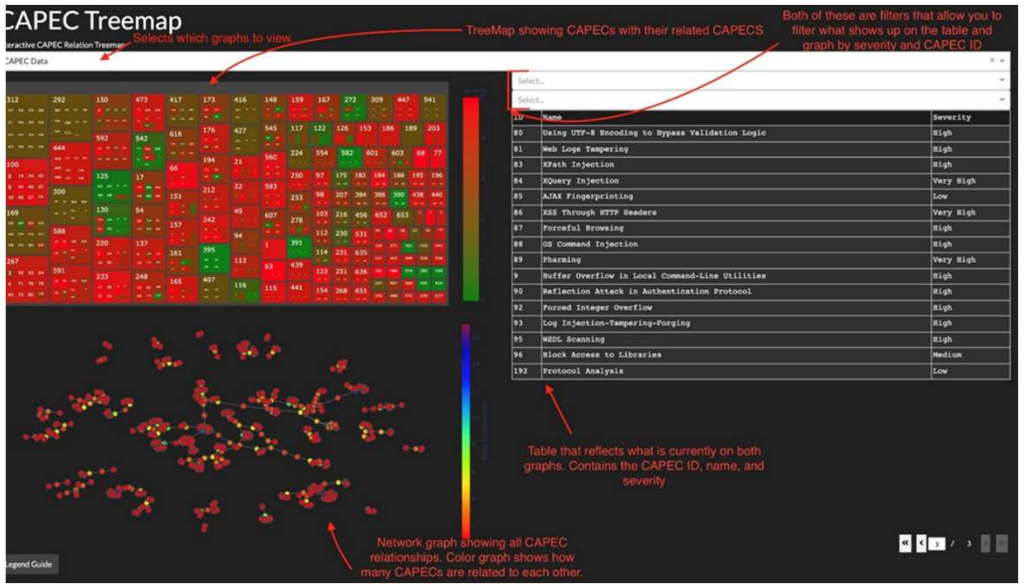
CAPEC attack Patterns

- Presents unique visualizations techniques for navigating the CAPEC taxonomy.
- Tree maps and network graphs are implemented using Dash, Plotly, Heroku, and MongoDB.
- The data obtained from MITRE'S CAPEC website in the form of a CSV is hosted on a MongoDB database.

Visualization of the CAPEC Data

- Visualization of CAPEC Data
- Graph display
- CAPEC Data or External Mapping
- Visualization of a tree map created using Plotly
- CVS is created with the columns parent, child, and severity.
- A network graph showing how a CAPEC attack pattern is related to other CAPEC attack patterns.

The figure below demonstrates the tree map and network graph to visualize CAPEC data

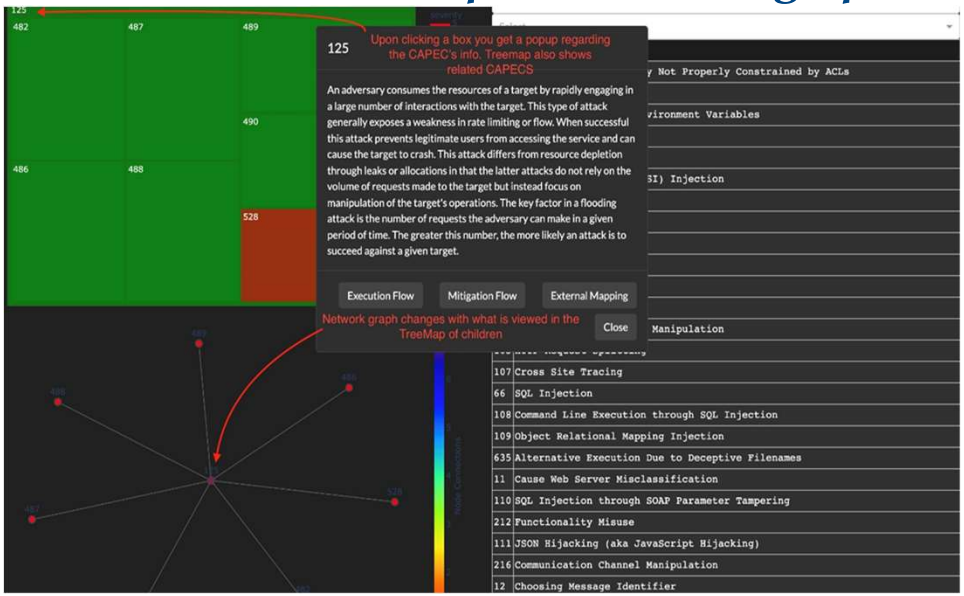


Visualization of the CAPEC Data

Continued

- Visualization dashboard allows user to select a CAPEC ID from the tree map to view detailed information of the CAPEC attack pattern.
- For example, in figure 3, if a user click on CAPEC-125 in the tree map, a window will pop up showing the description of CAPEC-125

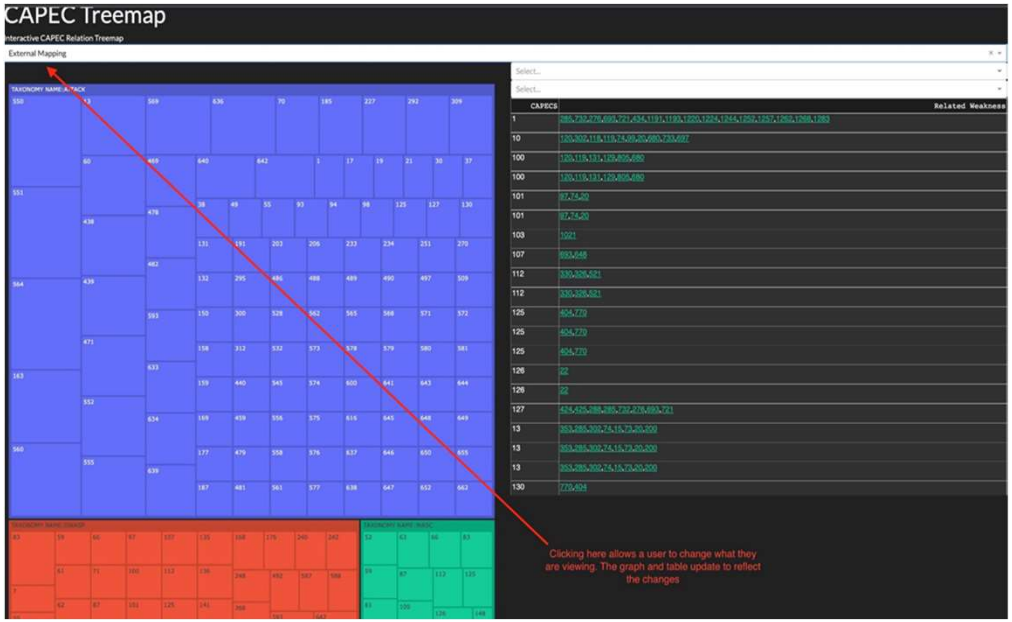
Figure 3 demonstrates the interaction between the tree map and network graph



Visualization of the CAPEC External Mapping

- The CAPEC attack patterns are mapped to ATT&K, OWASP, WASC and CWE weaknesses.
- In the figure , the left top rectangle in blue color shows the CAPEC IDs that are mapped to the ATT&K taxonomy.
- The left bottom rectangle in orange color shows the CAPEC IDs that are mapped to OWASP.
- The right bottom rectangle in green color shows the CAPEC IDs that are mapped to WASC.

Figure 4 demonstrates the attack patterns that are mapped to these taxonomies

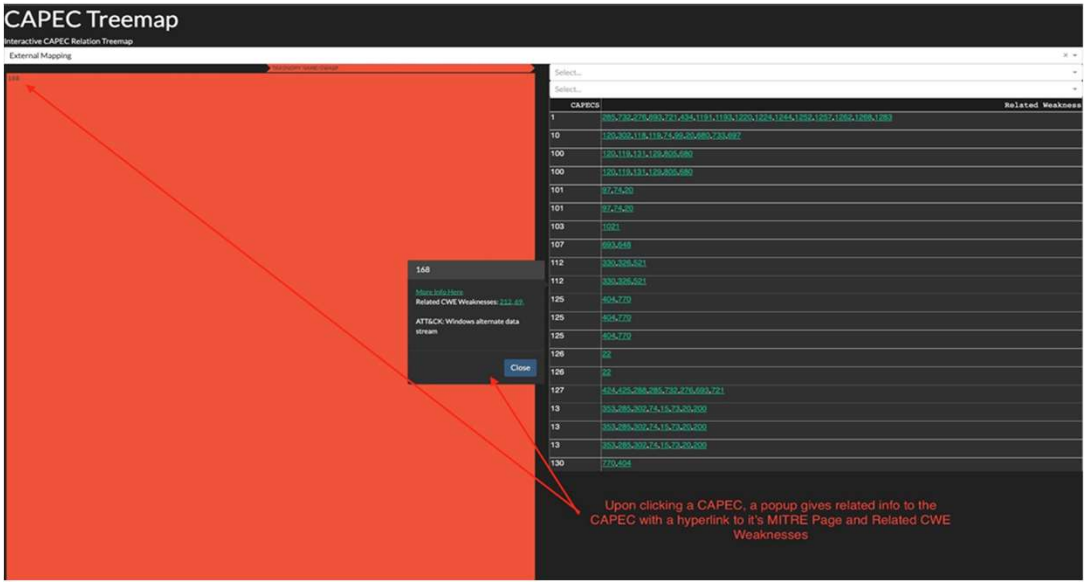


Visualization of the CAPEC External Mapping

Continues

- User can select and CAPEC ID
- Dashboard demonstrates the external mapping of any particular attack pattern.
- Figure 5 demonstrates the CAPEC-168.

Figure 5 demonstrates the pop up window to display external mapping information of CAPEC attack pattern.



CAPEC Treemap

- Website demonstrates different attacks of CAPEC through their taxonomy name.
- The interactive CAPEC relation treemap.

- https://ncat-app.88vos00tcm0k8.us-east-2.cs.amazonlightsail.com/

Related Work

- Noel visualized the overall hierarchical structure of CAPEC attack patterns using network graph, Sunburst visualization, Circular tree map, and Voronoi tree map.
- Conducted text mining and computed hierarchical clusters and grouped related attack patterns through automatic analysis.
- Used bipartite graph to visualize cross references from CAPEC attack patterns to CWE weaknesses.
- The goal of our tool is to allow users to receive such information easily.

Related Work

Continues

- Regainia and Salva proposed a methodology that takes as inputs CAPEC attack patterns, and infers relationships between attacks, weaknesses, security principles and patterns to generate the classification and Attack Defense Trees.
- Used software repositories like CVE(Common Vulnerabilities and Exposures) and CAPEC to help develop secure software.
- Developed a recommender system that recommends attack patterns relevant to the system under development based on software requirements and design documents.

Conclusion and Future Work

- Describe a web-based interactive visualization dashboard for the CAPEC attack patterns.
- Hierarchical structure of CAPEC attack pattern using tree map and network graph.
- The goal of this research
- This tool will help users to make use of CAPEC attack patterns.
- Developing secure software or conducting other security activities.
- For our future work, we want to conduct user study for the dashboard to assess the effectiveness of the tool in helping users understanding the structure of CAPEC.
- Make use of CAPEC attack patterns in their security tasks.

References

- [1] The Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/
- [2] Balzer, M., Noack, A., Deussen, O., & Lewerentz, C. (2004). Software landscapes: visualizing the structure of large software systems. In IEEE TCVG.
- [3] Johnson, B. (1992, June). TreeViz: treemap visualization of hierarchically structured information. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 369-370).
- [4] Scheibel, W., Trapp, M., Limberger, D., & Döllner, J. (2020). A taxonomy of tree map visualization techniques. In VISIGRAPP (3: IVAPP) (pp. 273-280).
- [5] Vliegen, R., Van Wijk, J. J., & van der Linden, E. J. (2006). Visualizing business data with generalized treemaps. IEEE Transactions on visualization and computer graphics, 12(5), 789-796.
- [6] Stančin, I., & Jović, A. (2019, May). An overview and comparison of free Python libraries for data mining and big data analysis. In 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 977-982). IEEE.
- [7] Plotly. "Introduction to Dash". https://dash.plotly.com/introduction
- [8] Heroku. https://www.heroku.com/home
- [9] MITRE ATT&CK. https://attack.mitre.org/
- [10] OWASP. https://owasp.org/
- [11] The Web Application Security Consortium (WASC). Threat Classification. http://projects.webappsec.org/w/page/13246978/Threat%20Classification

References

- [12] Common Weakness Enumeration. https://cwe.mitre.org/
- [13] Fekete, J. D., & Plaisant, C. (2002, October). Interactive information visualization of a million items. In IEEE Symposium on Information Visualization, 2002. INFOVIS 2002. (pp. 117-124).
- [14] Noel, S. (2015). Interactive visualization and text mining for the capec cyber-attack catalog. In Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics.
- [15] Regainia, Loukmen & Salva, Sébastien. (2017). A Methodology of security pattern classification and of attack-defense tree generation. The 3rd International Conference on Information Systems Security and Privacy, DOI:10.5220/0006198301360146.
- [16] Seehusen, F. (2015, June). Using CAPEC for risk-based security testing. In International Workshop on Risk Assessment and Risk-driven Testing (pp. 77-92). Springer, Cham.
- [17] M. Vanamala, X. Yuan and K. Roy, Topic modeling and classification of common vulnerabilities and exposures database. 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD 2020).
- [18]. V. Mounika, X. Yuan and K. Bandaru, Analyzing CVE database using unsupervised Topic Modelling," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), 2019, pp. 72-77, doi: 10.1109/CSCI49370.2019.00019.
- [19] M. Vanamala, J. Gilmore, X. Yuan and K. Roy, Recommending attack patterns for software requirements document, 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 1813-1818, doi: 10.1109/CSCI51800.2020.00334.

Thank You