Automating Cybersecurity Attack Behavior Analysis and Detection using Graph-driven Algorithms

Yonghyun Kim, Madhukar Shrestha, Jeehyun Oh
Faculty Advisors: Dr. Junghwan (John) Rhee, Dr. Grace Park, Dr. Fei Zuo

COMPUTER SCIENCE

UNIVERSITY OF Central Oklahoma

1 PROBLEM AND MOTIVATION

According to American Advisor Groups, there is a cyber-attack every 39 seconds, an average of 2244 incidents a day. These cyber-attacks involve exploiting software's weaknesses, common in most programs. Once attackers break into a computer system, in addition to the damage to the software often pursue privilege escalation and other following attacks with stronger Capabilities to pursue further and wider damages.

Cyber-attack damages may encompass files, accounts, software, and operating systems. Automating cybersecurity incident analysis and narrowing down the scope of analysis is essential to speed up the analysis and respond to the attacks faster, which is an important value for Security Operation Centers (SoCs).

2 OBJECTIVE

This project focuses on designing and implementing automated attack investigation and detection techniques based on graph structures.

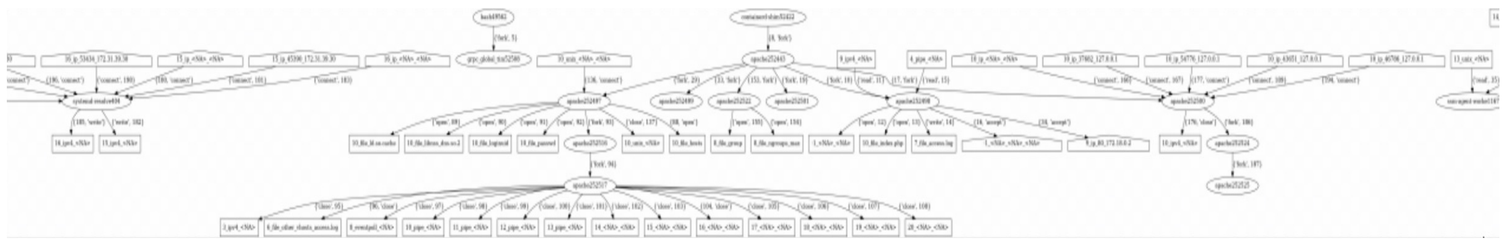
- Due to a large body of information, we implement a backtracking mechanism to automate a laborious intrusion analysis.
- We implement an attack detection approach that compares a benign state and a state under an attack detecting suspicious activities based on divergence from the normal graph structure.

3 BACKTRACKING ALGORITHM

```
foreach event E in log { /* read events from latest to earliest */
    foreach object O in graph {
        if (E affects O by the time threshold for object O) {
            if (E's source object not already in graph) {
                add E's source object to graph
                set time threshold for E's source object to time of E
            }
            add edge from E's source object to E's sink object
        }
    }
}
```

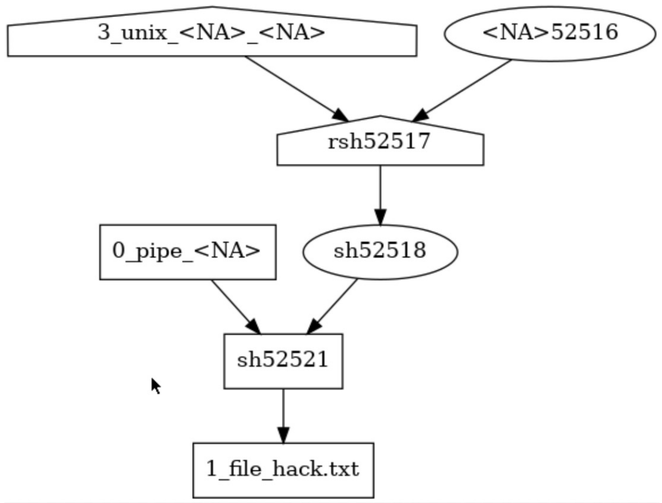
The backtracking algorithm reconstructs a timeline of events during a cyber-attack by following their dependencies.
1. The backtracking algorithm goes over all the processes and saves timelines and information about them.
2. After reviewing all the processes once, it goes back to the beginning to analyze the relationship between each process.
3. If processes do not have any relationship with the suspicious process, it is filtered the unrelated process out.

4 DEPENDENCY GRAPH



- The above graph is a part of the whole complex graph.
- Each node indicates a process, a file, or a network address. Edges connect processes and the resources that are used. Therefore, we can see the process hierarchy and the detailed attack behavior occurred during an attack scenario.
- The total number of nodes of this big graph was 53880.

5 REDUCING THE GRAPH



- Despite the total number of dependency graph nodes is as high as 53880, the number of nodes essential to an attack can be reduced to 7 using the backtracking algorithm.
- Unrelated activities were filtered out and the suspicious activity is only remained.
- Due to the above simplified dependency graph, we can easily find the "1_file_hack.txt" file is resulted in the victim computer after an interaction of a few processes.

6 EVALUATION RESULT

Vulnerable Case	The number of nodes in the whole graph	The number of nodes in the reduced graph	% of the reduced graph
CVE-2018-19518	53880	7	0.000123
CVE-2021-41773	47968	10	0.000208
CVE-2021-42013	49720	10	0.000201
CVE-2021-35042	193549	4	0.000021

7 CONCLUSION

- The result shows the implementation of backtracking algorithm filters out nodes unrelated to the cyberattack effectively.
- There result shows that the algorithm can effectively make the analysis and detection of cybersecurity attacks more efficient.

8 FUTURE WORK

- We are working on an automated intrusion detection algorithm using a deep learning technique and natural language processing.
- Combining graph reduction techniques and AI based attack detection mechanism can produce an efficient cybersecurity solution.

9 REFERENCES

- Samuel K., Peter C., "Backtracking Intrusions", *Department of Electrical Engineering and Computer Science at University of Michigan*. 19 October, 2003.
- Martin G., Martin R., Matthias K., Bogdan F., Erhard R. "Intrusion Detection on System Call Graphs. February, 2018.
- AAG. "How often cyber attacks occurs?". Web. June 19, 2020