Advanced Computer Forensics
Ruiyang Liu 85C576
Conference Paper Summary – Group #2

Paper selected: Analyzing Multiple Logs for Forensic Evidence
Paper author: Ali Reza Arasteh, Mourad Debbabi, Assaad Sakha, and Mohamed Saleh
Word count: 569 word

In recent years, attacks on IT system have increased at an incredible speed, and especially for cyber security and attacks. As defenders, an important area is security forensics, since we need to gather, process, and analyze evidence. When we look back to previous works, there are some works focus on gathering informations as forensics, but there is little works can both automate and formalize forensic science and evidence.

Current researches on formal and automatic analysis of forensic evidence can be categorized into baseline analysis, root cause analysis, common vulnerability analysis, timeline analysis and semantic integrity check analysis.[1] Moreover, there are some contribution focus on log analysis and correlations, especially alert correlation. However, as we look deeper into these works, they are mainly focus on correlation, intrusion detections, etc. But, formal forensic log analysis and formal verification is a huge and important part in forensic science. In short, this paper propose a new approach for log analysis which is based on computational logic and formal automatic verification.

To explain, the paper uses computational logic to transit log informations into abstract events, and construct tree of events to model of logs. As a result, the model contains terms of algebra in a tree-way. The whole logging system is modeled as a tree which is able to represent possible different interleaving of events from the logs. As mentioned, the paper need to find a proper way to express the logic and relations of logs. The paper choose a temporal, dynamic, modal, and linear logic which is called ADM. These features are useful in gathering and expressing forensic properties and system invariants. In the end, the paper put things together into a tableau-based proof system which contains model checking algorithms.

---

[1]Analyzing Multiple Logs for Forensic Evidence, Ali Reza Arasteh, Mourad Debbabi, Assaad Sakha, and Mohamed Saleh

When constructing the model of log systems and express some specific properties, the paper develops a log parser. The parser will parse the logs and construct them into sequences of algebraic terms(events). The model for the system will eventually be a tree. After the model has been constructed, the model and logic can be sent to a model checker which will check if the model satisfies the formula. The framework and process can successfully check log in an automatic and formalized way.

The paper also offer some attack scenarios, e.g. intrusion, compromise, misuse and withdrawal, and the author give some attack example in the ADM logic and semantics. Intrusion means attacker breaches the system using different techniques, e.g. buffer overflow, malicious code, etc. Compromise consists of events pertaining to the preparation for malicious activity, e.g. creating user, changing password, installing or uninstalling services or apps, etc. Misuse means using the compromised system for attacker's own malicious purposes, e.g. local or remote login, open a connection to the system, etc. Withdrawal means attacker tries to cover his tracks cleaning the system from his malicious activities, e.g. uninstalling a service or app, clearing the log files, etc.

In conclusion, this paper proposed a model checking approach to formal analysis of logs. In the future, they aim to update a more sufficient version of their processing system.