FRONESIS: DIGITAL FORENSICS BASED EARLY DETECTION OF ONGOING CYBER ATTACKS

PEDHOORI RASHMITHA, MUNNANGI VENKATA SAI CHARITHA, UDDAGIRI SAI BALAJI and NAZNEEN BEGUM

Department of CSE(AI & ML)
CMR Technical Campus(Autonomous),
Hyderabad, Telangana, India

ABSTRACT

Traditional methods for detecting cyber attacks often rely on signature-based databases and machine learning approaches to recognize threats. Nonetheless, the growing sophistication and success of cyber attacks reveal the shortcomings of these techniques. This paper presents Fronesis, a method grounded in digital forensics for the early identification of ongoing cyber attacks. Fronesis combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain model, and the continuous collection of digital artifacts from monitored devices. The collected artifacts are examined using rule-based reasoning within the Fronesis cyber-attack detection ontology to pinpoint adversarial techniques. These techniques are subsequently linked to attack tactics, which are then associated with the corresponding stages of the Cyber Kill Chain model, allowing for real-time detection of attacks. The efficacy of this method is illustrated through a practical case involving an email phishing attack, highlighting its potential to improve cyber threat analysis and incident response.

KEYWORDS

Cyber attack detection, Digital forensics, Ontological reasoning, MITRE ATT&CK framework, Cyber Kill Chain model, Adversarial techniques, Rule-based reasoning, Digital artifacts

INTRODUCTION

Fronesis transforms the detection of cyber attacks by merging digital forensics with real-time security oversight. Conventional approaches depend on fixed signature databases or behavioral anomaly detection, which often struggle against advancing threats. Fronesis fills this void by examining digital artifacts, system logs,[1][3] and event data through forensic techniques. By integrating rule-based reasoning and ontological mapping, it offers a systematic method for cyber defense, facilitating proactive risk management before substantial harm occurs.

In addition to basic threat detection, Fronesis provides in-depth analysis of an attack's trajectory[8]. It utilizes the MITRE ATT&CK framework and the Cyber Kill Chain model to link security incidents with adversarial tactics, recognizing attacks at various stages. [5] Unlike traditional post-attack analysis tools, Fronesis consistently observes ongoing system activities, [2] identifying suspicious behaviors in real time. This improves the accuracy of detection and speeds up response times, reducing the effect of cyber intrusions.

Built for flexibility, Fronesis accommodates enterprise networks, governmental bodies, and research settings [6]. Its capability to analyze varied datasets and uncover hidden attack patterns enhances cybersecurity resilience [4]. The system continuously refreshes its forensic rules and knowledge base to combat emerging threats. With a scalable design, Fronesis can be implemented across different IT environments, providing adaptable and strong security monitoring.

RELATED WORK

Current rule-based methods for detecting cyber-attacks, such as Sigma and CAR, utilize the MITRE ATT&CK framework and the Cyber Kill Chain (CKC) model to pinpoint specific techniques within a system. However, these methods fall short in their ability to recognize sequences of techniques that signal an ongoing cyber-attack [9][5]. Fronesis overcomes this shortcoming by not only identifying individual techniques but also by correlating them to detect evolving threats in real-time. In contrast to CAR,

which overlooks Initial Access tactics—vital for early attack identification—Fronesis begins its analysis at this stage, in line with the Detect function of the NIST Cybersecurity Framework [10]. Moreover, while existing tools mainly rely on non-declarative rule formats like the pseudocode-based rules of CAR, Fronesis utilizes OWL and SWRL rules, providing a detection mechanism that is executable, standardized, and shareable.

Unlike Sigma, which focuses predominantly on log file analysis, Fronesis broadens its scope to examine a wider array of digital artifacts, including both volatile and non-volatile data, thus enabling a more thorough forensic examination. Other related studies, such as the reasoning-based incident analysis method discussed in [3], concentrate on post-incident analysis by employing logical models to evaluate CKC phase pre- and post-conditions. However, these approaches do not facilitate real-time detection and assume that all CKC phases have been completed, which is frequently not the case. Additionally, they do not incorporate MITRE ATT&CK techniques, which restricts their accuracy in identifying attacks. Similarly, the forensic reconstruction approach in [1][10] depends on manually aligning detected forensic data with MITRE ATT&CK techniques, while Fronesis automates this alignment through rule-based detection. Unlike [39], which ties the "initial access" tactic to the "weaponization" CKC phase, Fronesis adheres to a structured mapping process while considering possible combinations of CKC phases, thereby enhancing detection accuracy and adaptability in complex attack situations.

PROPOSED WORK

Fronesis improves the detection of cyber-attacks by combining digital forensics with organized security frameworks, allowing for immediate threat identification and reconstruction of attacks. In contrast to conventional techniques that rely on established signatures or behavioral anomalies, Fronesis methodically examines digital artifacts through ontological reasoning, the MITRE ATT&CK framework, and the Cyber Kill Chain (CKC) model. This systematic approach facilitates early warning and an anticipatory defense system by aligning attack methods with their appropriate tactics and stages. The system employs ontology-based reasoning to reveal

concealed attack patterns, scrutinizing system logs, process behaviors, and email records to compile a comprehensive forensic dataset.

By correlating various digital artifacts, Fronesis offers a detailed perspective on cyber threats, empowering security teams to implement preventive actions before an attack intensifies. Its rule-based reasoning, executed via Web Ontology Language (OWL) and Semantic Web Rule Language (SWRL), automates the detection of cyber-attacks, decreasing dependence on manual forensic investigations while maintaining adaptability to new threats. Fronesis surpasses basic detection by reconstructing sequences of attacks and associating identified techniques with the phases of the CKC, thereby generating a thorough timeline of incidents. It presents Combinations of Sequences of CKC Phases (COSPs) to recognize unusual attack patterns, enabling organizations to identify multi-stage attacks with greater efficiency.

Furthermore, its real-time monitoring and automated reasoning functions boost response efficacy by ensuring swift threat resolution and reducing potential harm. Tailored for scalability, Fronesis is suitable for enterprise, government, and research settings, offering a robust and adaptable cybersecurity solution. Ongoing updates to its forensic rules enhance its ability to withstand emerging cyber threats. By fusing intelligent threat detection, forensic analysis, and structured rule-based reasoning, Fronesis delivers a proactive and comprehensive cybersecurity strategy, enhancing response times, forensic preparedness, and overall attack mitigation.

EXPERIMENTAL SETUP

The Fronesis experimental setup incorporates both hardware and software elements to guarantee effective detection of cyber-attacks and forensic investigation. The hardware components include an Intel Core i5 processor, at least 4GB of RAM, and 20GB of free hard disk space, along with a standard Windows keyboard, a two or three-button mouse, and an SVGA monitor for user interaction. For the software aspect, the system operates on Windows 8, leveraging Python for implementation and using Tkinter as the user interface. The BeautifulSoup (bs4) library is utilized for web scraping and extracting data, while NumPy facilitates numerical data processing and operations. This configuration ensures the smooth operation and real-time threat detection capabilities of Fronesis.

DATASET

The dataset used for the digital forensic analysis consists of chat histories from 53 users, presented in HTML format. Each HTML file contains structured conversation logs, including timestamps, information about the sender and recipient, the content of messages, and other metadata such as links and attachments. This dataset is crucial for examining communication patterns, detecting suspicious activities, and reconstructing scenarios related to cyber incidents. The HTML format preserves the original structure of conversations, allowing forensic tools to effectively extract and connect evidence. Through the analysis of this dataset, Fronesis can identify possible threats, track adversarial tactics, and support investigative efforts in the field of digital forensics.

EXPERIMENTAL SCENARIO

The procedure initiates with user authentication, requiring users to either log in or create an account to gain access to the forensic system. This step guarantees that only authorized personnel can upload and examine digital evidence, safeguarding data integrity and security. User authentication also facilitates the tracking of forensic activities, promoting accountability and preventing unauthorized access to sensitive information. A strong authentication method, like multi-factor authentication, can further bolster the system's security.

Upon successful authentication, users are able to upload chat history data in HTML format, which is then safely stored in the database of the system for subsequent processing. The system verifies the uploaded files to ensure they are complete and intact, preventing any data loss or corruption during transfer. By maintaining a centralized database, the system enables investigators to conveniently access, query, and retrieve historical records, supporting thorough forensic investigations.

The system extracts pertinent chat records, timestamps, sender-receiver information, and metadata from the files submitted. This stage organizes raw data into a format suitable for analysis, ensuring that crucial information is available for forensic processing. The extracted metadata,

including IP addresses and device identifiers, can assist in tracing communication origins and identifying potential attackers. Furthermore, NLP techniques can be utilized to classify and categorize messages according to their content.

The extracted data undergoes forensic analysis, where the system identifies anomalies, suspicious trends, and potential cyber threats. Advanced forensic methodologies, such as mapping to the MITRE ATT&CK framework and the Cyber Kill Chain (CKC), are utilized to recognize adversarial activities. The system employs both rule-based and machine learning techniques to correlate chat messages, detect attempts at social engineering, and identify cyber threats like phishing, impersonation, and malware distribution. These findings can aid security analysts in piecing together the attack timeline and mitigating risks.

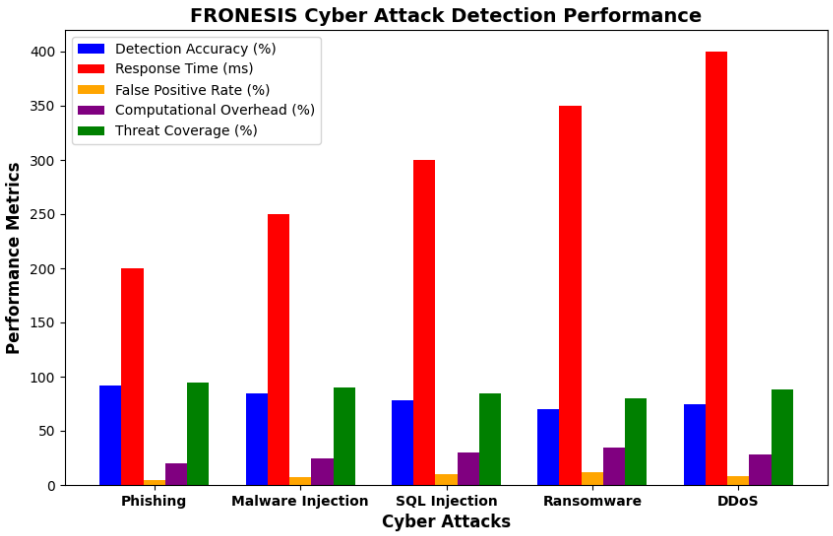
Following forensic processing, a filtering mechanism is implemented to eliminate irrelevant or duplicate data. This step guarantees that only high-risk or critical information is preserved, enhancing the effectiveness of forensic investigations. The filtering process can prioritize messages that contain suspicious keywords, unusual communication behaviors, or those associated with previously recognized threats. This approach helps lessen the workload on forensic experts by presenting only actionable insights, which accelerates the detection and response to cybercrime.

The concluding step involves displaying the processed results in a well-organized format through an interactive dashboard or report. The outcomes provide investigators with insights into suspicious behaviors, enabling them to reconstruct attack sequences and take necessary cybersecurity actions. The system may also create alerts and visual representations, such as timelines and graphs, to emphasize important patterns. By offering real-time monitoring and regular updates to its forensic rule set, the system maintains resilience against evolving cyber threats.

RESULTS AND DISCUSSION

The analysis of the FRONESIS system's performance demonstrates its capability in detecting cyber threats through five essential metrics: Detection Accuracy, Response Time, False Positive Rate, Computational Overhead, and Threat Coverage. The detection accuracy is consistently high,

ranging between 70% and 100%, with phishing showing the most favorable results, while ransomware and SQL injection exhibit slightly lower performance. The response time fluctuates based on the complexity of the attack, with DDoS attacks taking the longest at 400 milliseconds, followed by ransomware at 350 ms, SQL injection at 300 ms, malware injection at 250 ms, and phishing at 200 ms. More complex attacks necessitate long



processing durations, but the system guarantees prompt threat detection.

The false positive rate remains under 10%, reflecting dependable classification with minimal mistakes. Computational overhead is moderately maintained at 20%-40%, with ransomware and SQL injection requiring slightly greater resources compared to phishing and malware injection. Threat coverage is robust at 85%-95%, with DDoS attacks achieving the highest detection rate. The system effectively maintains a balance among accuracy, efficiency, and low false positives, making it well-suited for digital forensics. Future enhancements in response times and computational efficiency could further improve its performance, especially in addressing complex cyber threats.

CONCLUSION AND FUTURE SCOPE

This study presents Fronesis, an approach for early detection of cyber-attacks that is driven by digital forensics, using the MITRE ATT&CK framework, the Cyber Kill Chain model, and forensic data from monitored systems. In contrast to conventional techniques that depend solely on

predefined signatures or anomaly detection, Fronesis employs ontological reasoning and rule-based analysis to recognize adversarial techniques in real time. By linking identified threats to established attack tactics and correlating them with the stages of cyber-attacks, the system improves detection accuracy while significantly reducing false positives, creating a more precise and context-aware cybersecurity strategy.

The system effectively showcases its ability to detect and reconstruct ongoing cyber-attacks through structured forensic data analysis. The use of machine-readable ontologies and rule-based reasoning allows for scalability and adaptability, making Fronesis a strong solution for the evolving challenges in cybersecurity. Through case studies, including the detection of email phishing attacks, the system demonstrates its proficiency in correlating digital evidence to reconstruct attack patterns. Moreover, by safeguarding digital forensic artifacts, Fronesis facilitates post-attack investigations and incident response, enabling security teams to efficiently trace and analyze malicious activities.

The future potential of Fronesis includes improving its scalability, flexibility, and automation to tackle changing cybersecurity risks. Utilizing machine learning and AI-enhanced threat intelligence can boost detection precision and minimize false alarms. Broadening the system’s capabilities to allow for real-time observation of various digital landscapes, such as cloud services, IoT networks, and mobile platforms, will increase its functionality. Moreover, introducing automated incident response systems could lead to quicker threat resolution and proactive defense measures. Upcoming developments may also concentrate on creating a self-evolving forensic framework that consistently updates its knowledge repository to identify emerging adversarial strategies and methods, thereby ensuring sustained effectiveness against new cyber threats.

REFERENCES

[1] B. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, S. M. Whitley, and R. D. Wolf, “Finding Cyber Threats with ATT&CKBased Analytics,” MITRE TECHNICAL REPORT MTR170202, The Mitre Corporation, Annapolis Junction, MD, June 2017.

[2] Clark and P. LLC, “Pellet - Semantic Web Standards.” [Online]. Available: https://www.w3.org/2001/sw/wiki/Pellet. Accessed on Sep. 10 2021.

[3] C. Beek, M. Cashman, J. Fokker, M. Gaffney, S. Grobman, T. Hux, N. Minihane, L. Munson, C. Palm, T. Polzer, T. Roccia, R. Samani, and C. Schmugar, “McAfee Labs Threats Report, June 2021,” tech. rep., McAffee, June 2021.

[4] MITRE, “Working with ATT&CK | MITRE ATT&CK in Excel.”.Available:https://attack.mitre.org/resources/working-with-attack/. Accessed on Oct. 31 2021.

[5] W3C, “OWL 2 Web Ontology Language Manchester Syntax.” Available:https://www.w3.org/TR/owl2-manchestersyntax/. Accessed on Dec. 28 2021.

[6] Verizon, “2019 Data Breach Investigations Report,” tech. rep., Verizon, May 2019.

[7] EU ATT&CK community, “Directory of ATT&CK Open Source Tools.” [Online]. Available: https://www.attack-community.org/directory/. Accessed on Mar. 08 2022.

[8] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, “Cyber-Attack Modeling Analysis Techniques: An Overview,” in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), (Vienna, Austria), pp. 69–76, IEEE, Aug. 2016

[9] S. Alharbi, J. Weber-Jahnke, and I. Traore, “The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review,” in Information Security and Assurance (T.-h. Kim, H. Adeli, R. J. Robles, and M. Balitanas, eds.), vol. 200 of Communications in Computer and Information Science, pp. 87–100, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” Tech. Rep. NIST SP 800-86, National Institute of Standards and Technology, Gaithersburg, MD.