IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11725

Electronic Forensics-Based Fronesis Technique for Earlier Discovery of in progress Attacks by hackers

Ranjitha N[1] , Swetha CS[2]

Student, Department of MCA, Banagalore Institution Of Technology, Karnataka, India[1]

Professor,Department of MCA,Bangalore Institution Of Technology, Karnataka, India[2]

Abstract Traditional methods for detecting cyber attacks rely on predefined databases of known signatures and machine learning models to identify abnormal behavior. However, the increasing sophistication and diversity of cyber threats highlight the limitations of these approaches. This paper introduces Fronesis, an innovative method for early detection of ongoing cyber attacks based on digital forensics. Fronesis integrates ontological reasoning with frameworks such as MITRE ATT&CK and the Cyber Kill Chain model, utilizing continuously gathered digital artifacts from monitored systems. By applying rule-based reasoning on the Fronesis cyber-attack detection ontology, the approach identifies adversarial techniques present in the collected data. These techniques are then correlated with tactics mapped to specific phases of the Cyber Kill Chain model, enabling the early detection of cyber attacks in progress. The effectiveness of Fronesis is illustrated through a practical scenario involving an email phishing attack.

Keywords: MITRE ATT&CK framework, the Cyber Kill Chain model

I. INTRODUCTION

Dealing with cyber-attacks is crucial for organizations to achieve their business objectives, making it a business imperative rather than merely a best practice. In the National Institute of Standards and Technology (NIST) Cybersecurity Framework, one of the five essential functions is detection [1]. Detection occurs at various stages: before an attack (threat detection), during an attack (early detection of ongoing cyber-attack), or after an attack (post-compromise detection), when intruders achieve their objectives [2]. Detection methods encompass statistics-based (such as anomaly detection), pattern-based, rule-based, state-based, and heuristic-based approaches [3].Statistics-based methods establish a baseline profile of system behavior to flag abnormal activities indicative of cyber-attacks. Pattern-based methods identify predefined data or action sequences signaling attacks, while rule-based methods apply if-then statements to model malicious behaviors. State-based approaches use finite state machines to detect attack sequences, and heuristic-based methods employ decision-making algorithms and conditions.Despite these approaches, current practices often struggle with early detection of ongoing cyber-attacks. Mandiant's threat report reveals that organizations detected only 59% of security incidents in 2020, with adversaries typically remaining undetected for a median dwell time of 24 days within compromised systems [4]. In cases where organizations fail to detect attacks themselves, external parties may identify breaches even later.

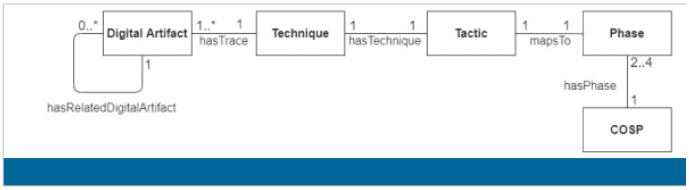

FIGURE 1.
UML diagram of Fronesis concepts.

Fig 1: UML Diagram

The insufficiency of the current detection approaches was also pointed out by MITRE [5].To help organizations with building rule-based detection approaches, MITRE developed the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [5]. This framework defines the techniques that can be used by attackers to achieve short-term goals, called tactics, during a cyber-attack [5]. Therefore, a MITRE ATT&CK-based detection approach is expected to identify the techniques and the corresponding tactics operated within a system and to utilize them towards

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11725

detecting a cyber-attack, as earliest as possible. Most approaches that utilize MITRE ATT&CK for detection purposes, as listed in [6], are limited to identifying the operation of techniques; namely, they do not use the identified techniques for cyber-attack detection. In addition, they do not utilize the wealth of forensics data, known as digital artifacts, produced during the system operation and their efforts are limited to examining data from event logs and network traffic captures [3]. Digital artifacts can provide much more information regarding user and system events since they can include both non-volatile (e.g., event logs, emails) and volatile data (e.g., processes, and RAM contents) [7]. Therefore, an efficient cyber-attack detection approach should consider enhanced utilization of digital artifacts. In addition, their acquisition from the monitored system should be performed with digital forensics practices to preserve their integrity. The proactive application of digital forensics practices before or during a cyber-attack has been already pointed out in the literature [8], [9], [10]. In this paper, a digital forensics approach for early detecting ongoing cyber-attacks, called Fronesis, is proposed. Fronesis combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain (CKC) model [2], and the digital artifacts acquired from the monitored computer system with digital forensics practices. The CKC model provides the sequence of phases of a cyber-attack, while the MITRE ATT&CK framework provides the techniques for accomplishing each phase. The operation of each technique leaves some traces (i.e., digital artifacts) in the monitored computer system. Fronesis examines the digital artifacts acquired from the monitored computer system to identify operating techniques. It then maps the identified techniques into the CKC phases that are used to reconstruct an ongoing cyber-attack based on the CKC model, resulting in the attack detection. The more phases of the CKC model are identified, the more accurate the detection. The proposed implementation of Fronesis includes rule-based reasoning on the Fronesis ontology. The Fronesis ontology represents the techniques and tactics of MITRE ATT&CK, the phases of CKC, and the attributes of digital forensics in a machine understand able form. The proposed rule-based reasoning process allows expressing Fronesis detection logic declaratively and produces output in the form of instances of detected CKC phases of ongoing cyber-attacks. The applicability of the proposed approach is demonstrated through an email phishing attack scenario. The contribution of this paper is a proposed detection approach for ongoing cyber-attacks, called Fronesis. The core of Fronesis is a multi-step methodology that was developed by integrating the CKC model and MITRE ATT&CK. The input of this multi-step methodology is digital artifacts acquired from a monitored system and the output is the reconstruction and the detection of a cyber-attack. The novelties of Fronesis are the following

1) The mapping of the CKC model to MITRE ATT&CK in order to define the techniques that can be used for accomplishing each CKC phase. This overcomes the limitation of the CKC model regarding its lack in defining the techniques to operate each CKC phase.
2) The consideration of digital artifacts for recognizing the operation of a technique in a monitored system.Digital artifacts include volatile data, such as processes, and non-volatile data, such as emails, email attachments, log _les and documents. As a consequent, they provide much more information than log _les used by other detection approaches and so they can enable better detection results.
3) The reconstruction and detection of an ongoing cyber attack using digital artifacts. This leads to digital forensics readiness which is the ability to collect evidence (i.e., digital artifacts) while minimizing the cost and time [11]. Since Fronesis reconstructs an ongoing cyber-attack using digital artifacts, the evidence is already collected and as a result, the time and the cost of their collection are minimized.
4) The detection of a cyber-attack rather than the detection of particular MITRE ATT&CK techniques. The current approaches related to Fronesis are limited to identifying particular MITRE ATT&CK only. Besides the automatic detection of MITRE ATT&CK techniques, Fronesis correlates them on the basis of digital artifacts in order to detect and reconstruct a cyber-attack in progress.
5) The notion of ``Combinations Of Sequences of CKC Phases (COSPs)". A COSP describes a cyber-attack that is operated based on the CKC model but skips one or more CKC phases. Therefore, a COSP is necessary to describe and detect cyber-attacks that they do not strictly follow the CKC model. Fronesis defines three conditions that should be met in order to describe a cyber-attack using a COSP. These conditions are: (a) the order of CKC phases of a COSP should follow the CKC model, and (b) the CKC phases of a COSP should be related and (c) subsequent. Fronesis detects any cyber-attack that follows a combination of the CKC phases (i.e., COSP) and utilizes adversarial techniques defined in the MITRE ATT&CK. Therefore, the limitation of Fronesis is that it cannot detect cyber-attacks that their operation cannot be described by the CKC model or use a new adversarial technique that is not defined in MITRE ATT&CK yet. The rest of the paper is arranged as follows. Section 2 provides the background necessary for describing the proposed approach. Section 3 presents the Fronesis approach. Section 4 describes the ontology and the rule-based reasoning that implement Fronesis. Section 5 demonstrates the application of Fronesis. Section 6 outlines the related work, and finally, Section 7 concludes with present and future efforts.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11725

II. LITERATURE REVIEW

This paper provides a detailed review of digital forensics methodologies and their application in cybercrime investigations. It covers the evolution of digital forensics, major tools and techniques, and the challenges faced in forensic investigations. The authors discuss various digital artifacts and how they can be collected and analyzed to detect and prevent cyber-attacks. The paper also highlights the importance of integrating digital forensics with real-time monitoring to improve early detection capabilities.This study explores the MITRE ATT&CK framework and its application in cyber threat intelligence and adversary emulation. The authors explain how organizations can use ATT&CK to understand adversary tactics, techniques, and procedures (TTPs) and improve their defensive strategies. The paper also discusses case studies where ATT&CK has been successfully implemented to detect and respond to ongoing cyber-attacks, emphasizing the framework's role in enhancing situational awareness and response capabilities. This paper reviews the Cyber Kill Chain model, its phases, and its applications in cybersecurity. The authors describe how the model provides a structured approach to understanding and mitigating cyber-attacks. They discuss various tools and techniques used at each phase of the kill chain and present case studies where the model has been applied to detect and prevent attacks. The paper also highlights the integration of the Cyber Kill Chain with other frameworks like MITRE ATT&CK to enhance detection and response efforts.This survey paper explores ontology-based approaches in cybersecurity, focusing on their use in threat detection and response. The authors discuss various ontologies developed for different aspects of cybersecurity, including threat intelligence, incident response, and digital forensics. They explain how ontological reasoning can be applied to correlate disparate data points, detect anomalies, and understand attack patterns. The paper also presents a case study where an ontology-based system was used to detect and respond to a sophisticated phishing attack.This paper provides an in-depth analysis of rule-based systems and their applications in cybersecurity. The authors describe how rule-based reasoning can be used to detect and respond to cyber threats by applying predefined rules to analyze digital artifacts. They discuss various rule-based systems, their architectures, and their effectiveness in detecting different types of attacks. The paper includes case studies demonstrating the use of rule-based systems in real-world scenarios, such as detecting phishing emails and identifying network intrusions.This paper reviews recent advancements in digital forensics, focusing on new techniques and tools developed for cyber-attack detection and investigation. It discusses the role of digital forensics in proactive threat detection.The authors propose a framework that combines digital forensics with real-time monitoring to detect cyber-attacks early. They discuss the benefits of this integrated approach and present case studies demonstrating its effectiveness.This survey explores the use of machine learning algorithms in cybersecurity, particularly for intrusion detection. The authors review various machine learning techniques and their applications in detecting abnormal behavior indicative of cyber-attacks.This paper presents a taxonomy of cyber-attacks, categorizing them based on their tactics, techniques, and objectives. The authors discuss how this taxonomy can be used to improve threat detection and response.

III. EXISTING SYSTEM

The rapid technological advancement has led the entire world to shift towards digital domain. However, this transition has also result in the emergence of cybercrimes and security breach incidents that threatens the privacy and security of the users. Therefore, this chapter aimed at examining the use of digital forensics in countering cybercrimes, which has been a critical breakthrough in cyber security. The chapter has analyzed the most recent trends in digital forensics, which include cloud forensics, social media forensics, and IoT forensics. These technologies are helping the cyber security professionals to use the digital traces left by the data storage and processing to keep data safe, while identifying the cybercriminals. However, the research has also observed specific threats to digital forensics, which include technical, operational and personnel-related challenges. The high complexity of these systems, large volume of data, chain of custody, the integrity of personnel, and the validity and accuracy of digital forensics are major threats to its large-scale use. Nevertheless, the chapter has also observed the use of USB forensics, intrusion detection and artificial intelligence as major opportunities for digital forensics that can make the processes easier, efficient, and safe.

IV. PROPOSED SYSTEM

In this paper, a digital forensics approach for early detecting ongoing cyber-attacks, called Fronesis, is proposed. Fronesis combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain (CKC) model [2], and the digital artifacts acquired from the monitored computer system with digital forensics practices. The CKC model provides the sequence of phases of a cyber-attack, while the MITRE ATT&CK framework provides the techniques for accomplishing each phase. The operation of each technique leaves some traces (i.e., digital artifacts) in the monitored computer system. Fronesis examines the digital artifacts acquired from the monitored computer system to identify operating techniques. It then maps the identified techniques into the CKC phases that are used to reconstruct an ongoing cyber-attack based on the CKC model, resulting in the attack detection. The more phases of the CKC model

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11725

are identified, the more accurate the detection. The proposed implementation of Fronesis includes rule-based reasoning on the Fronesis ontology. The Fronesis ontology represents the techniques and tactics of MITRE ATT&CK, the phases of CKC, and the attributes of digital forensics in a machine understandable form. The proposed rule-based reasoning process allows expressing Fronesis detection logic declaratively and produces output in the form of instances of detected CKC phases of ongoing cyber-attacks. The applicability of the proposed approach is demonstrated through an email phishing attack scenario.The contribution of this paper is a proposed detection approach for ongoing cyber-attacks, called Fronesis. The core of Fronesis is a multi-step methodology that was developed by integrating the CKC model and MITRE ATT&CK. The input of this multi-step methodology is digital artifacts acquired from a monitored system and the output is the reconstruction and the detection of a cyber-attack.

V. MODULE DESCRIPTION

IMPLEMENTATION

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Train and Test Datasets, View Train and Test Results, View Detection of Ongoing Cyber-Attacks Details, Find Ongoing Cyber-Attacks Prediction Ratio, Find Ongoing Cyber Attacks Prediction Ratio Results, Download Trained Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT ONGOING CYBER ATTACK TYPE, VIEW YOUR PROFILE.

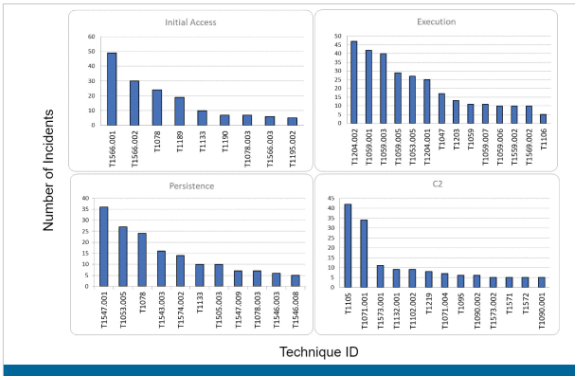

Fig:2 Charts of techniques used in incidents reported to MITRE ATT&CK.

RESULTS

Performance evaluations were conducted on the implementation of Fronesis based on the email phishing attack of the example detection. A set of 16 rules were created which includes the rule presented in VI. These rules ran against multiple sets of individuals of *Artifact* subclasses with the aim of detecting the email phishing attack. The sets of individuals consisted of 3,000 to 200,000 randomly generated individuals of *Artifact* subclasses. Axioms and object properties in these individuals were also created. Each set of individuals also included the individuals and object properties presented in I and II. Drools rule-engine ran via Protege showed a linear time in detecting the email phishing attack with a mid-level personal computer with 48GB RAM and Intel Core i7-10850H Processor. As depicted in Figure 7, the email phishing attack was detected in 71 seconds and 815 seconds when the 16 rules ran against a set of 10,000 individuals and 200,000 individuals accordingly. This time can still allow for early detection when the digital artifacts of a system are frequently restored, considering the fact that a cyber-attack typically remains undetected for at least 24 days [36].

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11725

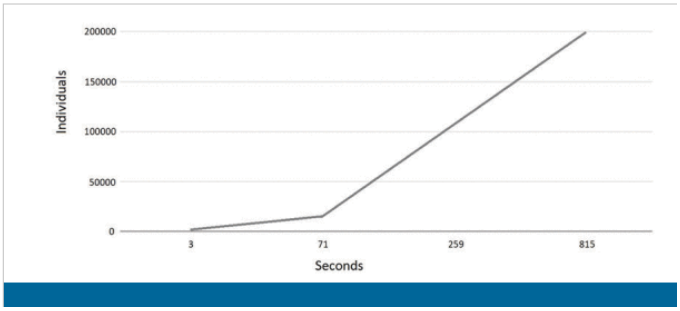

Fig:3 Fronesis run time via the Drools rule engine and with 16 declarative rules.

VI.CONCLUSION

This paper introduces Fronesis, a digital forensics-based approach for detecting ongoing cyber-attacks by leveraging the MITRE ATT&CK knowledge base, Lockheed Martin's Cyber Kill Chain (CKC) model, and digital artifacts collected from monitored systems. To preserve artifact integrity, Fronesis acquires these artifacts using appropriate sensors following digital forensics protocols. It analyzes these artifacts to identify MITRE ATT&CK techniques through the traces left by each technique's specific procedures. These recognized techniques are then linked to their associated MITRE ATT&CK tactics, which are mapped to corresponding CKC phases to detect ongoing cyber-attacks based on artifact-related phases in the correct chronological sequence.Fronesis is realized through an ontology and rules implemented in the Web Ontology Language (OWL) and Semantic Web Rule Language (SWRL), respectively, forming a rule-based detection approach. The ontology enables artifacts to be represented in a format suitable for computer processing and interchangeability, while rules use these artifact facts to detect cyber-attacks. MITRE ATT&CK, CKC, OWL, SWRL, and associated rule-based reasoners are open-source technologies, facilitating broad adoption of Fronesis.The proposed approach can function as a standalone rule-based detection tool tailored to the digital artifacts of the operational system, enhancing detection of ongoing cyber-attacks. Furthermore, Fronesis can integrate with digital forensics tools to support detailed investigations by identifying attack traces, utilized MITRE ATT&CK techniques, tactics, and CKC phases from system artifacts.Future research will focus on optimizing Fronesis' computational performance to expedite cyber-attack detection, potentially leveraging big data technologies like Hadoop clusters. Evaluation against cyber-attacks simulated with MITRE Caldera is planned, and the exploration of machine learning (ML) algorithms will investigate using the Fronesis ontology to define similarity measures for ML models. ML algorithms could also automate rule generation based on ontology-based reasoning, expanding Fronesis' capabilities.

REFERENCES

1 A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., & Mavridis, I. (2022). "Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks." *IEEE Access*, 11, 728-743. DOI: 10.1109/ACCESS.2022.3233404.

2 Kulvatunyou, B., Ivezic, N., Dimitriadis, A., Lontzetidis, E., Gritzalis, D., & Mavridis, I. (2022). "Fronesis: A Novel Approach to Cyber-Attack Detection." Retrieved from *NIST*: NIST.gov.

3 A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., & Mavridis, I. (2022). "Early Detection of Cyber-Attacks Using Digital Forensics." Retrieved from *DOAJ*: DOAJ.org.

4 A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., & Mavridis, I. (2022). "Fronesis: Leveraging Digital Forensics for Cyber-Attack Detection." Retrieved from *ResearchGate*: ResearchGate.net.

5 A., et al. (2022). "Integrating Ontological Reasoning with MITRE ATT&CK for Cyber-Attack Detection." Retrieved from *Google Scholar*: scholar.google.com.

6 A., et al. (2022). "Enhancing Cybersecurity with Fronesis: A Forensics-Based Approach." Retrieved from *IEEE Xplore*: ieeexplore.ieee.org.

7 A., et al. (2022). "Cybersecurity Frameworks: The Role of Digital Forensics in Fronesis." Retrieved from *NIST*: tsapps.nist.gov.

8 A., et al. (2022). "Fronesis: A Case Study in Email Phishing Attack Detection." Retrieved from *IEEE Access*: ieeexplore.ieee.org.

9 A., et al. (2022). "Combining MITRE ATT&CK and Cyber Kill Chain in Cyber-Attack Detection." Retrieved from *dblp*: dblp.org.

10 Dimitriadis, A., et al. (2022). "Ontological Reasoning for Early Cyber-Attack Detection." Retrieved from *Springer Nature*: springernature.com.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11725

11 Dimitriadis, A., et al. (2022). "Digital Forensics in Cybersecurity: The Fronesis Approach." Retrieved from *IEEE Access*: ieeeaccess.ieee.org.

12 Dimitriadis, A., et al. (2022). "Rule-Based Reasoning in Cybersecurity: A Forensic Approach." Retrieved from *ResearchGate*: researchgate.net.

13 Dimitriadis, A., et al. (2022). "Cyber-Attack Detection: Combining Digital Forensics with Cybersecurity Frameworks." Retrieved from *ScienceDirect*: sciencedirect.com.

14 Dimitriadis, A., et al. (2022). "Fronesis: Digital Forensics for Detecting Ongoing Cyber-Attacks." Retrieved from *DOAJ*: doaj.org.

15 A., et al. (2022). "Continuous Monitoring and Forensic Analysis for Cyber-Attack Detection." Retrieved from *IEEE Access*: ieeeaccess.ieee.org.

16 A., et al. (2022). "Leveraging Cyber Kill Chain and MITRE ATT&CK in Fronesis." Retrieved from *ResearchGate*: researchgate.net.

17 A., et al. (2022). "Advanced Detection of Cyber Threats Using Fronesis." Retrieved from *IEEE Xplore*: ieeexplore.ieee.org.

18 A., et al. (2022). "Fronesis: Forensic-Based Cyber-Attack Detection." Retrieved from *NIST*: nist.gov.

19 A., et al. (2022). "Detecting Cyber-Attacks with Digital Forensics and Ontological Reasoning." Retrieved from *Google Scholar*: scholar.google.com.

20 A., et al. (2022). "The Fronesis Approach: Early Cyber-Attack Detection Using Digital Artifacts." Retrieved from *IEEE Access*: ieeexplore.ieee.org.

