Utilitas Mathematica

ISSN 0315-3681 Volume 122, 2025

Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks

[1] Paka Akhila

PG Scholar, Department of Computer Science & Engineering, Siddhartha Institute of Technology and Sciences, Hyderabad, India.

[2] Mr. K Vijay

Assistant Professor, Department of Computer Science & Engineering, Siddhartha Institute of Technology and Sciences,

ABSTRACT

Traditional attack detection approaches utilize predefined databases of known signatures about already-seen tools and malicious activities observed in past cyber-attacks to detect future attacks. More sophisticated approaches apply machine learning to detect abnormal behavior. Nevertheless, a growing number of successful attacks and the increasing ingenuity of attackers prove that these approaches are insufficient. This paper introduces an approach for digital forensics-based early detection of ongoing cyber-attacks called Fronesis. The approach combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain model, and the digital artifacts acquired continuously from the monitored computer system. Fronesis examines the collected digital artifacts by applying rule based reasoning on the Fronesis cyber-attack detection ontology to identify traces of adversarial techniques. The identified techniques are correlated to tactics, which are then mapped to corresponding phases of the Cyber Kill Chain model, resulting in the detection of an ongoing cyber-attack. Finally, the proposed approach is demonstrated through an email phishing attack scenario.

1. INTRODUCTION

Dealing with cyber-attacks is a critical factor for organizations to achieve their business goals; it is a business driven factor rather than a best practice. To address cyber attacks, one of the five cyber security functions is detection, as defined in the Cyber security Framework developed by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) [1]. Detection can take place before a cyber-attack is launched (threat detection), where attackers perform reconnaissance and weaponization activities. It can also take place during a cyber attack (early detection of ongoing cyber-attack) or after a cyber-attack is accomplished (post-compromise

detection), where intruders accomplish their original objectives [2]. Detection approaches are classified as statistics-based (i.e., anomaly or behavioral-based), pattern-based, rule based, state-based, and heuristic-based [3]. Statistics-based approaches create the profile of a monitored system and use this profile to detect cyber-attacks as abnormal activities that are beyond an ordinal baseline.

KNN Classifier Algorithm:

K-nearest neighbor method can be used for both regression and classification predictive problems. This method helps in interpret output, calculate time and predictive power. The Machine learning techniques are used in various fields. KNN is also one of the machine learning method. This is also called as method of sample-based learning. This will contain the data of past datasets and can be used while predicting the new datasets. This will apply function called as distance function like Manhattan or Euclidean distance.

Classifications Algorithms

Onto the part you've probably been waiting for all this time: training machine learning algorithms. To be able to test the performance of our algorithms, I first performed an

80/20 train-test split, splitting our balanced data set into two pieces. To avoid overfitting, I used the very common resampling technique of k-fold cross-validation. This simply means that you separate your training data into k parts (folds) and then fit your model on k-1 folds before making predictions for the kth hold-out fold. You then repeat this process for every single fold and average the resulting predictions.

2. LITERATURE SURVEY

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

3. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

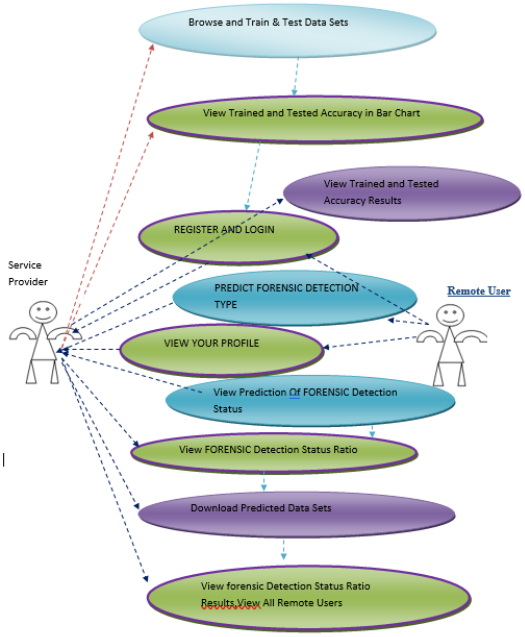
The rapid technological advancement has led the entire world to shift towards digital domain. However, this transition has also result in the emergence of cybercrimes and security breach incidents that threatens the privacy and security of the users. Therefore, this chapter aimed at examining the use 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.

3.2 PROPOSED SYSTEM:

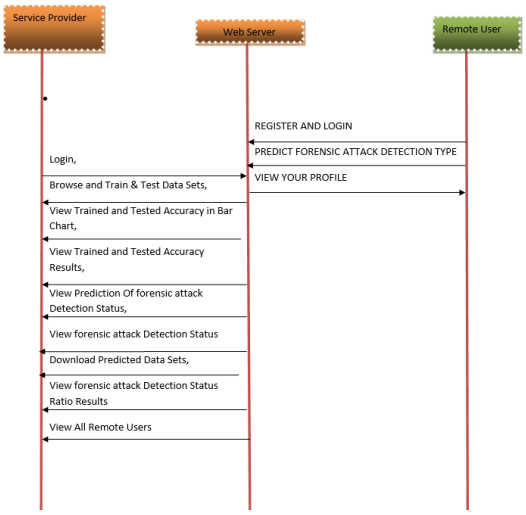
In this paper, a digital forensics approach for early detecting ongoing cyber-attacks, called Fronesis, is proposed. Fronesis combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain (CKC) model [2], and the digital artifacts acquired from the monitored computer system with 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.

4. SYSTEM DESIGN

4.1 USE CASE DIAGRAM



4.2 SEQUENCE DIAGRAM



5. IMPLEMENTATION

5.1 Input and Output Designs

5.1.1 Logical design

The logical design of a system pertains to an abstract representation of the data flows, inputs and outputs of the system. This is often conducted via modeling, using an over-abstract (and sometimes graphical) model of the actual system. In the context of systems design are included. Logical design includes ER Diagrams i.e. Entity Relationship Diagrams

5.1.2 Physical design

The physical design relates to the actual input and output processes of the system. This is laid down in terms of how data is input into a system, how it is verified / authenticated, how it is processed, and how it is displayed as output. In Physical design, following requirements about the system are decided.

1. Input requirement,
2. Output requirements,
3. Storage requirements,
4. Processing Requirements,

5.2 Input & Output Representation

5.2.1 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple.

5.2.2 Objectives

Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

6. CONCLUSION

This paper proposed Fronesis; a digital forensics-based cyber-attack detection approach based on the combined utilization of the MITRE ATT&CK knowledge base, Lockheed Martin's Cyber Kill Chain (CKC) intelligence model, and digital artifacts acquired from the monitored system. Digital artifacts are acquired with proper sensors following digital forensics practices to ensure that the integrity of digital

artifacts is preserved. Fronesis examines the digital artifacts in order to recognize MITRE ATT&CK techniques, based on the traces left by the particular procedures of each technique. The recognized techniques are then associated with their MITREATT&CK tactics which are mapped to corresponding CKC phases. An ongoing cyber-attack is detected whether the phases are related based on their artifacts and in the correct chronological order. The realization of Fronesis was enabled via an ontology and rules represented respectively in the Web Ontology Language (OWL) and the Semantic Web Rule Language (SWRL) making Fronesis a ruled-based detection approach.

7. REFERENCES

1) W. Khan, A. Ahmad, A. Qamar, M. Kamran, and M. Altaf, ‘‘SpoofCatch: A client-side protection tool against phishing attacks,’’ IT Prof., vol. 23, no. 2, pp. 65–74, Mar. 2021.
2) B. Schneier, ‘‘Two-factor authentication: Too little, too late,’’ Commun. ACM, vol. 48, no. 4, p. 136, Apr. 2005.
3) S. Garera, N. Provos, M. Chew, and A. D. Rubin, ‘‘A framework for detection and measurement of phishing attacks,’’ in Proc. ACM Workshop Recurring malcode, Nov. 2007, pp. 1–8.
4) R. Oppliger and S. Gajek, ‘‘Effective protection against phishing and web spoofing,’’ in Proc. IFIP Int. Conf. Commun. Multimedia Secur. Cham, Switzerland: Springer, 2005, pp. 32–41.
5) T. Pietraszek and C. V. Berghe, ‘‘Defending against injection attacks through context-sensitive string evaluation,’’ in Proc. Int. Workshop Recent Adv. Intrusion Detection. Cham, Switzerland: Springer, 2005, pp. 124–145.