BOOK CHAPTER | *"Intentions Speaks Louder Than Voice"*

Analysis of Attack Intention Recognition

Tsatsu K. Sabblah
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: tsabblah@gmail.com
Phone: +233244926764

ABSTRACT

With the rapid development of network technology, network security problems are gradually increasing, and the network attack situation is very severe (Chen, Yanhua, Li, & Gao, 2019). In a complex attack scenario, timely detection of potential attack behaviours and timely identification and pre-judgment of attack intentions are important components of security risks. However, the attack behavior in the network presents complexity, multi-step and uncertainty, which brings new technical challenges to attack intent analysis. Aiming at the problem that the attack intention of multi-step complex attack is difficult to identify. Intrusion intention recognition is to interpret and judge the purpose, vision and intention of attackers through analyzing a large number of low-level alarm information, which is to give a reasonable explanation of a large number of attack data. This paper focuses on identifying attack intention in order to can determine the real purpose of attackers and predict the subsequent attack behavior, which is the premise and foundation of threat analysis and an important part of network security situation awareness.

Keywords: Attack Intention, Multi-Stage Attack, Networks, Casual Network Approach, Systems, Cyber Security

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Tsatsu, K. Sabblah (2022): Analysis of Attack Intention Recognition
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 259-262
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P41

1. INTRODUCTION

Today's information systems face sophisticated hackers who combine multiple vulnerabilities to penetrate networks with devastating impact (Hu, Liu, Yang, Zhang, & Zhang, 2018). Most network attacks are not single attack actions. They are multistage, multihost attacks, which are composed of a series of attack actions, leading to the network security facing huge threats and challenges. Attack intention and path evaluations aim to model and measure the security related properties of hacker breaching the enterprise network from the attacker's perspective, which allows the administrator to quantitatively estimate the overall resilience of network systems against attacks (Hu, Liu, Yang, Zhang, & Zhang, 2018).

2. RELATED LITERATURE

There are a number of papers that present approaches for classification and detection of cyberattack network flows, with varying accuracies tested on different datasets. Perry et al., (2018) in their study on differentiating and predicting cyberattack behaviours applied LSTM-RNNs using the 2017 Collegiate Penetration Testing Competition (CPTC) dataset. They were able to train one model for classifying attack teams and another for predicting the next alert. The first model was found to have a 55% classification accuracy by using only the first 80% of an attack sequence. The prediction model achieved 80% accuracy with 80% training. The models produced however did not differentiate between different attack types and did not present an algorithm that could be applied in real time classification and prediction.

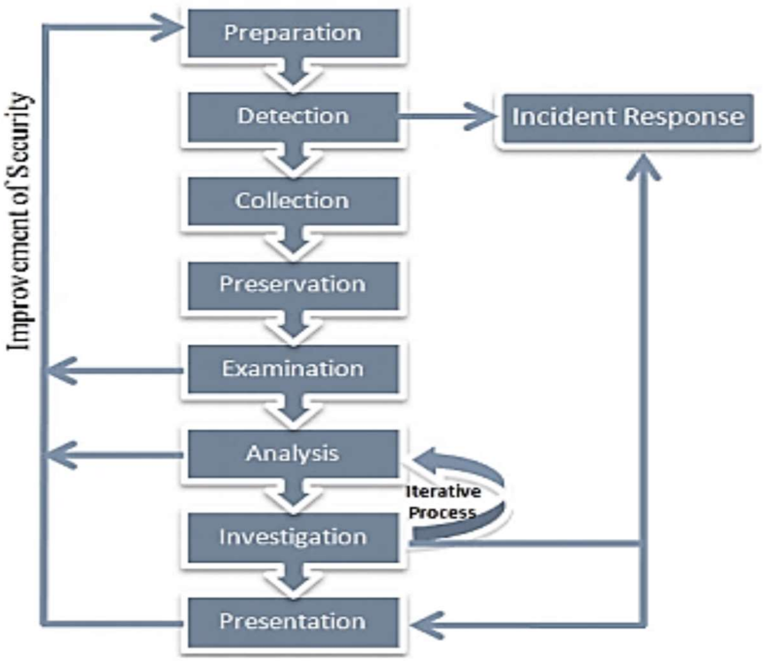

Figure 1: Generic Process Model
Source: (Ahmed & Zaman, 2017)

3. RESEARCH GAPS

Existing protection systems are still limited in their capacities to ensure network information has sufficient, confidentiality, integrity, and availability.

4. RESEARCH FINDINGS

An attack path analysis model approach to constructing attack path graphs can also recognize the intrusive intention and simultaneously calculate the threat of intention. This approach can offer protective measures at minimum cost with the theory of minimum cut. Four models have been used to analyse attack intention recognition. These are casual network, attack path, Graphical and Dynamic Bayesian networks. Each of these models have their own limitations:

Table 1: Models for Analyzing Attack Intentions

Model	Limitation
Casual Network	-If malicious actions are different from the predefined scope of attack, it is hard to identify them. -It is difficult to distinguish deception and actual plans of attackers. -It is difficult to determine the actual number of attackers
Attack path	-Only presents the first step toward identifying intrusive intention
Graphical	-Only presents the first step toward identifying intrusive intention
Dynamic Bayesian networks	-Given that the attack assumption is based on the latest action, it will not work in a case of uncertain attack.

5. IMPLICATIONS FOR ONLINE SAFETY AND CYBERCRIME PROSECUTION IN AFRICA

Africa is rapidly expanding in terms of population, economics, and global significance. Africa now has 1.21 billion people (up from 800 million in 2000), with a median age of only 19.5 years, making it the world's youngest population (Symantec Corporation, 2016). With the rise of youth comes a diversified population seeking meaningful jobs, social participation, freedom of expression, and enhanced global connectivity. Mobile smart device ownership is increasing exponentially, social media use is increasing, and the Internet of Things (IoT) is becoming a reality in Africa.

Even the most conservative assessments indicate that Africa is ready to make significant gains and contribute to global growth in the future (Symantec Corporation, 2016). However, with increased wealth and technology come new risks and weaknesses that could stymie progress. Policymakers will need to implement effective policies and awareness initiatives to stem the rising tide of cyber threats in order for Africa to realize its full potential and reap the full dividend from the development of the digital economy, which is the most important driver of innovation, competitiveness, and growth today.

6. CONCLUSION

The rapid development in network technologies has only helped increase network attacks and hide their malicious intent. Attack intention is the ultimate attack goal which the attacker attempts to achieve by executing various methods or techniques, and recognizing it will help security administrators select an appropriate protection system.

7. RECOMMENDATION FOR POLICY AND PRACTICES

Although several antivirus software, firewalls and IDS exist to detect and protect IT infrastructures from many known kind of cyberattacks, cybercriminals in turn have become more skilled in developing new advanced and more complex techniques to gain access and damage critical IT infrastructure. There will be a need to develop future policies on the application of machine learning that will pave a way to develop cyber defense methods that can automatically detect any unusual new patterns in network traffics.

8. DIRECTION FOR FUTURE WORKS

Using a casual network approach is effective for detecting network attacks that have similar intentions. For future study, an experiment should be performed to evaluate the efficiency of detecting an attack's intention.

REFERENCES

1. Ahmed, A. A., & Zaman, N. A. (2017). Attack Intention Recongnition: A Review. *International Journal of Network Security* , 244-250.
2. 2. Chen, B., Yanhua, L., Li, S., & Gao, X. (2019). Attack Intent Analysis Method Based on Attack Path Graph. *9th International Conference on Communication and Network Security*, (pp. 97-102).
3. 3. Chuanlong, Y., Zhu, Y., Fei, J., & He, X. (2017). 'A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*, (pp. 21954-21961).
4. 4. Hu, H., Liu, Y., Yang, Y., Zhang, H., & Zhang, Y. (2018). New Insights into Approaches to Evaluating Intention and Path for Network Multistep Attacks. *Mathematical Problems in Engineering* , 1-13.
5. 5. Perry, Ian, Li, L., Sweet, C., Su, S.-H., Cheng, F.-Y., & Yang, S. J. (2018). Differentiating and Predicting Cyberattack Behaviors Using LSTM. *IEEE Conference on Dependable and Secure Computing*, (pp. 1-8).
6. L. Sikos (2020): Packet analysis for network forensics: A comprehensive survey Computer Science. Digit. Investig.. DOI:10.1016/j.fsidi.2019.200892Corpus ID: 212863330