BOOK CHAPTER | *"Beyond Intentions"*

Attack Intention Recognition Techniques

Terry Kwaku Boateng
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: terry.boateng77@gmail.com
Phone: +233550349706

ABSTRACT

When sensitive information is transmitted over computer networks, it faces serious risks. Existing security systems are still limited in their ability to ensure the confidentiality, integrity, and availability of network data. The rapid advancement of network technologies has only aided in the proliferation of network attacks and the concealment of their malicious intent. This paper examines attack types and the method of observing an attacker's behavior and inferring his intent using known attack scenarios. Attacks have gotten more deadly than ever as networking technology advances, deploying new safeguards to disguise harmful conduct. The ultimate attack goal that the attacker attempts to achieve by executing various methods or techniques is known as attack intention, and recognizing it will assist security administrators in selecting an appropriate protection system.

Keywords: Attack Intention Recognition, Causal Network Approach, Cyber Security, Network Forensics Investigation.

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

Citation: Terry Kwaku Boateng (2022): Attack Intention Recognition Techniques
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 301-306
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P48

1. INTRODUCTION

As a result of the advancement of hacking and anti-forensics technology, information security over a network has become more difficult. In any system, sensitive information should be treated confidentially because it poses a great risk to the owners if it is made public. Human and technological failures, accidents and disasters, fraud, business espionage, and deliberate destruction are all potential threats to information. [1, 2, 4]. Activities such as unauthorized access, damage to computer data or programs, obstruction of the functions of computer systems or networks, interception of data, and computer espionage are categorized as cybercrimes [7, 8, 10, 11, 12, 13]. Cybercrimes are broad in scope and are defined as attacks that involve the use of computers or networks to commit the crimes. According to [3, 4, 9], cyber-attacks can be categorized into unauthorized access, malicious code (malware), and interruption of services.

Figure 1 shows common types of network threats. Network forensics, as a part of network security, works with laws and guiding principles established in the judicial system to deal with cyber criminals. Network forensics has two approaches: reactive and proactive. Reactive network forensics is a traditional approach that deals with cybercrime cases a period of time after an attack. The reactive forensic approach consumes considerable time during the investigation phase. Proactive network forensics is a new, different approach that focuses on investigating concurrently with an attack [5, 6].

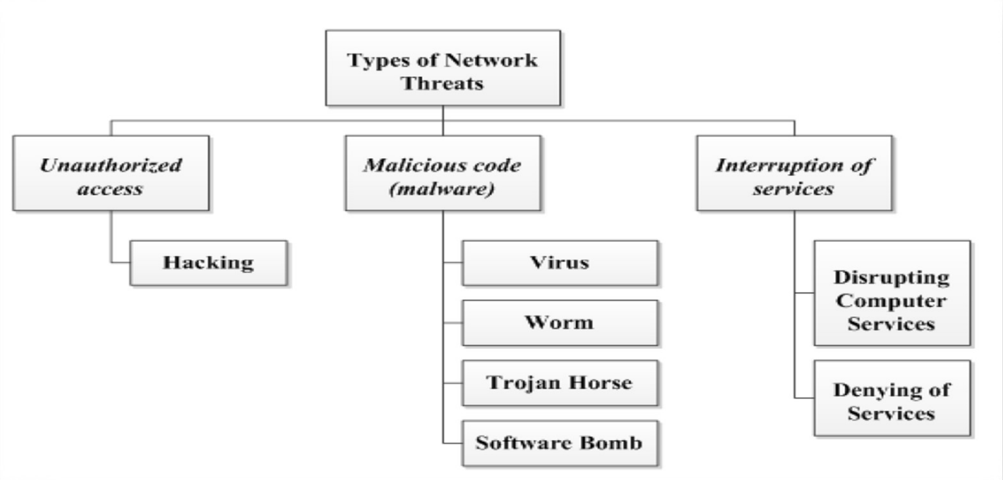

Fig 1: Common Types of Network Threats

2. RELATED LITERATURE

We provide below a tabular outlook for related literatures

Table 1: Related Literature

Author	Title	Findings and Conclusions
Abdulghani Ali Ahmed & Noorul Ahlami Kamarul Zaman	Attack Intention Recognition: A Review	Sensitive information faces critical risks when it is transmitted through computer networks. Existing protection systems are still limited in their capacities to ensure network information has sufficient confidentiality, integrity, and availability. The rapid development in network technologies has only helped increase network attacks and hide their malicious intent. This paper analyzes attack types and classifies them according to their intent. A causal network approach is used to recognize attackers' plans and predict their intentions. 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 and appropriate protection system.

Author	Title	Findings and Conclusions
Hao Bai, Kunsheng Wang, Changzhen Hu, Gang Zhang & Xiaochuan Jing	Boosting performance in attack intention recognition by integrating multiple techniques	In network forensics, attack intentions analyses play a major role to help and accelerate decision–making for apprehending the real perpetrator. Infact, attack intention analysis is a prediction factor to help investigators to conclude a case with high accuracy. However, current techniques in attack intention analysis only focus on recognizing an alert correlation for certain evidence and predicting future attacks. In reality, more prediction factors should be used by the investigators to come to a more concise decision such as attack intention, incident path …, etc. This paper will propose an attack intention analysis model, which focus on reasoning of attacks under uncertainty intention. A new model will be introduced using a combination of a mathematical Dempster–Shafer (D-S) evidence theory with a probabilistic technique through a causal network to predict an attack intention. We found that by analyzing the attacker's intention, forensic investigation agents will be able to audit and perform evidence in an efficient way. Experiments were performed on samples of probability of attack intentions to evaluate the proposed model. Arguably, attack intention analysis model may produce a clear and impact factor for investigator decision–making.
Abdulghani AliAhmed & Mohammed Falah Mohammed	SAIRF: A similarity approach for attack intention recognition using fuzzy min-max neural network	Sensitive information can be exposed to critical risks when communicated through computer networks. The ability of cybercriminals to hide their intention to attack obstructs existing protection systems causing the system to be unable to prevent any possible sabotage in network systems. In this paper, we propose a Similarity approach for Attack Intention Recognition using Fuzzy Min-Max Neural Network (*SAIRF*). In particular, the proposed *SAIRF* approach aims to recognize attack intention in real time. This approach classifies attacks according to their characteristics and uses similar metric method to identify motives of attacks and predict their intentions. In this study, network attack intentions are categorized into specific and general intentions. General intentions are recognized by investigating violations against the security metrics of confidentiality, integrity, availability, and authenticity. Specific intentions are recognized by investigating the network attacks used to achieve a violation. The obtained results demonstrate the capability of the proposed approach to investigate similarity of network attack evidence and recognize the intentions of the attack being investigated.

Author	Title	Findings and Conclusions
Wu Peng, Zhigang Wang & Junhua Chen	Research on Attack Intention Recognition Based on Graphical Model	Intention recognition is the ability to predict an opposing forcepsilas high level goals. Knowing an attackerpsilas intention can support the decision-making of the network security administrators. Furthermore intent analysis plays an import role in the calculation of the inherent threat value. So how to recognize attack intention has become a research hot in network security domain recently. In this paper taxonomy of attack intention characterized by consequences of attack and targets of attack is introduced at first. Then a graphical model based on network security state is presented and used to recognize attack intention. D-S evidence theory is also introduced to deal with the uncertainty in the process of intent inference. Next algorithms of intention recognition and threat assessment are given in detail in order to offer a way to assess the network security situation. Finally several experiments are done in a local network. The results of the experiments prove the feasibility and validity of this method.
Abdulghani Ali Ahmed	Investigation Approach for Network Attack Intention Recognition	Sensitive information has critical risks when transmitted through computer networks. Existing protection systems still have limitations with treating network information with sufficient confidentiality, integrity, and availability. The rapid development of network technologies helps increase network attacks and hides their malicious intentions. Attack intention is the ultimate attack goal that the attacker attempts to achieve by executing various intrusion methods or techniques. Recognizing attack intentions helps security administrator develop effective protection systems that can detect network attacks that have similar intentions. This paper analyses attack types and classifies them according to their malicious intent. An investigation approach based on similarity metric is proposed to recognize attacker plans and predict their intentions. The obtained results demonstrate that the proposed approach is capable of investigating similarity of attack signatures and recognizing the intentions of Network attack.

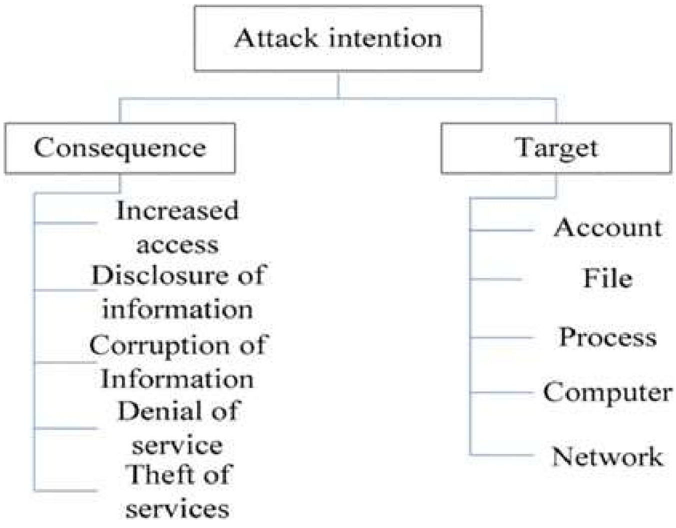

Figure 2: Attack Intention

3. RESEARCH GAPS/FINDINGS

Relevant information was found during the research and has proven that there are different types of attack intention recognition techniques and examines various attack types. Some research went to classify them according to their intent. A gap that was discovered within various researches was the ability to evaluate the efficiency of detecting an attack's intention.

4. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

Cyber safety in Africa needs to move from the usual traditional approach, which is the Reactive network forensics approach which deals with cybercrime cases after an attack to the new Proactive network forensics approach, which focuses on investigating concurrently with an attack. The Proactive network forensics has merits in saving time and money during investigation, as they work concurrently with the occurrence of the cybercrime. Understanding attackers' behavior will help network and security administrators recognize their intentions and better predict their activities.

5. CONCLUSION

This article examines several methods for recognizing attack intentions, including causal networks, path analysis, graphical attacks, and DBNs with Markova assumptions. These approaches are interrelated and distinct from one another. We conclude that a causal network technique is useful for identifying network assaults with comparable objectives based on a survey of existing literature and a careful evaluation of its benefits and drawbacks. For future research, an experiment will be conducted to examine the effectiveness of detecting the intent of an attack. This can involve testing multiple approaches for detecting attack intentions and observing how each strategy operates in a real-world lab context.

REFERENCES

[1] A. A. Ahmed, A. Jantan, and M. Rasmi, “Service violation monitoring model for detecting and tracing bandwidth abuse," Journal of Network and Systems Management, vol. 21, no. 2, pp. 218-237, 2013.

[2] A. A. Ahmed, A. Jantan, and T. C. Wan, “Sla-based complementary approach for network intrusion detection," Computer Communications, vol. 34, no. 14, pp. 1738-1749, 2011.

[3] A. A. Ahmed, A. Jantan, and T. C. Wan, “Real-time detection of intrusive traffic in qos network domains,"IEEE Security & Privacy, vol. 11, no. 6, pp. 45-53, 2013.

[4] A. A. Ahmed, A. Jantan, and T. C. Wan, “Filtration model for the detection of malicious traffic in large scale networks," Computer Communications, vol. 82, no. 59-70, pp. 15-23, 2015.

[5] A. A. Ahmed, A. S. Sadiq, and M. F. Zolkipli,"Traceback model for identifying sources of distributed attacks in real time," Security and Communication Networks, 2016.

[6] M. Rasmi and A. Al-Qerem, "Pnfea: A proposal approach for proactive network forensics evidence analysis to resolve cyber crimes," International Journal of Computer Network and Information Security, vol. 7, no. 2, pp. 1-25, 2015.

[7] T. W. Che, J. F. Ma, Na Li, and C. Wang, "A security quantitative analysis method for access control based on security entropy," International Journal of Network Security, vol. 17, no. 5, pp. 517-521, 2015.

[8] B. B. Gupta, R. C. Joshi, and M. Misra, "Ann based scheme to predict number of zombies in a ddos attack.," International Journal of Network Security,vol. 14, no. 2, pp. 61-70, 2012.

[9] M. S. Hwang and C. C. Lee, "Research issues and challenges for multiple digital signatures.," International Journal of Network Security, vol. 1, no. 1, pp. 1-7, 2005.

[10] C. C. Lee, M. S. Hwang, and I-En Liao, "On the security of self-certified public keys," International Journal of Information Security and Privacy, vol. 5, no. 2, pp. 55-62, 2011.

[11] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol.," International Journal of Network Security, vol. 15, no. 1, pp. 64-67, 2013.

[12] S. Saurabh and A. S. Sairam, "Increasing accuracy and reliability of ip traceback for ddos attack using completion condition," International Journal of Network Security, vol. 18, no. 2, pp. 224-234, 2016.

[13] Z. Yunos, R. Ahmad, and N. A. M. Sabri, "A qualitative analysis for evaluating a cyber terrorism framework in malaysia," Information Security Journal: A Global Perspective, vol. 24, no. 1-3, pp. 15-23, 2015.