International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.297-308
http://dx.doi.org/10.14257/ijsia.2016.10.5.28

Improving Analysis Phase in Network Forensics By Using Attack Intention Analysis

Mohammad Rasmi[1,*], Khaled E. Al-Qawasmi[2]

[1]*Department of Software Engineering,* [2]*Department of InternetTechnology*
Zarqa University, Zarqa, 13132, Jordan
[1]*mmousa@zu.edu.jo,* [2]*kqawasmi@zu.edu.jo*

Abstract

The increasing amount of cyber crimes has motivated network forensics researchers to develop new techniques to analyze and investigate these crimes. Reconstructing useful evidence of a cybercrime is difficult due to the vagueness of the analysis phase processes. The analysis phase is challenging because it provides detailed information on the intention and strategy of the attack. This paper aims to show the importance of reconstructing attack intentions in order to improve the analysis phase in network forensics. Intentions are identified through an algorithm called Attack Intention Analysis, which predicts cyber crime intentions by combining mathematical evidence theory and a probabilistic technique. In this paper, the attack intention model will be improved to present the motivation behind cyber crimes. The results of the comparison of the attack intention analysis methods prove that the AIA algorithm is more accurate.

Keywords*: Cyber Crime, Attack Evidence, Network Forensics, Attack Analysis, Attack Intention.*

1. Introduction

Based on the McAfee Labs Threats Report in August 2015, the attacker types, and their resources are expanded which increase the sophisticated cybercrime as shown in Figure 1. Nowadays, most organizations develop their IT system based on new techniques, such as Cloud Computing, Internet of Things (IoT), and Big data. Accordingly, the cybercrime effects into different types of network and devices. [1]

Analysis phase in network forensics involves determining the significance of the cybercrime data by drawing conclusions based on evidence of the cyber crime. Also, it supports the investigation phase to establish an accurate decision and minimize the time and cost of the investigation process by utilizing well-analyzed cyber crime evidence. However, the analysis phase should support the investigation phase to extract useful evidence to clearly understand the intentions and techniques of the cybercrime attackers [2, 5]. Pilli et al. reported, feedback of the analysis phase can be utilized to improve the security tools. However, according to Baryamureeba and Tushabe and Pilli et al., the analysis phase faces plenty of challenges and is improperly defined.

The lack of network forensic standardization and expertise makes the analysis phase more difficult [3-7]. Furthermore, the amount of evidence collected from raw traffic has increased. Thus, complex processes are essential to analyze all evidences [8].

Most techniques, such as alert correlation and intrusion scenario that work within IDS, are also utilized in network forensics to understand and analyze cyber crime behavior. The drawback of most of these techniques is that they are created to prevent future attacks and minimize cybercrime damage. These techniques are not developed to specifically analyze evidence in network forensics to resolve cyber crimes [4, 9, 10]. Therefore,

* Mohammad Rasmi is the Corresponding Author

ISSN: 2005-4262 IJGDC

innovative methods and techniques are required in the analysis of cyber crime evidence to help investigators in decision-making. The analysis of cyber crime evidence should produce useful information and increase the possibility of obtaining evidence based on attack intention and strategy.

The main aim of security analysts is to recognize cybercrime tactics. The analysis of the cyber crime plan reconstructs the scenario to determine the attack intention and strategy through a graph algorithm with methods for intrusive intention recognition. This algorithm was utilized by [11, 12]. Attack recognition is a significant research area in artificial intelligence and is still being developed in network security domain; as such, intention and strategy analysis has become an important research topic [11, 12].

Recently, there is a need of security analysts as mentioned by US Department of Labor's Bureau of Labor Statistics states that "Employment of information security analysts is projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations."

Determining the reasonable factors such as attack intentions and similar attack strategies increases the possibility of obtaining cyber crime evidence. These factors reduce the amount of effort and processing cost during the investigation phase by maximizing the probability ratio of retrieving similar cyber crime cases. Attack intention as the main factors in the network forensic analysis phase are described in the succeeding sections. The suitable analysis methods, such as mathematical theories, and probabilistic techniques are also explained.

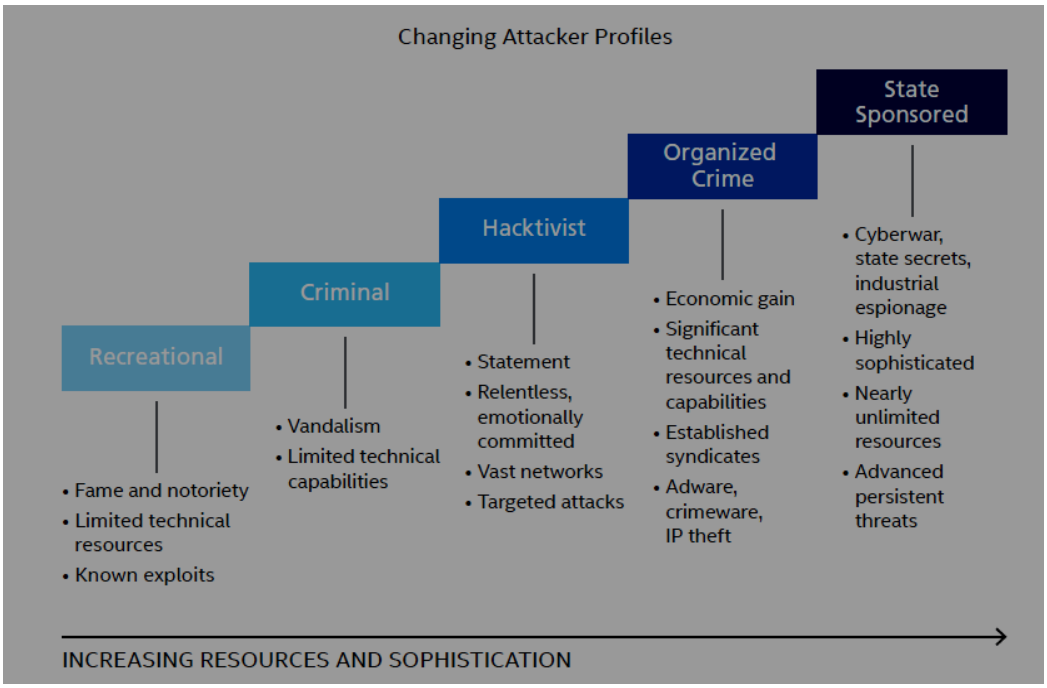

Figure 1. The Expansion Of Attacker Types, Their Resources, And Their Sophistication. [1]

2. Related Work

Attack intention analysis infers the motive of an attack based on the cyber crime actions. In addition to providing more details about the evidence of the cyber crime and the behavior of the attacker, thereby making the identification of the criminal easier.

Attack intention affects arbitrary and appropriate adjudication because it explains the motive of the cybercrime attack. According to a May 23, 2012 report written by Finklea and Theohary, "without knowing the criminal intent or motivation, however, some activities of cyber criminals and other malicious actors may appear on the surface to be similar, causing confusion as to whether a particular action should be categorized as cyber crime or not." Thus, establishing the attack intention is necessary to generate accurate data to enhance the investigation process through decision making and to apprehend the real perpetrator.

Attack intention is established when a potential attack is predicted, as mentioned by [12], and when the goal of an attacker is identified. Recently, cyber attacks have become more complicated, which makes determining the real intentions more difficult. Even experts have difficulty determining the method of intrusion [10]. An attacker goes through an order of logical steps to reach his goal and utilizes tools to hide or camouflage his patterns from his victims. Therefore, changing attack patterns are a major challenge in network forensics [5]. According to Huang et al. [10], network environments with a large number of attack methods make pattern recognition more difficult. For example, the main problem in IDS is false reading (either false positive or false negative), especially in misuse-based and anomaly-based detection as described by [9-11]. In short, the limitations of the security sensors and network monitoring tools make attack observation inaccurate and incomprehensible [11].

The architecture proposed by Huang et al. [10] analyses intention by predicting potential attack behavior through IDS, where the attack intention represents the attack goal. The goal tree, which is a graphical representation of the reduction of goals to sub-goals, is utilized in this architecture. The "OR", "AND", and "ordered-AND" tree is an instance representation of the goal tree that represent the search area to determine the goal of the cyber crime. In addition, the aforementioned architecture represents the attacker's intention to integrate the management in the intrusion. The disadvantages of this architecture on the attack intention analysis are summarized as follows:

- Limited to the attacks that follow a specific path and apply the same strategy.
- Limited to attacks that are related, ordered, and have correlated steps, such as flooding, spoofing, and sniffing attacks.

The probabilistic approach was introduced by [11] to correlate and analyze attacks. The Defense Advanced Research Projects Agency and Grand Challenge Problem data were utilized to evaluate this approach. Two data sets were used to identify these strategies, correlate isolated scenarios, and predict future attacks. The probabilistic approach employs a probabilistic-based reasoning method and statistical analysis through casual networks for attack correlation. The causal network is a Bayesian network that represents the probabilistic relationships between pieces of cyber crime evidence. In addition, this approach has been utilized by [11] to minimize the damages in the system by developing an algorithm to correlate the attack scenario in the low-level correlation analysis. The main component of the probabilistic approach is an attack tree obtained from a defined library of attacks.

An attack scenario should have a hierarchical architecture [11]. An attack tree utilized to define the attack libraries and then incorporated into the causal network by assigning the probability of evidence and likelihood of the attack intentions. An attack tree analysis predicts a set of attack libraries represented by a graph and linked to the attack graphs. Typically, this approach is time-consuming due to the manual implementation. The alternative technique employs the checking model [14] as an automatic graph to construct the attack. According to Qin and Lee [11], the strength of this model lies in the ability to evaluate protocols efficiently. This model is also more robust than other techniques, such as simulation or theorem techniques, but it has limited scalability.

Technique that employed by [12] depends on determining the intention from the attack path. The researchers presented an attack path graph generation algorithm to propose a

method for intrusive intention recognition. They concluded that the proposed method is incomplete and represents only the initial phase of attack intention. Moreover, the researchers found that attack intentions depend on the vulnerability of the attack, which means that the technique is unsuitable for large amounts of evidence.

A new architecture of the intrusive intention recognition model was presented by [15], which based on the security state graph to recognize intrusive intentions. They designed an algorithm to generate security state graphs for intention inference. According to the researchers, the main behavioral intentions of an intruder (such as DoS on the Web server on a host, gain root privilege of a host, and compromise database on a host) are established through time observation, launch host, target host, and rules, such as intruder preconditions, network preconditions, intruder effects, and network effects.

A new taxonomy of attack intention was proposed by [16], which determines attack intentions with the Dempster-Shafer (D–S) evidence theory; a mathematical theory of evidence that generalizes the Bayesian probability theory. The technique of the new taxonomy follows the stages of the attack and determines the target. The taxonomy classifies attacks into two types; the first type is consequence-based attacks, such as increased access, disclosure of information, and denial of services. The second type classifies attacks through targets, such as computers, networks, and files. The technique combines the state of each intruder in terms of capability, skills, and tools with the state of the system, such as interest and opportunity, to determine the intention list and attack likelihood and to estimate the threat. However, the technique predicts future attacks depending on the identified intentions. The D–S evidence theory that was applied in this research did not use or mention the main concepts of the D–S evidence theory: belief and plausibility functions. The D–S technique is most similar to the technique proposed by [15]; both techniques employ the same algorithm to generate a security state graph.

The generating attack scenario method was applied by [17] to recognize attack intention. They employed a forward-search algorithm to generate the attack scenarios and describe the attack intentions. However, this method does not calculate the probability of attack intentions, which must be done in future studies. This method differs from other methods in utilizing a search algorithm to generate the attack scenario. The search algorithm is utilized with an alert aggregation module to determine the attack intentions through the attack behavior. Attack behavior is represented by post condition, pre-condition, attack type, attack destination, and attack source. Thus, this method is limited to a specific type of evidence.

An integrated method was proposed by [18] to reconstruct the attack path and intentions. In addition to correlating the alerts generated from IDS or other security tools to construct the attack scenario. The proposed method employs the Frequent Pattern (FP) growth algorithm to determine the frequent attack patterns. These patterns are then rebuilt and re-correlated to reconstruct the attack path. The FP-growth algorithm works with frequent patterns without candidate generation by compressing a large database into a compact FP-tree structure. Jiawei et al. [19] provided elaborate details about the FP-growth algorithm.

The method that been utilized to integrate multiple techniques is significant because it correlates the alerts of the attack with frequent pattern mining techniques to rebuild the attack path. The proponents of this method claim that the method can be utilized when a complete follow-up attack intention analysis is required. However, the method cannot analyze attack intentions completely. It only recognizes the intentions individually based on the attack path steps, which are considered evidence.

This paper concludes that the techniques proposed to reconstruct the attack path in advance to enhance the ability of alert correlations in IDS are not specifically for cyber crime analysis in network forensics. Most of these techniques are limited to variety-types of attacks, especially multi-stage attacks, and do not present all the potential attack intentions.

A causal network is defined in the form of a causal polytree with observable quantities and unknown parameters or hypotheses, as mentioned by [9, 11]. A polytree is a directed graph with exactly one directed path between any two nodes. A causal network is a Bayesian network that explicitly requires causal relationships. The Bayesian network is a probabilistic graphical model; it is a statistical model that represents knowledge about an uncertain domain through a set of random variables, such as nodes, and pre-defines the dependency relationship between these variables as edges. This present study is interested in uncertain evidence, such as the destination IP address and locations and types of services, to analyze attack intentions, which are uncertain factors in cyber crimes.

The causal network is an important component of security research. Its application was described in the preceding sections. The causal network is employed to recognize the attack plan, establish the attack strategies, and determine the alert correlation to construct the attack scenario [9, 11]. The technique proposed by [18] is employed to recognize the attack intentions. According to [20, 21], the causal network can be combined with CBR to establish causal knowledge of cyber crimes and evidence to optimize performance when developing an actual system.

The research [27] employs a causal network to represent the probabilistic relationship among attacks, evidence, and attack intentions. The causal network is also utilized because it can determine observable quantities and unknown parameters or hypotheses. When an attack intention is established, the causal network predicts the impact of external intervention based on the data obtained prior to the intervention.

The Dempster-Shafer (D–S) theory was introduced by Shafer in 1976 as a new approach to representing the uncertainty of evidence. This mathematical theory generalizes the Bayesian probability theory. The D–S theory is not commonly applied because the formalism of this theory is difficult to understand. The D–S theory is considered as one of the most interesting alternatives in the field of reasoning with uncertainty [22]. Bayesian networks or fuzzy sets are often utilized in the reasoning field where the D–S theory is more relevant.

From a different view, Shi et al. [23] stated that the D–S theory has the advantage of its ability to present and process information. The theory is an issue, especially in multi-sensor data fusion. The D–S theory helps identify epistemic probabilities or degrees of belief. It combines evidence from different sources represented by a belief function and considers all the available evidence.

The D–S evidence theory was employed by [24] in the security field to investigate a new traffic incident pattern recognition approach. They employed the D–S theory to combine the results from the multi-class probability support vector machines with the data set from different sources to improve the accuracy and robustness of the fault diagnosis. A new detection fusion called the intrusion detection system data fusion model was presented by [25] to correlate and merge alerts produced by different IDSs. According to the researchers, the use of the D–S theory as a part of the investigation provides effective solutions to IDS problems in terms of alert correlation and detection accuracy.

The research [27] applies the basic rules of the D–S theory to determine the potential attack intentions. The D–S theory adopted by [16] to determine attack intentions. The D–S evidence theory applied in the [16] research did not consider the main concepts of the theory nor the beliefs and plausibility functions.

3. Intentions Analysis in Network Forensics

Investigators consider several prediction factors, such as attack intention and strategy, to come up with a more precise decision. Attack intention analysis as a prediction factor helps accelerate the decision-making process for the apprehension of the real perpetrator. However, most of the currently used techniques for attack intention analysis are focusing on recognizing the alert correlation among certain pieces of evidence.

This section presents the attack intention analysis that focuses on the reasoning behind uncertain intentions. The attack intention analysis model as proposed by [26] is improved and introduced in this phase. The new model that combines the mathematical D–S evidence theory with a probabilistic technique through a causal network to predict attack intentions is also introduced.

Figure 2. presents the set of processes that determines attack intentions, and it is improved from the proposed model in [26]. The attack type must be detected according to the predefined processes. Attack features should be constructed to establish the correlation among the collected evidence. This set of processes must be defined before analyzing attack intentions. The processes of preparation, detection, collection, and examination of evidence in generic network forensics [5] should be predefined as mentioned before.

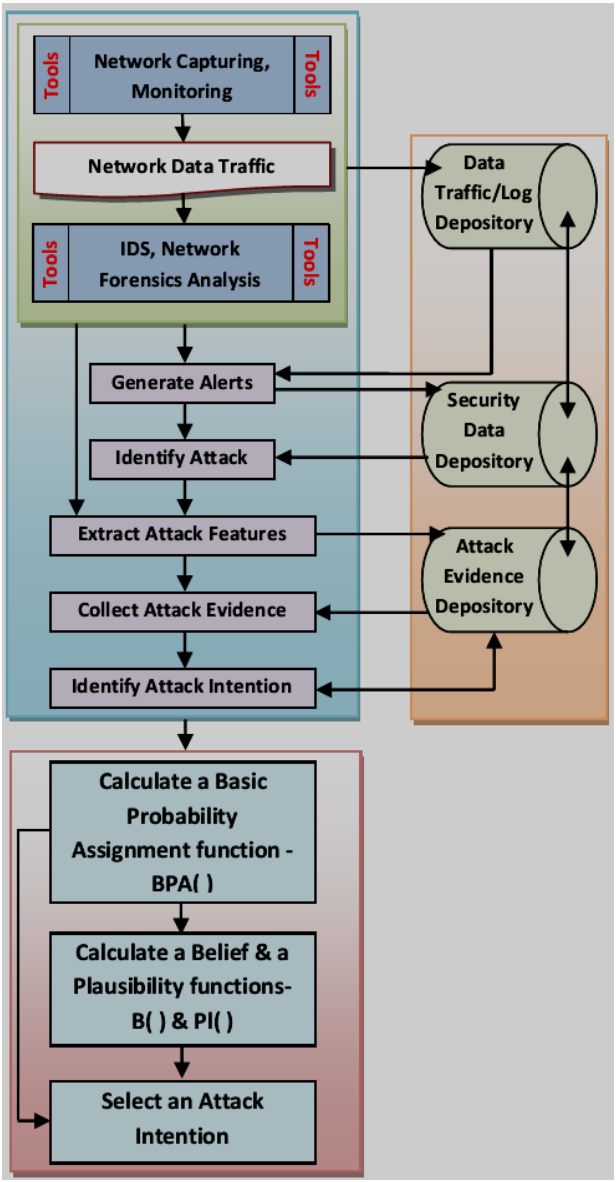

Figure 2. Attack Intention Process Model Based on D-S Evidence Theory

The new model adopts the D–S theory to identify uncertain intentions and determine the intentions that can be ignored or discarded. The causal network represents the probabilistic relationship of attacks, evidence, and attack intentions.

The prediction of attack intentions depends on the nature of the attack, which is determined based on the attack evidence. The detection of attacks depends on the multiple security sensors and detection system products (both commercial and non-commercial security products, such as IDS). A specific attack occurs depending on the accuracy of these products. The proposed process model assumes that the attack is defined and detected accurately. This model assumes that the detection systems, whether open sources like Snort or commercial like Kaspersky, have been utilized to detect an attack. The ratio of the attack that is correctly detected is conducted after calculating the average of all the detection rates based on the detection systems.

Three major factors affect the process of defining intentions: preliminary hypotheses, the probability of the attack detection, and evidence collection. A preliminary hypothesis depends on the accuracy of the attack detection, evidence, and initial potential intention.

The probability ratio for each piece of evidence is computed through the probabilistic laws in the causal network according to the available evidence. The probability ratio of each intention with given conditional evidence is also computed depending on the probability results.

The proposed model can be used to better understand the algorithm of Attack Intention Analysis (AIA) which presented by [27].

4. Attack intention Analysis Phases

The flowchart in the Figure 3. helps to better explain the logic of the attack intention analysis component. It also illustrates the flow of cyber crime evidence through the component as the main operations of attack intention analysis are performed. These operations help investigators analyze evidence to predict attack intentions in a proactive manner.

The flowchart presents how the AIA algorithm [27] identifies attack intention. The AIA algorithm assumes that a set of uncertain attack intentions {i1, i2, i3 … in} exists; each one is connected and dependent on one or more pieces of evidence. Each intention has a low and unimportant prior probability between 0.001 and 0.006 that does not affect the prediction of real intentions. The prior probability of an attack intention represents the general assumption in real-life crime law that a suspect is innocent until proven guilty, which means that the attack intention approaches an undefined value in the first step.

The first phase of the flowchart identifies the new attack in advance through the security data repository to retrieve attack evidence from the attack evidence depository. The evidence set for the new attack called {EV} is generated. The set contains attack evidence. However, all the predefined attacks preserved in the attack evidence depository must be retrieved. The predefined attack with the evidence set {EV} generates an attack intention set for the new attack called {I}. The causal network is utilized in the second phase to assign a probability value to each piece of evidence in the set {EV} depending on the specific intention, which is computed based on the probability value for each attack intention in the set {I}. The second phase generates the attack intention hypothesis {H}, which describes the probability for each intention depending on one or more pieces of evidence. The hypothesis computes the Be( ), Pl( ), and BPA( ) functions through the D–S evidence theory. The Basic Probability Assignment (BPA) The BPA function is characterized by the exact belief in the proposition represented by the intention. The belief and plausibility probability are obtained from the BPA function. The function BPA() is called a belief or support function be( ) when it satisfies Be (Ø) = 0 and be (EVs) = 1, where EVs is a set of evidence. In other words, the function is the amount of justified support provided by EVs. The function is generally regarded as the lower probability function of the D–S theory in probabilistic formalisms. The plausibility function Pl( ) is the amount of potential support provided to EVs, which means that supporting evidence is not provided to EVs. The plausibility function is generally regarded as the upper

probability function of the D–S theory in probabilistic formalisms. The final phase selects the potential intentions, such as the high probability ratio of the BPA( ) function.

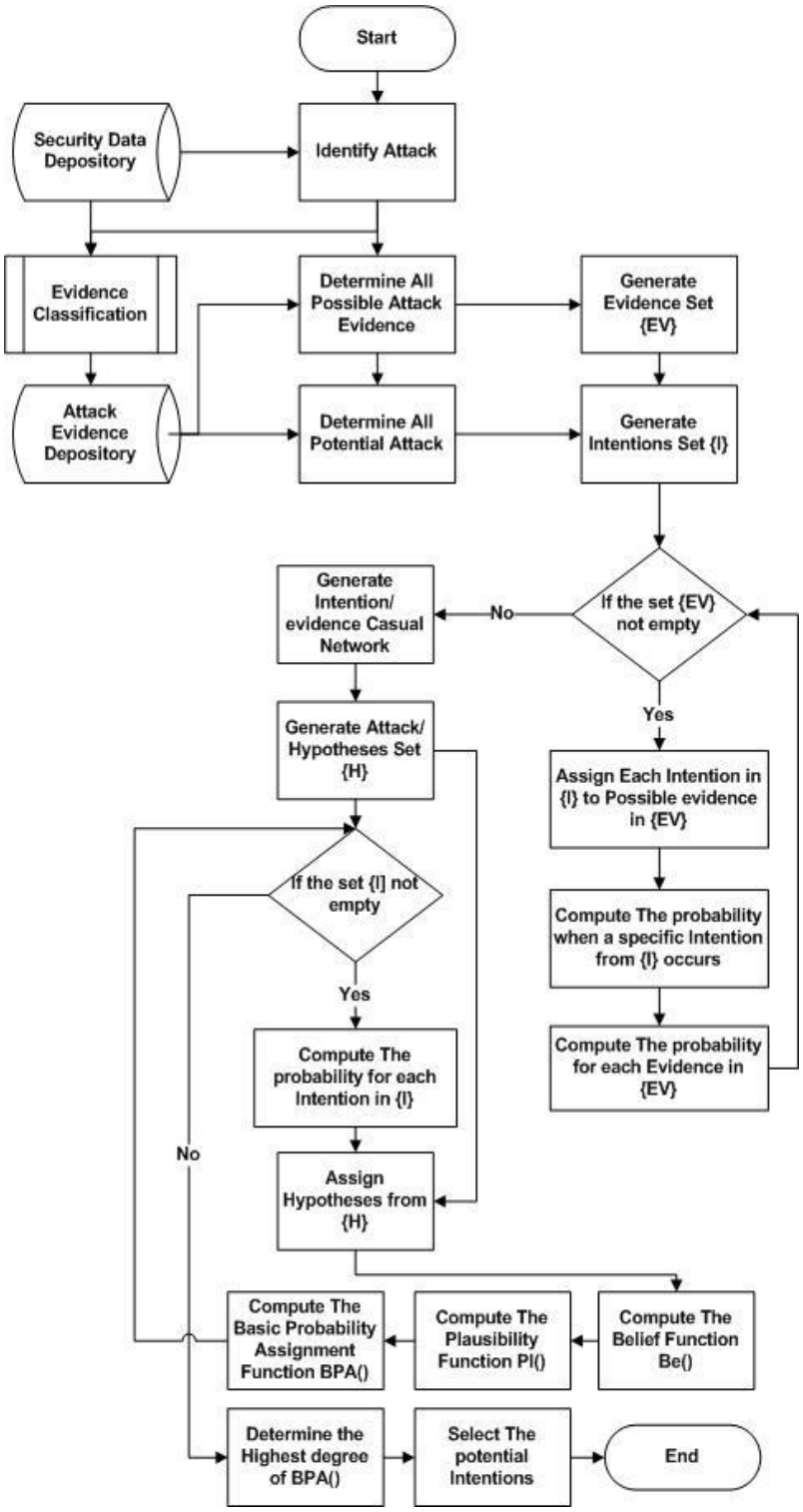

Figure 3. Attack Intention Analysis Flowchart

5. Comparison Results

Network security breaches are widely targeted by cyber attackers in the digital world. For example, botnets cause much harm in today's Internet world. Fortunately, a high

number of new malware that cause damage are detected and reported by network security detection and monitoring tools. The PCAP file for network data traffic is analyzed to apply the AIA algorithm to a backdoor attack [27].

An attack intention cannot be determined and attack cannot be solved without evidence [26, 27]. On the one hand, if the AIA algorithm collects a single piece of evidence for each intention, the probability of belief that this single piece of evidence is an actual attack intention will not be as accurate as when the evidence is combined with other evidence. On the other hand, an attack intention supported by more evidence increases the probability that it is an actual attack; thus, the accuracy of this intention increases.

The accuracy of prediction for any intention is related to the amount of collected evidence and the strength related to the intention. The amount of evidence affects the accuracy of detecting the BPA values. If we assume that intention has been influenced by five pieces of evidence and we detected only four particular pieces of evidence, the accuracy will be lower than if we detected accurately all the five pieces of evidence.

According to the results, which presented by [27], the backdoor attack was detected with 98.68% accuracy. The result shows that the potential attack intention was to spy on the users of the compromised machines (spying) and to spread the virus further by automatically scanning the entire network range and propagating the virus via vulnerabilities with a 0.595856914 probability ratio. The accuracy of the detection probability ratio of the attack intentions is 0.788. This accuracy value is calculated by the following equation:

Accuracy = (TPDR + TNDR) / (TPDR + TNDR + FPDR + FNDR)
Where

Accuracy is the ratio of the total number of correct attack intention predictions.

TPDR is the ratio of the attack that is correctly detected.

TNDR is the ratio of the attack intention that is correctly detected.

FPDR is the ratio of the attack that is incorrectly detected.

FNDR is the ratio of the attack intention that is incorrectly detected.

Most related studies in attack intention analysis [12, 15-18] as described above. Those researchers utilized a small sample for their experiments and evaluated their results based on specific evidence, such as CVE, OS, and host services. Table 1. shows the results of the comparison of the attack intention analysis that utilized the AIA algorithm with other analyzes. The results of the comparison are based on the evidence that used and appears in the related studies.

Most attack analysis approaches are based on alert correlation techniques. These techniques are connected to network forensic tool for assistance such as IDS to understand and analyze the cyber crime occurrence. The drawback of most of these techniques is that they are developed to prevent future attacks and minimize damage and not to analyze the cyber crimes through network forensics. Thus, innovative methods and techniques are needed in the analysis of the attacks to increase the amount of evidence by establishing the attack intention and strategy in advance, and help investigators in decision making and resolving cyber-crimes.

Table 1. A Comparison of the Attack Intention Analysis Results

	TPDR	TNDR	FPDR	FNDR	Accuracy
(Peng et al., [12])	0.980	0.019	0.981	0.020	0.500
(Wang and Peng, [15])	0.980	0.019	0.981	0.020	0.500
(Wu et al., [16])	0.980	0.019	0.981	0.020	0.500
(Hao et al., [18])	0.980	0.011	0.989	0.020	0.496
(Feng et al., [17])	0.980	0.034	0.966	0.020	0.507
(Rasmi and Aman, [27])	0.980	0.595	0.405	0.020	0.788

6. Conclusion and Future Work

This paper shows the importance of reconstructing attack intentions in order to improve the analysis phase in network forensics. The results of the comparison of the attack intention analysis methods prove that the AIA algorithm is more accurate. The aim of using AIA algorithm is to support the decision maker in selecting and predicting the actual attack intention by determining whether the best action is feasible or not. The intentions of the attack are determined, and the priority value is assigned to each one depending on the highest probability value after analyzing the evidence. The investigator determines the highest intention priority value.

Acknowledgment

This research is funded by the Deanship of Research and Graduate Studies in Zarqa University /Jordan.

References

[1] McAfee Labs Threats Report August 2015, http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf, (2015)
[2] Websense 2015 Threat Report, https://www.websense.com/assets/reports/report-2015-threat-report-en.pdf, (April 8, 2015)
[3] Mumba, E. R., & Venter, H. S., "Testing And Evaluating The Harmonized Digital Forensic Investigation Process In Post Mortem Digital Investigations", In Proceedings of the Conference on Digital Forensics, Security and Law (pp. 83-98), (2014)
[4] Vahid S Farrahi, Mahsa Kamali Sarvestani and Marzieh Ahmadzadeh, "A Novel Supervised Algorithm for Network Intrusion Detection with the Ability of Zero-day Attacks Identification", International Journal of Computer Applications, vol. 121, no. 19, (2015), pp. 47-50
[5] Pilli, E.S., R.C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges", Digital Investigation, vol. 7, no. (1-2), (2010), pp. 14-27.
[6] Baryamureeba, V. & Tushabe, F., "The Enhanced Digital Investigation Process Model", Proceeding of Digital Forensic Research Workshop. Baltimore, (2004)
[7] Mouhtaropoulos, A., Grobler, M. & Chang-Tsun, L., "Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives", Intelligence and Security Informatics Conference (EISIC), (2011)
[8] Merkle, L. D., "Automated network forensics,. In: Proceedings of the conference on genetic and evolutionary computation, (2008).
[9] Wei, W. and E.D. Thomas, "A Graph Based Approach Toward Network Forensics Analysis", ACM Trans. Inf. Syst. Secur., vol. 12, no. 1, (2008), pp. 1-33.
[10] Huang, M.-Y., R.J. Jasper, and T.M. Wicks, "A large scale distributed intrusion detection framework based on attack strategy analysis", Computer Networks, vol. 31, no. (23-24), (1999), pp. 2465-2475.
[11] Qin, X. and W. Lee., "Attack plan recognition and prediction using causal networks", in Computer Security Applications Conference, (2004)
[12] Peng, W., S. Yao, and J. Chen., "Recognizing Intrusive Intention and Assessing Threat Based on Attack Path Analysis. in Multimedia Information Networking and Security", International Conference, (2009)
[13] Finklea, K. M. & Theohary, C. A., "Cybercrime: Conceptual Issues for Congress and U.S", Law Enforcement. IN SERVICE, C. R., (May 23, 2012)

[14] Bonnie Brinton, A., James, V. H., Paul Benjamin, L. & Scott, L. S., "The application of model checking for securing e-commerce transactions" . Commun. ACM, vol. 49, (2006), pp. 97-101.
[15] Wang, Z. & Peng, W., "An Intrusive Intention Recognition Model Based on Network Security States Graph", Wireless Communications, Networking and Mobile Computing, (2009).
[16] Wu, P., W. Zhigang, and C. Junhua. "Research on Attack Intention Recognition Based on Graphical Model. in Information Assurance and Security", (2009).
[17] Feng, J., Yuan, Z., Yao, S., Xia, C. & Wei, Q., "Generating Attack Scenarios for Attack Intention Recognition", International Conference on Computational and Information Sciences. Chengdu, China, IEEE Computer Society, (2011)
[18] Hao, B., Kunsheng, W., Changzhen, H., Gang, Z. & Xiaochuan, J., "Boosting performance in attack intention recognition by integrating multiple techniques", Front. Comput. Sci China, vol. 5, (2011), pp. 109-118.
[19] Jiawei, H., Jian, P., Behzad, M.-A., Qiming, C., Umeshwar, D. & Mei-Chun, H. (2000) FreeSpan: frequent pattern-projected sequential pattern mining. Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining. Boston, Massachusetts, United States, ACM.
[20] Watson, I., "Case-based reasoning is a methodology not a technology. Knowledge-Based Systems", vol. 12, (1999), pp. 303–308.
[21] Aamodt, A. & Plaza, E., "Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches", Artificial Intelligence Communications, vol. 7, (1994), pp. 39-59.
[22] Burrus, N. & Lesage, D, "Theory of Evidence (DRAFT)",. IN CEDEX, L. K.-B. (Ed. France, Laboratoire de Recherche et Développement de l'Epita, (2003)
[23] Shi, C., Cheng, Y., Pan, Q. & Lu, Y., "A New Method to Determine Evidence Distance", International Conference on Computational Intelligence and Software Engineering (CiSE) Wuhan, (2010)
[24] Zeng, D., Xu, J. & Xu, G., "Data Fusion for Traffic Incident Detector Using D-S Evidence Theory with Probabilistic SVMs" , Journal of Computers, vol. 3, (2008), pp. 36-43.
[25] Tian, J., Zhao, W., Du, R., Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-M., Yin, H., Jiao, L., Ma, J. & Jiao, Y.-C. "D-S Evidence Theory and Its Data Fusion Application in Intrusion Detection Computational Intelligence and Security", Springer Berlin / Heidelberg, (2005)
[26] Rasmi, M., et al., "Attack Intention Analysis Model for Network Forensics", Software Engineering and Computer Systems, Springer Berlin Heidelberg, (2011), p p. 403-411.
[27] Rasmi, M. and A. Jantan, "AIA: Attack Intention Analysis Algorithm Based on D-S Theory with Causal Technique for Network Forensics - A Case Study". International Journal of Digital Content Technology and its Applications, vol.5, no. 9, (2011), pp. 230-237.

Authors

Mohammad Rasmi, is currently serving as an assistant professor in the Faculty of Science, Departments of Computer Science, Zarqa University. He received his PhD in Network Security from Universiti Sains Malaysia in 2013. He received a Master degree in Computer Information System from the AABFS in 2004, and BSc degree in computer science from Zarqa Private University in 1999. His research interests include network forensics, web security, E-government strategy, cloud computing and software engineering.

Khaled Alqawasmi, is working as Assistant Professor in the Department of Internet Technology at Zarqa University, Jordan. He obtained his PhD degree from Amman Arab University in 2010. His research interests include Digital Signal Processing (DSP), Software quality assurance, Multimedia, Web Engineering, web security, Web Semantic and Artificial Neural Networks.