World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:5, 2016

A Reasoning Method of Cyber-Attack Attribution Based on Threat Intelligence

Li Qiang, Yang Ze-Ming, Liu Bao-Xu, Jiang Zheng-Wei

***Abstract*—**With the increasing complexity of cyberspace security, the cyber-attack attribution has become an important challenge of the security protection systems. The difficult points of cyber-attack attribution were forced on the problems of huge data handling and key data missing. According to this situation, this paper presented a reasoning method of cyber-attack attribution based on threat intelligence. The method utilizes the intrusion kill chain model and Bayesian network to build attack chain and evidence chain of cyber-attack on threat intelligence platform through data calculation, analysis and reasoning. Then, we used a number of cyber-attack events which we have observed and analyzed to test the reasoning method and demo system, the result of testing indicates that the reasoning method can provide certain help in cyber-attack attribution.

***Keywords*—**Reasoning, Bayesian networks, cyber-attack attribution, kill chain, threat intelligence.

I. Introduction

WITH the rapid development and increasing complexity of computer systems and communication networks, a huge number of various devices connect to the Internet. Although it gives us facility on work and life, it still brings a great security risk, or even leads to a very serious consequence, such as cyber-attack. A special cyber-attack is targeted attacks. A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity [1]. Because those attackers have a certain level of expertise and sufficient resources to conduct their schemes over a long-term period; it is hard to defend targeted attack. For an individual, targeted attack leads to private information leakage. For enterprises and governments, targeted attack would lead to stopping the service or significant information leakage. Attribution of cyber-attack is important.

One definition of cyber-attack attribution is "determining the identity or location of an attacker or an attacker's intermediary [2]." The target of cyber-attack attribution is finding out the source of attacks among cyber space. There are several levels of attribution: 1) The host originating the attack, 2) Intermediary hosts, 3) ISPs through which the attack passes, 4) The individuals carrying out attacks, 5) The institutions supporting the attacks, 6) The political or government organization behind the attacks, 7) Geo-location of the attacks [3]. One result of attribution is slowing the paces of attacks. Powerful capacity of attribution is a kind of deterrence [4].

Lockheed Martin Corporation came up with the intrusion kill chain which is the basic of cyber-attack attribution analysis [5]. The intrusion kill chain defined seven steps of cyber-attack intrusion: Reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and action on objectives. These kill chain phases can describe the whole systematic process to target and engage an adversary to create desired effects. The use of intelligence-driven is a key component in this model and the indicator is the fundamental element of intelligence in this model.

Caltagirone et al. proposed Diamond model which breaks each cyber event into four vertices or nodes, the event is composed of four core features: Adversary, infrastructure, capability and victim [6]. Those features are edge-connected representing their underlying relationships and arranged in the shape of a diamond. It further defines additional meta-features to support higher-level constructs. The model provides opportunities to integrate intelligence in real-time for network defense, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies. Threat intelligence platform company ThreatConnect [7] used diamond model to analysis intrusion in APT report "Camerashy: closing the aperture on China's unit 78020" [8] .

Bayesian networks have strong reasoning ability in solving nondeterministic problems, which attract more and more attentions from lots of researchers. Zhai et al. [9] came up with an integrate and reason method using Bayesian networks about complementary intrusion evidence by alerts and report from security systems. Ning et al. [10] present a series of techniques to integrate two complementary types of alert correlation methods including those based on the similarity between alert attributes and those based on prerequisties and consequences of attacks, in addition, this paper presents techniques to hypothesize and reason about attacks possibly missed by IDSs based on the indirect causal relationship between intrusion alerts and the constraints. Wee et al. [11] introduce a network intrusion detection and analysis system to resolve the problems of data confidentiality, availability and integrity. This paper also proposed a methodology to resolve two problems: modeling the network intrusion detection domain, performing causal reasoning for intrusion detection and analysis based on the domain model constructed earlier.

The goal of this paper is to find out cyber-attack path and build evidence chain. The challenges of cyber-attack attribution we faced in technology including: huge numbers of attack

Li Qiang is with the Institute of Information Engineering, Chinese Academy of Science, Beijing, China, 100088, and University of Chinese Academy of Science, 100192. (e-mail: liqiang7@iie.ac.cn)

Yang Ze-Ming, Liu Bao-Xu and Jiang Zheng-Wei are with the Institute of Information Engineering, Chinese Academy of Science, Beijing, China, 100088. (e-mail: yangzeming@iie.ac.cn, liubaoxu@iie.ac.cn, jiangzhengwei@iie.ac.cn)

remaining trace data to analysis and lack of critical data because of limit network resource data we can access. In the fact of this, this paper proposes a reasoning method to create attack evidence chain in situation of data missing and complex trace data structure. This method can help to fill possible missing data and analyze the possible process of attack path among huge data.

The rest of this paper is organized as follows. Section II lists the related work. Section III describes the architecture of attack attribution and implement of reasoning method. Section IV shows experimental results and discussion. Section V discusses conclusion and future work.

II. Related Work

A. Threat Intelligence

According to Gartner definition, threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable device, about an existing or emerging menace or hazard to asset that can be used to inform decisions regarding the subject's response to that menace or hazard [12]. Threat intelligence is based on the collection of intelligence which using open source intelligence, social media intelligence, human intelligence or intelligence in the deep and dark webs. Key mission of threat intelligence is researching and analyzing trends and technical developments in cybercrime, cyber activism and cyber espionage [13]. Security companies like Fireeye, Kaspbersky, Dell security and ThreatConnect, etc. used threat intelligence in cyber-attack attribution.

B. Bayesian Network

Bayesian networks are graph models which represent probabilistic relationships among a group of variables, they provide a natural cause and effect information representation to discover underlying relationship among data [14]. As a directed acyclic graph, Bayesian network has been used in many areas, like machine learning and cellular networks. Bayesian reasoning uses Bayes' theorem, and the core issue of Bayesian reasoning is computing conditional probability. If evidence variable sets is E, query variable sets is Q, task of Bayesian reasoning is computing conditional probability of $Q \in Q$, on condition of given the prior condition of variable sets E=e, which can be formally described as:

$$p(Q|E=e) = \frac{p(Q, E=e)}{p(E=e)}$$

Bayesian reasoning is a method of under given the value of evidence node, which using Bayesian conditional probability method to calculate the query node's probability. There are three kinds of reasoning methods [15]:

1) Causal inference, also known as top-down inference, from reason to conclusion. According to certain evidence, we can compute the result probability.
2) Diagnostic inference, also known as bottom-up inference, from conclusion to reason, that is to say, calculating the reason probability leads to the conclusion.
3) Reasoning support is to explain the happened condition in order to analyze the interrelationship of various causes.

The three kinds of reasoning methods using graphs are shown in Fig. 1.

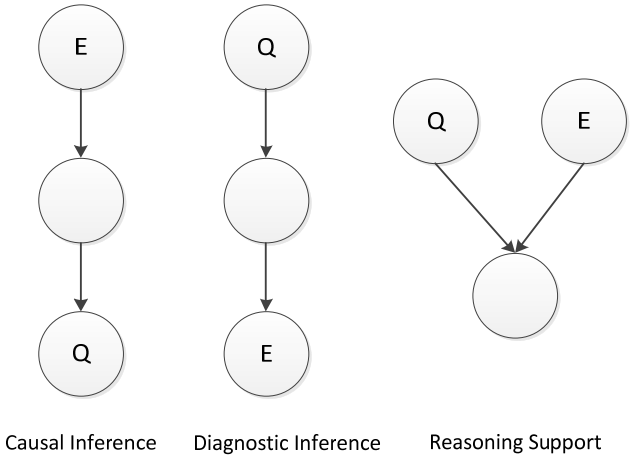

Fig. 1 Reasoning Model of Bayesian Networks

III. Architecture and Implement

A. Local Advantage Model Based on Threat Intelligence

Fig. 2 provides an overview of the theoretical model in cyber-attack attribution and response. Y-axis shows the phases of intrusion kill chain. X-axis shows the appropriate measure against those attacks. Respond to each step of cyber-attack, courses of action include find, fix, track, target, engage and assess. For example, some web scans or host scans that we detected can be regarded as information collection in phase of reconnaissance. Vulnerability information which can be used in developing attack code, also can be collected in assets vulnerability management to defense vulnerability attacks.

There are three types of platform system to support the whole model. Continuous monitoring platform can find and fix cyber-attack threats. Threat intelligence platform can be used to track and target the operator of cyber-attack. Comprehensive response platform provides engage and assess measures to against cyber-attack. Those platforms which provide the basic function are the foundation of cyber-attack attribution and response.

B. System Architecture

Fig. 3 illustrates the architecture of reasoning analysis. The framework architecture is composed of three main parts: The Input, the Analysis and the Output. The internal components of every architecture part and functionalities their provided are discussed in the following:

1) Input

The Input provides the threat intelligence which we can get and use from various channels and methods. Threat intelligence in Input parts can be divided into Inside Threat Intelligence and Outside Threat Intelligence. Basic detection systems like Firewall or IDS, comprehensive analysis systems like SIEM or SOC, and comprehensive information system like social

engineering information system or DNS history information system are considered as inside threat intelligence. Outside threat intelligence consists of intelligence from internet open-source channel, partner exchange channel and business purchase channel. Inside threat intelligence and outside threat intelligence are the input of reasoning analysis process.

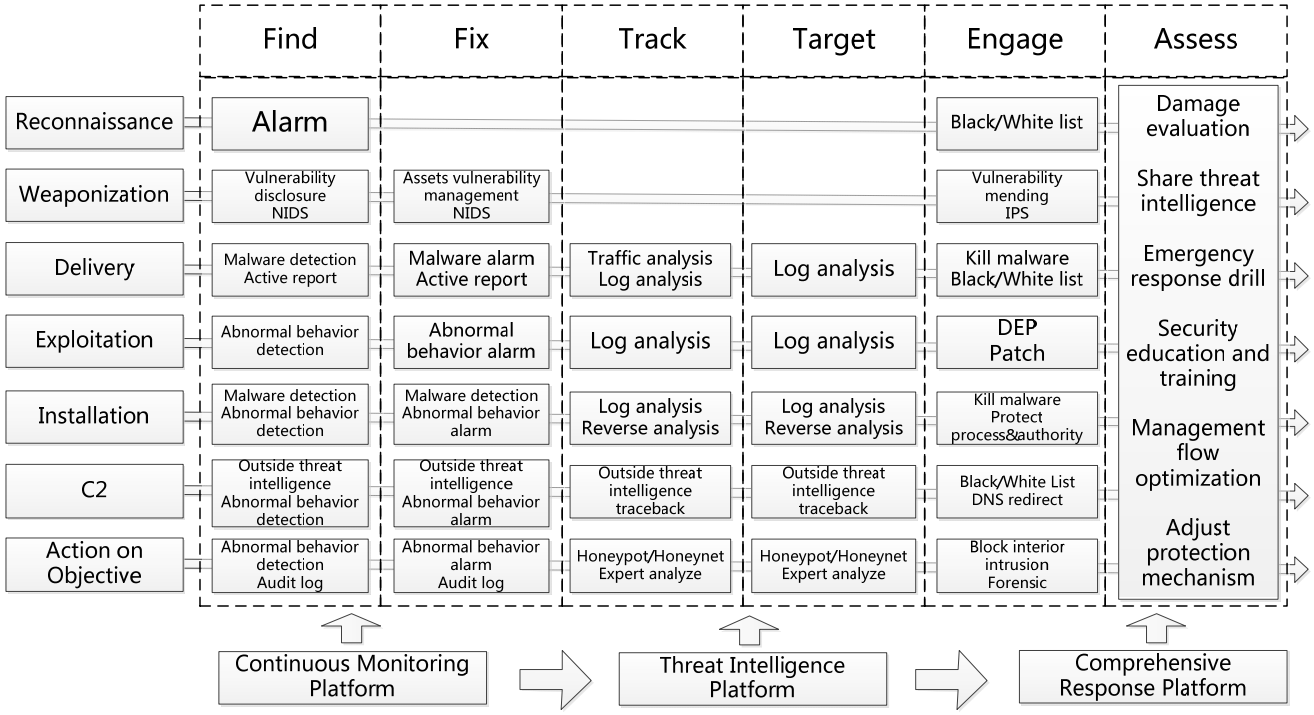

Fig. 2 Local advantage model based on threat intelligence

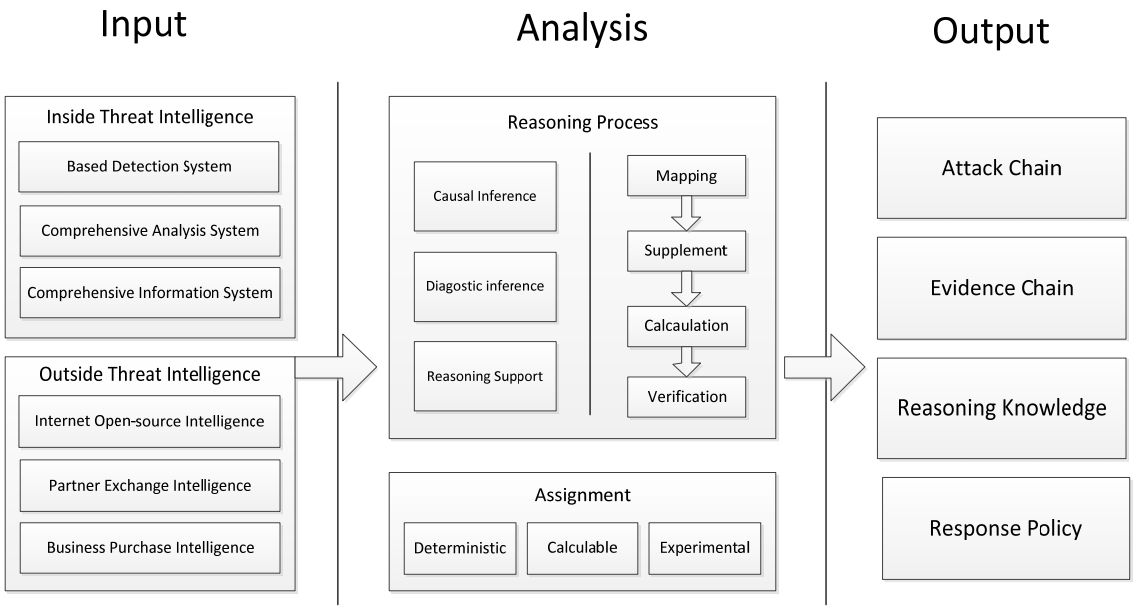

Fig. 3 Architecture of Reasoning Analysis

2) Analysis

The Analysis builds the heart part of system architecture. It includes assignment phase and reasoning phase. For reasoning analysis based on Bayesian networks, several statuses need to be assigned to probabilities or conditional probabilities. There are three methods in assignment phase, including deterministic, calculable and experimental. According to scenes of causal inference, diagnostic inference and reasoning support. The reasoning process was distributed into four stages: mapping, supplement, calculation and verification. The reasoning analysis process is the most significant work in cyber-attack attribution.

3) Output

Using Bayes' theorem, the target of reasoning analysis is to build attack chain and evidence chain of cyber-attack attribution. In addition, some reasoning knowledge will be created at the same time. According to the result of analysis, some response policies need to be proposed to strengthen defensive ability.

C. Assignment and Reasoning Process

1) Assignment Process

Assignment process can be divided into deterministic, calculable and experimental reasoning. Deterministic reasoning means you can get deterministic results after reasoning process. The conditional probability can be given a high value, for example, according to records of DNS resolution to ensure the suspicious IP address or domain name. Calculable probabilistic reasoning means that you can calculate the probability rely on similarity or statistics. Experimental reasoning means the probability or conditional probability need to be artificial marked based on experience.

2) Reasoning Process

There are four steps in reasoning process: mapping, supplement, calculation and verification. In mapping step, lots of event-related information need to map to seven phases of kill chains, and the corresponding value of probability and conditional probability need to be assigned. In supplement step, the missing or lost data need to add to corresponding location and give corresponding probability. In calculation step, relay on the applications developed in analysis process, we can calculate the conditional probabilities of each event nodes. In last step, verification, according to the situation of event, we can confirm one or more possible reasoning path. It can be used to ensure attack chain or evidence chain, reasoning process is shown in Fig. 4.

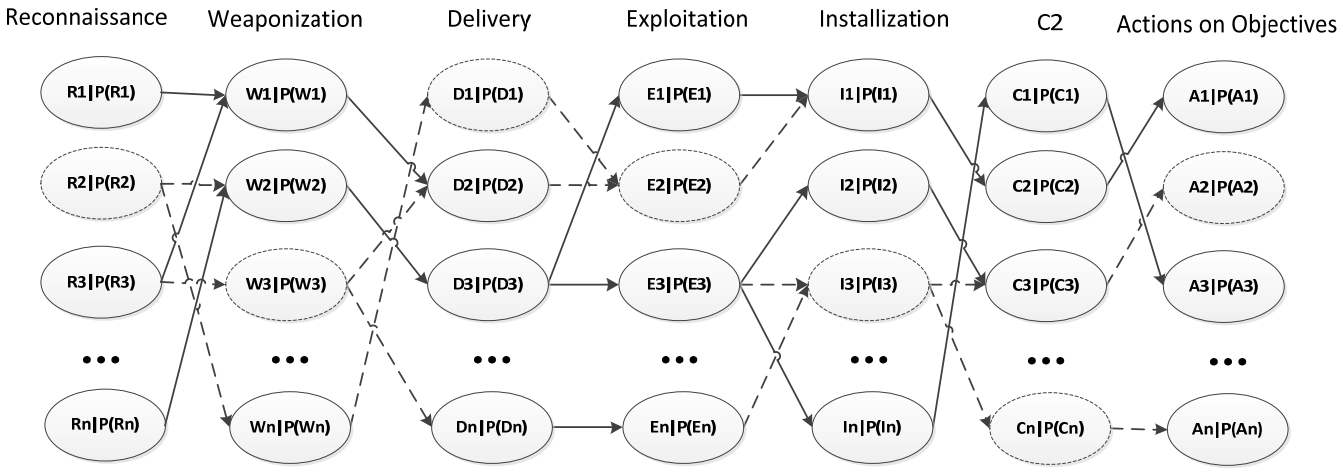

Fig. 4 Reasoning Process

3) Experimental Scheme

According to 24 cyber-attack events we have observed and analyzed, we develop a demo system to test and verify cyber-attack reasoning model and method. The 24 cyber-attack events include watering hole attack, email attack, vulnerability exploitation, cyberextortion, etc. The main content of testing method includes three parts: inputting original cyber-attack events message to the demo system, reasoning and computing process in demo system, comparing and analyzing the output result of demo system and original manual analysis report. Critical measurements for testing are the increasing data volume and the increasing effective evidence's scale.

IV. Experimental Results and Discussion

A. Experimental Results

At first, we input the original event information to reasoning system, including IP address, email, URLs, given strings, hash values of malwares, username, telephone number, etc. According to the given threshold for the probabilities in reasoning process, we select and count the result after data deduplication as shown in the tables. Table I shows the reasoning data growth scale after reasoning process, there are only two events that the increasing data we can get limit in one times. Seven events' data scale can enhance to one to five times. Nine events get five to ten times data growth, and six events get over tenfold data growth scale. Those massive growth of data mainly include social network relevant information, DNS resolution records and missing reasoning data, etc.

TABLE I
Reasoning Data Growth Scale

Growth scale (times)	<1	1-5	5-10	>10
Count	2	7	9	6

Table II shows the useful evidence output from cyber-attack reasoning system. The evidence is distinguished and selected through artificial method. There are eight events get less than 50% increasing evidence, nice events get about 50% to 100% increasing after system reasoning and manual handling. Four events get one to five times evidence data after the whole process, and two events get over five times increase. Those

increased data mainly include missing evidences, potential social network relevant information, domain's whois information, etc.

TABLE II
INCREASING EFFECTIVE EVIDENCE

Growth scale (times)	<0.5	0.5-1	1-5	>5
Count	8	9	4	2

B. Discussion

Using the reasoning system, we can get an obvious increase in data volume and effective evidences, especially relating to the attacker's social network gotten from DNS resolution records and social engineering library, which can relate to the identity information about attacker or attack group. In addition, we can get some invasion traces from log information system to confirm the attack host IP address. However, from same system intrusion events we can get limit information but IP address of C2. In this case, the effective information we can get is limited if the IP address related information not in the database.

V. CONCLUSION

In this paper, we aim at the design and verification of reasoning method in cyber-attack evidence discovering, which is based on threat intelligence, kill chain theory and Bayesian network theory. We developed a demo system for testing which allows data of cyber-attack events input into the system and more useful relevant information can be found and utilized in cyber-attack case analysis. In testing phase we get expected effect that more related data had been found automatically and more useful evidence information had been discovered by artificial analysis and selection. The testing experiment has reached the expected result: the reasoning method and corresponding analysis system can provide certain help in cyber-attack attribution.

In the future, we will adopt the new situation and demand to develop corresponding function and add more threat intelligence data, especially traces information in network devices and attackers' social information from search engine. At the same time, more cases testing will be carried out to test the effectiveness and robustness of the system.

REFERENCES

[1] Trend Micro, Targetted Attacks (EB/OL). http://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks, 2016-3-11.
[2] Wheeler D A, Larsen G N. Techniques for cyber attack attribution (R). Institute for Defense Analyses Alexandria VA, 2003.
[3] Kantzer Khanwei. Cyber Attack Attribution: An Asymmetrical Risk to US National Security (D). Princeton University Princeton, New Jersey, 2011.
[4] Tony Code. Attributions and Arrests: Lessons from Chinese Hacker (EB/OL). https://www.fireeye.com/blog/executive-perspective/2015/12/attributions_andarr.html, 2015-11-03.
[5] Hutchins E M, Cloppert M J, Amin R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains (J). Leading Issues in Information Warfare & Security Research, 2011, 1: 80.
[6] Caltagirone S, Pendergast A, Betz C. The diamond model of intrusion analysis (R). Center for Cyber Intelligence Analysis and Threat Research Hanover MD, 2013.
[7] ThreatConnect Inc. Methodology Creating Order, Pivot by Pivot (EB/OL). https://www.threatconnect.com/platform/methodology/, 2016-3-13.
[8] ThreatConnect Inc., Defense Group Inc. CAMERASHY- Closing the Aperture on China's Unit 78020 (EB/OL). http://www.threatconnect.com,2015-9-24.
[9] Zhai Y, Ning P, Iyer P, et al. Reasoning about complementary intrusion evidence (C)//Computer Security Applications Conference, 2004. 20th Annual. IEEE, 2004: 39-48.
[10] Ning P, Xu D, Healey C G, et al. Building Attack Scenarios through Integration of Complementary Alert Correlation Method (C) //NDSS. 2004, 4: 97-111.
[11] Wee Y Y, Cheah W P, Tan S C, et al. Causal Discovery and Reasoning for Intrusion Detection using Bayesian Network (J). International Journal of Machine Learning and Computing, 2011, 1(2): 185.
[12] Gartner. Definition: Threat Intelligence (EB/OL). https://www.gartner.com/doc/2487216/definition-threat-intelligence,2013-5-16.
[13] Paul Gervais, Nine Cyber Security Trends for 2016 (EB/OL). http://www.prweb.com/releases/2015/12/prweb13125922.htm, 2015-12-15.
[14] Ji J Z, Liu C N, Sha Z Q. Bayesian Belief Network Model Learning, Inference and Applications (J). Computer Engineering and Applications, 2003, 39(5): 24-27.
[15] Liu J N. Research on Bayesian Networks Inference (M). Hefei. Hefei University of Technology,2007.