Using the Actionable Intelligence Approach for the DPI of Cybercrime Insider Investigation

Da-Yu KAO

Department of Information Management, Central Police University, Taoyuan 333, Taiwan

dayukao@gmail.com

***Abstract*— Cybercrime threats are often originating from trusted, malicious, or negligent insiders, who have excessive access privileges to an organization's network, system, or data. The sophistication of insider threats has led to cybercrime issues. Even when an incident is detected, the follow-up countermeasures are required to analyze the results. The analysis of cybercrime insider investigation presents many opportunities for actionable intelligence on improving the quality and value of digital evidence. There are several advantages of applying Deep Packet Inspection (DPI) methods in cybercrime insider investigation. This study discusses the importance of actionable intelligence to conduct investigations and addresses the countermeasure of a cybercrime insider investigation with DPI to detect anomalies in network packets.**

Keywords—Deep Packet Inspection, Digital Evidence, Insider Investigation, Actionable Intelligence, Network Forensics

I. INTRODUCTION

Every organization must be vigilant when it comes to sensitive data protection. When cybercrime is causing significant economic damage, insider threats of increasing cyberattacks are often exposed to unauthorized access to data. Insider threats are challenging cybersecurity issues. They involve a variety of motivations and are very difficult to identify ahead of time [6]. Routine monitoring allows cybersecurity experts to decrease their risk exposure by quickly detecting unusual activities, undue work outside regular work hours, or excessive missing work [13]. Investigators should make specific observations and interpretations of the digital data, supply sufficient evidence in crime reconstruction, and prove the suspect's illegal access to the computer itself. When the thorough protection of network activities is essential to protect sensitive and individual data, continuous monitoring is highly recommended as part of information security controls in insider risk management. Digital evidence has become an essential part of crime scene investigation to collect live/volatile network information in cybersecurity breaches. Deep packet inspection (DPI) methods can be used to investigate and detect cybercrime attacks [5].

The purpose of forensic examination for a cybercrime investigation lies in the following various processes [15]: identification, individualization/classification, association, and reconstruction. While these processes were initially developed to examine and analyze evidence in terms of physical forensics, they are equally applicable to the digital forensics discipline. The cybercrime investigation focuses on (1) identifying the digital evidence from computer logs (identification), (2) finding the suspect ID/account and determining a typical class from evidence process (individualization/classification), (3) inferring interactions between the evidence and the suspect from copied data (association), and ordering the associations in time and space from necessary information (reconstruction). This study will develop new analysis technology to drill down into digital evidence based on the examination of insider threat incidents.

This study tries to recognize cybercrime insider issues from vast collections of computer logs and network packets in order to discover criminal activities more effectively from vague connections. The structure of this study is organized as follows. Section 2 provides a review of global trends in cybercrimes and insider threat detection. The sample case of Taiwan ATM heist is described in Section 3. Section 4 demonstrates the proposed actionable intelligence approach for the DPI of insider threat investigation. Finally, the last section concludes the study and makes some suggestions for future work.

II. LITERATURE REVIEWS

Insiders are authorized users that have legitimate access to business operations. Some are the result of a casual mistake or careless employee behavior. They will continue to seek to challenge security countermeasures, exploit potential vulnerabilities, and increase their knowledge of security procedures for nefarious purposes. Not all insider threats are malicious.

A. Global Trends in Cybercrimes

Cybercriminals are using more advanced malware to target computers, smartphones, and network devices. Illegal acquisition of data breaches is a prominent threat. Some hackers

Manuscript received Jan. 1, 2019. This work was a follow-up of the invited journal to the accepted & presented paper of the 21st Conference on Advanced Communication Technology (ICACT2019), and this research was partially sponsored by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109).

Da-Yu Kao is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (Corresponding Author phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dayukao@gmail.com).

are often involved in large-scale money theft through payment systems or politic espionage operations under the guidance of the government. They may present a hybrid of both forms for profit or their living. Russian crime rings are often suspected of being highly skilled in breaching data systems primarily for organized crime profit. That is shedding renewed light on how vulnerable the online system can be [10].

1) *Cybercrime Investigation*

Law Enforcement Agencies (LEAs) initiate an investigation when a crime is suspected. The presence of relevant, reliable, and sufficient evidence can officially open a case in LEAs. The criminal investigation begins with data on crime. The evidence can verify if a crime has been attributed to a specific person, which has a lot to do with the identification, collection, examination, analysis, and presentation of evidence in law [15]. As cybercrime continues to change, investigators must develop a working knowledge of big data approach to discover the truth, combat cybercrimes, and enforce the law.

2) *Network Packets*

The sources of computer logs or network packets can be used for the evidence. Computer logs were used to identify the attacker, including system logs, application logs, network logs, and database logs. Digital forensics provides investigators with evidence that might be traced back to a criminal event. All the information on the Internet is transferred using network packets. Cyber threats leave some traces in the packets. Since the packets make vast volumes of the data, the methods of big data can help to structure this data. Investigators can monitor the behavior and improve the analyses for identifying the root cause. They can reconstruct the series of events associated with the incident over the entire system and the Internet.

B. *Insider Threat Detection*

Insider activities on systems and networks at financial institutions are a significant great threat to sensitive/confidential data. Preventing, detecting, or investigating internal attacks is a troublesome task since insiders have enough knowledge to access sensitive data. There are still great difficulties in identifying insiders who attempt to conceal their activities by changing their behaviors over time [16].

1) *Big Data Analytics*

Pieces of evidence of malicious insider activity are often buried within big computer logs accumulated over months. Multiple classification models to achieve anomaly detection are evolving to determine insider threat over evolving stream activities. The methods of big data can help again in reconstructing high-level events on the base of low-level artifacts to indicate the areas of interest. An integrated platform for big data processing systems is critical to improve overall performance, analyze an incident, automate their processes, and ensure reliable, scalable, and cost-effective findings. The big data analytics can be applied for insider threat detection of cybercrimes, which are dynamic and heterogeneous [16]. Big data analytics can help investigators analyze such data to detect security violations.

2) *Deep Packet Inspection*

DPI enables the cybercrime investigator to analyze network packets in real-time interception according to their payload. Although packet sampling and selective data can improve performance, the risk of missing substantial evidence for relevant, reliable, or sufficient data is too substantial [5]. A complete picture of cybercrime investigation is identifying the suspects as well as the contents of their communications. Performing full-packet capture is excellent to maintain evidence of what happened after an alert is triggered. By performing DPI, investigators can view and analyze the traffic data with the full context. This study will propose a set of tasks to be conducted in an insider threat investigation using DPI.

III. SAMPLE CASE

A. *Taiwan ATM Heist in July 2016*

The threat of cybercrime is becoming increasingly complex and diverse in putting citizen's data or money in danger. The forensic investigation of Taiwan LEAs identified a piece of malware that allows criminals to attack ATMs directly. The ATM heist was committed without inserting cards or touching the ATM in any improper or illegal way, with the machines simply spitting out bills continuously. When the attackers had obtained control of ATM management service, money was withdrawn directly from the ATM by the attacker command. ATM malware is only active in July 2016. That is considered to be a higher-level attack because it requires access to the back end of the ATM and bypasses the need for capturing consumer bank card data [4]. Taiwan's dense network of surveillance cameras plays an essential role in helping investigators crack the ATM heist. Surveillance cameras fed police information about where the suspects located. This case has demonstrated a high level of technological and financial knowledge in conducting their cybercrimes and exploiting new opportunities for gain.

B. *Answering Some Questions*

The sheer amount of information to find relevant data can be overwhelming at the start of an investigation. A significant effort to keep up with the suspect still requires a continually changing effort in every investigation. A crime investigation can focus on identifying supporting materials to support or refute a case. It is a systematic examination to identify facts on who, what, when, where, and how. Investigators increasingly depend on digital data to find the available evidence, produce appropriate documentation, and verify the impact/context of a crime or incident [2]. Special attention is paid to the 4W1H questions to test case studies in the insider threat domain. The objective of this study is to systematize knowledge in the incident analysis of insider threats [6]. Some questions are initiated for answering this sample case [8].

1) *Who: Andrejs Peregudovs, Mihail Colibaba, and Nikolay Penkov*

The 19 suspects in the heist came from the following six nations: Russia, Moldova, Estonia, Romania, Latvia, and

Australia. They entered and exited Taiwan at different times to avoid police detection.

2) What: US$2.61 Million Theft in an ATM Looting

NT$83.27 million (US$2.61 million) was illegally withdrawn from 41 compromised ATMs of First Bank in Taiwan. On July 20, the police have recovered NT$17.17 million (US$535,700) in total. There is still NT$ 5.86 million (US$182,800) of the loot still unaccounted for (see Table I). Taiwan is a small island. It is quite natural for people to get together for exchanging intelligence. The police were well trained and highly capable of investigating cybercrime.

3) When: July 9 ~ 10, 2016

The group heist allegedly occurred on July 9 and 10, 2016. On July 17, 2016, Taiwan police arrested three suspects in Taiwan. All other suspects fled Taiwan before the police could get hold of them.

4) Where: Three Suspects Were Sentenced in Taipei, Taiwan

On May 18, 2017, Taiwan High Court upheld prison sentences of more than four years for these three Eastern Europeans. The three men will also have to pay fines between NT$300,000 (US$9,900) and NT$500,000 (US$16,500) for each person [8],

5) How: ATM Attacks Targeting Wincor Nixdorf Model

Attacks follow a similar pattern. Through these direct attacks, criminals can empty the cash cassettes of ATMs produced by a specific manufacturer running Microsoft Windows XP. The malware was triggered automatic cash disbursement and a command file installed into the bank's ATM Wincor Nixdorf model "ProCash 1500." Three different malware programs hacked these ATMs: 'cnginfo.exe' read data from the machine, 'cngdisp.exe' executed the money-delivery process, and 'sdelete.exe' deleted the former two programs.

C. Answering Follow-up Questions: Are there any insiders involved in this case?

Organizations should deal with malicious or accidental insider threats. Malicious insiders purposely cause harm to an organization by stealing, damaging, or disclosing information. Accidental insiders are tricked into causing damage or whose credentials have been stolen. That is always happening [3]. New questions and follow-up questions will arise during the investigation. When LEAs investigated how the bank's network was compromised and how the ATMs had been controlled, they found irregularities in the connections between the voice server in London, the bank's internal network and the ATMs in Taiwan. Because the bank's computer system is a closed network, insider assistance could not be ruled out yet in this case [8]. The compromised victim claimed there was no insider threat attack in this case. However, this may mislead investigators. It is important to note that victims do not have proper or effective ways to detect insider attacks. Preventing internal attacks is much more challenging than external breaches, as insiders with legitimate access unwittingly create vulnerabilities or intend to exploit an organization's cyber devices maliciously. It is necessary to identify high-risk insiders based on their behaviors, indicators, or work patterns [13].

TABLE I
MONEY FLOW IN TAIWAN ATM HEIST

Date	Money	Activity	Location
July 9 and 10, 2016	NT$83.27 million (US$2.61 million)	Seventeen suspects were illegally withdrawn	41 compromised ATMs of First Bank in Taiwan
July 11, 2016	NT$200,000	Two suspects have converted more than NT$200,000 into South Korean won, Australian dollars, and US dollars	Taiwan Taoyuan International Airport
July 17, 2016	NT$60.24 million	Two suspects were arrested. Some money was recovered	Taipei hotel.
July 20, 2016	NT$12.63 million	Police found Andrejs's bag	A hill near Xihu Park in Taipei's Neihu District
July 20, 2016	NT$4.54 million	Mr. Ko handed another bag to the police.	Taipei
Note: On July 11, 2016, two suspects converted more than NT$200,000 into South Korean won, Australian dollars and US dollars at Taiwan Taoyuan International Airport just before their departure.			

IV. THE PROPOSED ACTIONABLE INTELLIGENCE APPROACH FOR THE DPI OF INSIDER THREAT INVESTIGATION

While organizations often spend lots of resources on the awareness training of external criminals, insider risks are likely to result in costly security incidents. The risk of unintentional incidents continues to increase as insiders are often able to capitalize on their familiarity with internal systems to launch lucrative attacks without attracting notice [14]. The personal issue of insider threats is one of the significant factors in cyberattacks. The results of inadequate organization protections can be financial loss of operational capabilities as well as the material loss of business records. Monitoring employee activities may identify the potential warning signs of insider activities and prevent some attacks from causing significant harm to an organization. Organizations should establish a network activity baseline for anomalous behavior on intentional and unintentional insider threats through administrative, technical, and investigative safeguards. The appropriate method may mitigate the risk or any possible effects before an attack occurs.

This section discusses digital evidence processes, actionable intelligence practices, and their follow-up cybercrime investigation countermeasures that help combat insider threats.

Putting the risk management and investigation countermeasure together with technical controls into a single practice is one of the critical challenges of building an effective strategy. The readiness of cybercrime countermeasure is critical to reducing an insider threat. Cybercrime investigators will try their best to find evidence in computers or networks [7]. Investigators will benefit from a specially trained unit for insider threat monitoring and investigations. Such staff should ideally have experience or training in conducting a forensic analysis of an incident [14]. This proposed countermeasure ultimately combines host data and network traffic to raise early red flags for further analysis.

A. Actionable Intelligence as an Investigative Approach

Digital devices help people communicate locally and globally with ease, and can be used criminally. Investigators have much work to do and face the risk of missing evidence. It requires proper tradecraft to find evidence and develop actionable intelligence practices. The exploitation of digital evidence can provide a wealth of useful information. Actionable intelligence can be defined as "having the necessary information immediately available in order to deal with the situation at hand [9]." The international cooperation of mutual assistance in fighting cybercrime has developed to overcome the challenges as mentioned above through relevant laws, information exchange, data analysis, criminal investigations, or digital forensics. Investigators need to implement a prioritized approach to the identification, collection, examination, analysis, and presentation where different pieces of evidence are assessed for different suspects.

1) Cybercrime Investigation Ecosystem

Many international organizations or associations are collaborating and making efforts to combat cybercrime. LEAs are well-advised to consider Private-Public-Partnership (PPP) to bring research into reality for cybercrime investigation. The roles of LEAs include protecting citizens, maintaining law and order, and preventing, detecting and investigating a crime. A strategic cybercrime measure toward PPP needs to be developed in improving cybercrime investigation. The national-level strategy of leading actionable intelligence practices on cybercrime issues is proposed in Table II. It also presents a viewpoint of combating cybercrime ecosystem. This strategy focuses on the following key terms [11]: near-term, mid-term, and long term. Each term is further analyzed from people, process, and technology. Near-term draws a strategic roadmap to combat cybercrime. Mid-term develops Standard Operation Procedures (SOPs) to avoid fear, uncertainty, and doubt. Investigators can collect live data on the running system from endpoints, analyze it, identify the usual status of the system, and determine a deviation. Long-term facilitates cross-border cooperation on private and public organizations.

TABLE II
ACTIONABLE INTELLIGENCE APPROACH ON CYBERCRIME ISSUES

	Near-Term	Mid-Term	Long-Term
Cybercrime Governance	Draw a strategic roadmap to combat cybercrime	Develop SOPs to avoid fear, uncertainty, and doubt	Facilitate cross-border cooperation
People	Cybersecurity capacity building: Train personnel	Cybersecurity reporting mechanism: Collaborate with an international alliance	Private-Public-Partnership: Meet both needs
Process	National agency for cybersecurity: Form a working group	Legal Measures: Amend the existing IT law	International Cooperation: Discuss real-time issues
Technology	Cybersecurity strategy: Define visions, objectives, and action plan	R&D on advanced tools and technology: Develop a new methodology to fight against coming issues	Active Participation: Actively participate in international associations
Tasks	● Create new procedures or policies to deter, respond to, and prosecute cybercrime. ● Enhance the actionable intelligence capability to gather data, process information, and combat cybercrime.		

2) Comprehensive Actionable Intelligence of Cybercrime Investigation

Making sound judgments at low cost is a core role and an essential attribute for investigators, who must maximize the potential and exploit the possibilities to ensure things are what they see. Various kind of intelligence provides critical information on time to an appropriate audience for better-informed decision making. Actionable intelligence is related to the investigation or incident at hand into the broader intelligence mix [1]. Investigators have produced actionable intelligence from criminal investigation to gain knowledge in support of preventing cybercrime or pursuing criminals. The threats from criminals are becoming increasingly complicated. All practitioners, policy-makers, or investigators need to understand how they can find actionable intelligence at the scene. Investigators need to find out the evidence and convict suspects of their crimes with actionable intelligence within a limited period [9]. The effectiveness and efficiency of investigators can be judged in part by the capability to utilize their reasonable collection opportunity to access the digital device, support the evidence-gathering at the scene, collect

volatile/non-volatile evidence in the lab, pursue criminal immediately, and achieve successful prosecutions.

B. Cybercrime Insider Investigation Countermeasure: DPI

Detecting cyberattacks can be difficult to identify what can be done to combat the increased risk of insider threats [14]. Cybercrime investigations have faced difficulties with analyzing evidence in large datasets to verify the impact of an incident. Improving the relevancy, reliability, and sufficiency of incident response is a critical issue in tackling the large volume of computer logs and network packets. This study includes cybercrime insider investigation, which allows a more detailed and comprehensive incident analysis in DPI. While it may be challenging to protect against insider attacks, a practical investigation countermeasure can significantly reduce their impact. The goal is to create a process that allows the investigators to evaluate the digital evidence accurately. The critical part of any investigation is relevant, reliable, and sufficient evidence. Investigators need to prepare a checklist to discover the relevant data, gather evidence, and cross-reference the findings. The following practices in Fig. 1 are proposed to ensure that an investigation is forensically sound in law. Fig. 1 comes with subphases and activities for any digital investigation: civil, criminal, or corporate [2]. Implementation of these countermeasures for preventing insider attacks will provide organization investigative measures that can prevent or facilitate the early detection of many cyberattacks. That includes the following five consecutive/iterative phases: identity, collect, examine, analyze, and present.

1) Identify: Track the Pathway of an Insider Threat

It is crucial to collect the right data and preserve the crime scene as part of the preliminary investigation. Most auditing tools only alert users at the moment when cybercrime was detected. By contrast, DPI solutions allow investigators to track the insider's pathway by collecting all network packets and identifying any suspicious files. Collected packets are analyzed to generate statistics of used usernames, IP addresses, protocols, port services, type, and duration of the attack [12].

a) Payload-based inspection

Payload-based inspection is based on the analysis of payload in the application layer of network packets. Investigators can use predefined patterns like sensitive digital sources as signatures for each cyberattack and help them to distinguish attacks form each other.

b) Port-based identification

Port-based identification is known to be among the easiest and fastest method for analyzing network packets. Port numbers will not be affected by encryption schemes. Packet identification via port number uses the data in the TCP/UDP headers of the packets to extract the port number which is assumed to be associated with a particular application program.

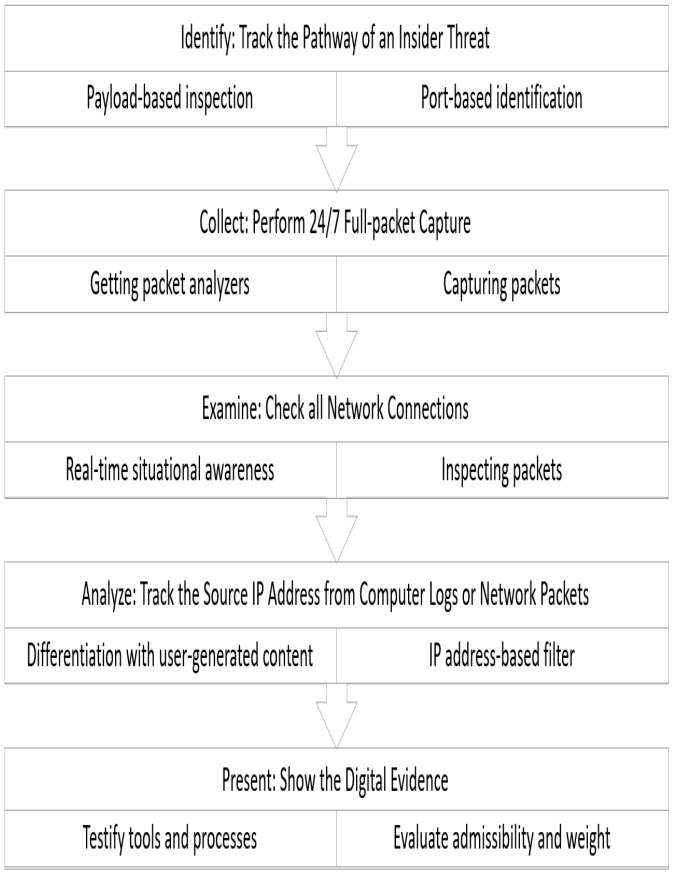

Fig. 1. Proposed cybercrime countermeasure of insider threat investigation

2) Collect: Perform 24/7 Full-packet Capture

As insider threats may occur anytime, DPI is an effective way to identify suspicious content in the headers or the payloads, excepting situations where the payload is encrypted [12]. Identification, tracking, and monitoring of computer systems can help avert or limit the exposure of sensitive data to insider attacks. When investigators monitor vital assets, they can react faster and with more precision to mitigate incidents [13]. Packet analyzers are used to monitor network traffic, detect a cybercrime, or get access to user names and passwords. They allow investigators to see each byte of data that passes from a computer or server across the network.

a) Getting packet analyzers

Network packets often contain a wealth of information that is relevant to the investigation. Investigators can download and install tcpdump, Wireshark or other packet analyzers for Windows, macOS, or UNIX-like systems from its official website.

b) Capturing packets

Much digital evidence can be gathered from the network than the host. Most Internet activities can be discovered and analyzed with the use of network sniffer methods. This countermeasure will introduce and reinforce a network packet mindset that investigators can use any DPI method and produce

worthwhile outcomes in finding out the fact. Investigators can start capturing packets and create a filter based on it.

3) Examine: Check all Network Connections

After a cybercrime occurs on the network, victims often suffer from data leakages for months or years. Investigators can recognize data patterns from the collected network packets to discover any digital trace evidence or identify behavior patterns [5]. By examining the connections among computers and to the Internet, DPI makes it possible to prove that the network is secure.

a) Real-time situational awareness

With DPI, investigators have real-time situational awareness about whether attackers are still present on the network, or whether any computers are still compromised.

b) Inspecting packets

Investigators can debug network protocol implementations, examine security problems, and inspect network protocol internals to view its details. Pattern recognition may help identify the suspicious IP address of the source attack and understanding the meaning or motivation behind anomalous behavior.

4) Analyze: Track the Source IP Address from Computer Logs or Network Packets

Some tools capture only sample traffic, perform statistical sampling of data, and generate reports based on host-based logs. The source IP address of the suspect is a crucial component of this countermeasure because not all possible data can be collected or analyzed simultaneously. Some data (e.g., network packets) may not be available instantaneously.

a) Differentiation with user-generated content

Investigators can differentiate users' activities within a single application from network packets.

b) IP address-based filter

IP address-based filter is a critical task in cybercrime investigations. In order to properly explore network packets, it is vital to recognize different sources of IP addresses.

5) Present: Show the Digital Evidence

Digital evidence may be used to identify the attacker by username, computer name, and private or public IP address.

a) Testify tools and processes

A digital video or camera can help investigators document the location and condition of everything. Hash values of digital sources and files should be created as early as possible. Investigators should be able to testify that they have validated their tools and processes.

b) Evaluate admissibility and weight

Investigators should examine the digital devices, produce an unbiased and accurate document, describe the forensic outcome, and assist the court in evaluating the admissibility and weight of any digital evidence.

V. CONCLUSIONS

The connections among terrorists, cybercriminals, and organized crime groups appear to be on the rise. An increasing trend of malicious/unintentional insider threats becomes one of the challenging cybersecurity issues. The involved employees can abuse their access privileges to steal funds from customer accounts or the organization. The ubiquity of the Internet has increased the accessibility of data sources, knowledge, or skills. The cost is high when terror or online attacks succeed. Most organizations do not have a dedicated team in detecting insider threats. They take a reactive approach and deploy resources when a problem is detected. A proactive approach to looking for insider threats is critical for an organization to look for the problem. If the investment is low, it is impossible to know the true extent of cyberattacks. A promising approach to ensure an efficient and effective strategy is a collaboration between various private and public organizations. Security agencies, intelligence agencies, and LEAs can apply similar techniques to advance counter-cybercrime measures to keep citizens safe or to prevent, pursue, protect, and prepare against cybercrime. They need to enhance their investigative ability to identify, collect, acquire, and preserve evidence. Its importance is growing to keep citizens, communities, and commerce safe. This study introduces the DPI method that can help investigators in developing new techniques and performing the digital investigation process in a forensically sound and timely fashion manner. This study also provides a survey of the packet inspection in cybercrime insider investigation. Case studies illustrate that DPI can be used to extract knowledge or insights from computer logs or network packets for cybercrime reconstruction. Efficient continuation efforts of data analysis fields such as statistics, machine learning, data mining, knowledge discovery, and predictive analytics are necessary for data extracting and analyzing in less period. Future research will analyze packets and identify the traces left by cyber threats.

REFERENCES

[1] Akhgar, B., Bayerl, P. S., Sampson, F. (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer Publishing, pp. 1-68, 2016.

[2] Arnes, A., *Digital Forensics*, John Wiley & Sons Ltd, pp. 46-318, 2018.

[3] Cole, E., "Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey," SANS Institute, pp. 3-21, Aug. 2017.

[4] Dalfonso, S., "ATM Malware: The Next Generation of ATM Attacks," https://securityintelligence.com/atm-malware-the-next-generation-of-atm-attacks/, 2014.

[5] Davis, J. J., *Machine Learning and FeatureEngineering for Computer Network Security*, Dissertation, Faculty of Science and Engineering, Queensland University of Technology, pp. 1-33, 2017.

[6] Homoliak, I, Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M., "Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," *ACM Computing Surveys (CSUR).* Vol. 52, No. 2, 2019.

[7] Kävrestad, J., *Guide to Digital Forensics: A Concise and Practical Introduction*, Springer International Publishing, pp. 3-8, 2107.

[8] Law and Regulations Retrieving System, "Criminal Appeals No.593/106 in Taiwan High Court," Judicial Yuan, May 18, 2017.

[9] Pearson, S. and Watson, R., *Digital Triage Forensics: Processing the Digital Crime Scene*, Elsevier Inc., Burlington, pp. 13-144, 2010.

[10] Rayman, N., "The World's Top 5 Cyber Crime Hotspots," http://time.com/3087768/the-worlds-5-cybercrime-hotspots/.

[11] Rishi, R., Kumar, P., and RAWAT, D. S., *Strategic National Measures to Combat Cybercrime: Perspective and Learnings for India*, Ernst & Young LLP, pp. 6-21, 2015.

[12] Rodrigues, G. A. P., Albuquerque, R. O., Deus, F. E. G., Sousa. R. T., Oliveira Júnior, G. A. O., Villalba, L. J. G., Tai-Hoon Kim, T. H., "Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection," *Applied Sciences*, Vol. 1082, pp. 1-29, Jul. 2017.

[13] Schulze, H., "Insider Threat 2018 Report," CA Technologies, pp. 3-31, 2018.

[14] SIFMA, *Cybersecurity: Insider Threat Best Practices Guide (2nd Edition)*, Securities Industry and Financial Markets Association, pp. 5-53, Feb. 2018.

[15] Stephenson, P., *Official (ISC)²® Guide to the CCFP CBK*, Boca Raton, FL: Auerbach Publications, pp. 293-404, 2014.

[16] Thuraisingham, B., Masud, M. M., Parveen, P., Khan, L., *Big Data Analytics with Applications in Insider Threat Detection*, CRC Press, pp. 181-432, 2017.

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.