

Cybercrime Countermeasure of Insider Threat Investigation

Da-Yu KAO

Department of Information Management, Central Police University, Taiwan

camel@mail.cpu.edu.tw

Abstract—The threat of cybercrime is becoming increasingly complex and diverse on putting citizen's data or money in danger. Cybercrime threats are often originating from trusted, malicious, or negligent insiders, who have excessive access privileges to sensitive data. 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 paper introduces DPI method that can help investigators in developing new techniques and performing digital investigation process in forensically sound and timely fashion manner. This paper provides a survey of the packet inspection, which can be applied to cybercrime insider investigation.

Keywords—deep packet inspection, insider threat, cybercrime investigation, digital evidence

I. INTRODUCTION

When cybercrime is causing major economic damage, insider threats of increasing cyber-attacks are often exposed to unauthorized access to data. Law enforcement agencies (LEAs) should make certain 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. Deep packet inspection (DPI) methods can be used to investigate and detect cybercrime attacks [4]. Digital evidence has become an essential part of crime scene investigation to collect live/volatile network information in cybersecurity breaches.

The purpose of forensic examination with respect to a cybercrime investigation lies in the following various processes [9]: 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 essential logs (identification), (2) finding the suspect ID/account and determining a common 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 cybersecurity incidents.

This paper tries to recognize cybercrime insider issues from huge collections of network logs and packets in order to discover criminal activities more effectively from vague connections. The structure of this paper is organized as follows. Section 2 provides a review of global trends in cybercrimes and insider threat detection. Section 3 describes the sample case of Taiwan's Russian mafia group on banks and payment systems in July 2016. Section 4 demonstrates the proposed cybercrime countermeasure of insider threat investigation. Finally, the last section concludes the paper and makes some suggestions for future work.

II. LITERATURE REVIEWS

Insiders are authorized users that have legitimate access to business operations. They will continue to seek to challenge security countermeasures, exploit potential vulnerabilities, and increase their knowledge of security procedures for nefarious purposes.

A. Global Trends in Cybercrimes

Russian crime rings are often suspected of being highly skilled in breaching data systems primarily for organized crime profit. This is shedding renewed light on how vulnerable online system can be [7]. Some hackers 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.

1) Cybercrime Investigation

Criminal investigation actually begins with data on a crime. The presence of relevant, reliable, and sufficient evidence can officially open a case in LEAs. The evidence can verify if a crime has been committed and if it can be attributed to a specific person, which has a lot to do with forensic science, the identification, collection, examination, analysis, and presentation of evidence in law [9]. 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

All the information on the Internet are transferred using network packets. Cyber threats leave some traces in the

packets. Since the packets make huge volumes of the data, the methods of big data can help to structure this data.

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. Evidences of malicious insider activity are often buried within big system logs accumulated over months. Multiple classification models to achieve anomaly detection are evolving to determine insider threat over evolving stream activities. There are still great difficulties in identifying insiders who attempt to conceal their activities by changing their behaviors over time [10].

1) Big Data Analytics

The methods of big data can help again in reconstructing high-level events on the base of low-level artefacts to indicate the areas of interest. The big data analytics can be applied for insider threat detection of cybercrimes, which are dynamic and heterogeneous in nature [10]. Big data analytics can help LEAs analyze such data to detect for security violations.

2) Deep Packet Inspection

DPI enables the cybercrime investigator to analyze Internet traffics in real-time interception according to their payload. Although network packet sampling and selective data capture can improve performance, the risk of missing important evidence for relevant, reliable or sufficient data is too substantial [4]. Performing full-packet capture is great 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.

III. SAMPLE CASE

A. Taiwan's Russian Mafia Group on Banks and Payment Systems in July 2016

Taiwan's dense network of surveillance cameras plays important roles in helping investigators crack the first ATM heist. Surveillance cameras fed police important information about where the suspects located. The forensic investigation of Taiwan LEAs identified a piece of ATM 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. The ATM malware is only active in July 2016. Through these direct attacks, criminals can empty the cash cassettes of ATMs produced by a specific manufacturer running Microsoft Windows XP. This 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 [3, 6]. 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

A crime investigation can focus on identifying supporting materials to support or refute a case. It is a systematic examination with the purpose of identifying facts on who, what, when, where, and how. LEAs increasingly depend on digital data to find the available evidence, produce appropriate documentation, and verify the impact/context of a crime or incident [2]. Some questions are initiated for answering this sample case.

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

On July 9 and 10, 2016, 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 has 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 1). Taiwan is a small island. It is quite easy for people to get together for meeting and exchanging intelligence. The police were well trained and highly capable in investigating cybercrime.

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 was illegally withdrawn	from 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	at Taiwan Taoyuan International Airport
July 17, 2016	NT\$60.24 million	Two suspects were arrested. Some money was recovered	from the Taiepi hotel.
July 20, 2016	NT\$12.63 million	police found Andrejs's bag	on a hill near Xihu Park in Taipei's Neihu District
July 20, 2016	NT\$4.54 million	Mr. Ko handed another bag to police.	In Taipei

Note: On July 11, 2016, two suspects have converted more than NT\$200,000 into South Korean won, Australian dollars and US dollars at Taiwan Taoyuan International Airport just before their departure.

3) *When: July 9 ~ 10, 2016*

The group heist allegedly occurred between July 9 and 10, 2016.

4) *Where: Three Suspects Were Charged in Taipei*

On July 17, 2016, Taiwan police arrested 3 suspects in Taiwan. All other suspects fled Taiwan before police could get hold of them.

5) *How: ATM Attacks Targeting Wincor Nixdorf Model*

Attacks follow a similar pattern. Malware was triggered automatic cash disbursement and a command file installed into the bank's ATM Wincor Nixdorf model "ProCash 1500." These ATMs were hacked by three different malware programs: '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?*

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 [6]. Cybercrime investigators will try their best to find evidence in computers or networks [5].

IV. THE PROPOSED CYBERCRIME COUNTERMEASURE 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 human issue of insider threats is one of the major factors in cyber-attacks. The results of inadequate organization protections can be financial loss of operational capabilities as well as 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 actionable intelligence practices and its follow-up cybercrime investigation countermeasure that helps combat insider threats.

A. *Actionable Intelligence Practices*

Digital devices help people communicate locally and globally with ease, and can be used in a criminal way. The international cooperation of mutual assistance in fighting cybercrime has developed to overcome the aforementioned challenges through relevant laws, information exchange, data analysis, criminal investigations, or digital forensics.

1) *Practices on Cybercrime Issues*

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 crime [8]. A strategic cybercrime measure toward actionable intelligence of 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 2. It also presents a viewpoint of combating cybercrime ecosystem. This strategy focuses on the following key terms [8]: 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. Long-term facilitates cross-border cooperation on private and public organizations.

2) *The Longer Arm of Cybercrime Investigation*

Making sound judgments at low cost is a core role and important attribute for LEAs, who must maximize the potential and exploit the possibilities to ensure things are what they see. Various kind of intelligence provide important information in a timely manner to an appropriate audience for better informed decision making. Actionable intelligence is related to the investigation or incident at hand within the wider intelligence mix [1]. LEAs have produced actionable intelligence from criminal investigation to gain knowledge in support of preventing cybercrime or pursuing terrorists. The threats from criminals are becoming increasingly complicated. It is essential for all practitioners, policy-makers or LEAs to understanding how they can find actionable intelligence at scene. The effectiveness and efficiency of LEAs can be judged in part by the capability to utilize their intelligent collection opportunity to access the digital device, support the evidence-gathering at scene, collect volatile/non-volatile evidence in lab, pursue criminal immediately, and achieve successful prosecutions.

B. *Cybercrime Investigation Countermeasure*

Cybercrime investigations have faced difficulties to analyze evidence in large datasets to verify the impact of an incident. Much digital evidence can be gathered from the network than the host. Investigators can recognize data patterns from the collected network packets to discover any digital trace evidence or identify behavior patterns [4]. This study includes cybercrime insider investigation, which allows more detailed and comprehensive incident analysis in DPI. The following countermeasures in Fig. 1 are proposed to ensure that an investigation is forensically sound in law [2]. This includes five consecutive/iterative phases, through the reporting to the final presentation of the findings.

TABLE II. ACTIONABLE INTELLIGENCE PRACTICES 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 on Private-Public-Partnership
People	Cybersecurity Capacity Building: Train personnel on cybercrime investigation, forensic analysis and digital evidence	Cybersecurity Reporting Mechanism: Collaborate with 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 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 rapidly gather data, accurately process information, and strategically combat cybercrime.		

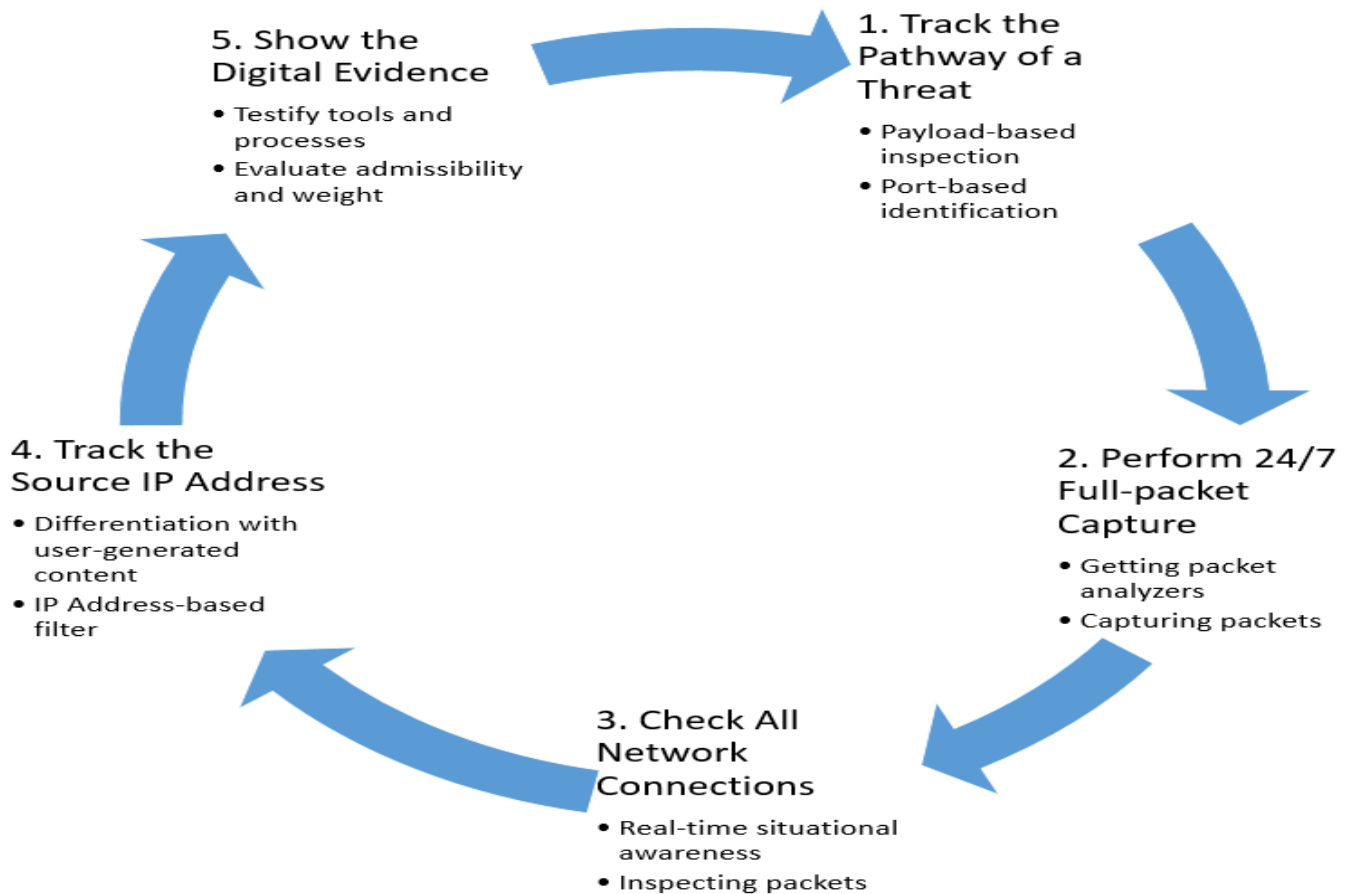


Fig. 1. Proposed cybercrime countermeasure of insider threat investigation

1) *Track the Pathway of a Threat*

Most auditing tools only alert users at the moment when a cybercrime was detected. By contrast, DPI solutions allow investigators to track the attackers' pathway by collecting all network packets and identifying any suspicious files.

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 from 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.

2) *Perform 24/7 Full-Packet Capture*

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*

Investigators can download and install tcpdump, Wireshark or other packet analyzers for Windows, MacOS, or other UNIX-like system from its official website.

b) *Capturing packets*

Investigators can start capturing packets and create a filter based on it.

3) *Check All Network Connections*

After a cybercrime occurs on the network, victims often suffer from data leakages for months or years. 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.

4) *Track the Source IP Address*

Some tools capture only sample traffic, perform statistical sampling of data, and generate reports based on host-based logs.

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 an important task in cybercrime investigations. In order to properly explore network packets, it is vital to recognize different sources of IP addresses.

5) *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 that 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

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. The connections among terrorists, cybercriminals and organized crime groups appear to be on the rise. A promising approach to ensure efficient and effective strategy is collaborations between various private and public organizations. Security agencies, intelligence agencies and LEAs can apply similar techniques to advance counter-terrorism measures to keep citizens safe, or to prevent, pursue, protect and prepare against cybercrime or terrorism. It is essential for them to enhance their investigative ability to identify, collect, acquire, and preserve evidence. Its importance is growing to keep citizens, communities and commerce safe. This paper proposes a set of tasks to be conducted in insider threat investigation using DPI. Case studies illustrate that DPI can be used extract knowledge or insights from host-based logs or network-based packets for cybercrime reconstruction. An efficient continuation efforts of data analysis fields such as statistics, machine learning, data mining and knowledge discovery, and predictive analytics are required for data extracting and analyzing in less period of time. Future research will analyze packets and identify the traces left by cyber threats.

ACKNOWLEDGMENT

This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-107) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 107-2221-E-015-002-.

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] Dalfonso, S., "ATM Malware: The Next Generation of ATM Attacks," <https://securityintelligence.com/atm-malware-the-next-generation-of-atm-attacks/>, 2014.
- [4] Davis, J. J., *Machine Learning and Feature Engineering for Computer Network Security*, Dissertation, Faculty of Science and Engineering, Queensland University of Technology, pp. 1-33, 2017.
- [5] Kävrestad, J., *Guide to Digital Forensics: A Concise and Practical Introduction*, Springer International Publishing, pp. 3-8, 2107.
- [6] Pan, J., "ATM heist suspects behind bars," <http://www.taipetimes.com/News/taiwan/archives/2016/07/20/2003651412>
- [7] Rayman, N., "The World's Top 5 Cyber Crime Hotspots," <http://time.com/3087768/the-worlds-5-cybercrime-hotspots/>.
- [8] 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.
- [9] Stephenson, P., *Official (ISC)²® Guide to the CCFP CBK*, Boca Raton, FL: Auerbach Publications, pp. 293-404, 2014.
- [10] Thuraisingham, B., Masud, M. M., Parveen, P., Khan, L., *Big Data Analytics with Applications in insider Threat Detection*, CRC Press, pp. 181-432, 2017.



Dayu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. He is responsible for various recruitment efforts and training programs for Taiwan civil servants, police officers or ICT technicians. He has an extensive background in law enforcement and a strong interest in information security, ICT governance, technology-based investigation, cyber forensics, human resource development, and public sector globalization. He was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.