2015

Cyber Black Box: Network intrusion forensics system for collecting and preserving evidence of attack

Jong-Hyun Kim
Electronics and Telecommunications Research Institute, Korea

Joo-Young Lee
Electronics and Telecommunications Research Institute, Korea

Yangseo Choi
Electronics and Telecommunications Research Institute, Korea

Sunoh Choi
Electronics and Telecommunications Research Institute, Korea

Ik-kyun Kim
Electronics and Telecommunications Research Institute, Korea

DOI: 10.4225/75/57b3fd1ffb88f
This paper was originally presented at The Proceedings of [the] 13th Australian Digital Forensics Conference, held from the 30 November – 2 December, 2015 (pp. 104-110), Edith Cowan University Joondalup Campus, Perth, Western Australia.

CYBER BLACK BOX: NETWORK INTRUSION FORENSICS SYSTEM FOR COLLECTING AND PRESERVING EVIDENCE OF ATTACK

Jong-Hyun Kim, Joo-Young Lee, Yangseo Choi, Sunoh Choi, and Ik-kyun Kim
Electronics and Telecommunications Research Institute, Korea
{jhk, julee, yschoi92, suno, ikkim21}@etri.re.kr

Abstract

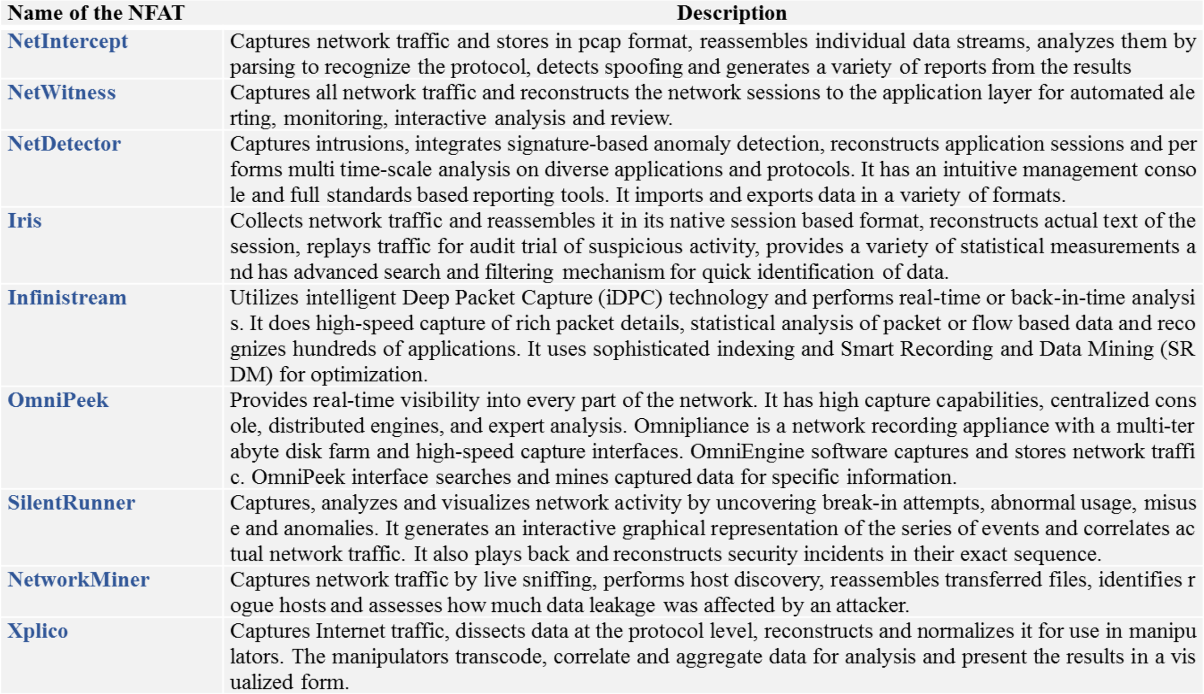
Once the system is compromised, the forensics and investigation are always executed after the attacks and the loss of some useful instant evidence. Since there is no log information necessary for analyzing an attack cause after the cyber incident occurs, it is difficult to analyze the cause of an intrusion even after an intrusion event is recognized. Moreover, in an advanced cyber incident such as advanced persistent threats, several months or more are expended in only analyzing a cause, and it is difficult to find the cause with conventional security equipment. In this paper, we introduce a network intrusion forensics system for collecting and preserving the evidence of an intrusion, it is called Cyber Black Box that is deployed in Local Area Network environment. It quickly analyzes a cause of an intrusion event when the intrusion event occurs, and provides a function of collecting evidence data of the intrusion event. The paper also describes the experimental results of the network throughput performance by deploying our proposed system in an experimental testbed environment.

Keywords
Cyber Attacks, Network Forensics, Attack Cause Analysis

INTRODUCTION

Recently, cyber-attacks against public communications networks are getting more sophisticated intelligent and varied. Moreover, in some cases, one local domain could make systematic attacks against another domain to steal its confidential information and intellectual property. Therefore, the issue of cyber-attacks is now regarded as a new major threat to national security. The conventional way of operating individual information security systems such as IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) may not be sufficient to cope with those attacks committed by highly-motivated attackers with significant resources. For real-time response cyber threats, not only individual security system, but also global cooperative security management system should be provided since there are global problems which cannot be solved by any single entity as well as single domain or single company. For a systematic response to the cyber threat, the level of threats, the level of risk assessment, and a step-by-step alarm are required.

Table 1: Description of Network Forensic Analysis Tools (NFATs) (Pilli et al., 2010)



Name of the NFAT	Description
NetIntercept	Captures network traffic and stores in pcap format, reassembles individual data streams, analyzes them by parsing to recognize the protocol, detects spoofing and generates a variety of reports from the results
NetWitness	Captures all network traffic and reconstructs the network sessions to the application layer for automated alerting, monitoring, interactive analysis and review.
NetDetector	Captures intrusions, integrates signature-based anomaly detection, reconstructs application sessions and performs multi time-scale analysis on diverse applications and protocols. It has an intuitive management console and full standards based reporting tools. It imports and exports data in a variety of formats.
Iris	Collects network traffic and reassembles it in its native session based format, reconstructs actual text of the session, replays traffic for audit trial of suspicious activity, provides a variety of statistical measurements and has advanced search and filtering mechanism for quick identification of data.
Infinistream	Utilizes intelligent Deep Packet Capture (iDPC) technology and performs real-time or back-in-time analysis. It does high-speed capture of rich packet details, statistical analysis of packet or flow based data and recognizes hundreds of applications. It uses sophisticated indexing and Smart Recording and Data Mining (SRDM) for optimization.
OmniPeek	Provides real-time visibility into every part of the network. It has high capture capabilities, centralized console, distributed engines, and expert analysis. Omnipliance is a network recording appliance with a multi-terabyte disk farm and high-speed capture interfaces. OmniEngine software captures and stores network traffic. OmniPeek interface searches and mines captured data for specific information.
SilentRunner	Captures, analyzes and visualizes network activity by uncovering break-in attempts, abnormal usage, misuse and anomalies. It generates an interactive graphical representation of the series of events and correlates actual network traffic. It also plays back and reconstructs security incidents in their exact sequence.
NetworkMiner	Captures network traffic by live sniffing, performs host discovery, reassembles transferred files, identifies rogue hosts and assesses how much data leakage was affected by an attacker.
Xplico	Captures Internet traffic, dissects data at the protocol level, reconstructs and normalizes it for use in manipulators. The manipulators transcode, correlate and aggregate data for analysis and present the results in a visualized form.

Current cyber incident response is always after the attacks occur, which always lose some important data of the intrusion. To solve these security issues, we need some new approaches to enhance the investigation of the network attack. A generic process model for network forensics is proposed which is built on various existing models of digital forensics. Computer Forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in an admissible manner (Osles, L., 2001). Otherwise, network forensics deals with capture, recording, and analysis of network traffic for detecting intrusions and investigating them in order to discover evidential information about the source of security attacks (Gary, P., 2001).

The functionality of various Network Forensic Analysis Tools (NFATs) and network security monitoring tools, available for forensics examiners is discussed in (Pilli *et al*., 2010). Computer forensic is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media (Osles, L., 2001). Network forensics is commonly used to describe the task of analyzing information collected on active networks from various intrusion detection, auditing, and monitoring capabilities for the purpose of protection. The network forensics tools always combine the ability to passively monitor, capture all network traffic, analyze traffic, track down security violations and protect against future violations and attacks. The essential functions of network forensics tool is to capture network traffic, to analyze the traffic according to the user's needs, to discover useful and interesting things about the analyzed traffic (Corey *et al*., 2002; Reith *et al*., 2002; Manzano *et al*., 2001; Davidoff *et al*., 2012). For the purpose of the network forensics, we always need the logging system to capture the network traffic fully. There are many tools for building network traffic analysis and statistical event records (Ioannidis *et al*., 2002; McCanne *et al*., 1993; Anagnostakis *et al*., 2001; Risso *et al*., 2001). They often use a promiscuous packet interface to pass visible traffic into an internally decision engine which discloses the content of the packets and counting them into statistical data and logging key details into backend disks (Rizzo *et al*., 2012; Deri *et al*., 2013). In our system, we will use the logging approach for the information gathering, including network flow, windows PE (Portable Executable) files and so on. After obtaining the network traffic data, forensics analysis is needed. In this paper, we present the architecture of a real time network intrusion forensics system, which can expedite the investigation of the incident and improve the ability of emergence response. The remaining of the paper is organized as follows: First, technical goals and design approaches of the system are discussed. And then the system architecture and technical functions are described, we explain the experimental results and give the conclusion in the last section.

TECHNICAL GOALS AND DESIGN APPROACHES

Cyber Black Box System Goals

In the network security field, a cyber intrusion event denotes a case of attacking an information communication network and a system associated with the information communication network in a way such as hacking, a computer virus, a logic bomb, a mail bomb, and so on. In the related works, since analysis is mainly used as an action against a cyber intrusion event, there are limitations in quick cause analysis and post-action. They cannot give a complete picture for the forensics analysis when the attacks are end. In addition, since there is no log information necessary for analyzing an attack cause after the cyber incident occurs, it is difficult to analyze the cause of an attack.

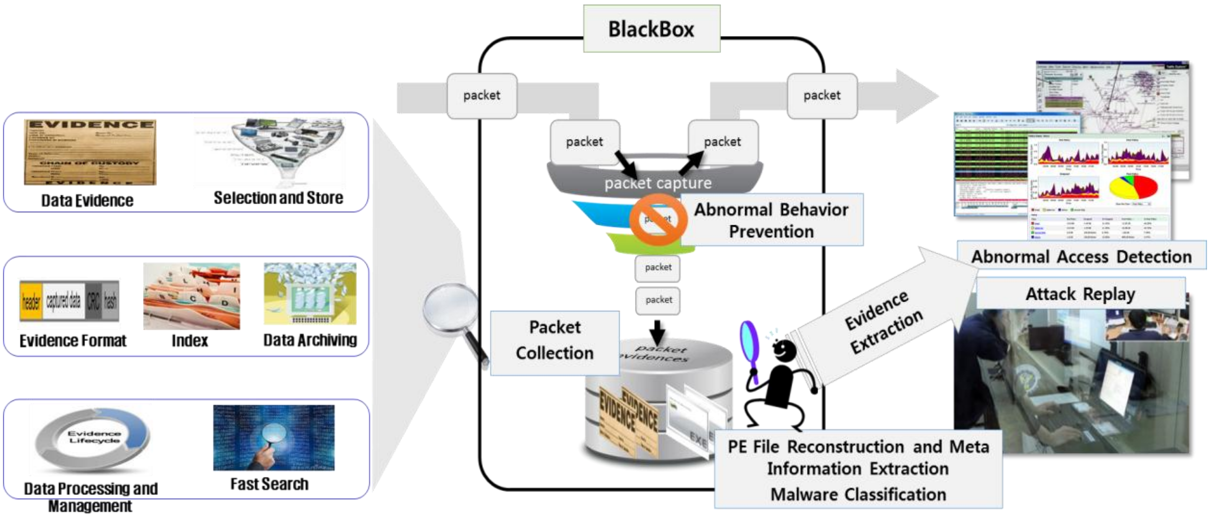


Figure 1: Technical design of cyber black box for network forensics

Accordingly, the goals of our cyber black box system are security response and forensics. It quickly analyzes a cause of an intrusion event when the intrusion event occurs, and provides a function of collecting evidence data of the intrusion event. Figure 1 shows that the cyber black box system includes a data collector configured to collect entire packet data, flow data, and a portable executable (PE) file from monitored network traffic and a server configured to analyze a cause of a cyber intrusion event and reproduce the cyber intrusion event, based on the collected entire packet data, flow data, and PE file. It also provides the process in data on the authenticity, integrity, reliability, originality, such as the securing by the evidence legally binding.

Traffic & Flow Information Gathering

The proposed system saves the audit data and digests information of the intrusion. It can gather the network traffic and flow data (e.g., Netflow), and send to the forensics server. Network traffic capture may become the bottleneck of the system when the traffic is huge, but the waiving of the some traffic may result in the losing of trace or evidence. The solution of the trade-off depends on the burden of real time traffic. We developed a network interface card dealing with 10Gbps traffic without loss of traffic data. It may encode the entire packet data, the flow data, and the PE file which are stored in the buffer as a file having the PCAP format. It may also store the entire packet data, the flow data, and the PE file, which are encoded by the encoding unit in units of a file, as the preservation data.

Transmitted File Reconstruction

The proposed system performs the function of reconstructing the transmitted file which is extracted from the stored traffic data collected by the cyber black box system, and performs a function for storing additional metadata that is collected from one file reconfiguration. When a network packet is arrived, it is confirmed whether the packet includes a PE file or not. If it is, then the packet is collected to reconstruct the PE file from the packet payload. For reconstructing the correct file, the TCP reassemble functionality has been implemented as well. Once a PE file is constructed, the file is examined by header analysis technology. Header analysis technology detects malwares based on the information of PE header. There is lots of information in PE header for executing a file.

Virtual Volume based Storage Management

Virtual volume management is performed solely for the storage device. Storing the collected data provides several APIs to execute the traffic information gathering module. The proposed system performs a function to provide the integrity of the data when stored in the virtual volume storage to preserve the collected data for the evidence of attacks. Moreover, the storage management supports a write once read many (WROM) function. It can be understood that the storage unit supporting the WORM function is a storage medium in which data is written once and from which the data is read a plurality of times like CD-ROMs. Therefore, the storage unit may preserve the entire packet data, the flow data, and the PE file for a long time.

Cyber Incident Cause Analysis

Cyber incident cause analysis may request the preserved data and management data from a data collector. Here, the preserved data may include the decoded entire packet data, flow data, PE file, and metadata associated with the PE file, and the management data may include summary data as well as flow data. The summary data is data generated by summarizing the entire packet data, the flow data, and the PE file which are classified as the preserved data. In detail, it also provides the user interface to the cause analysis for performing a function of analyzing the cause of cyber incidents based on the data collected in the cyber black box system.

SYSTEM ARCHITECTURE AND TECHNICAL FUCTIONS

In general aspect, a method of collecting evidence data of a cyber intrusion event includes: (1) extracting entire packet data from monitored network traffic; (2) analyzing the extracted entire packet data based on an Internet protocol (IP), a port, and a protocol to extract, as flow data, a bundle of packet data having the same feature; (3) extracting, as a portable executable (PE) file, a bundle of packet data having a PE format from the extracted entire packet data; (4) temporarily storing in a buffer, and collecting the extracted entire packet data, flow data, and PE file; (5) applying a hash function to each of the temporarily stored entire packet data, flow data, and PE file to generate a hash value; and storing, as the evidence data, the generated hash value and the temporarily stored entire packet data, flow data, and PE file in a storage unit. Figure2 shows the architecture of the proposed system, called cyber black box. There are two physical systems in the architecture. We describe the detail function of each module (block) on the cyber black box system in this section.

From the figure 2, TFGB (**T**raffic & **F**low **G**athering **B**lock) block is able to accommodate 10Gbps network traffic via a network interface card (NIC), store collected packets, extract the traffic information of the network flow and generate the session data. A method of extracting the flow data can analyze all packet data extracted by the packet extraction unit, based on an Internet protocol (IP), a port, and a protocol. It may collect packet data having the same feature in units of a certain time, based on a result of the analysis, and may bundle the packet data, collected in units of the certain time, in a specific file having the PCAP format to extract one piece of flow data (or a flow packet). Another method of extracting the flow data can extract the flow data by sampling a certain-rate packet of entire packet data in a deterministic packet sampling scheme. The extracted flow data may be temporarily stored in the virtual volume based storage. By connecting a plurality of the hard disk to store a total of 10Gbps traffic data without loss of traffic to select a structure for storing in parallel. The hash value generating unit may apply a hash function to each of the entire packet data and the flow data to generate a hash value (SHA-256), for ensuring data integrity of each of the entire packet data and the flow data which are stored in the virtual volume based storage. The generated hash value is also stored in the storage unit and is preserved for a long time.

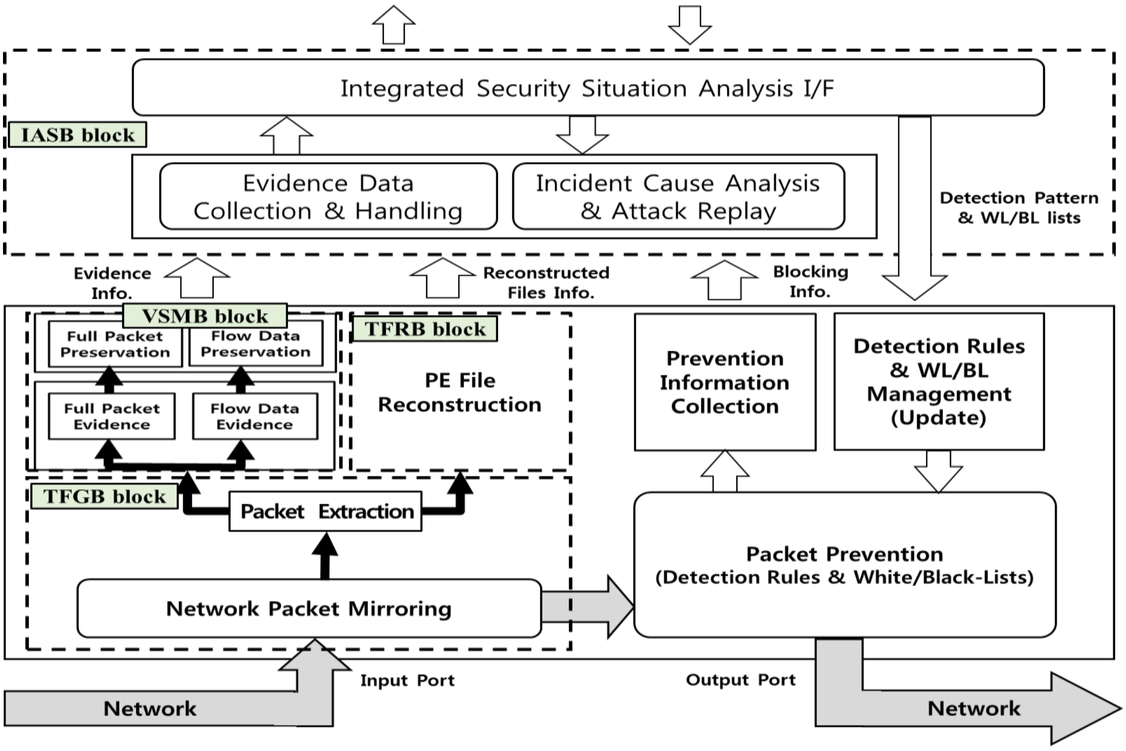

Integrated Security Situation Analysis I/F
IASB block
Evidence Data Collection & Handling
Incident Cause Analysis & Attack Replay
Detection Pattern & WL/BL lists
Evidence Info.
Reconstructed Files Info.
Blocking Info.
VSMB block
Full Packet Preservation
Flow Data Preservation
Full Packet Evidence
Flow Data Evidence
TFRB block
PE File Reconstruction
Prevention Information Collection
Detection Rules & WL/BL Management (Update)
TFGB block
Packet Extraction
Network Packet Mirroring
Packet Prevention (Detection Rules & White/Black-Lists)
Input Port
Output Port
Network
Network

Figure 2: Architecture of the cyber black box for network intrusion forensics

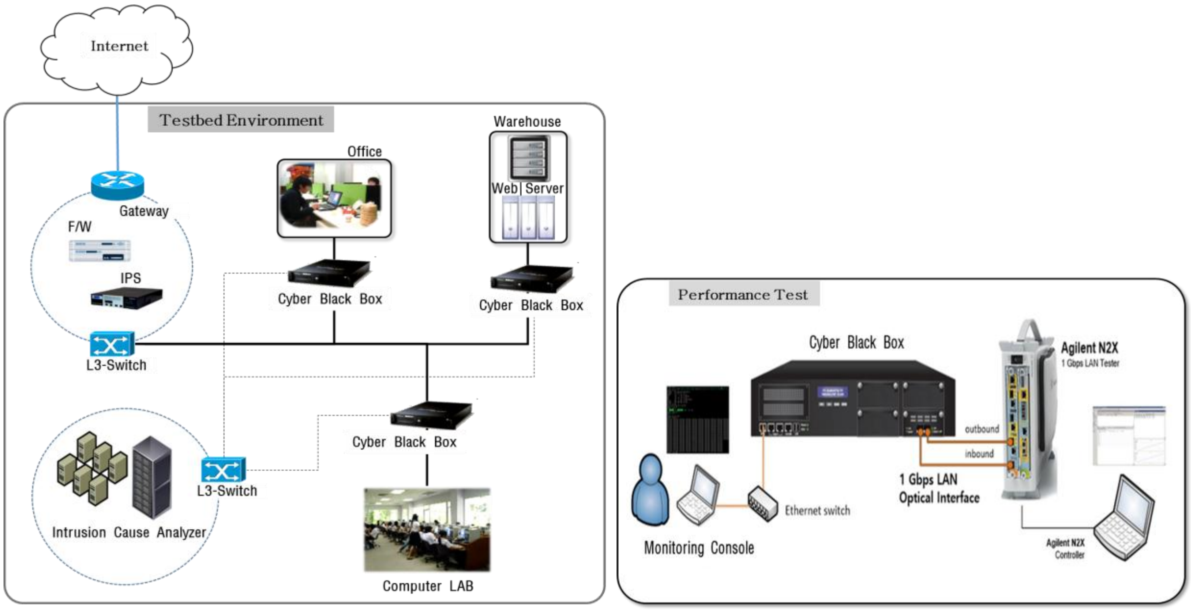
TFRB (**T**ransmitted **F**ile **R**econstruction **B**lock) block performs the function of reconstructing the transmitted file which is extracted from the stored data collected by TFGB, and performs a function for storing additional metadata that is collected from one file reconfiguration. The transmitted file may be the PE (Portable Executable) file from the entire packet data extracted from the packet extraction unit. For example, the PE file extraction unit may select packets having PE file information (or a PE format) in the entire packet data extracted by the packet extraction unit. It also collects all packets having the selected PE file information, and can reassemble (or reconfigure) all the collected packets having the PE file information. The extracted PE file is also temporarily stored in the virtual volume based storage. TFRB provides the ability to analyze the network service protocols such as HTTP, SMTP, FTP, POP3, and so on. It also determines which protocol a file is sent by and calculates the hash value (SHA-256) for the file, and stores the metadata information that is collected between the extracted files in the directory specified in the csv file format.

VSMB (**V**irtual volume based **S**torage **M**anagement **B**lock) block stores the entire packet data, the flow data, and the PE file which are encoded by the encoding unit in units of a file as the preserved data. It receives the hash value that generated by the hash value generation unit, for each of the entire packet data, the flow data, and the PE file. And then it stores the received hash value as evidence data. Moreover, VSMB block supports a write once read many (WROM) function to ensure integrity of the stored data in the virtual volume based storage. It also prevents the forgery as well as modification of the data stored in the storage. The entire packet data, the flow data, and the PE file that are stored in the VSMB block and are encoded in units of a file can be supplied to the server according to a request of the server. That is, when an intrusion event occurs or another necessary case occurs, the encoded entire packet data, flow data, and PE file can be supplied to the server as the evidence data including at least one of the management data and the preserved data, for analyzing a cause of the intrusion event and reproducing the intrusion event. It provides the capability to create or destroy the virtual volumes of the storage systems for the data protection as well as the file storage management.

IASB (**I**ntrusion **A**nalysis & **S**cenario generation **B**lock) block provides the user interface to perform a function of analyzing the cause of the cyber incident based on the data collected in the cyber black box system. That is, it provides, as various pieces of visual information, an analysis result of the cause of the intrusion event to a user through a GUI. A method of reproducing the cyber incident can extract a cyber-attack scenario (for example, an attack time, an IP address where the cyber-attack is performed, and etc.), based on the evidence data which is collected at a cyber-attack time. It also reconstructs the cyber-attack scenario based on the extracted information and reproduces a corresponding cyber incident according to the reconstructed attack scenario. The result of the cause analysis can be supplied to an external system through the external cooperation protocol. The supply of the analysis result can be limited in order for the result to be supplied to an authenticated external system. That is, the external cooperation system sets a security grade in an external system and gives an appropriate authority to the external system according to the set of security grade. The external system may be a security-related system provided in a security company, a public institution, a portal company, a general company, and so on.

EXPERIMENTAL RESULTS

In this section, we present the experimental results of the cyber black box system. We designed and implemented the system using the C programming language on the CentOS Linux 7.1 platform. For all the experiments we used a single machine with 64GB DDR3 RAM, two Quad-Core 2.6 Ghz CPUs, 4TB SATA-300 32 MB Buffer 7200 rpm disk with a RAID-Z configuration.



(a) *(b)*

Figures 3: (a) Experimental Testbed Environment, (b) Network Traffic Throughput Performance test

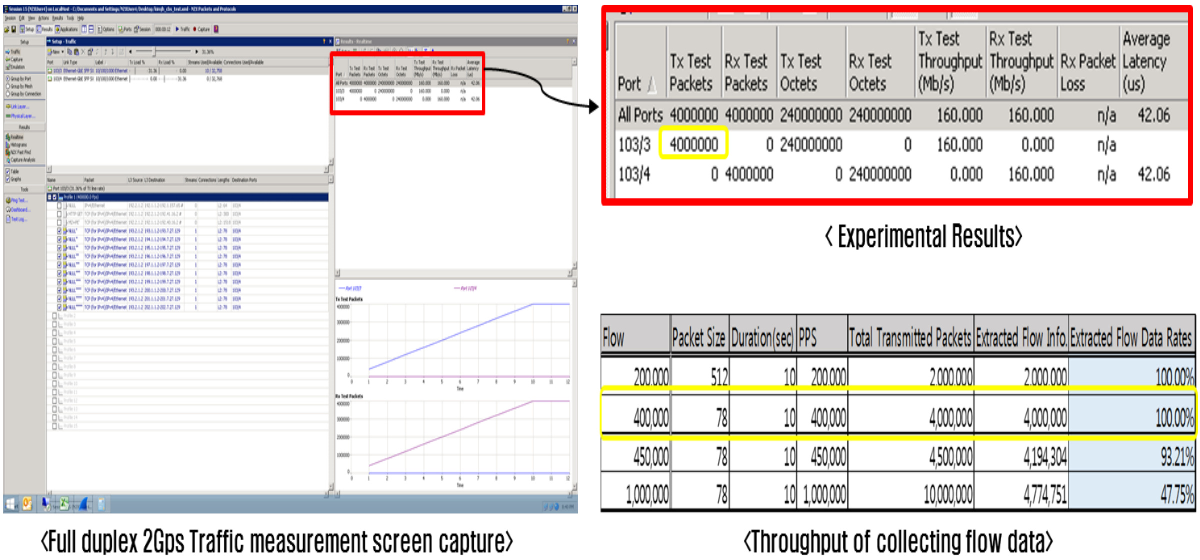
For experiments we used the network flow data captured over a 12 hour period of one weekday at our testbed environment. In details, we deployed our proposed system in an experimental testbed with monitoring points at the network perimeter, in front of warehousing servers, and at the computer Lab as shown in figure 3 (a). We simulated the scenario where the attack was not detected by IDSs, but anomalies were discovered later at the victim machine. We also conducted the traffic throughput test with an Agilent N2X tool as shown in figure 3 (b).

It is verified that our proposed system could collect the attack event data and related flow records without the loss of network packets in a total of 2Gbps traffic. However, we observed that there were some loss of network packets in case that the size of a packet is less than 128 Byte as shown in table 2.

Table 2: Summary of network packet processing performance in a total of 2Gbps traffic

Packet Size	Port	Tx Packets	Rx Packets	Tx pps	Rx pps	loss(%)
64 Byte	All Ports	535,714,286	535,553,897	2,976,190	2,975,299	0.02993928
	inbound	267,857,143	267,777,370	1,488,095	1,487,652	
	outbound	267,857,143	267,776,527	1,488,095	1,487,647	
128 Byte	All Ports	304,054,056	304,047,383	1,689,189	1,689,152	0.00219468
	inbound	152,027,028	152,023,714	844,595	844,576	
	outbound	152,027,028	152,023,669	844,595	844,576	
256 Byte	All Ports	163,043,480	163,043,480	905,797	905,797	0
	inbound	81,521,740	81,521,740	452,899	452,899	
	outbound	81,521,740	81,521,740	452,899	452,899	
512 Byte	All Ports	84,586,468	84,586,468	469,925	469,925	0
	inbound	42,293,234	42,293,234	234,962	234,962	
	outbound	42,293,234	42,293,234	234,962	234,962	
1024 Byte	All Ports	43,103,450	43,103,450	239,464	239,464	0
	inbound	21,551,725	21,551,725	119,732	119,732	
	outbound	21,551,725	21,551,725	119,732	119,732	
1518 Byte	All Ports	29,258,778	29,258,778	162,549	162,549	0
	inbound	14,629,389	14,629,389	81,274	81,274	
	outbound	14,629,389	14,629,389	81,274	81,274	
Random	All Ports	55,486,751	55,486,751	308,260	308,260	0
	inbound	27,743,372	27,743,379	154,130	154,130	
	outbound	27,743,379	27,743,372	154,130	154,130	

For another experimental results, our proposed system collected at least 400,000 flow records per second and stored those data into the virtual volume based storage which supports WORM function. Figure 4 shows the experimental results and network traffic throughput performance with 1Gbps LAN optical Interface of N2X tool. We also confirmed that TFRB block performed the function of reconstructing the transmitted file which was extracted from the stored traffic packets collected by TFGB block, and performed a function for storing additional metadata that was collected from one file reconfiguration.



Port	Tx Test Packets	Rx Test Packets	Tx Test Octets	Rx Test Octets	Tx Test Throughput (Mb/s)	Rx Test Throughput (Mb/s)	Rx Packet Loss	Average Latency (us)
All Ports	4000000	4000000	240000000	240000000	160.000	160.000	n/a	42.06
103/3	4000000	0	240000000	0	160.000	0.000	n/a	
103/4	0	4000000	0	240000000	0.000	160.000	n/a	42.06

〈 Experimental Results〉

Flow	Packet Size	Duration(sec)	PPS	Total Transmitted Packets	Extracted Flow Info.	Extracted Flow Data Rates
200,000	512	10	200,000	2,000,000	2,000,000	100.00%
400,000	78	10	400,000	4,000,000	4,000,000	100.00%
450,000	78	10	450,000	4,500,000	4,194,304	93.21%
1,000,000	78	10	1,000,000	10,000,000	4,774,751	47.75%

〈Full duplex 2Gps Traffic measurement screen capture〉

〈Throughput of collecting flow data〉

Figure 4: The experimental results and network traffic throughput performance

For the network traffic throughput performance, we used the following formula;

*Rx pps * (Packet Size + 12bytes(Inter Packet Gap) + 7bytes(MAC Preamble size) + 1byte(SFD)) * 8bits*

For the overall performance of network traffic processing, we evaluated that our proposed system could keep up with traffic rates up to 2.0 Gbps for our experimental implementation. We also measured the maximum processing performance by exploiting the various packet size from a N2X tool.

CONCLUSION

Since the intrusion cannot be avoided fully, the deployment of intrusion forensics system is needed. As described above, in a related research against a cyber-attack, since several months or more are expended in only analyzing a cause of an intrusion event and there is no information necessary for analyzing an attack cause, it is unable to know the cause of attack even after the intrusion event occurs. However, according to our proposed system, entire packet data, flow data, and a PE file can be collected as evidence data from network traffic and also stored in the storage medium for a long time, and thus, a cause of an intrusion event is quickly analyzed based on the evidence data preserved in the storage medium. This paper described the architecture of cyber black box system for network forensics and verified network throughput performance by deploying our proposed system in an experimental testbed environment. The future work is the research of the cooperative mechanism between our system and the security equipment such as IPSs (Intrusion Prevention Systems), WAFs (Web Application Firewalls) and so on.

ACKNOWLEDGMENTS

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.B0101-15-0300,The Development of Cyber Blackbox and Integrated Security Analysis Technology for Proactive and Reactive Cyber Incident Response)

REFERENCES

Anagnostakis, K. G., Ioannidis, S., Miltchev, S., & Smith, J. M. (2001) Practical network applications on a lightweight active management environment. In *Proc. of the 3rd International Working Conference on Active Networks (IWAN)* (pp. 101- 115)

Corey, V., Peterman, C., Shearin, S., Greenberg, M.S., & Van Bokkelen, J. (2002) Network forensics analysis. In *Proc. of IEEE Internet Computing*. 6(6), (pp. 60 –66)

Davidoff, S. & Ham, J. (2012) *Network Forensics: Tracking Hackers through Cyberspace,* Pearson Education.

Deri, L., Cardigliano, A., & Fusco, F. (2013) 10 Gbit line rate packet-to-disk using n2disk. In *Proceedings of IEEE INFOCOM Workshop on Traffic Monitoring and Analysis* (pp.3399-3404)

Gary, P. (2001) *A Road Map for Digital Forensic Research*. Technical Report DTRT0010-01, DFRWS.

Ioannidis, S., Anagnostakis, K. G., Ioannidis, J., & Keromytis, A. D. (2002) xPF: packet filtering for lowcost network monitoring. In *Proc. of the IEEE Workshop on High-Performance Switching and Routing (HPSR)* (pp. 121-126)

Manzano, Y. & Yasinsac, A. (2001) Policies to Enhance Computer and Network Forensics. In *Proc. of 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop*

McCanne, S. & Jacobson, V. (1993) The BSD packet filter: A new architecture for user-level packet capture. In *Proc. of the USENIX Technical Conf.*

Osles, L. (2001) *Computer forensics: The key to solving the crime*

Pilli. E.S., Joshi, R.C., & Niyogi, R. (2010) Network forensic frameworks: Survey and research challenges. *The International Journal of Digital Forensics & Incident Response archive*. 7(1-2) (pp.14-27)

Reith, M., Carr, C., & Gunsch, G., (2002) An Examination of Digital Forensic Models. *International Journal of Digital Evidence*. 1(3)

Risso, F. & Degioanni, L. (2001) An Architecture for High Performance Network Analysis. In *Proc. of the 6th IEEE Symposium on Computers and Communications (ISCC 2001)*

Rizzo, L. (2012) netmap: a novel framework for fast packet I/O. In *Proceedings of USENIX conference on Annual Technical Conference* (pp. 9-9)