Introduction to a Network Forensics System for Cyber Incidents Analysis

Yangseo Choi*, Joo-Young Lee*, Sunoh Choi*, Jong-Hyun Kim*, Ikkyun Kim*

**Cyber Security Research Division*, ETRI, Daejeon, South Korea

{yschoi92, joolee, suno, jhk, ikkim21}@etri.re.kr

***Abstract*— Recently, sophisticated attacks are increased against specific business companies, organizations and various facilities and the attackers are trying to remove attack traces such as system logs and related information on the victim systems. Therefore, it is getting more difficult to collect the information for attack analysis. In order to overcome this situations, companies and organizations have started to collect the network traffic as secondary information for attack analysis. However, most of them are focusing on gathering the network packets. But one of the most important parts is to extract the useful information for attack analysis from the collected data. In this paper, we suggest a network forensics system, Cyber Blackbox, which is focused on the traffic analysis.**

***Keywords*—Network forensics, cyber blackbox, attack analysis, network security, information security**

Yangseo Choi (BS'96–MS'00-Ph.D'11) is a Principal Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He joined ETRI, Daejeon, Rep. of Korea, in 2000, and he worked on the anti-cyber terror technology research team. Since 2006, he has been involved in the development of DDoS prevention system, virtual machine security system for Cloud environment. His research interests include Network security, Hacking technologies, and Network forensics.

Joo-Young Lee (BS'96-BS'99) is a Senior Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). She is joined ETRI, Daejeon, Rep. of Korea, in 1999, and she's working on the project 'Cyber Blackbox development for cyber incidents analysis.' Her research interests include Digital forensics, Cryptography, Network security, and Network forensics.

Sunoh Choi (BS'05-MS'08-Ph.D'14) is a Senior Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He is joined ETRI, Daejeon, Rep. of Korea, in 2014, and He's working on the project 'Cyber Blackbox development for cyber incidents analysis.' His research interests include Database security, Network security, Attack detection and analysis, Digital forensics, and Network forensics.

Jonghyun Kim (-) is a Principal Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He is joined ETRI, Daejeon, Rep. of Korea, in 2007, and He's working on the project 'Cyber Blackbox development for cyber incidents analysis.' His research interests include Digital forensics, Network security, Network forensics, and Visualization.

Ikkyun Kim (-) is a Principal Researcher in the Software Contents Research Laboratory at Electronics and Telecommunications Research Institute (ETRI). He is joined ETRI, Daejeon, Rep. of Korea, in 2002, and He's working on the project 'Cyber Blackbox development for cyber incidents analysis' and 'Targeted attack Identification and Traceback Technology Development.' His research interests include Digital forensics, Network security, Network forensics, and Visualization.