Network Abnormal Behavior Analysis System

Sunoh Choi, Yangseo Choi, Jooyoung Lee, Jonghyun Kim and Ikkyun Kim

Network Security Research Group

Electronoics and Telecommunication Research Institute

{suno, yschoi92, joolee, jhk, ikkyun21}@etri.re.kr

***Abstract*— As cyber attacks have increased in recent years, network forensics, which collects and analyzes network packets as well as digital forensics, has been studied. However, high-speed networks such as 1 or 10 Gbps networks have many network flows. For example, a 1 Gbps network has hundreds of millions of network flows per day. Analyzing network traffic in this situation is very difficult and time-consuming. In this paper, we propose a system that can analyze network abnormal behavior quickly and easily. We first propose a system that stores the tcp flag when generating network flows. Second, we present some ways to use the tcp flag in network flows to analyze network anomalies such as persistent outbound connections.**

***Keyword*—Network Forensics, Network Flow**

Sunoh Choi (BS'05-MS'08-Ph.D'14) is a Senior Researcher in the Network Security Research Group at Electronics and Telecommunications Research Institute (ETRI). He has received BS and MS from Korea University and Ph.D from Purdue University. He has 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, and Network forensics..

Yangseo Choi (BS'96–MS'00-Ph.D'11) is a Principal Researcher in the Network Security Research Group at Electronics and Telecommunications Research Institute (ETRI). He has 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-MS'99) is a Principal Researcher in the Network Security Research Group at Electronics and Telecommunications Research Institute (ETRI). She has 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.

Jonghyun Kim (-) is a Principal Researcher in the Network Security Research Group at Electronics and Telecommunications Research Institute (ETRI). He has 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 director in the Network Security Research Group at Electronics and Telecommunications Research Institute (ETRI). He has 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.