Big Data Analysis System Concept for Detecting Unknown Attacks

Sung-Hwan Ahn*, Nam-Uk Kim*, Tai-Myoung Chung**

*Department of Electrical and Computer Engineering, Sungkyunkwan University

** College of Information and Communication Engineering, Sungkyunkwan University

shahn@imtl.skku.ac.kr, nukim@imtl.skku.ac.kr, tmchung@ece.skku.edu

***Abstract*— Recently, threat of previously unknown cyber-attacks are increasing because existing security systems are not able to detect them. Past cyber-attacks had simple purposes of leaking personal information by attacking the PC or destroying the system. However, the goal of recent hacking attacks has changed from leaking information and destruction of services to attacking large-scale systems such as critical infrastructures and state agencies. In the other words, existing defense technologies to counter these attacks are based on pattern matching methods which are very limited. Because of this fact, in the event of new and previously unknown attacks, detection rate becomes very low and false negative increases. To defend against these unknown attacks, which cannot be detected with existing technology, we propose a new model based on big data analysis techniques that can extract information from a variety of sources to detect future attacks. We expect our model to be the basis of the future Advanced Persistent Threat(APT) detection and prevention system implementations.**

***Keyword*— Computer crime, Alarm systems, Intrusion detection, Data mining**

Sung hwan Ahn received his B.S. degrees in Computer Media Engineering from Kangnam University, Yongin, Korea in 2011. He is currently working toward his M.S in Electrical and Computer Engineering at Sungkyunkwan University. His research interests are internal information security, big data analysis, network security, and privacy.

Nam-Uk Kim received his B.S. and M.S. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2009 and 2012, respectively. He is now currently working toward his Ph.D. in Electrical and Computer Engineering at Sungkyunkwan University. His research interests are information security, network, mobile application security and SDN.

Prof. Tai myoung Chung received his first B.S. degree in Electrical Engineering from Yonsei University, Korea in 1981 and his second B.S. degree in Computer Science from University of Illinois, Chicago, USA in 1984. He received his M.S. degree in Computer Engineering from University of Illinois 1987 and his Ph.D. degree in Computer Engineering from Purdue University, W. Lafayette, USA in 1995. He is currently a professor of Information Communication Engineering at Sungkyunkwan University, Suwon, Korea. He is now a vice-chair of the Working Party on Information Security & Privacy, OECD.