Computationless Abnormal Data-Flow Detection based on Microcurrent Measurement

Hye Lim Jung[1], Sungkyu Ahn[1], Sung Hoon Baek[2], and Ki-Woong Park [1*]
[1]*Department of Information Security, Sejong University, Seoul, Korea*
fhyello13, yiimfng@gmail.com, woongbak@sejong.ac.kr
[2]*Department of Computer System Engineering, Jungwon University, Chungbuk 28024, Korea*
shbaek@jwu.ac.kr

The number of victims of ransomware is increasing despite attempts to defend them, as variants of ransomware are continuously being developed. Research and technology that detects and repairs ransomware variants to prevent damage from ransomware ensure a high level of security; however, they require additional tradeoffs, including computing resources, to effectively apply them. In this study, to address these problems, we proposed a solution that uses the electrical characteristics of a capacitor to detect abnormal data flow generated at input-output channels of storage by consecutive encryption calculation. We observed that based on Shannon's information entropy, the encrypted files and normal files, i.e., unencrypted files, can be distinguished based on entropy results. Through this, we assume that both types of files will affect the voltage change generated at multiple inputoutput channel of storage according to data flow. Consequently, we expect that this voltage change can be detected by using a capacitor, and abnormal data flow can be identified by calculating entropy. This study shows the possibility of computationless abnormal data flow to detect abnormal data flow using a hardware-based capacitor module. Moreover, we expect that since our method utilizes hardware characteristics, it will detect the ransomware avoiding the anti-ransomware detection technique relatively more accurately compared with the software-based detection technique. Our future work aims to perform this experiment on real storage devices such as SSD.

Hye-Lim Jung received the B.S. degree in the department of information security from Daejeon University in 2015, and the M.S. degrees in the department of information security from Daejon University 2017. She is a Ph.D. Student of Sejong Univerity. Her research interests include system security and secure storage system.

Sungkyu Ahn received the B.S. degree in the department of information security from Daejeon University in 2015, and the M.S. degrees in the department of information security from Daejon University 2017. He is a Ph.D. Student of Sejong Univerity. His research interests embedded system security and secure storage system.

Sung Hoon Baek received the B.S. degree in electronics engineering from Kyungpook National University, Korea, in 1997, the M.S.degree in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST) in 1999, the Ph.D. degree in electrical engineering from KAIST in 2008. He worked for Electronics Telecommunication Research Institute (ETRI) as an R&D staff from 1999 to 2005 and for Samsung Electronics as a senior R&D staff from 2008 to 2011. He has been an assistant professor in the department of computer system engineering at Jungwon University since 2011. His research interests include storage system, operating system, and parallel processing.

Ki-Woong Park received the B.S. degree in computer science from Yonsei University, South Korea, in 2005, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology in 2007 and 2012, respectively. He was a Senior Researcher with the National Security Research Institute. He is currently a Professor with the Department of Computer and Information Security, Sejong University. His research interests include security issues for cloud and mobile computing systems as well as the actual system implementation and subsequent evaluation in a real computing system. He was a recipient of the 2009-2010 Microsoft Graduate Research Fellowship.