Meetings International
SciTechnol
International Conference on
FORENSIC RESEARCH & TECHNOLOGY
&
ANNUAL BIOMARKERS CONGRESS
September 17-18, 2018 | Osaka, Japan
Yulai Xie, J Forensic Toxicol Pharmacol 2018, Volume: 7
DOI: 10.4172/2325-9841-C2-010

Yulai Xie

Huazhong University of Science and Technology, China

Unifying intrusion detection and forensic analysis via provenance awarenes

The existing host-based intrusion detection methods are mainly based on recording and analyzing the system calls of the invasion processes (such as exploring the sequences of system calls and their occurring probabilities). However, these methods are not efficient enough on the detection precision as they do not reveal the inherent intrusion events in detail (e.g., where are the system vulnerabilities and what causes the invasion are both not mentioned). On the other hand, though the log-based forensic analysis can enhance the understanding of how these invasion processes break into the system and what files are affected by them, it is a very cumbersome process to manually acquire information from logs which consist of the users' normal behavior and intruders' illegal behavior together. We use provenance, the history of an object that explicitly represents the dependency relationship between the damaged files and the intrusion processes, rather than the underlying system calls, to detect and analyze intrusions. Provenance more accurately reveals and records the data and control flow between files and processes, reducing the potential false alarm caused by system call sequences. Moreover, the warning report during intrusion can explicitly output system vulnerabilities and intrusion sources, and provide detection points for further provenance graph based forensic analysis. Experimental results show that this framework can identify the intrusion with high detection rate, lower false alarm rate, and smaller detection time overhead compared to traditional system call based method. In addition, it can analyze the system vulnerabilities and attack sources quickly and accurately.

Biography

Yulai Xie received the B.E. and Ph.D. degrees in computer science from Huazhong University of Science and Technology (HUST), China, in 2007 and 2013, respectively. He was a visiting scholar at the University of California, Santa Cruz in 2010 and a visiting scholar at the Chinese University of Hong Kong in 2015. He is now an associate professor in school of computer from Huazhong University of Science and Technology (HUST) in China. His research interests mainly include digital provenance, intrusion detection, network storage and computer architecture.

ylxie@hust.edu.cn

Notes: