VirtAV: an Agentless Antivirus System based on In-Memory Signature Scanning for Virtual Machine

Tang Hongwei[1,2,3], Feng Shengzhong[1,3], Zhao Xiaofang[2,3], Jin Yan[2]

[1]Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen China

[2]Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China

[3]University of Chinese Academy of Sciences, Beijing 100049, China

tanghongwei@ict.ac.cn, sz.feng@siat.ac.cn, zhaoxf@ ict.ac.cn, jinyan@ncic.ac.cn

Abstract—Antivirus is an important issue to the security of virtual machine (VM). According to where the antivirus system resides, the existing approaches can be categorized into three classes: internal approach, external approach and hybrid approach. However, for the internal approach, it is susceptible to attacks and may cause antivirus storm and rollback vulnerability problems. On the other hand, for the external approach, the antivirus systems built upon VMI technology cannot find and prohibit viruses promptly. Although the hybrid approach performs virus scanning out of the virtual machine, it is still vulnerable to attacks since it completely depends on the agent and hooks to deliver events in the guest operating system. To solve the aforementioned problems, based on in-memory signature scanning, we propose an agentless antivirus system VirtAV. VirtAV can monitor the specific event of the guest VM that is defined as the first instruction-fetch operation on a newly updated host memory page frame, and can scan virus in the page when the event occurs. As an external approach, VirtAV doesn't rely on any event or agent in the guest OS, so it guarantees the security of itself to the greatest extent. In addition, it provides full life cycle protection for VMs, no matter which state (running, paused, resumed or migrated) they are in. We implemented a prototype by extending Qemu/KVM hypervisor. Experimental result demonstrates that the function of VirtAV is verified (by finding 100% of the 3546 sample viruses) and the overhead of VirtAV on guest performance is acceptable. Especially, VirtAV has little impact on the performance of common desktop applications, such as video playing, web browsing and Microsoft Office series.

***Keyword*—agentless, antivirus, antivirus storm, virtual machine, virus signature**

Hongwei Tang is a PhD candidate at the University of Chinese Academy of Sciences. He received his B.S. degree from Nankai University (China) in 2006 and M.S. degree from University of Chinese Academy of Sciences in 2009. Currently, he is a senior member of China Computer Federation (CCF) and a research associate at Institute of Computing Technology of Chinese Academy of Sciences (ICT, CAS). His research interests include cloud computing, virtual machine and operating system.

Shengzhong Feng received his Ph.D. degrees in computer science from Beijing Institute of Technology in 1997. He was employed by Institute of Computing Technology, Chinese Academy of Sciences. From 2005 to 2007, he investigated gene chip algorithm design as a visiting professor in University of Toronto, Canada. Currently, he is the executive director of the China Mathematics Software Association and a committee member of High Performance Computing Association. He has published over 30 research papers, most of them are indexed by SCI/EI. His research interests include high performance computing, grid computing and bioinformatics.

Xiaofang Zhao received her Ph.D. degrees in computer science from Institute of Computing Technology, Chinese Academy of Sciences. Currently, she is the director of computer application research center in Institute of Computing Technology, Chinese Academy of Sciences. She is a senior member of China Computer Federation (CCF) and a member of Engineering and Technology Committee. Her research interests include computer architecture of next generation, security of computer system and information security.

Yan Jin received the B.S., M.S., and Ph.D. degrees in computer science from Harbin Institute of Technology, Harbin, China, in 2001, 2003, and 2008, respectively. He was a research fellow in department of Electrical and Computer Engineering, University of Nevada, Las Vegas (UNLV) from 2008 to 2011. Since 2012, he has been an associate professor in Institute of Computing Technology, Chinese Academy of Sciences. His research interests include network security, cloud computing and cloud security.