Learning from Rootkits

Patrick Stewin*

*Security in Telecommunications
Technische Universität Berlin, D-10587 Berlin, Germany
patrickx{at}sec.t-labs.tu-berlin.de

A rootkit is malicious code with certain stealth capabilities. It is placed on a target platform by an attacker. Stealth is an important rootkit property, since the attacker's goal is to hide the malicious code from the user. Therefore, rootkit developers try to find more *advanced* environments to hide their rootkits as documented by the rootkit evaluation: Rootkits moved from user space to kernel space and beyond.

One approach to obtain stealthiness is to somehow isolate the rootkit from the host platform. Our focus is on modern x86 platforms. On such platforms security researchers demonstrated rootkits (according to the ring protection model) not only running in user space (ring 3) or kernel space (ring 0) but also in ring -1 (Virtual Machine Monitor [2]), ring -2 (System Management Mode [1]) and ring -3 (Intel Active Management Technology [3]) in recent years. Obviously, the lower the ring the more isolated is the rootkit from the user.

Goals Our goal is to understand these isolated execution environments to: (i) develop countermeasures against such powerful and stealthy rootkits and to (ii) use them to enhance the platform's security properties. These isolated execution environments could be perfectly used to run code related to the Trusted Computing Base (TCB) such as a runtime monitor.

Challenges As yet, security research in this area has been done mainly on rootkits. To run code related to the TCB in an isolated environment, such as ring -3, certain challenges arise. For example, we need evidence that the environment is *bullet proof.* The herein before mentioned rootkits show, that the isolated environments are not bullet proof. Furthermore, we must understand the properties of these environments to realize an appropriate measurement strategy, i.e., how, when and what to measure when monitoring the platform. An important challenge arising in this context is the time-of-check-time-of-use (TOCTOU) problem.

References

[1] S. Embleton, S. Sparks, and C. Zou, "Smm rootkits: a new breed of os independent malware," in *SecureComm '08: Proceedings of the 4th international conference on Security and privacy in communication networks.* New York, NY, USA: ACM, 2008, pp. 1–12.

[2] J. Rutkowska, "Subverting Vista kernel for fun and profit," Black Hat USA, Aug. 2006. [Online]. Available: `http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf`

[3] A. Tereshkin and R. Wojtczuk, "Introducing Ring -3 Rootkits," Black Hat USA, Jul. 2009. [Online]. Available: `http://www.blackhat.com/presentations/bh-usa-09/TERESHKIN/BHUSA09-Tereshkin-Ring3Rootkit-SLIDES.pdf`