Establishing and Maintaining Root of Trust on Commodity Computer Systems

Virgil Gligor

Carnegie Mellon University
Pittsburgh, PA 15213
virgil@andrew.cmu.edu

ABSTRACT

Suppose that a trustworthy program must be booted on a commodity system that may contain *persistent* malware. *Establishing root of trust* (RoT) ensures the system has all and only the content chosen by a trusted verifier or the verifier discovers unaccounted content, with high probability. Obtaining such an assurance is challenging because malware can survive in system states across repeated secure- and trusted-boot operations and act on behalf of a powerful remote adversary. I this presentation, I illustrate both the theoretical and practical challenges of RoT establishment *unconditionally*; i.e., without secrets, trusted hardware modules (e.g., TPMs, HSMs) or adversary computation bounds. I also illustrate the only unconditional solution to this problem known to date.

Establishing root of trust forces the adversary to repeat the malware-insertion attack, perhaps at some added cost. However, the inherent size and complexity of commodity OS components (aka., the "giants") render them vulnerable to such successful attacks. In contrast, small and simple software components with rather limited function and high-assurance security properties (aka., the "wimps") can, in principle, be resistant to attack. *Maintaining root of trust* assures a user that a commodity computer's wimps are isolated from, and safely co-exist with, adversary-controlled giants. However, regardless how secure program isolation may be, *I/O separation* must also be achieved despite the pitfalls of commodity architectures that encourage I/O hardware sharing, not isolation. In this presentation, I also illustrate the challenges of I/O separation and present and approach that enables the co-existence secure wimps with insecure giants, via an example of a system implemented at CMU.

CCS Concepts/ACM Classifiers

Security and privacy → System security; Trusted computing

Author Keywords

Root of trust establishment; persistent malware; unconditional malware detection; application isolation; I/O separation; on-demand I/O channels

BIOGRAPHY

Virgil D. Gligor is a Professor of ECE at Carnegie Mellon University. His research has ranged from access control, penetration analysis, and denial-of-service, to applied cryptography. He was an Associate Editor of several ACM and IEEE journals and the *Editor in Chief* of the IEEE Transactions on Dependable and Secure Computing. He received the *2006 National Information Systems Security Award* jointly given by NIST and NSA, the *2011 Outstanding Innovation Award* of the ACM SIGSAC, and the *2013 Technical Achievement Award* of the IEEE Computer Society. He was inducted into the *National Cyber Security Hall of Fame*.

REFERENCES

[1] Virgil D. Gligor, Maverick Woo, "Establishing Software Root of Trust Unconditionally," in Proc. of NDSS, Feb., 2019.

[2] Virgil D. Gligor, "Dancing with the Adversary – A Tale of Wimps and Giants," in Proc. of 22nd SPW, Cambridge, UK, (LNCS 8809) March 2014.

AsiaCCS '19, July 9–12, 2019, Auckland, New Zealand.

ACM ISBN 978-1-4503-6752-3/19/07.
DOI: https://doi.org/10.1145/3321705.3329913