Intel Software Guard Extensions - Introduction and Open Research Challenges

Matthias Schunter
Intel Labs, Portland, OR, USA
Intel Collaborative Research Institute for Secure Computing, Darmstadt, Germany
matthias.schunter@intel.com

ABSTRACT

Hardware-enhanced security is an important pillar of secure systems in general and software protection in particular. This presentation will survey the recently announced Intel® Software Guard Extensions (Intel® SGX) as well as innovative usages for building secure systems using security-enhanced hardware.

Intel SGX is an Intel technology for application developers who are seeking to protect select code and data from disclosure or modification. Intel SGX makes such protections possible through the use of enclaves, which are protected areas of execution. Security critical application code can be put into an enclave by special instructions and is then hardware protected from attacks by other potentially malicious software. An enclave can therefore be shielded against attacks by untrusted application parts, by other applications, and also against attacks by a compromised operating system.

Keywords

hardware-enhanced security, isolation, confidentiality, integrity, privacy, enclaves

BIO

Matthias Schunter (Dr.-Ing, MBA) is the Chief Technologist of the Intel Collaborative Research Institute for Secure Computing and a Principal Engineer at Intel Labs. His current research focuses on scalable security for IoT infrastructures. He has conducted research in diverse areas such as virtual systems security, trusted computing, enterprise privacy management, security protocols, and cryptography. Prior to joining Intel, he joined IBM Research - Zurich in 2001 and has lead their research on cloud security and was technical leader of the EU Project TClouds. He holds an MBA from Warwick University, a Doctorate from Saarland University, and a Diploma in Computer Science from Hildesheim University. Dr. Schunter is author or co-author of more than sixty technical papers and twenty patent filings on security and privacy. A full CV can be found at http://www.schunter.org/.

SPRO'16 October 28-28 2016, Vienna, Austria

ACM ISBN 978-1-4503-4576-7/16/10...$15.00

DOI: http://dx.doi.org/10.1145/2995306.2995307