Rethinking Side Channel Security on Untrusted OS

PI: Yinqian Zhang, Ohio State University

Objective

The objective of this project is to systematically study the side channel security of the shielded execution protected by Intel Software Guard eXtension (SGX) when the underlying operating systems are considered as untrusted.

Background

SGX is designed to protect both confidentiality and integrity of shielded execution from powerful adversaries who have full control of the entire OS, but their security guarantees have not yet been thoroughly investigated against the notorious vector of information leakage—side-channel attacks.

Traditional research on side channel security precludes powerful adversaries who are able to compromise the OS kernels. However, as direct accesses to the shielded programs are prohibited by SGX, side-channel attack vectors have become the most dangerous vulnerabilities that allow information exfiltration.

Goals

- Advance the state-of-the-art research on side channel security by exploiting model-checking techniques to automatically identify information leakage through shared resources.
- Evaluate the severity of side-channel attacks by privileged attackers, by systematically exploring the privileges of an operating system that may be exploited by attackers to construct side-channel attacks with higher fidelity, efficiency, and robustness.
- Conduct a preliminary exploration of potential research directions towards effective mitigation of privileged side channel attacks.

Approach

- Identify side-channel information leakage using model checking
  - Model shared hardware and software resources as finite state machines
  - Check non-interference property automatically using SPIN model checker
  - Validate identified side-channel information leakage in practice
- Re-evaluate the severity of privileged side channel attacks
  - Investigate key challenges to conduct side-channel attacks in practice
  - Exploit OS privilege to improve the effectiveness of side-channel attacks

Progress so far

- Deepened our understanding of traditional side-channel attacks and defenses [CCS’16a, CCS’16b, RAID’16]
- Detecting privileged side-channel attacks via timed execution [in submission]

On-going research efforts

- Model checking for side-channel attack vector detection on untrusted OS
- Discovering software vulnerabilities in shielded programs under privileged side-channel threat models.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

University #1 Logo

University #2 Logo