Review “CFI-SGX”

Name: Wenhui Zhang

Paper Name：

Lee, S., Shih, M. W., Gera, P., Kim, T., Kim, H., & Peinado, M. (2017, August). Inferring fine-grained control flow inside SGX enclaves with branch shadowing. In *26th USENIX Security Symposium, USENIX Security* (pp. 16-18).

Contribution:

This attack paper proposes an exploit named branch shadowing attack. This attack is a side channel attack based on branch prediction history traces. Before this work, researchers has demonstrated that SGX is vulnerable to page fault based attacks, and this paper is a real world demonstration of this attack. In this paper, 2 new techniques are proposed: “1) a last branch record (LBR)-based history-inferring technique and 2) an advanced programmable interrupt controller (APIC)-based technique to control the execution of an enclave in a fine grained manner.”

Motivation:

SGX leaves branch history uncleared, when enclave mode switches. This releases fine grained execution traces for assisting adversaries. However, exploiting branch prediction side channel is challenging: 1) measuring branch execution time is too noisy; 2) pausing an enclave right after execution of a certain code block is hard; (3) existing of ASLR makes it hard to guess addresses of branch prediction; (4) since branch target buffer(BTB) is limited, it is easily over-written.

Related works:

Side-channel attacks against Intel SGX: (1) Monitor page-fault or page-access sequence is Noise-free, but coarse-grained (page address). [Oakland15, ASIACCS16, Security17]; (2) Measure cache hit/miss timing is Fine-grained (cache line), but noisy [EuroSec17, DIMVA17, ATC17, WOOT17].

Methodology:

Attacker knows the source code or binary of a target enclave; Attacker can frequently interrupt the target enclave’s execution to execute attack code; Attacker prevents or disrupts the target enclave from accessing a trusted time source.

Step 1: Prepare a shadow copy of an SGX program to monitor it with LBR;

Step 2: Interrupt SGX execution and monitor shadow code with LBR;

Results:

The author claims that they could recover 66% of a 1024-bit RSA private key from a single run (~10 runs are enough to fully recover it), for sliding-window exponentiations.

Take away:

Branch shadowing: Fine-grained and deterministic side-channel attack on SGX

- Reveal direction and/or execution of individual branch instrs

Proposed hardware- and software-based countermeasures

- Branch history flushing and obfuscation