FORESHADOW

Breaking the Virtual Memory Abstraction

Akkapaka Saikiran - 180050005
Aniruddha Chidar - 180050008
Saumya Goyal - 180050092
Shalabh Gupta - 180050095
Shashank Roy - 180050097

Introduction

- Speculative Execution
- Abuse of speculative execution: Meltdown
- Good news: Enclaves (eg. SGX)
- Breaking SGX: Foreshadow

Meltdown Overview : FLUSH + RELOAD

Step 1: Dereference pointer to unauthorized memory - illegal! Leads to page fault

Step 2: Fetch secret dependent array index into cache in transient execution window

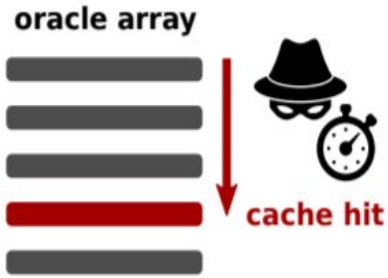
Step 3: User fault handler compares array access time

Listing 1: x86 assembly.

```
1 meltdown:
2   // %rdi: oracle
3   // %rsi: secret_ptr
4
5   movb (%rsi), %al
6   shl $0xc, %rax
7   movq (%rdi, %rax), %rdi
8   retq
```

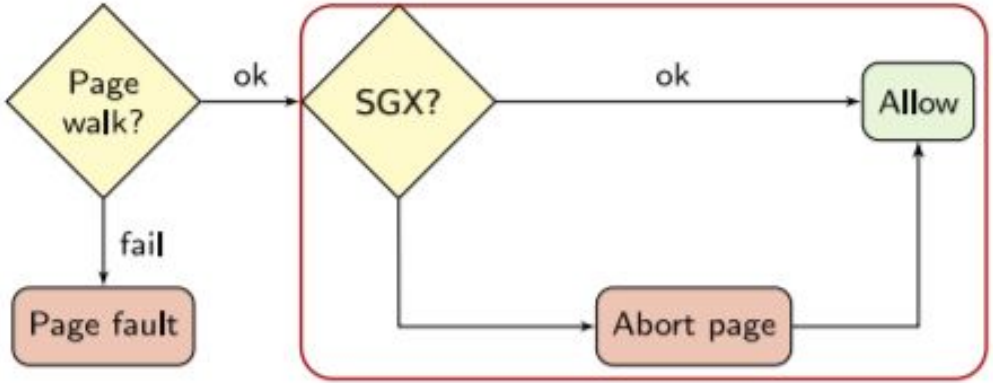
Listing 2: C code.

```
1 void meltdown(
2       uint8_t *oracle,
3       uint8_t *secret_ptr)
4 {
5   uint8_t v = *secret_ptr;
6   v = v * 0x1000;
7   uint64_t o = oracle[v];
8 }
```



SGX: What is special?

- Define private regions of memory: **enclaves**
- External access to enclave lead to **abort page semantics**
- Reads return -1 (`0xff`), writes ignored
- No exception raised - meltdown unsuccessful



L1TF mechanism

- Trigger page fault to evade abort page semantics
  - Unmap page table entry using `mprotect()` system call
- Strict caching requirements: Required that enclave loads are served from L1 cache
  - Doesn't work if data in L2
  - Intel dubbed this **L1 Terminal Fault** (L1TF)
- Deduce secrets using Flush and Reload
  - Enclave entry/exit flushes TLB, reload oracle array for fast access

Mitigations

- Side channel hardening techniques don’t work
    - TSX detection can be evaded through advanced versions of Foreshadow
- Silicon based and microcode patches by Intel
- Hardware-software co-mitigation strategies possible
    - Like ensuring L1 cache flushed on enclave entry/exit

Acknowledgement

- We are very grateful for the help received from Jo Van Bulck

- References:
  - Images taken from USENIX
  - Demo taken from Jo Van Bulck
  - Other references for report

Demo Upcoming! Get ready to know the enclave secrets