Side-Channel Attacks and Defenses for SGX and SEV

Yinqian Zhang
Associate Professor
Computer Science & Engineering
The Ohio State University
Userland TEEs on Commodity Processors

Software Guard Extension (2015)

Secure Encrypted Virtualization (2016-2017)
Side-Channel Threats on Intel SGX

**Privileged Adversary**

- CPU management
  - CPU Scheduling
  - Interrupt delivery and handling
- Memory management
  - Paging
  - Segmentation
- I/O management
  - Network
  - Storage
  - Display
Side-Channel Threats on AMD SEV

Privileged Adversary
- CPU management
  - CPU Scheduling
  - Interrupt delivery and handling
- Memory management
  - Paging
  -Segmentation
- I/O management
  - Network
  - Storage
  - Display
Example: Deterministic Page Fault Side Channels

Application

```
ec_mul(r,G):
res = 0
nbits = |r|
for (i = nbits-1; i >=0; i--):
    res = dup_point(res)
if (test_bit(r[i])):
    res = add_points(res, G)
return res
```

Kernel

```
| 0 | 51 | 9 | 12 |
---|----|---|----|
| D | A | G | W |
```

```
| 52 | 62 | 63 |
---|----|----|
| X | D | P |
```

```
<table>
<thead>
<tr>
<th>CR3</th>
<th>Page Global Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Page Upper Directory</td>
</tr>
<tr>
<td></td>
<td>Page Middle Directory</td>
</tr>
<tr>
<td></td>
<td>Page Table</td>
</tr>
<tr>
<td></td>
<td>Page Table Entry</td>
</tr>
</tbody>
</table>
```

```
Page Trace
P1
P2
P1
P3
P2
P1
...```

```
Page Fault Handler
```
Example: Fine-Grained CPU Preemption
More Issues with AMD SEV

- Lack of memory integrity
  - Chosen plaintext attacks
  - Fault injection attacks
  - Page table manipulation
- Unencrypted VMCB
  - Inference by reading register values at VMExit
  - ROP attacks by altering register values
- Page fault side channel
  - Page offset mask
- Unprotected I/O
  - IOMMU & ASID

Li, Zhang, Lin, Solihin, “Exploiting Unprotected I/O Operations in AMD’s Secure Encrypted Virtualization”, Usenix Security 2019
Side-Channel Attack Surface

Translation Units
- fetcher
- decoder
- issuer
- scheduler

Page tables
- paging caches
- STLBT
- ITLB
- DTLB

Cache & Memory
- DRAM
- LLC
- L2
- L1-I
- L1-D
- LFB

Execution Units
- port 0
- port 1
- port 2
- port 3
- port n

Execution Units
- BPU
- BTB
- RSB
Solutions to SGX/SEV side-channel attacks
Solutions to SGX Side Channels?

Cross-VM/Process Attacks

SGX Attacks

OS

Enclave

Enclave

Hypervisor

VM

VM
Three Ideas of Mitigating SGX Side Channels

**Vulnerability Detection**
- Analyzing enclave code to eliminate
  - Secret-dependent memory access
  - Spectre gadgets


Three Ideas of Mitigating SGX Side Channels

**Vulnerability Detection**
- Analyzing enclave code to eliminate
  - Secret-dependent memory access
  - Spectre gadgets

**Attack Prevention**
- Preventing side-channel attacks by enforcing oblivious execution

Three Ideas of Mitigating SGX Side Channels

__Vulnerability Detection__
- Analyzing enclave code to eliminate
  - Secret-dependent memory access
  - Spectre gadgets

__Attack Prevention__
- Preventing side-channel attacks by enforcing oblivious execution

__Attack Detection__
- Detecting side-channel attacks at runtime via program instrumentation

Chen, Zhang, Reiter, Zhang, “Detecting Privileged Side-Channel Attacks in Shielded Execution with DEJA VU”, ACM AsiaCCS 2017

Side-Channel Attacks and Defenses for SGX and SEV

Yinqian Zhang
Associate Professor
Computer Science & Engineering
The Ohio State University

Thank You!
yinqian@cse.ohio-state.edu