An Off-Chip Attack on Hardware Enclaves via the Memory Bus

Dayeol Lee¹, Dongha Jung³, Ian T. Fang¹, Chia-Che Tsai¹,², Raluca Ada Popa¹

¹ UC Berkeley
² Texas A&M University
³ SK Hynix Inc.
Trusted Execution Environments (TEEs)

- Sensitive App
- Other Apps
- OS / Hypervisor
- Trusted Processor
- Enclave
- DRAM

- Integrity
- Confidentiality
- Remote Attestation
Memory Encryption of Intel SGX

Processor Cores

Memory Encryption Engine

DRAM

Enclave

Trusted

Untrusted
Access Pattern Leakage via Side Channel

Hunspell [Xu et al., 17]

Spell Checker:

for each word in input text:
...
dictionary.search(word)
...

Dictionary (Hash Table):

casetable[0]  cask  book  ...
table[1]  cry  rich  ...
...
Access Pattern Leakage via Side Channel

Hunspell [Xu et al., 17]

Input Text

... The **book** was written by ...

Access Pattern:

... 0xf9 0xa0 0xc4 0xd8 0xc7 ...

Spell Checker:

```python
for each word in input text:
...
dictionary.search(word)
...
```

Dictionary (Hash Table):

```
<table>
<thead>
<tr>
<th>Table</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>table[0]</td>
<td>cask</td>
</tr>
<tr>
<td></td>
<td>0xa0</td>
</tr>
<tr>
<td>table[1]</td>
<td>cry</td>
</tr>
<tr>
<td></td>
<td>0xc4</td>
</tr>
<tr>
<td></td>
<td>book</td>
</tr>
<tr>
<td></td>
<td>0xd8</td>
</tr>
<tr>
<td></td>
<td>rich</td>
</tr>
<tr>
<td></td>
<td>0xc7</td>
</tr>
</tbody>
</table>
```

“book”
Side-Channel Attacks on SGX Enclaves

- Cache Side-Channel Attacks
  - Brasser’17, Schwarz’17, Moghimi’17, VanBulck’18

- Page Table-Based Attacks
  - Controlled-Channel'15, VanBulck’17
Side-Channel Attacks on SGX Enclaves

- **Cache Side-Channel Attacks**
  - Brasser’17, Schwarz’17, Moghimi’17, VanBulck’18

- **Page Table-Based Attacks**
  - Controlled-Channel'15, VanBulck’17

- **Mitigations**
  - Varys ’18, Chen et al.’18, Gruss et al. ’17, T-SGX’17, DéJà Vu ’17

- **TEEs from Academia**
  - Keystone’20, Sanctum’16
Membuster: Demonstrating “Off-Chip Attack”

Victim

Attacker

MMU

Cache

DRAM

- Cache Side-Channel Attacks
  - Brasser'17, Schwarz'17, Moghimi'17, VanBulck'18
- Page Table-Based Attacks
  - Controlled-Channel'15, VanBulck'17
- Mitigations
  - Varys'18, Chen et al.'18, Gruss et al.'17, T-SGX'17, Déjà Vu '17
- TEEs from Academia
  - Keystone'20, Sanctum'16
MEMBUSTER: Demonstrating “Off-Chip Attack”

- **Cache Side-Channel Attacks**
  - Brasser’17, Schwarz’17, Moghimi’17, VanBulck’18

- **Page Table-Based Attacks**
  - Controlled-Channel'15, VanBulck’17

- **Mitigations**
  - Varys ’18, Chen et al.’18, Gruss et al. ’17, T-SGX’17, DéJà Vu ’17

- **TEEs from Academia**
  - Keystone’20, Sanctum’16

None of these can mitigate
**MEMBUSTER: Demonstrating “Off-Chip Attack”**

- Hard to detect or mitigate on chip
  - No interference with SW
  - Resource partitioning does not work

- Oblivious memory access
  - Performance impact

- Address bus encryption
  - Infeasible in commodity DRAM
Challenges of the Off-Chip Attack

- Address Translation and Synchronization
Challenges of the Off-Chip Attack

- Address Translation and Synchronization
- Lossy Channel due to Cache Hierarchy
Challenges of the Off-Chip Attack

- Address Translation and Synchronization
- Lossy Channel due to Cache Hierarchy
- Unusual Behavior in SGX
Challenges of the Off-Chip Attack

- Address Translation and Synchronization
- Lossy Channel due to Cache Hierarchy
- Unusual Behavior in SGX
Maximizing Side-Channel Information

- **Goal:**
  - Increase cache misses
  - Avoid detectable interference

- **Cross-core cache priming**
  - Cache eviction in PRIME+PROBE Attack

- **Problems**
  - Insufficient memory access bandwidth
  - Large last-level cache
  - Hundreds of milliseconds to evict all
Maximizing Side-Channel Information

- Observation 1
  The address mapping is untrusted
Maximizing Side-Channel Information

- Observation 1
  The address mapping is untrusted

- Observation 2
  The attacker only needs to observe “critical” memory accesses

Idea: Squeeze the Cache!
Cache Squeezing in a Nutshell

Critical Pages

Virtual Pages (Victim)

EPC Pages

LLC Sets

OS Pages

No interrupt nor fault

Small slowdown
Evaluation

• Hardware
  § Intel i5-8400 (Coffee Lake)
  § LLC: 9MB, 6-slice, 12-way set associative, 2048 sets
  § DRAM: Non-ECC DDR4-2400 UDIMM 8GB
  § Interposer/signal analyzer from SK Hynix

• Software
  § Two attack examples: Hunspell and Memcached
  § Graphene-SGX with unmodified victim application
  § Modified SGX driver for cache squeezing
Hunspell Attack Results

- Randomly-generated words (Random) and Wizard of Oz (Wizard)
- Squeezing+Priming recovers most of the data

No interference: hard to detect with on-chip techniques
Conclusion

• Membuster: an off-chip attack via the memory bus
  ▪ Performed on commodity CPU and DRAM
  ▪ Non-interfering with victim application
  ▪ Previous on-chip solutions or other TEEs do not defeat the attack

• Costly mitigation techniques
  ▪ Oblivious memory access
  ▪ Alternative TEE architecture (e.g., memory bus encryption)

Thank You!
Thank You!

Dayeol Lee (dayeol@berkeley.edu)
Chia-Che Tsai (chiache@tamu.edu)
Raluca Ada Popa (raluca.popa@berkeley.edu)