Flush+Flush: A Fast and Stealthy Cache Attack

Daniel Gruss, Clémentine Maurice, Klaus Wagner and Stefan Mangard
Graz University of Technology
July 8, 2016 — DIMVA 2016
Motivations

- cache side channels are **stealthy** attacks $\rightarrow$ not detected by IDS
Motivations

- cache side channels are **stealthy** attacks → not detected by IDS
- but cache attacks have a large impact on the cache
  → use **performance counters** for detection [HF15; Pay16]
  → detect abnormal behavior
Contributions

- novel attack **Flush+Flush**
  - **stealthier** than previous cache attacks
  - **faster** than previous cache attacks

- framework to evaluate cache attacks
  - in terms of performance and detectability
  → https://github.com/IAIK/flush_flush
1. Introduction

2. Flush+Flush

3. Conclusion and future work
Caches on Intel CPUs

- L1 and L2 are private
- last-level cache
  - divided in slices
  - shared across cores
  - inclusive
  - hash function for addressing [MLSNHF15]
Access-driven cache attacks

Attacker monitors **its own activity** to find sets accessed by victim.

- **Flush+Reload**
  - [GBK11]
  - [YF14]
  - [GSM15]

- **Prime+Probe**
  - [Per05]
  - [LYGHL15]
  - [MNHF15]

Exploit timing difference between cache hits and cache misses
Flush+Reload

**step 0:** attacker maps shared library → **shared memory, shared in cache**
Flush+Reload

**step 0**: attacker maps shared library → shared memory, shared in cache
Flush+Reload

**step 0**: attacker maps shared library → shared memory, shared in cache

**step 1**: attacker *flushes* the shared line with `clflush`
Flush+Reload

**step 0**: attacker maps shared library → shared memory, shared in cache

**step 1**: attacker flushes the shared line with `clflush`

**step 2**: victim loads data while performing encryption
Flush+Reload

step 0: attacker maps shared library → shared memory, shared in cache
step 1: attacker flushes the shared line with clflush
step 2: victim loads data while performing encryption
step 3: attacker reloads data → fast access if the victim loaded the line
Prime+Probe

Attacker address space

Cache

Victim address space

**step 0**: attacker fills the cache (prime)
Prime+Probe

step 0: attacker fills the cache (prime)
Prime+Probe

step 0: attacker fills the cache (prime)
Prime+Probe

**step 0**: attacker fills the cache (prime)

**step 1**: victim evicts cache lines while performing encryption
Prime+Probe

**step 0**: attacker fills the cache (prime)

**step 1**: victim evicts cache lines while performing encryption
**Prime+Probe**

- **Step 0**: attacker fills the cache (prime)
- **Step 1**: victim evicts cache lines while performing encryption
Prime+Probe

**step 0**: attacker fills the cache (prime)
**step 1**: victim evicts cache lines while performing encryption
Prime+Probe

**step 0**: attacker fills the cache (prime)
**step 1**: victim evicts cache lines while performing encryption
Prime+Probe

**step 0**: attacker fills the cache (prime)

**step 1**: victim evicts cache lines while performing encryption

**step 2**: attacker probes data to determine if the set was accessed
Prime+Probes

- **Step 0**: Attacker fills the cache (prime)
- **Step 1**: Victim evicts cache lines while performing encryption
- **Step 2**: Attacker probes data to determine if the set was accessed
step 0: attacker fills the cache (prime)
step 1: victim evicts cache lines while performing encryption
step 2: attacker probes data to determine if the set was accessed
Examples of cache attacks

Covert channel:
- cross-VM, cross-core: 600kbps [LYGHL15]

Side channel:
- cross-VM, cross-core side-channel attacks on crypto algorithms
  - RSA: 96.7% of key bits in 1 signature [YF14]
- tracking user behavior in the browser, in JavaScript [OKSK15]
1. Introduction

2. Flush+Flush

3. Conclusion and future work
Which performance counters (1)

We analyzed events w.r.t cache attacks and benign programs:

- 23 hardware and cache performance events with `perf_event_open`
- `UNC_CBO_Cache_Lookup` of CBo with MSRs
  - `rmq`: only possible to monitor 4 events simultaneously
Which performance counters (2)

Detecting cache attacks and Rowhammer

1. \texttt{CACHE\_MISSES} → occur after data is flushed
2. \texttt{CACHE\_REFERENCES} → occur when reaccessing memory
3. \texttt{L1D\_RM} → occur after data is flushed
4. \texttt{LL\_RA} → occur when reaccessing memory
Which performance counters (3)

Detecting cache attacks and Rowhammer *without false positives*
Which performance counters (3)

Detecting cache attacks and Rowhammer *without false positives*

- heavy activity on the cache
Which performance counters (3)

Detecting cache attacks and Rowhammer *without false positives*

- heavy activity on the cache
- very short loops of code $\rightarrow$ low pressure on the iTLB
Which performance counters (3)

Detecting cache attacks and Rowhammer without false positives

- heavy activity on the cache
- very short loops of code → low pressure on the iTLB
  → normalize the events by ITLB_RA+ITLB_RM
Detection, non-normalized

- Cache misses (non-normalized)
- Cache hits (non-normalized)

Clémentine Maurice, Graz University of Technology
July 8, 2016 — DIMVA 2016
Detection, normalized

![Bar chart showing cache misses and hits normalized for Firefox, OpenTTD, stress -m 1, Flush+Reload, and Rowhammer.](chart.png)

Cache misses (normalized)  
Cache hits (normalized)
Stealthier cache attack: Flush+Flush

- motivation: detecting cache attacks with perf counters is not enough
Stealthier cache attack: Flush+Flush

- motivation: detecting cache attacks with perf counters is not enough
  - Flush+Flush: new cache attack, based on clflush timing leakage
    - stealthier than Prime+Probe and Flush+Reload
    - faster than Prime+Probe and Flush+Reload
**clflush timing leakage (1)**

- **clflush on cached data**

![Diagram](image-url)

- L1
- L2
- LLC
clflush timing leakage (1)

- **clflush on cached data**
  - goes to LLC, flushes line
clflush timing leakage (1)

- **clflush on cached data**
  - goes to LLC, flushes line

```
core 0
  L1
  L2
  LLC
```

```
core 1
  ...... (clflush on non-cached data goes to LLC, does nothing)
```
**clflush timing leakage (1)**

- **clflush on cached data**
  - goes to LLC, flushes line
  - flushes line in L1-L2

- **clflush on non-cached data**
  - goes to LLC, does nothing
  - fast
clflush timing leakage (1)

- clflush on cached data
  - goes to LLC, flushes line
  - flushes line in L1-L2
  \[ \rightarrow \text{slow} \]
clflush timing leakage (1)

- clflush on cached data
  - goes to LLC, flushes line
  - flushes line in L1-L2
  → slow

- clflush on non-cached data
clflush timing leakage (1)

- **clflush on cached data**
  - goes to LLC, flushes line
  - flushes line in L1-L2
  - → slow

- **clflush on non-cached data**
  - goes to LLC, does nothing
clflush timing leakage (1)

- **clflush on cached data**
  - goes to LLC, flushes line
  - flushes line in L1-L2
  \[ \rightarrow \text{slow} \]

- **clflush on non-cached data**
  - goes to LLC, does nothing
  \[ \rightarrow \text{fast} \]
clflush timing leakage (2)

![Graph showing execution time (in cycles) vs. number of cases for Ivy hit, Ivy miss, Haswell hit, Haswell miss, Sandy hit, and Sandy miss.]
Flush+Flush

**step 0**: attacker maps shared library → shared memory, shared in cache
Flush+Flush

**step 0**: attacker maps shared library → shared memory, shared in cache
Flush+Flush

**step 0**: attacker maps shared library $\rightarrow$ shared memory, shared in cache

**step 1**: attacker *flushes* the shared line
Flush+Flush

step 0: attacker maps shared library → shared memory, shared in cache
step 1: attacker flushes the shared line
step 2: victim loads data while performing encryption
Flush+Flush

**Step 0**: Attacker maps shared library → shared memory, shared in cache.

**Step 1**: Attacker flushes the shared line.

**Step 2**: Victim loads data while performing encryption.

**Step 3**: Attacker flushes data → high execution time if the victim loaded the line.
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Hit</th>
</tr>
</thead>
</table>

Flush+Flush spy

| F     | H   |

Victim

Clémentine Maurice, Graz University of Technology
July 8, 2016 — DIMVA 2016
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th></th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>$F$</th>
<th>$F$</th>
<th>$F$</th>
<th>$F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$H$</td>
<td>$H$</td>
<td>$H$</td>
</tr>
</tbody>
</table>

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim
Flush+Reload vs. Flush+Flush

### Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
</tr>
</tbody>
</table>

### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

### Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th></th>
<th>Reload</th>
<th></th>
<th>Reload</th>
<th></th>
<th>Reload</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td></td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

Clémentine Maurice, Graz University of Technology
July 8, 2016 — DIMVA 2016
### Flush+Reload vs. Flush+Flush

#### Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

#### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

#### Victim

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim
# Flush+Reload vs. Flush+Flush

### Flush+Reload spy

<table>
<thead>
<tr>
<th></th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

### Victim

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

|       |       |       |       |       |       |       |       |
Flush+Reload vs. Flush+Flush

**Flush+Reload spy**

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
</tr>
</tbody>
</table>

**Flush+Flush spy**

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

**Victim**

- Reload
- Miss
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim

Clémentine Maurice, Graz University of Technology
July 8, 2016 — DIMVA 2016
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

Reload

Miss
## Flush+Reload vs. Flush+Flush

### Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

### Victim

- Reload
- Miss
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

<table>
<thead>
<tr>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Miss</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

- Reload
- Miss
Flush+Reload vs. Flush+Flush

### Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

### Victim

- Reload
- Miss
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th></th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

<table>
<thead>
<tr>
<th></th>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
<td></td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>
### Flush+Reload vs. Flush+Flush

#### Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

#### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

#### Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
</tr>
</tbody>
</table>

Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Flush+Flush spy

| F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F |
| H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H | H |

Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>
# Flush+Reload vs. Flush+Flush

## Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Hit</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

## Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

## Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>
Flush+Reload vs. Flush+Flush

### Flush+Reload spy

## Flush+Reload vs. Flush+Flush

### Flush+Reload spy

<table>
<thead>
<tr>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
<th>Flush</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
<td>Hit</td>
<td>Miss</td>
</tr>
</tbody>
</table>

### Flush+Flush spy

<table>
<thead>
<tr>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

### Victim

<table>
<thead>
<tr>
<th>Reload</th>
<th>Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miss</td>
<td>Miss</td>
</tr>
</tbody>
</table>

Clémentine Maurice, Graz University of Technology  
July 8, 2016 — DIMVA 2016
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Reload vs. Flush+Flush

Flush+Reload spy

Flush+Flush spy

Victim
Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size (KBps)</th>
<th>capacity</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size (KBps)</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td></td>
<td>✗</td>
</tr>
</tbody>
</table>
# Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
## Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity  (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>4</td>
<td>54</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>4</td>
<td>52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>4</td>
<td>34</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>4</td>
<td>54</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>4</td>
<td>52</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>4</td>
<td>34</td>
<td>✗</td>
<td></td>
</tr>
</tbody>
</table>
Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>4</td>
<td>54</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>4</td>
<td>52</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>4</td>
<td>34</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Flush+Flush: Covert channel

<table>
<thead>
<tr>
<th>technique</th>
<th>packet size</th>
<th>capacity (KBps)</th>
<th>receiver stealth</th>
<th>sender stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Flush</td>
<td>28</td>
<td>496</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>28</td>
<td>298</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Flush+Reload</td>
<td>4</td>
<td>54</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>4</td>
<td>52</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>4</td>
<td>34</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Flush+Flush: Side channel on AES T-tables (1)

Number of encryptions to determine the upper 4 bits of a key byte

<table>
<thead>
<tr>
<th>technique</th>
<th>number of encryptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Reload</td>
<td>250</td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>350</td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>4800</td>
</tr>
</tbody>
</table>

→ same performance for Flush+Flush and Flush+Reload
Stealth comparison on 256 million encryptions

<table>
<thead>
<tr>
<th>technique</th>
<th>time (s)</th>
<th>stealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flush+Reload</td>
<td>215</td>
<td>✗</td>
</tr>
<tr>
<td>Prime+Probe</td>
<td>234</td>
<td>✗</td>
</tr>
<tr>
<td>Flush+Flush</td>
<td>163</td>
<td>✓</td>
</tr>
</tbody>
</table>

→ Flush+Flush is the only **stealthy spy process**
→ others need to be slowed down too much to be practical
Countermeasures

- `clflush`
  - unprivileged line eviction
Countermeasures

- clflush
  - unprivileged line eviction → make it privileged

- leaks timing information → make it constant-time
- rdtsc unprivileged timing → make it privileged
- fine-grained timing → make it coarse-grained
- disable shared memory
Countermeasures

- `clflush`
  - unprivileged line eviction $\rightarrow$ make it *privileged*
  - leaks timing information
Countermeasures

- clflush
  - unprivileged line eviction $\rightarrow$ make it privileged
  - leaks timing information $\rightarrow$ make it constant-time
Countermeasures

- `clflush`
  - unprivileged line eviction $\rightarrow$ make it `privileged`
  - leaks timing information $\rightarrow$ make it `constant-time`

- `rdtsc`
  - unprivileged timing
Countermeasures

- **clflush**
  - unprivileged line eviction → make it **privileged**
  - leaks timing information → make it **constant-time**

- **rdtsc**
  - unprivileged timing → make it **privileged**
Countermeasures

- **clflush**
  - unprivileged line eviction → make it **privileged**
  - leaks timing information → make it **constant-time**

- **rdtsc**
  - unprivileged timing → make it **privileged**
  - fine-grained timing
Countermeasures

- **clflush**
  - unprivileged line eviction → make it privileged
  - leaks timing information → make it constant-time

- **rdtsc**
  - unprivileged timing → make it privileged
  - fine-grained timing → make it coarse-grained
Countermeasures

- **clflush**
  - unprivileged line eviction $\rightarrow$ make it **privileged**
  - leaks timing information $\rightarrow$ make it **constant-time**

- **rdtsc**
  - unprivileged timing $\rightarrow$ make it **privileged**
  - fine-grained timing $\rightarrow$ make it **coarse-grained**

- disable shared memory
1. Introduction

2. Flush+Flush

3. Conclusion and future work
Conclusion and future work

- `clflush` leaks enough information to enable a side channel
- Flush+Flush is a novel cache attack that makes no memory access → faster and stealthier than previous cache attacks
Conclusion and future work

- `clflush` leaks enough information to enable a side channel
- Flush+Flush is a novel cache attack that makes no memory access
  → faster and stealthier than previous cache attacks

Future work

- new detection mechanism
- exploit timing difference of slices
Flush+Flush: A Fast and Stealthy Cache Attack

Daniel Gruss, Clémentine Maurice, Klaus Wagner and Stefan Mangard
Graz University of Technology
July 8, 2016 — DIMVA 2016
References I


References II


References III


Last-level cache addressing

![Diagram of last-level cache addressing]

- Physical address:
  - Tag: 35 bits
  - Set: 17 bits
  - Offset: 6 bits

- Set: 0
- Offset: 30
- Line:
  - Slice 0
  - Slice 1
  - Slice 2
  - Slice 3

- Offset:
  - 11
Bonus: Even more timing leakage

![Graph showing the number of cases for different cores over execution time.](image-url)
Performance counters: Usages

- answers “what’s happening in the system?”
- performance tuning $\rightarrow$ find bottlenecks
- side-channels [BM15]
- reverse-engineering microarchitecture [MLSNHF15]
- attack detection [DMSTWSS13; HF15; Pay16]