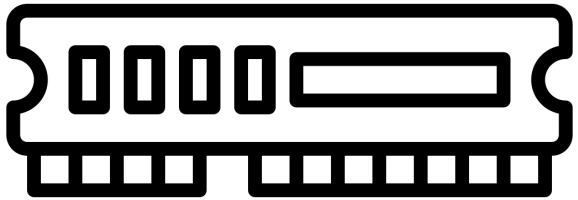
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY
TU Graz Graz University of Technology
SCHUTZWERK

CacheWarp: Software-based Fault Injection using Selective State Reset

Ruiyi Zhang, Lukas Gerlach, Daniel Weber, Lorenz Hetterich,
Youheng Lü, Andreas Kogler, Michael Schwarz

Cache – “Too low-level to me?”

SCHUTZWERK



Memory

Code

Variable

Stack

Heap

Cache

Warp – “INVD”

SCHUTZWERK

- Flushes the cache without triggering a write-back
  - modified values are lost

- Do not use it when memory coherence should be considered

- Safe Version – “WBINVD”
  - Write back all value in the cache before invalidating the cache

- Privileged Instruction…

SCHUTZWERK

AMD SEV

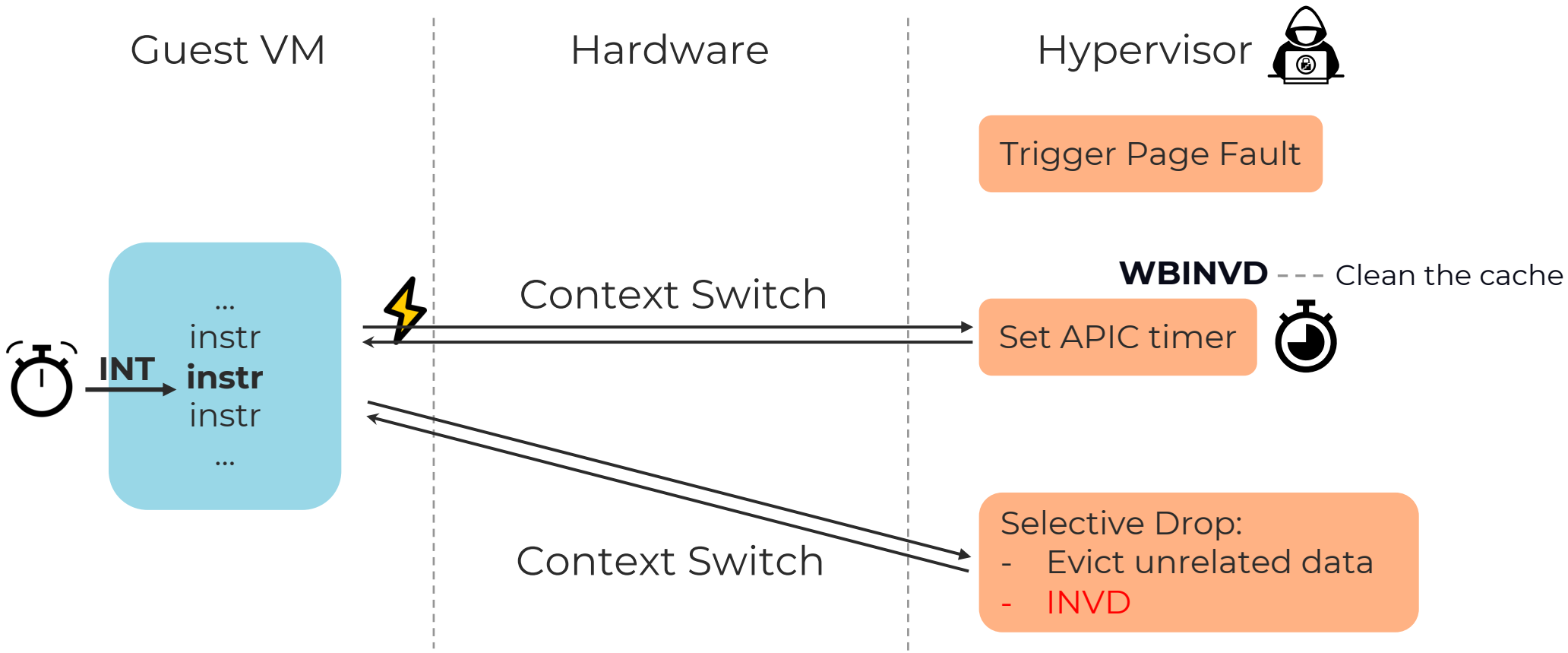
SECURE
ENCRYPTED
VIRTUALIZATION

- Strong Threat Model
- Encrypt the Entire VM
- Confidentiality – SEV-ES
- Integrity – SEV-SNP

… …

Selective State Reset

SCHUTZWERK



[1] J. Van Bulck, F. Piessens, and R. Strackx, “SGX-Step: A Practical Attack Framework for Precise Enclave Execution Control,” in Workshop on System Software for Trusted Execution,2017.22)

[2] M. Li, Y. Zhang, H. Wang, K. Li, and Y. Cheng, “Cipherleaks: Breaking constant-time cryptography on amd sev via the ciphertext side channel,” in USENIX Security Symposium, 2021.

[3] L. Wilke, J. Wichelmann, A. Rabich, and T. Eisenbarth, “Sev-step: A single-stepping framework for amd-sev,” 2023.

SCHUTZWERK

Exploits

Attacking Sudo

SCHUTZWERK

```
int uid = 0;
uid = getuid();
if (uid == 0){
  win();
}
```

Dropped via INVD

- Variable initialized with 0
- root uid = 0:
  - no password check

- More generic exploit primitive required
- Idea: Target Control Flow
- Use stale return address to “warp back in time”

Timewarp – High Level

SCHUTZWERK

```
a = ret1();

b = ret2();

if (a == b) {
  win();
}
```

INVD return address

```
a = ret1();
a = ret2();
b = ret2();

if (a == b) {
  win();
}
```

Timewarp - Animation

SCHUTZWERK

Demo

Attacking SSH

SCHUTZWERK

- Login with wrong password

```
real_pw = shadow_pw(user);
                    INVD return address
test_pw = xcrypt(user_input);

if (real_pw == test_pw) {
  win();
}
```

```
real_pw = shadow_pw(user);
real_pw = xcrypt(user_input);
test_pw = xcrypt(user_input);

if (real_pw == test_pw) {
  win();
}
```

Summary

SCHUTZWERK

- First attack breaks integrity of SEV-SNP
- Single Instruction abuse - INVD
- Mitigation via firmware and microcode update

Github:

github.com/cispa/CacheWarp

Demo:

cachewarpattack.com

Blogpost:

schutzwerk.com/en/blog/cachewarp/