Software-based Side-Channel Attacks and Defenses in Restricted Environments

Michael Schwarz
Graz University of Technology

Side Channels
Unintentional Information Leakage due to Hardware Side Effects
- Power consumption
- Execution Time
- CPU caches

Side Channels: Attacks and Building Blocks
- Attacks on Cryptography and User Input
- Measure Subtle Timing Differences
- Detect and Exploit Hardware Vulnerabilities
- We Found Spectre, Meltdown, and ZombieLoad

Side-Channel Protection for Browsers
- Identifying Attack Building Blocks
- Side-Channel Protection for Browsers
- Implementation as Chrome Extension

Restricted Environments
- TEEs
- Browser
- VMs

FANTASTIC Timers
Enable Timing Attacks in modern browsers
- Timing Primitives using Concurrency
- Techniques to Increase Timer Resolution
- Data Exfiltration from VM via DRAM

DECAF
Automatically Detect, Exploit, and Mitigate Double-Fetch Bugs
- Cache Attack plus Fuzzing
- Find and Exploit Bugs in TEEs
- Generic Exploitation Prevention

KeyDrown
Attacks on Key Presses and a Generic Protection
- First Cache Attack from Inside an Intel SGX Secure Enclave
- Fastest Self-Built Timing Primitive
- Novel Side-Channel Attack Combining Cache and DRAM

Facts & Numbers
- Authored papers, 7 accepted
- Presentations, 1 Keynote
- CVEs and Bug Bounties
- Co-authored papers, 11 accepted
- Awards, 2 Best Paper
- Advised Students, 1 Master Thesis

Conclusion
- Abstraction Layers Introduce Side Channels
- Always Underestimated Side Channels
- Removing and Restricting Features Not a Solution
- Researching Attacks Necessary to Find Effective Countermeasures

Hiding Attacks in Trusted Execution Environments
- First Cache Attack from Inside an Intel SGX Secure Enclave
- Fastest Self-Built Timing Primitive
- Novel Side-Channel Attack Combining Cache and DRAM

JavaScript Template Attacks
Automatically Inferring Host Information for Targeted Exploits
- Cache Attack plus Fuzzing
- Find and Exploit Bugs in TEEs
- Generic Exploitation Prevention

DECAF
Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features
- Cache Attack plus Fuzzing
- Find and Exploit Bugs in TEEs
- Generic Exploitation Prevention

JavaScript Zero: Real JavaScript and Zero Side-Channel Attacks
- First Cache Attack from Inside an Intel SGX Secure Enclave
- Fastest Self-Built Timing Primitive
- Novel Side-Channel Attack Combining Cache and DRAM

Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features
- Cache Attack plus Fuzzing
- Find and Exploit Bugs in TEEs
- Generic Exploitation Prevention