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

Assessors
Ass. Prof. Daniel Gruss
Prof. Frank Piessens

Michael Schwarz
Graz University of Technology

Defense
5.11.2019, 14:30
IFEG042

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

JavaScript Zero
REAL JavaScript and ZERO SIDECANAL HOLE ATTACKS

Protecting Browsers from Side-Channel Attacks
- JavaScript Templates
- Always Undetectable
- Security Features Not a Solution
- Researching Attacks Necessary to Find Effective Countermeasures

FANTASTIC TIMERS
HIGH-RESOLUTION MICROARCHITECTURAL ATTACKS IN JS

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

Restricted Environments
Gunilla Barends
- TEEs
- Enclave
- VMM
- Direct Physical Access
- Instruction Set

Facts & Numbers
- 7 Papers in Tracts (8 of 12)
- 24 Published Papers, 13 Tract 2
- 30 Presentations, 3 Keynotes
- 7 Awards, 2 Best Papers
- 11 Coauthors, 3 Co-advisors

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

Tamper Attacks with Decaf
Automatically Detect, Expose, and Mitigate Double-Fetch Bugs
- Cache Attack plus Fuzzing
- Fuzz and Expose Bugs in TEEs
- Generic Exploitation Prevention

KeyDrown
Attacks on Key Presses and a Generic Protection
- Two Novel Attacks on Keyboard Timings
- Generic Protection Against Keylogger Attacks
- Implementation for Smartphones and Laptops