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

Michael Schwarz
Graz University of Technology

TU Graz

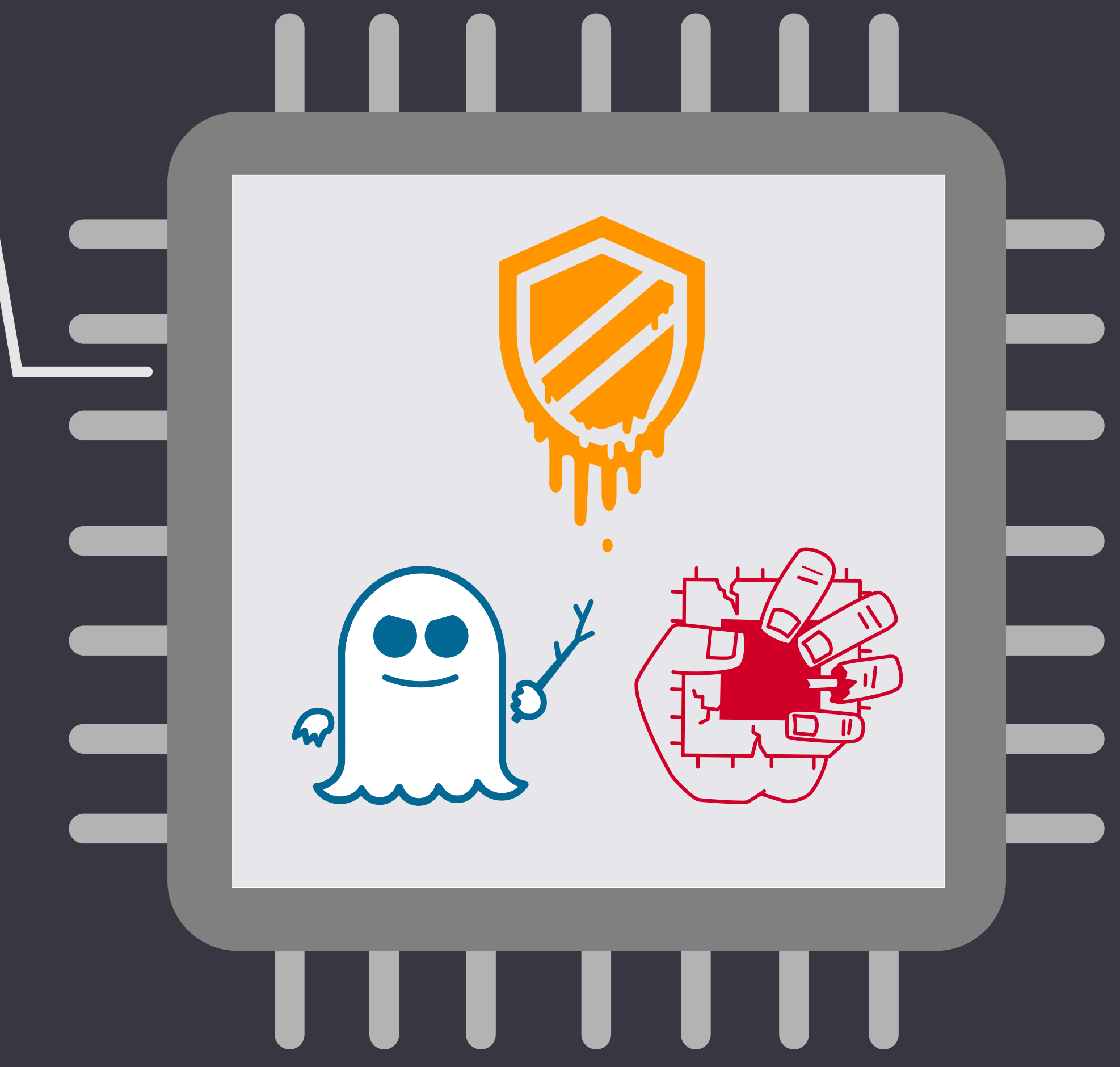
Side Channels

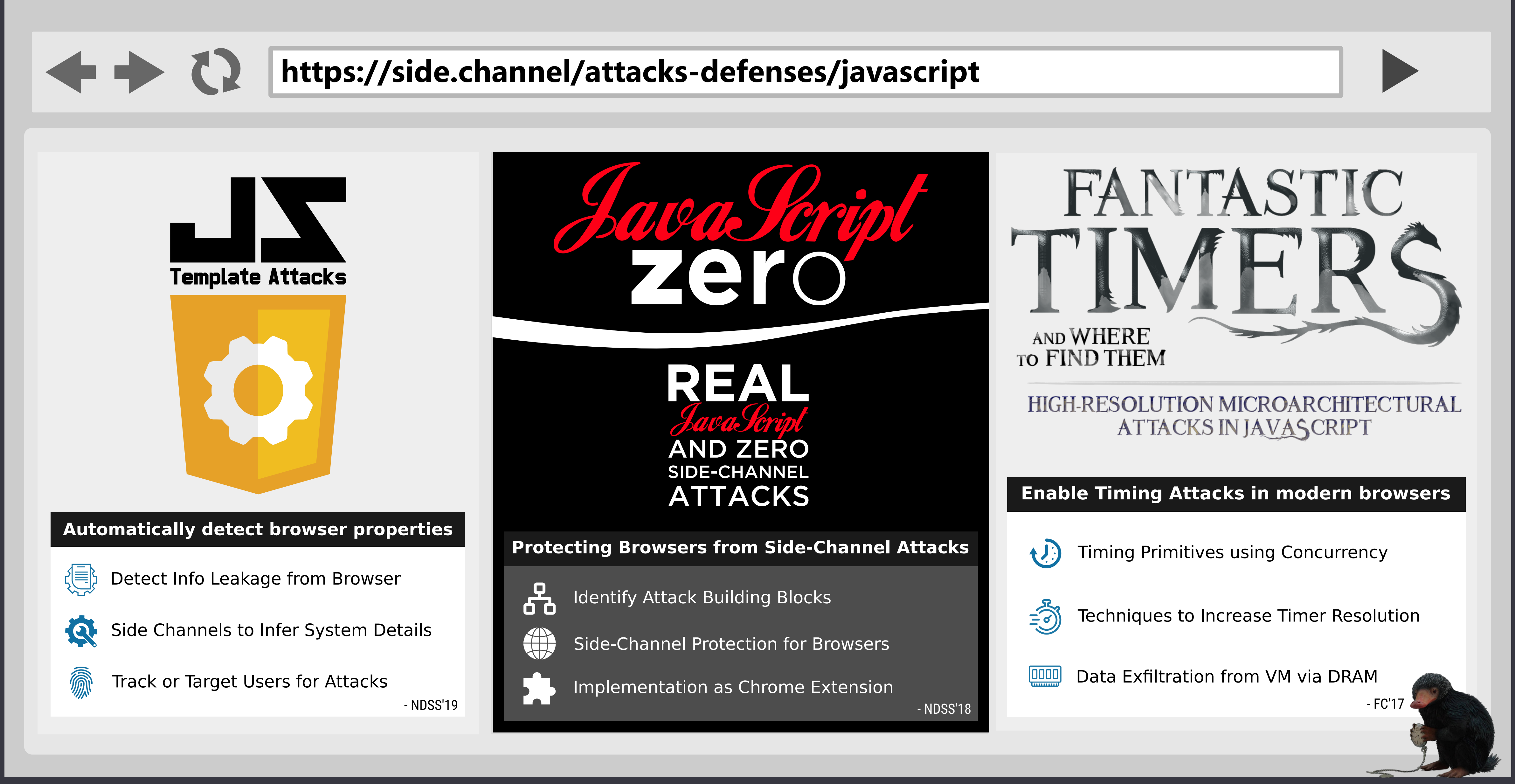
Unintentional Information Leakage due to Hardware Side Effects

- 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





JS Template Attacks

Automatically detect browser properties

- Detect Info Leakage from Browser
- Side Channels to Infer System Details
- Track or Target Users for Attacks

- NDSS'19

JavaScript zero

REAL JavaScript AND ZERO SIDE-CHANNEL ATTACKS

Protecting Browsers from Side-Channel Attacks

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

- NDSS'18

FANTASTIC TIMERS AND WHERE TO FIND THEM

HIGH-RESOLUTION MICROARCHITECTURAL ATTACKS IN JAVASCRIPT

Enable Timing Attacks in modern browsers

- Timing Primitives using Concurrency
- Techniques to Increase Timer Resolution
- Data Exfiltration from VM via DRAM

- FC'17

Restricted Environments

- TEEs
- Browser
- VMs
- Missing Features
- Filtered Instructions

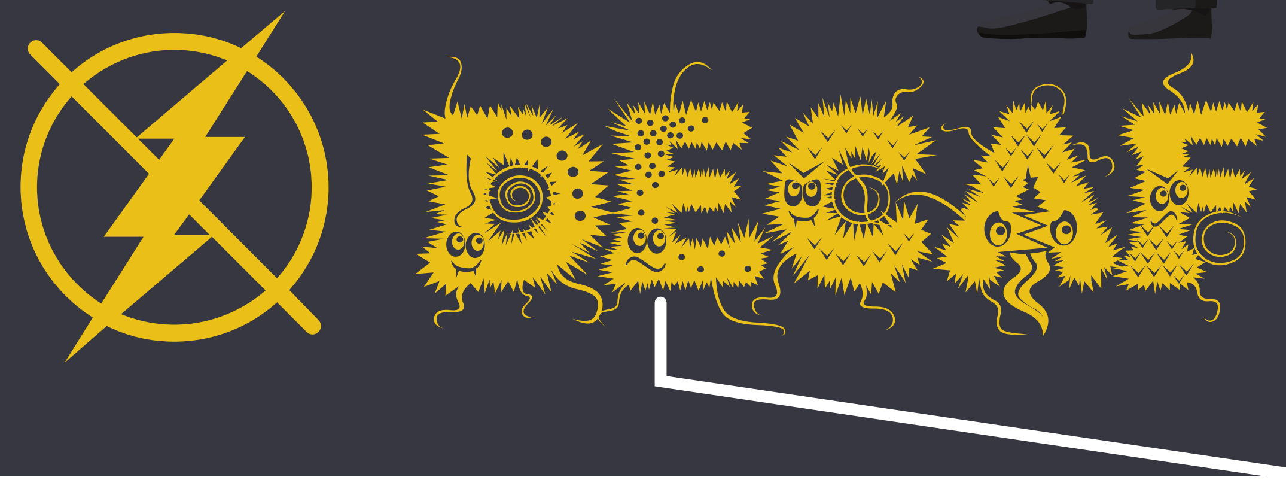
Facts & Numbers

11 Authored papers, 7 accepted	**14** Co-authored papers, 11 accepted
29 Presentations, 1 Keynote	**7** Awards, 2 Best Paper
11 CVEs and Bug Bounties	**10** Advised Students, 1 Master Thesis

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

- DIMVA'17

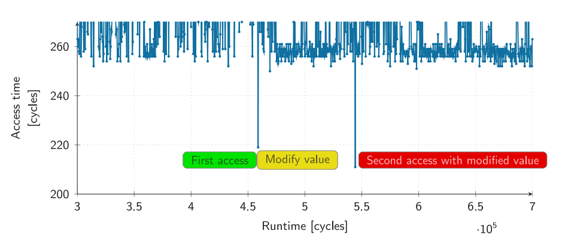


Conclusion

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

Automatically Detect, Exploit, and Mitigate Double-Fetch Bugs

- Cache Attack plus Fuzzing
- Find and Exploit Bugs in TEEs
- Generic Exploitation Prevention



- AsiaCCS'18

Attacks on Key Presses and a Generic Protection

- Two Novel Attacks on Keystroke Timings
- Generic Protection Against Keystroke Attacks
- Implementation for Smartphones and Laptops

- NDSS'18

Michael Schwarz, Clémentine Maurice, Daniel Gruss and Stefan Mangard.
Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript.
Financial Cryptography and Data Security 2017 (FC'17)

Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, Stefan Mangard.
Malware Guard Extension: Using SGX to Conceal Cache Attacks.
Detection of Intrusions and Malware, and Vulnerability Assessment 2017 (DIMVA'17)

Michael Schwarz, Moritz Lipp, Daniel Gruss, Samuel Weiser, Clémentine Maurice, Raphael Spreitzer, Stefan Mangard.
KeyDrown: Eliminating Software-Based Keystroke Timing Side-Channel Attacks.
Network and Distributed System Security Symposium 2018 (NDSS'18)

Michael Schwarz, Daniel Gruss, Moritz Lipp, Clémentine Maurice, Thomas Schuster, Anders Fogh, Stefan Mangard
Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features
ACM ASIA Conference on Information, Computer and Communications Security 2018 (AsiaCCS'18)

Michael Schwarz, Moritz Lipp, Daniel Gruss.
JavaScript Zero: Real JavaScript and Zero Side-Channel Attacks.
Network and Distributed System Security Symposium 2018 (NDSS'18)

Michael Schwarz, Florian Lackner, Daniel Gruss.
JavaScript Template Attacks: Automatically Inferring Host Information for Targeted Exploits.
Network and Distributed System Security Symposium 2019 (NDSS'19)