



Open Source Secure Enclaves Workshop
**Cross-Architecture Side
Channel Attack
Mitigation**

An Academic and Industry Collaboration
Proposal

Paul Gleichauf, ARM Research
paul.gleichauf@arm.com

The past year the bane of securing hardware: SCAs

Plethora of new attacks

- Major speculative execution exploits in the past few months
 - Spectre
 - Meltdown
 - Foreshadow series
- Demonstration of cross-industry cooperation to investigate, mitigate, and deploy patches and workarounds
- Consequences
 - Software patches upon patches
 - Customers faced with dilemma of choosing security or performance
 - Costly and delayed hardware redesigns

Proposal: An academic-industrial consortium

Create and pool architectural-level SCA mitigations

Search for cross-architectural solutions to avoid and inhibit large classes of SCAs

A lift-all-boats approach

- Cast a wide membership net
- Patent and funding pooling to fend off patent litigation for new inventions resulting from the work
- Model on historical precedents (UEFI?, others)
- Open source all work after a fixed period (circa 2 years?)

arm

The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks

Thank You!
Danke!
Merci!
谢谢!
ありがとう!
Gracias!
Kiitos!
감사합니다
धन्यवाद

arm