HotChips Security Tutorial

Ruby B. Lee, Vikas Chandra, Leendert vanDoorn and David Durham

HotChips, August 10, 2014
Cupertino, California
Motivation for Hotchips Security Tutorial

• Cyber Security is becoming increasingly important, as our daily lives, financial competitiveness and national security all depend on cyberspace interactions.

• Software-only security solutions often insufficient to stem attacks, or they degrade performance.

• Hardware support for security has not been sufficiently utilized – HW may be able to improve security significantly, without degrading performance.

• Hardware chip vendors are putting increasing emphasis on security features, which we survey in this tutorial.
Goals of Tutorial

- Give an introduction to:
  - Basic security concepts
  - Secure system design techniques
  - Threats tackled by industry and the defenses used
    - ARM
    - AMD
    - INTEL
  - University research in hardware security
  - Pointers to further reading.
Invited Speakers

• Ruby B. Lee, Forrest G. Hamrick Professor, Princeton University
• Vikas Chandra, Principal Engineer R&D, ARM, and Rob Aitken, Fellow, ARM
• Leendert vanDoorn, Corporate Fellow, AMD
• David Durham, Senior Principal Engineer, Intel
Agenda

9:00 - 9:05 AM: Welcome and Introduction
9:50 – 10:35 AM: Mobile Hardware Security (Vikas Chandra, ARM)
10:35 - 11:20 AM: Secure Systems Design (Leendert vanDoorn, AMD)
11:20 - 11:35 AM: Break
11:35 - 12:20 PM: Mitigating Exploits, Rootkits and Advanced Persistent Threats (David Durham, Intel)
12:20 - 12:50PM: University Research in Hardware Security (Ruby Lee)
12:50 - 1:00 PM: Q&A Wrap Up (All)

If you have more questions, you may also try to sit with the presenters at lunch after the tutorial.