Roots of Trust in Mobile Devices

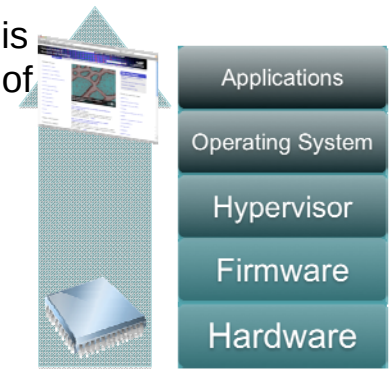
ISPAB
February 2012

Andrew Regenscheid
Computer Security Division
Cryptographic Technology Group

NIST National Institute of Standards and Technology

Roots of Trust

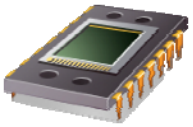
- Every computer system is built with multiple levels of abstraction.
- Generally, higher layers must trust lower layers
- Initial source(s) of trust - the ***roots of trust***



NIST National Institute of Standards and Technology

Roots of Trust in Devices

- Roots of trust are hardware/software components that are inherently trusted.
  - They must be secure by design.
  - Should be small and protected.
  - Ideally implemented in hardware, or protected by hardware.
- They are trusted to perform one or more security-critical functions, e.g.,
  - Measure and/or verify software
  - Protect cryptographic keys
  - Perform device authentication



NIST National Institute of Standards and Technology

Boot Firmware as a RoT

- As the first code that executes at power-on, boot firmware ***is*** a root of trust in modern computers.
- Boot firmware a potential DoS target, and could inject very low-level malware under the OS.
- If secure, a system can bootstrap trust from this firmware, verifying code before execution.
- NIST guidelines on BIOS security in PCs
  - SP800-147, *BIOS Protection Guidelines*
  - SP800-155, *BIOS Integrity Measurement Guidelines*
- Strong adoption of BIOS protections by PC industry.

NIST National Institute of Standards and Technology

RoT in Mobile Devices

- Working to identify properties and capabilities of roots of trust needed to secure next-gen mobile devices.
- Work expected to include:
  - Boot firmware protections
  - Secure measurement of firmware
  - Secure storage
  - Device authentication
  - Application and data isolation

NIST National Institute of Standards and Technology

Challenges in Mobile Space

- Greater risk of physical attacks, motivating use of hardware protections.
- Multiple semi-independent processors and interfaces
  - General CPU, baseband radio, NFC
  - 3G/4G/WiFi/Bluetooth interfaces
- Power and space-constraints
  - SoC-based designs
  - Shared flash memory

NIST National Institute of Standards and Technology

Assurance of Security Mechanisms

- Security mechanisms on mobile devices can be rooted in hardware and/or protected firmware.
- Mobile OSes provide or manage many security mechanisms:
  - Software verification
  - Application and data isolation
  - Data protection
- Roots of trust in hardware/firmware can provide greater assurance that these mechanisms are functioning properly.

NIST National Institute of Standards and Technology

Bring-Your-Own-Device

- Organizations need assurance that devices comply with their security practices.
- Current practice is to configure devices and distribute them to users.
- Strong roots of trust can transform the industry.
  - Shift emphasis from ***configuring*** compliance to ***measuring*** compliance.
  - Allow employee-owned devices that comply with organization-defined policies.

NIST National Institute of Standards and Technology

Questions

Contact Information

Andrew Regenscheid

andrew.regenscheid@nist.gov

NIST
National Institute of Standards and Technology