Towards a secure mobile system

Haohui Mai, Shuo Tang, Sam King
University of Illinois
Increasing usage of smart phones
And increasing security concerns
Backing up security guarantees for a full-blown mobile system with mathematical proofs?

Theorem 1: System X is secure.

... 

Q.E.D.
Overview

• Quick look of today’s mobile system
• Our approach
• Current status
The Android architecture
Lessons learned

• Mobile system are monolithic, complex system
  – 1~2 MLOC for Linux kernel
  – ~12 MLOC for Android framework

• Wide attack surfaces

• Trust them all
  – An exploit in one component can compromise the whole system
Why proving is difficult?

• Scalability
  – Difficult for current formal verification to scale
• Ad-hoc security invariants
  – Difficult to collect sufficient information for proofs

Theorem 1: System X is secure.
Proof: We trust our system.
Q.E.D.
IBOS [OSDI’10]

- Align security invariants with hardware protection
- Enforce security invariants in one place
- Reduce the size of TCB by more than 100x
Towards a verified kernel
Design Principles

• High level abstraction, close to application

• Minimize the trust
  – Verification is done at the level of LLVM IR => Compiler frontend is not trusted

• Hit different nails with right hammers
  – Memory safety: Safe language
  – Functional invariants: Hoare-logic style proofs
  – Even higher level invariants: Model checking
Current status

• Work in progress
• A minimal ARM kernel working on a real phone
  – Without proofs
• Second iteration of design and implementation
DISCUSSION