Nov. 7, 2011

Secure App Execution On Commercial Mobile Devices By Means Of Bare Metal Hypervisors

KATRIN HOEPER, KEVIN GUDETH, RON BUSKEY (*MOTOROLA SOLUTIONS)*

MATTHEW PIRRETTI

Outline

Motivation

Why COTS?

Security Challenges

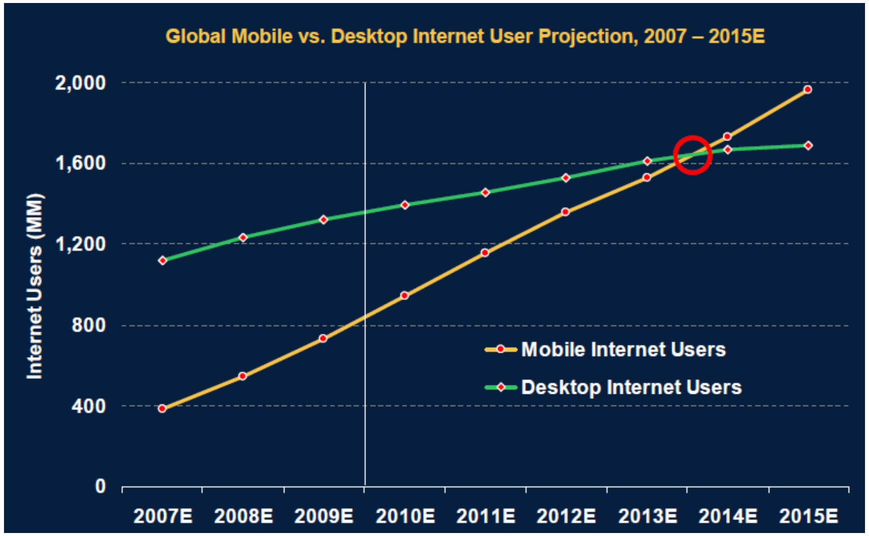
Recommended Solution

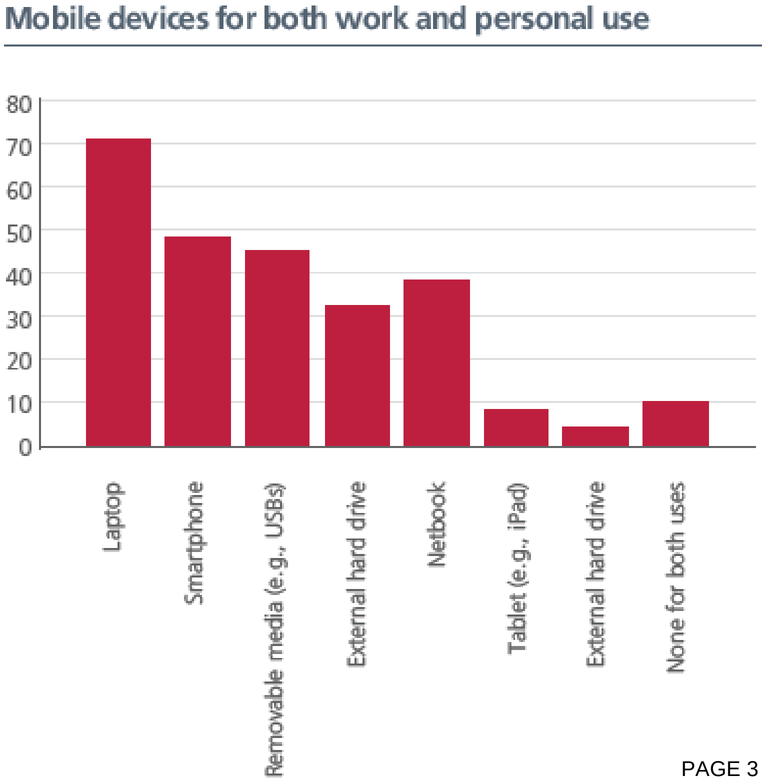
Conclusions

Motivation

Mobile devices become dominant computing platform

- estimated 10B+ mobile units vs 1B+ desktop units
- # sensitive apps on personal mobile devices growing



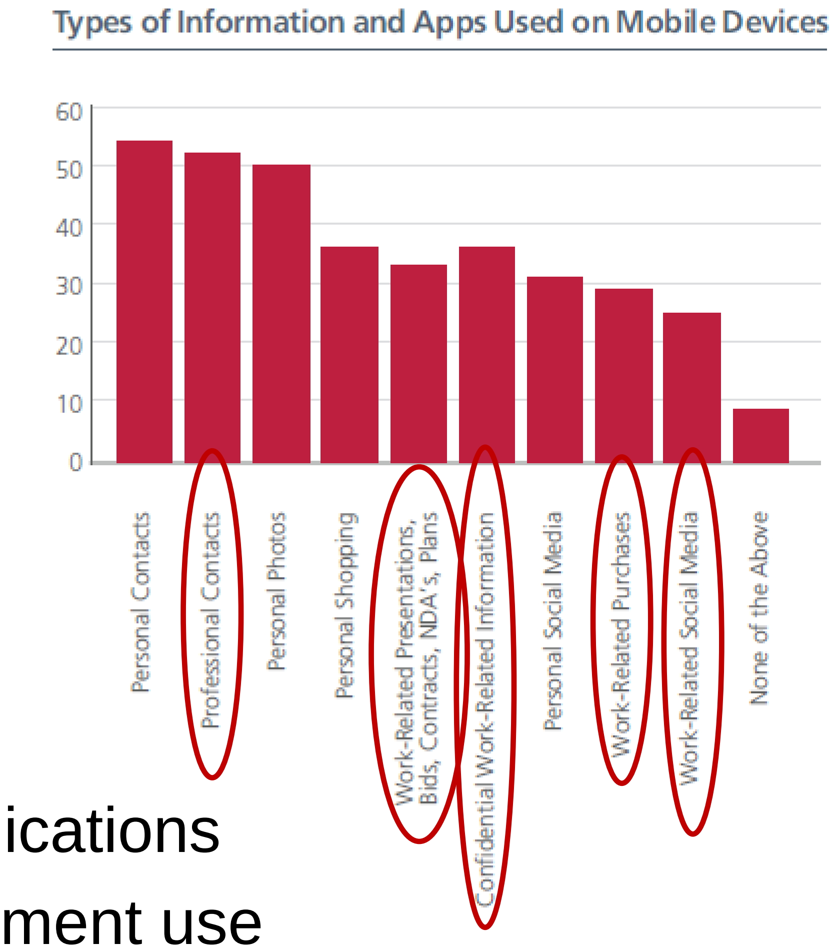


1. Morgan Stanley Research "Internet Trends", April 2010
2. CyLab & McAfee, "Mobility and Security", May 2011

Security Sensitive Apps

Already prominent

- corporate email
- other corporate applications



Types of Information and Apps Used on Mobile Devices

Emerging

- electronic wallets
- mobile eHealthCare
- broad band public safety applications
- less conspicuous law enforcement use

1. CyLab & McAfee, "Mobility and Security", May 2011

Why COTS?

Benefits of Commercial-Off-The-Shelf (COTS) Devices

- cost reduction
- shorter time to market
- reduced number of carried devices
- maintained user experience
- inconspicuous form factor

Past Solutions

Meet security requirements of sensitive applications by running the apps on a special-purpose device

- custom hardware design
- locked down capability
- limited or no general connections allowed
- hardened operating system

Security Challenges

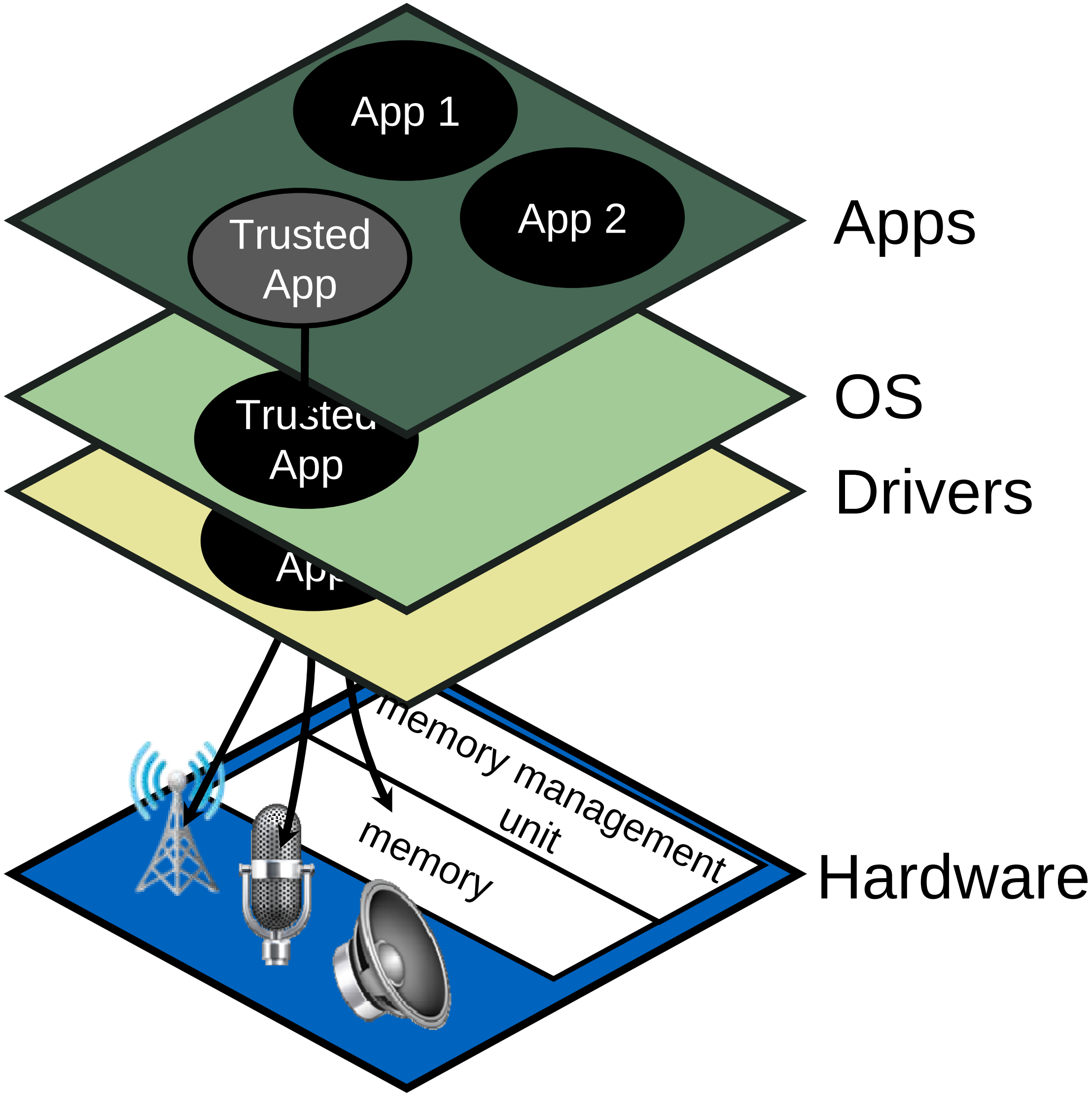
Establish trust within commercial products

Verify execution of sensitive applications/processes

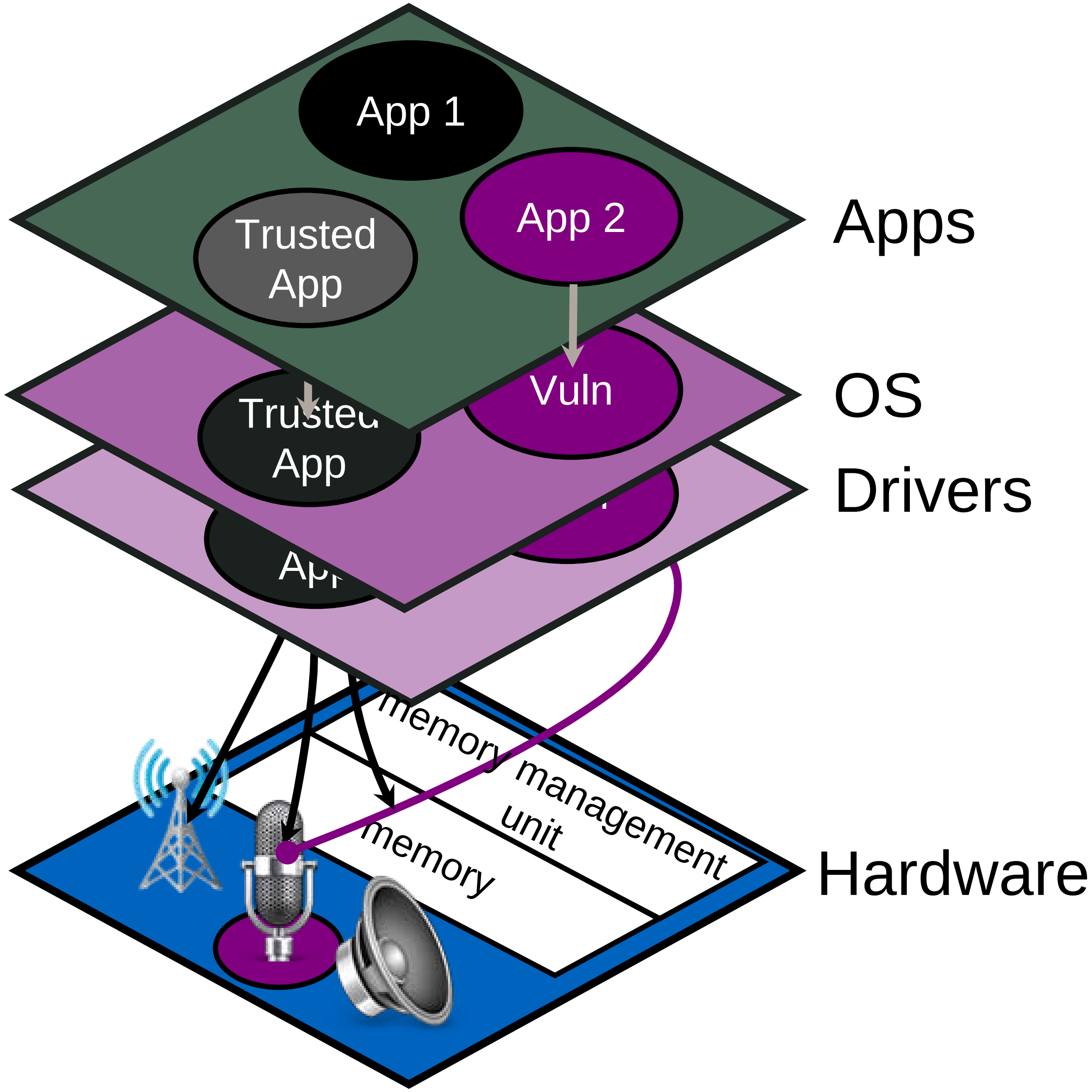
Expect attack vectors through

- compromise of the OS
- presence of malicious or exploitable applications
- compromise of software-based crypto

Security Exploit



Security Exploit



Design Principles

Minimize trusted computing base (TBC)

Isolate trusted applications

Reuse trusted software

Be OS-agnostic

Don’t rely on technical competency of users

Minimize performance degradation

Keep changes to COTS devices to a minimum

Enable portability to new hardware

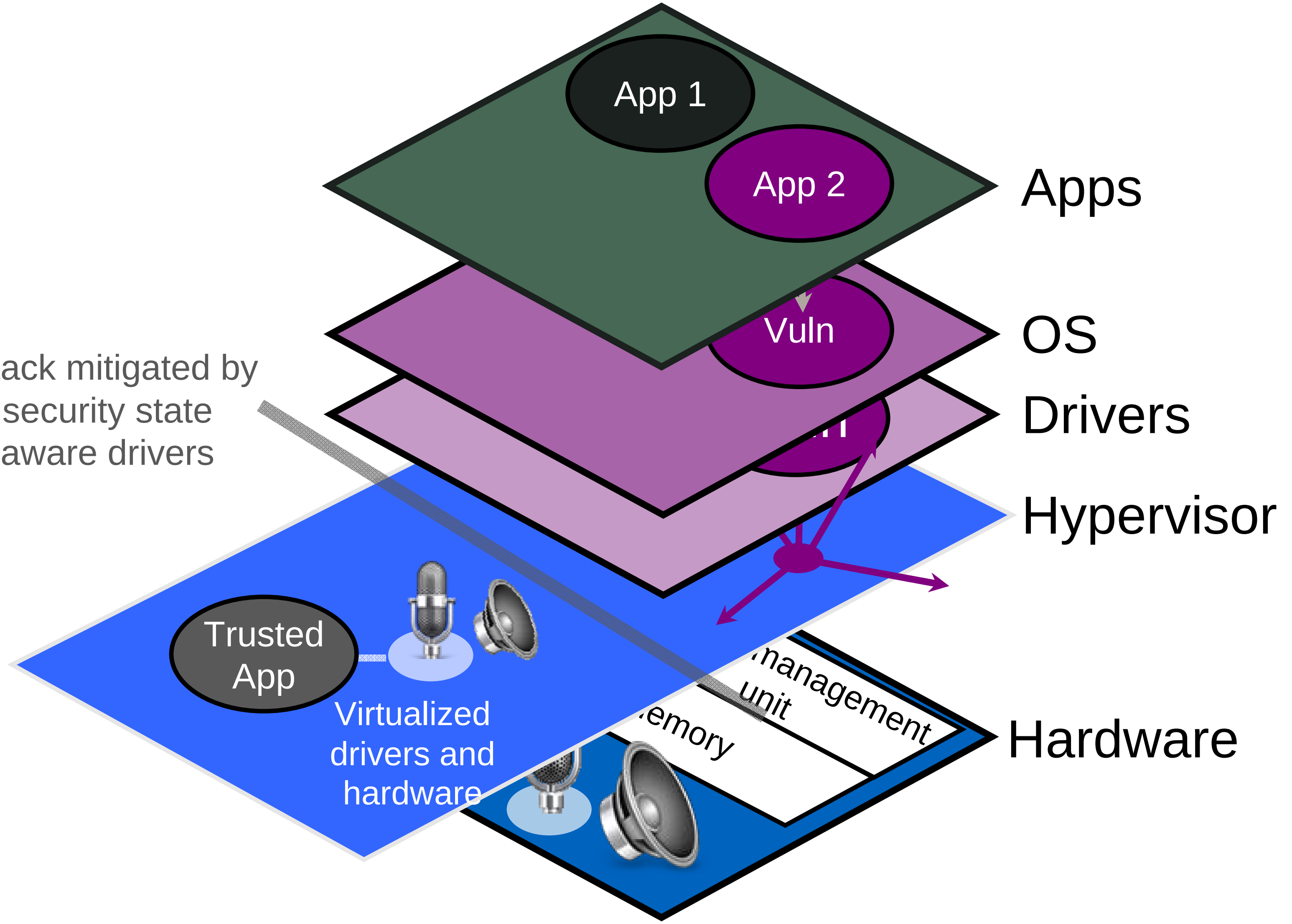
Uniformly enforce system policy

Our Recommended Solution

Bare metal hypervisor

- runs directly on the processor
- all guest OSs run in their own virtual machine
- shared security-critical device drivers run in individual VMs and are security state aware
- (optionally) individual trusted applications may run in their own virtual machine

Exploit Mitigation



Attack mitigated by security state aware drivers

Virtualized drivers and hardware

Example Use Cases

Perform cryptographic operations in common, trusted, and formally verified partition or in external trusted hardware accessed through virtualized driver

Provide a policy enforcement engine that is isolated from each guest OS

Isolate trusted from untrusted apps

Provide multiple OS environments

Conclusions

In our recommended solution, bare metal hypervisors

- enable the satisfaction of all design principles
- provide a tool for meeting security and privacy standards and implementation guidelines
- remove significant costs associated with special purpose hardware
- build on the features of COTS devices rather than restrict their use

Thank you!

Katrin.Hoeper@motorolasolutions.com

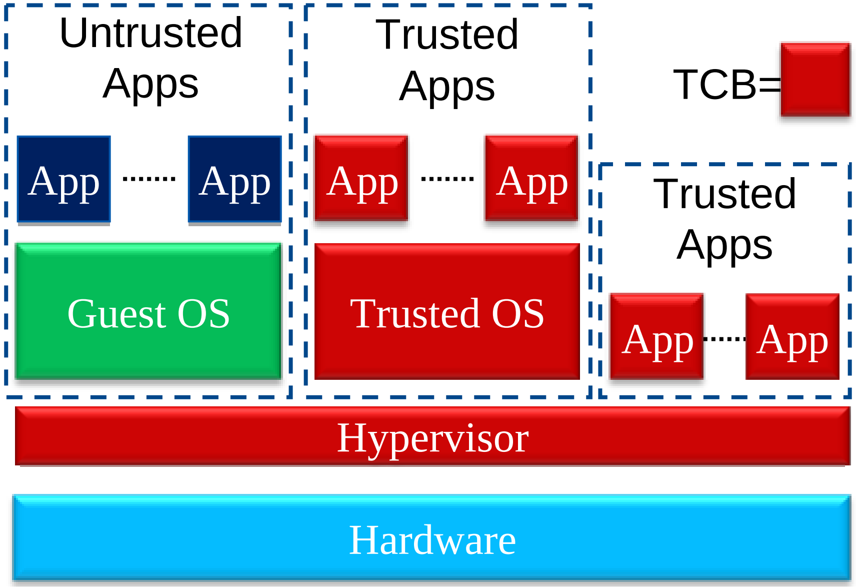
Kevin.Gudeth@motorolasolutions.com

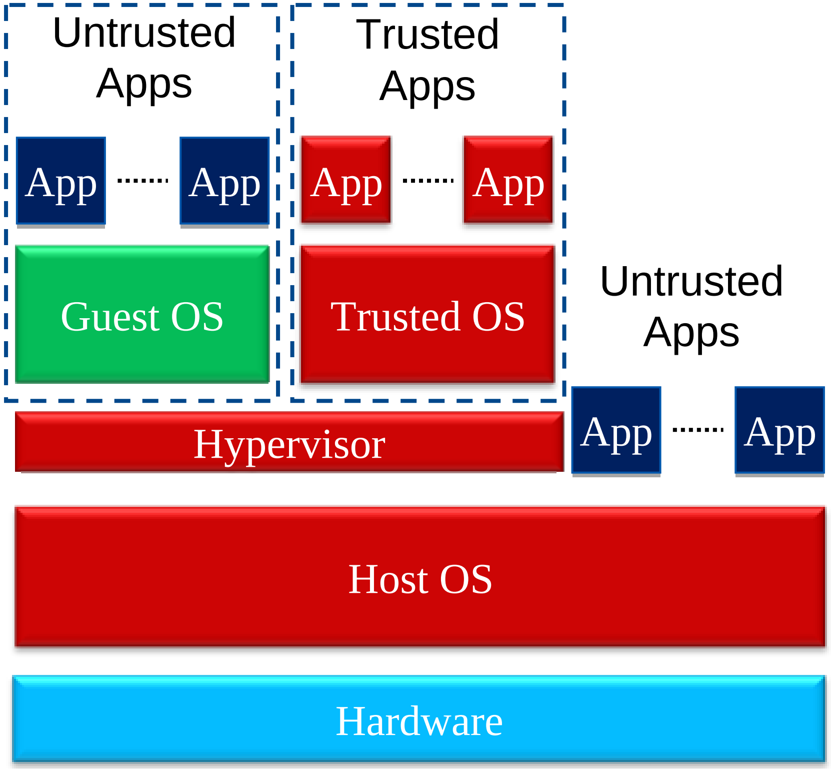
Ron.Buskey@motorolasolutions.com

Matthew Pirretti

Back Up Slides

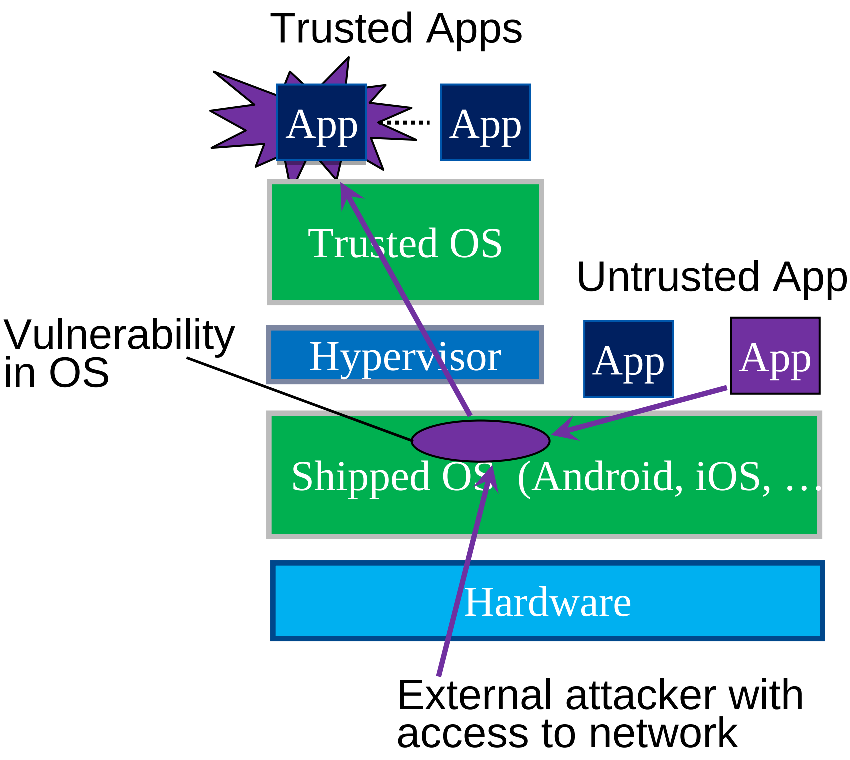
Baremetal vs Hosted Hypervisor





Position Paper: Delivering Secure Applications on Commercial Mobile Devices: The Case for Bare Metal Hypervisors, K. Gudeth, M. Pirretti. K. Hoeper and R. Buskey, 2011 ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices.

Attack Scenarios



Trusted Apps

App

App

Trusted OS

Untrusted Apps

Vulnerability in OS

Hypervisor

App

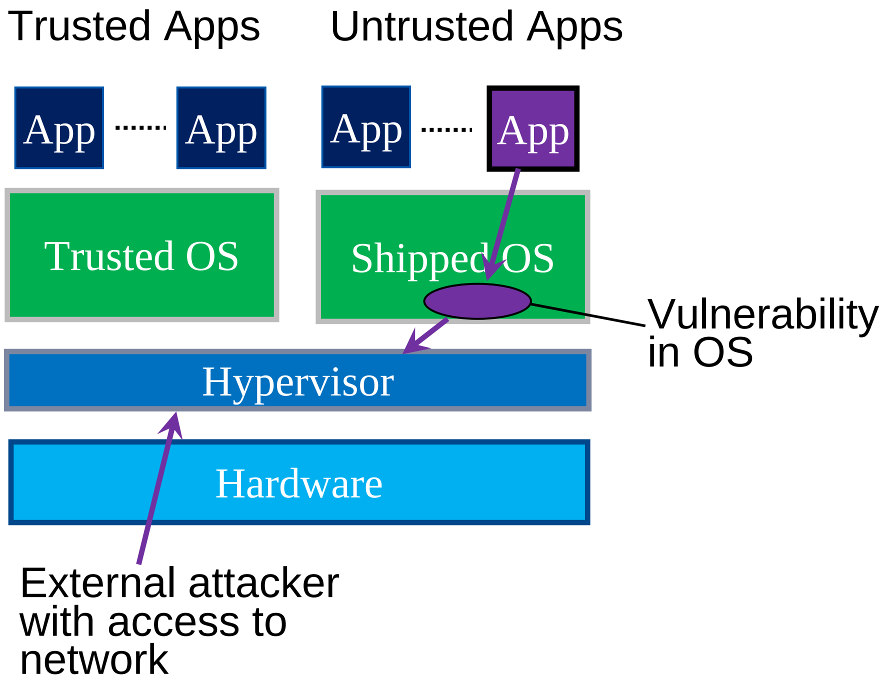
App

Shipped OS (Android, iOS, …

Hardware

External attacker with access to network

Hosted Hypervisor



Trusted Apps

Untrusted Apps

App

App

App

App

Trusted OS

Shipped OS

Vulnerability in OS

Hypervisor

Hardware

External attacker with access to network

Baremetal Hypervisor

Position Paper: Delivering Secure Applications on Commercial Mobile Devices: The Case for Bare Metal Hypervisors, K. Gudeth, M. Pirretti. K. Hoeper and R. Buskey, 2011 ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices.