

Mobile Device Security through Virtualization

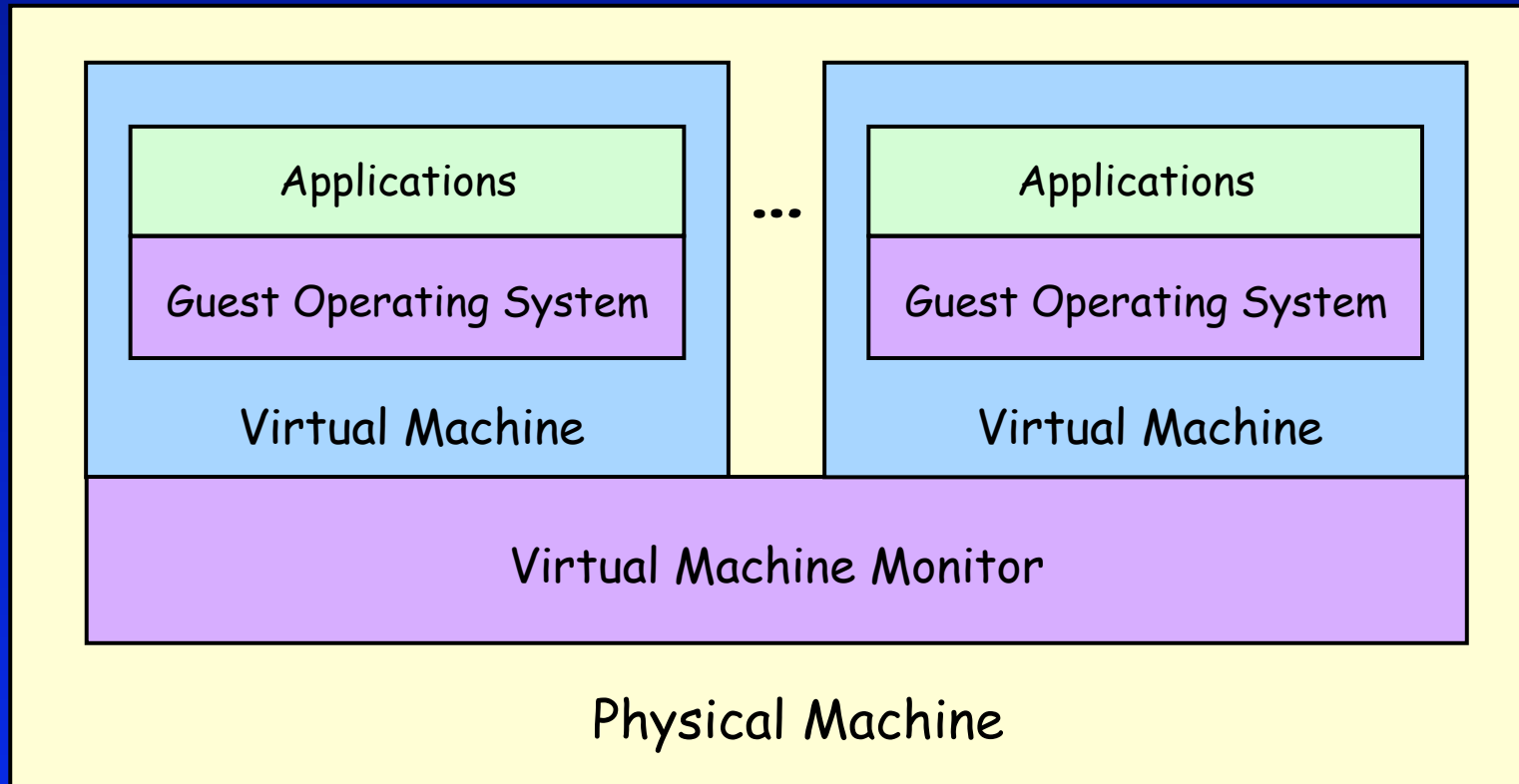
Ramón Cáceres
AT&T Labs

NSF Wireless Networking Workshop
10 April 2008

Motivation

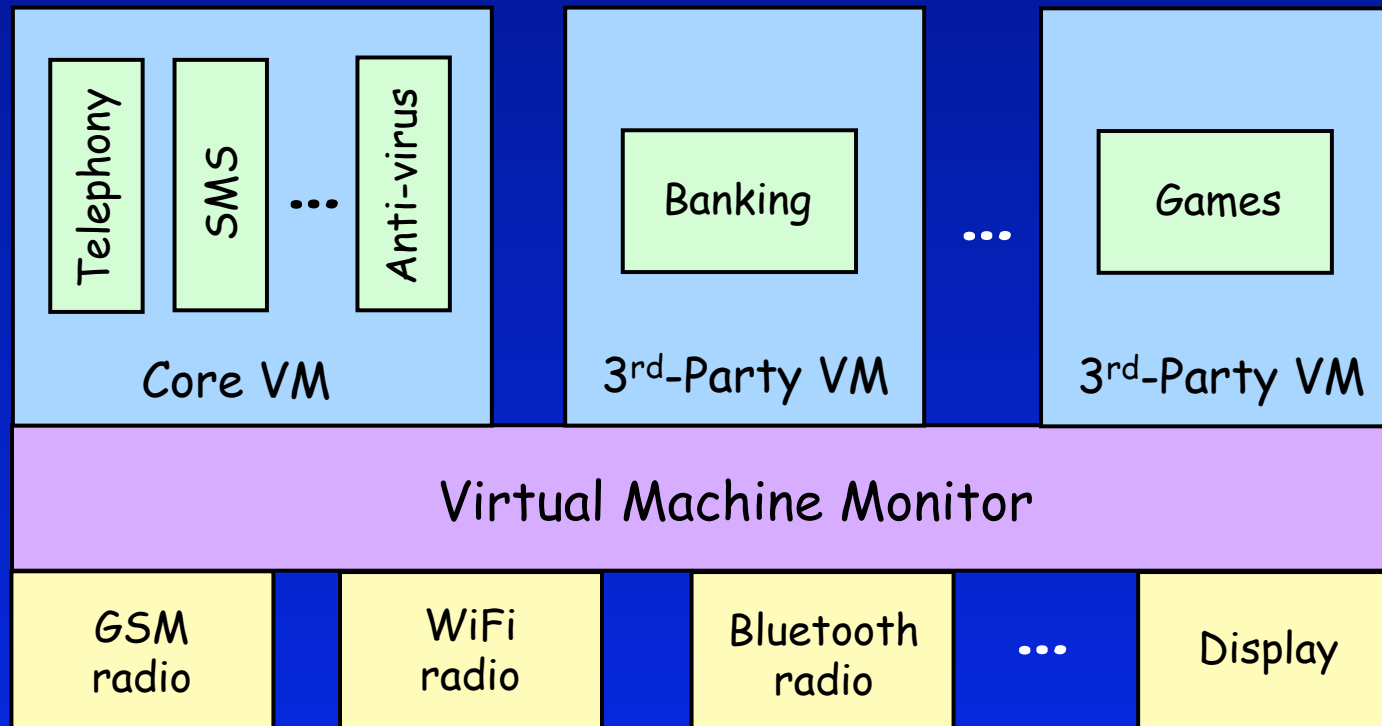
- Mobile phones poised to become the dominant personal computing platform
- Unprecedented adoption level and rate
- Rapidly acquiring the capabilities of PCs
...but also their **security vulnerabilities**
- Made worse by several factors
 - Promiscuous in design and use
 - Often tied to billable account
- Mobile phone malware already seen

Virtualization can help



- Isolation and mediation
- Encapsulation, migration, ...

Some use cases



- Core apps and services in one VM
- 3rd-party apps and services in isolated VMs
- Mediated access to all physical resources

Research issues 1

- Virtualization level
 - System level (i.e., complete OS plus apps)?
 - Application level (i.e., API to single app)?
 - Language level (e.g., Java VM)?
 - Tradeoffs in security, portability, performance, ...

Research issues 2

- Resource limitations
 - Display
 - Battery
 - ...
- Usability
 - How to expose isolation to user?
 - Can user trust the I/O path?
 - Small display is a challenge

Research issues 3

- Sharing vs. isolation
 - How to allow controlled sharing (e.g., cut and paste between VMs)?
 - Not specific to mobile case
- Enhancing natural security
 - Integrity attestation?
 - Mandatory access control?
 - Secure hardware (e.g., MTM)?
 - Not specific to mobile case

MobiVirt: Workshop on Virtualization in Mobile Computing

Held in conjunction with MobiSys 2008
Breckenridge, CO, USA
June 17, 2008

Abstracts due April 14
5-page papers due April 21

<http://mobivirt08.cs.duke.edu>