11/18

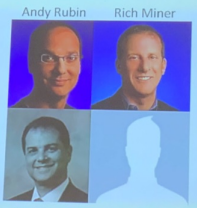
- Jeremy Andrus, Christoffer Dall, Alexander Van.t Hof, Oren Laadan, and Jason Nieh, Cells: A Virtual Mobile Smartphone Architecture, *SOSP'11, October 2011*.
- W. Enck, P. Gilbert, B.G. Chun, L. P. Cox, J. Jung, P. McDaniel, A. N. Sheth, TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones , *OSDI'10, October 2010*

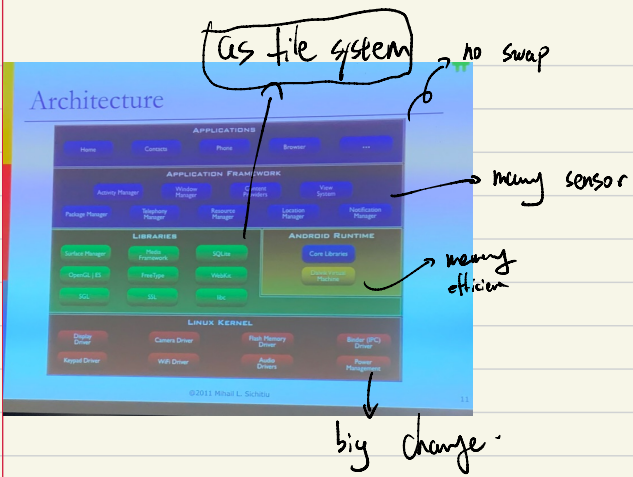
OHA (Open Handset Alliance)

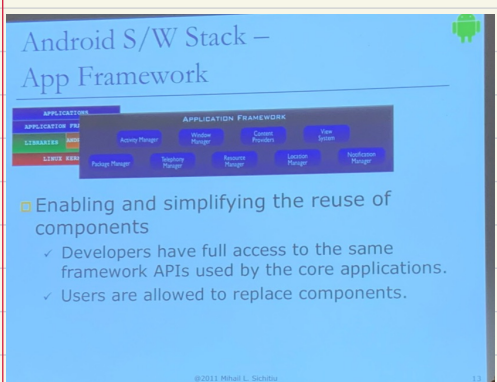
- A business alliance consisting of 47 companies to develop open standards for mobile devices

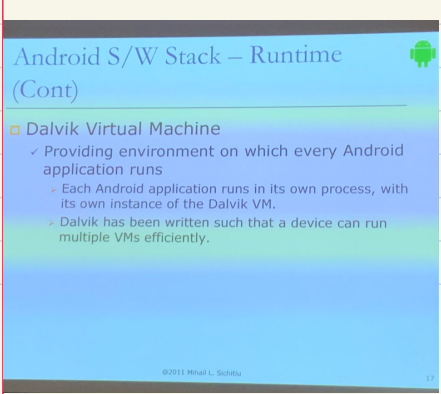
Background

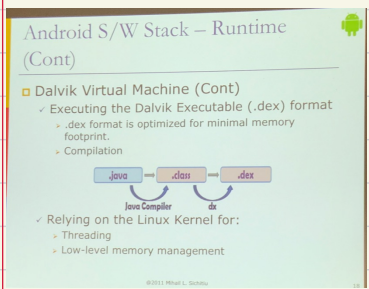
- Android Inc. was founded in Palo Alto, California in October, 2003 by Andy Rubin, Rich Miner, Nick Sears, and Chris White.
- Their goal was to develop a "smarter mobile device that was more aware of its owner's location and preferences."

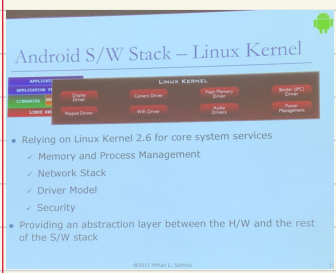



as file system
no swap
Architecture
Applications
Home
Contacts
Phone
Browser
...
Application Framework
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
Libraries
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
libc
Android Runtime
Core Libraries
Dalvik Virtual Machine
Linux Kernel
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
Wifi Driver
Audio Drivers
Power Management
©2011 Mihail L. Sichitiu
11
many sensor
many efficient
big change.

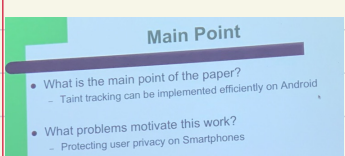

Android S/W Stack – App Framework
Application Framework
Enabling and simplifying the reuse of components
Developers have full access to the same framework APIs used by the core applications.
Users are allowed to replace components.
©2011 Mihail L. Sichitiu
13

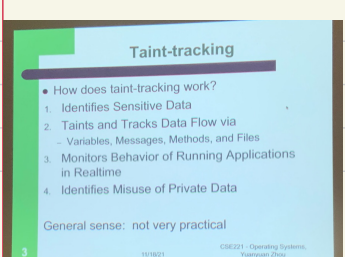

Android S/W Stack – Runtime (Cont)
Dalvik Virtual Machine
Providing environment on which every Android application runs
Each Android application runs in its own process, with its own instance of the Dalvik VM.
Dalvik has been written such that a device can run multiple VMs efficiently.
©2011 Mihail L. Sichitiu
17

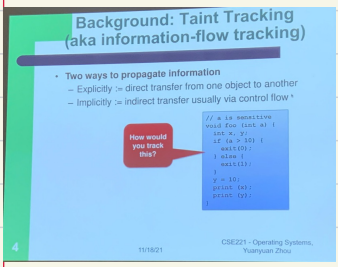

Android S/W Stack – Runtime (Cont)
Dalvik Virtual Machine (Cont)
Executing the Dalvik Executable (.dex) format
.dex format is optimized for minimal memory footprint.
Compilation
.java
.class
.dex
Java Compiler
dx
Relying on the Linux Kernel for:
Threading
Low-level memory management
@2011 Mihail L. Sichitiu

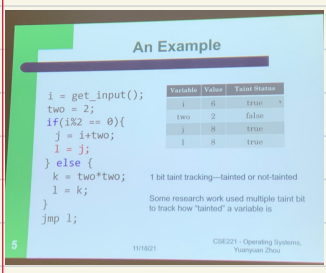

Android S/W Stack – Linux Kernel
LINUX KERNEL
Relying on Linux Kernel 2.6 for core system services
Memory and Process Management
Network Stack
Driver Model
Security
Providing an abstraction layer between the H/W and the rest of the S/W stack
@2011 Mihail L. Sichitiu

Taint track


Main Point
What is the main point of the paper?
Taint tracking can be implemented efficiently on Android
What problems motivate this work?
Protecting user privacy on Smartphones

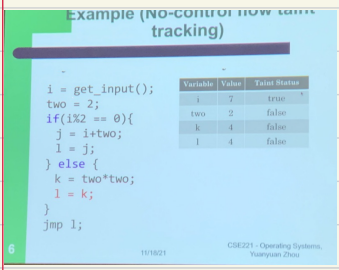

Taint-tracking
How does taint-tracking work?
1. Identifies Sensitive Data
2. Taints and Tracks Data Flow via
Variables, Messages, Methods, and Files
3. Monitors Behavior of Running Applications in Realtime
4. Identifies Misuse of Private Data
General sense: not very practical
3
11/18/21
CSE221 - Operating Systems, Yuanyuan Zhou



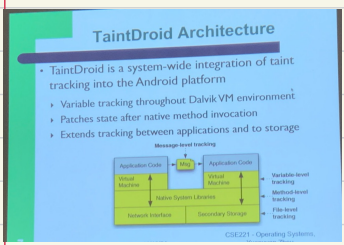


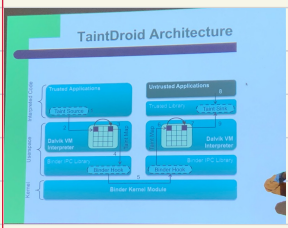
too

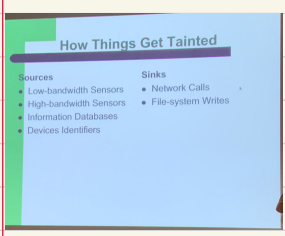
Causions



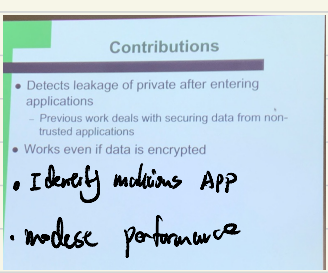
ignore control flow deps





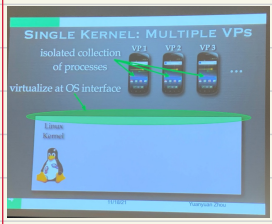


Performance : 3.5% memory
27% overhead.



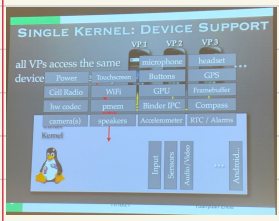
Main Point

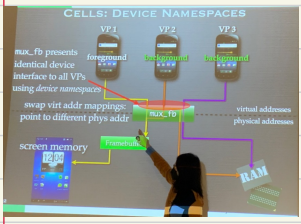
- What is the main point of the paper?
  - Supporting multiple Virtual phones on one physical phone
- What problems motivate this work?
  - Work phone vs Private Phone



Details

- One foreground VP for displaying and multiple background VPs
- Remap OS resource id to virtual ones
  - Now each VP has its own private virtual namespaces
- Foreground VP has direct access to hardware
- If the foreground VP does not acquire exclusive access, the hardware can be shared by background VPs.
  - Kernel-Level Device Virtualization to support transparency and performance by introducing *device namespace*
  - User-Level Device Virtualization to support portability and transparency by proxy





only process isolation