AirBag: Boosting Smartphone Resistance to Malware Infection

Chiachih Wu **Yajin Zhou** Kunal Patel
Zhenkai Liang and Xuxian Jiang

North Carolina State University **National University of Singapore**

Popularity of Smartphones

40 years ago

Source: theatlantic.com

Nowadays

Source: sandiway.blogspot.com

Popularity of Android Phones

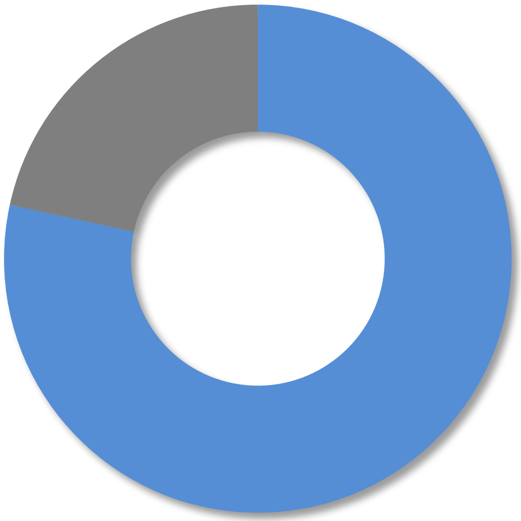
Data Source: http://www.gartner.com

Popularity of Android Phones

iPhone

Windows Phone

BlackBerry



Year 2013

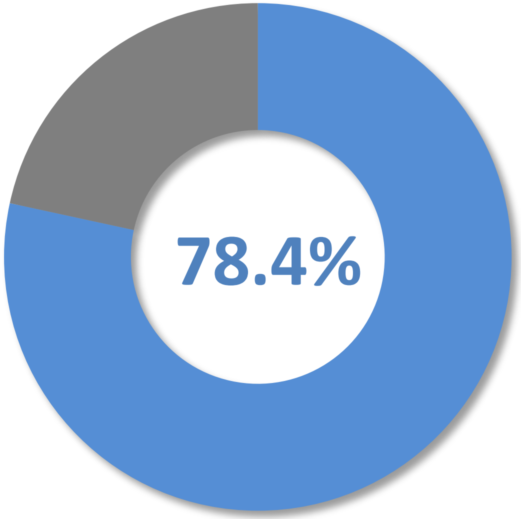
Data Source: http://www.gartner.com

Popularity of Android Phones

iPhone

Windows Phone

BlackBerry



Year 2013

Data Source: http://www.gartner.com

Apps Are Becoming Popular

Apps Are Becoming Popular

Apps Are Becoming Popular

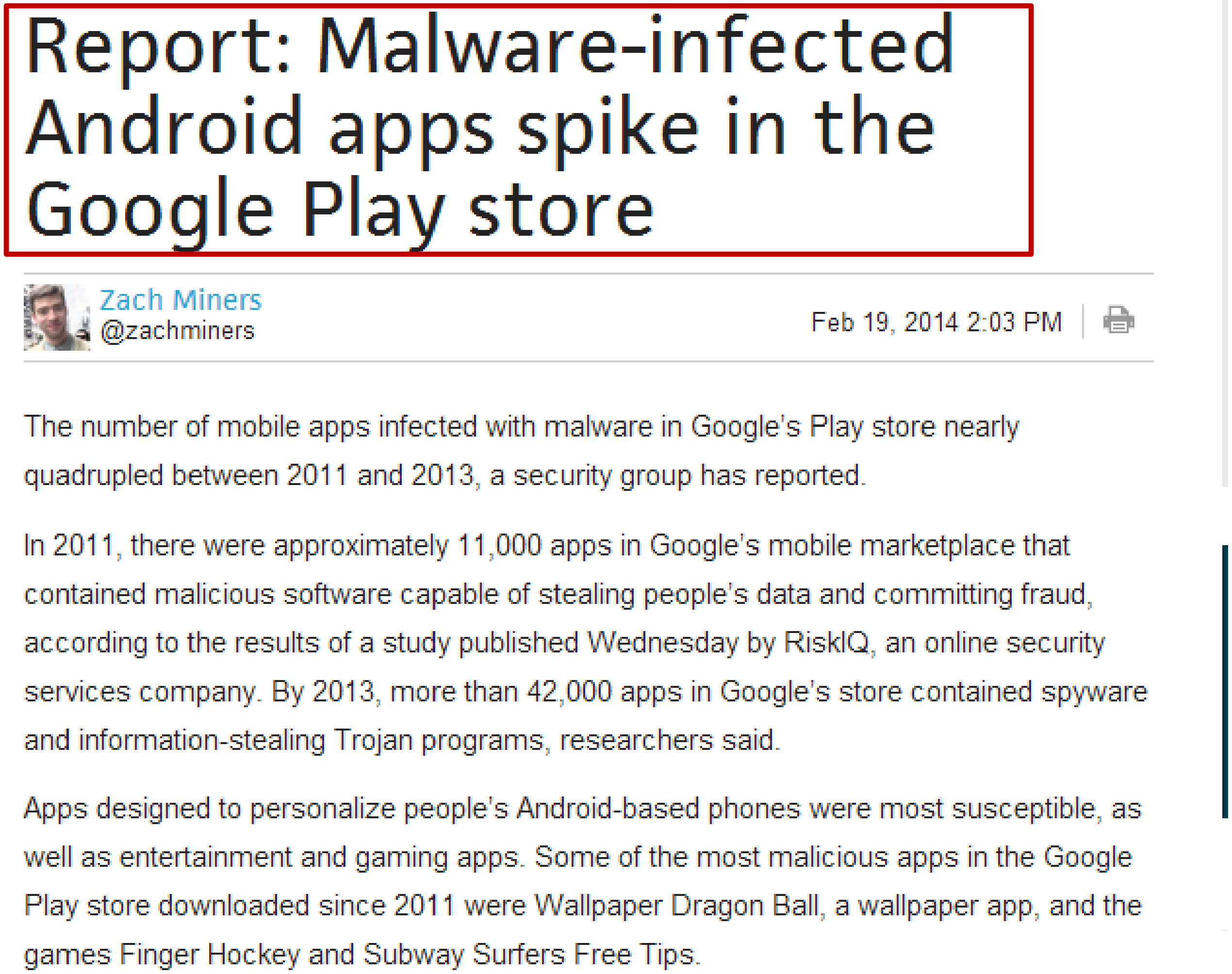
Apps Are Becoming Popular

Apps Are Becoming Popular

Apps Are Becoming Popular

So Are the Malicious Apps

So Are the Malicious Apps



Report: Malware-infected Android apps spike in the Google Play store

Zach Miners
@zachminers

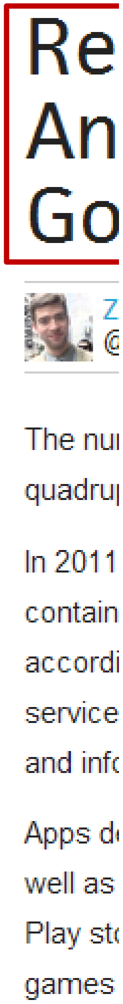
Feb 19, 2014 2:03 PM

The number of mobile apps infected with malware in Google's Play store nearly quadrupled between 2011 and 2013, a security group has reported.

In 2011, there were approximately 11,000 apps in Google's mobile marketplace that contained malicious software capable of stealing people's data and committing fraud, according to the results of a study published Wednesday by RiskIQ, an online security services company. By 2013, more than 42,000 apps in Google's store contained spyware and information-stealing Trojan programs, researchers said.

Apps designed to personalize people's Android-based phones were most susceptible, as well as entertainment and gaming apps. Some of the most malicious apps in the Google Play store downloaded since 2011 were Wallpaper Dragon Ball, a wallpaper app, and the games Finger Hockey and Subway Surfers Free Tips.

So Are the Malicious Apps



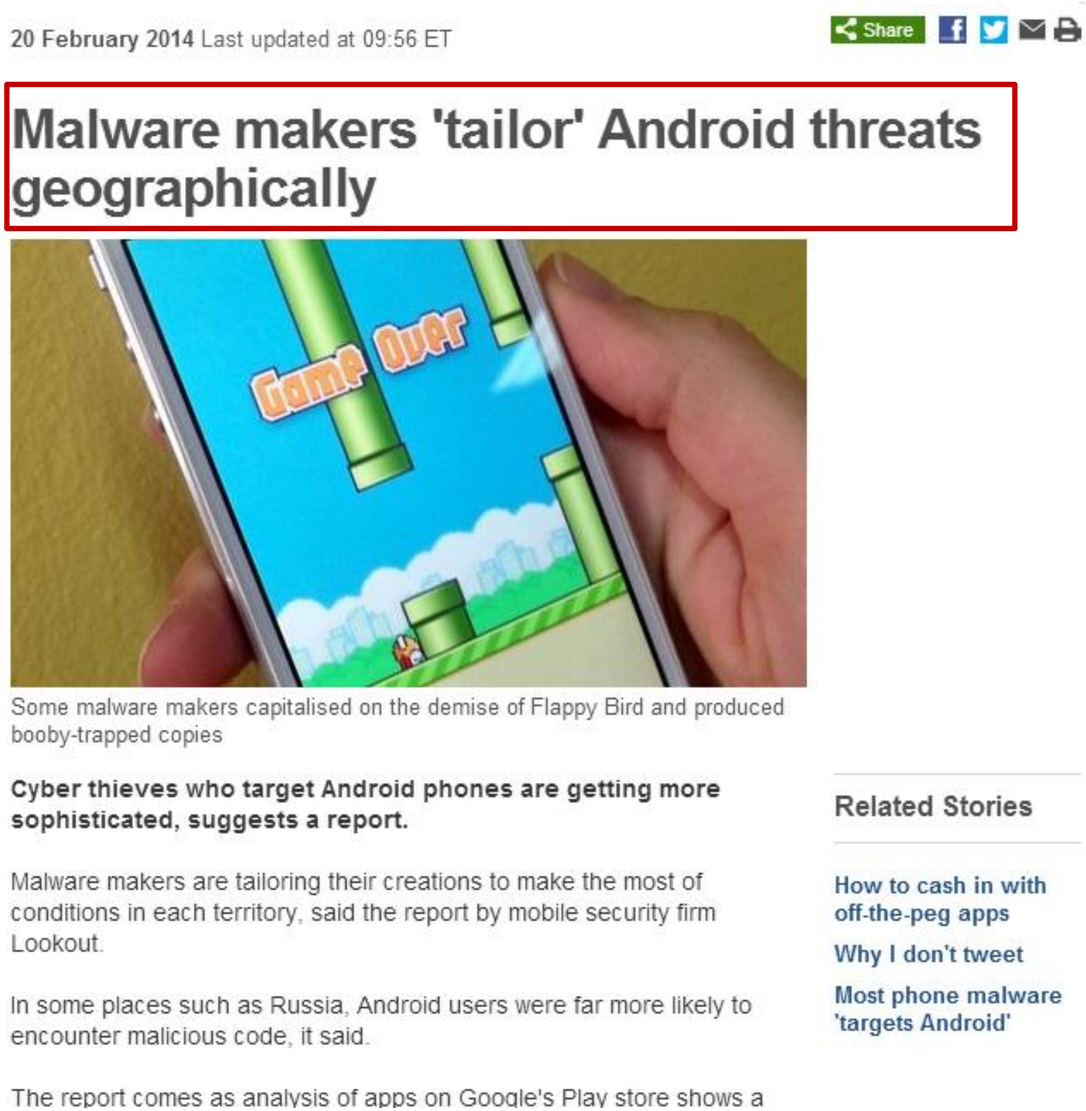
Re
An
Go

Z
@

The nu
quadru

In 2011
contain
accordi
service
and info

Apps d
well as
Play st
games



20 February 2014 Last updated at 09:56 ET

Malware makers 'tailor' Android threats geographically

Some malware makers capitalised on the demise of Flappy Bird and produced booby-trapped copies

Cyber thieves who target Android phones are getting more sophisticated, suggests a report.

Malware makers are tailoring their creations to make the most of conditions in each territory, said the report by mobile security firm Lookout.

In some places such as Russia, Android users were far more likely to encounter malicious code, it said.

The report comes as analysis of apps on Google's Play store shows a

Related Stories

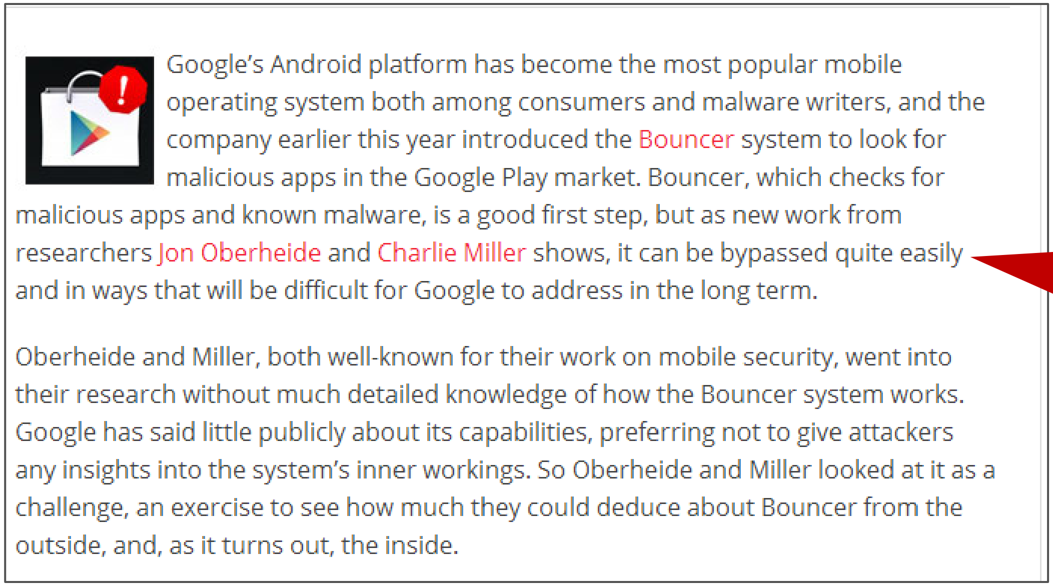
- How to cash in with off-the-peg apps
- Why I don't tweet
- Most phone malware 'targets Android'

Server-side Solutions

- Google Play: Bouncer

Server-side Solutions

- Google Play: Bouncer



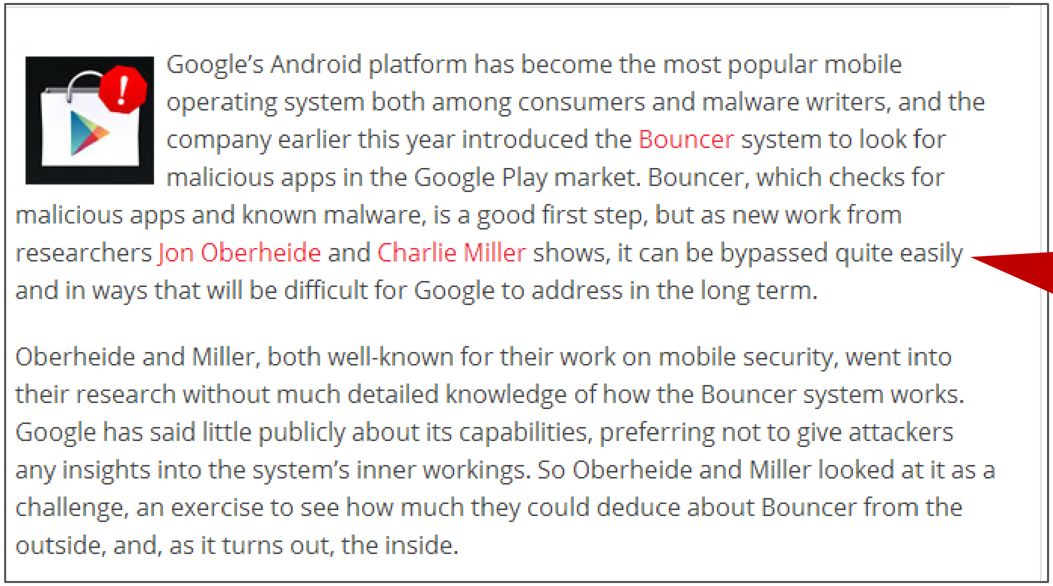
Google's Android platform has become the most popular mobile operating system both among consumers and malware writers, and the company earlier this year introduced the Bouncer system to look for malicious apps in the Google Play market. Bouncer, which checks for malicious apps and known malware, is a good first step, but as new work from researchers Jon Oberheide and Charlie Miller shows, it can be bypassed quite easily and in ways that will be difficult for Google to address in the long term.

Oberheide and Miller, both well-known for their work on mobile security, went into their research without much detailed knowledge of how the Bouncer system works. Google has said little publicly about its capabilities, preferring not to give attackers any insights into the system's inner workings. So Oberheide and Miller looked at it as a challenge, an exercise to see how much they could deduce about Bouncer from the outside, and, as it turns out, the inside.

It can be bypassed quite easily and in ways that will be difficult for Google to address in the long term.

Server-side Solutions

- Google Play: Bouncer



Google's Android platform has become the most popular mobile operating system both among consumers and malware writers, and the company earlier this year introduced the Bouncer system to look for malicious apps in the Google Play market. Bouncer, which checks for malicious apps and known malware, is a good first step, but as new work from researchers Jon Oberheide and Charlie Miller shows, it can be bypassed quite easily and in ways that will be difficult for Google to address in the long term.

Oberheide and Miller, both well-known for their work on mobile security, went into their research without much detailed knowledge of how the Bouncer system works. Google has said little publicly about its capabilities, preferring not to give attackers any insights into the system's inner workings. So Oberheide and Miller looked at it as a challenge, an exercise to see how much they could deduce about Bouncer from the outside, and, as it turns out, the inside.

It can be bypassed quite easily and in ways that will be difficult for Google to address in the long term.

- Third-party app markets

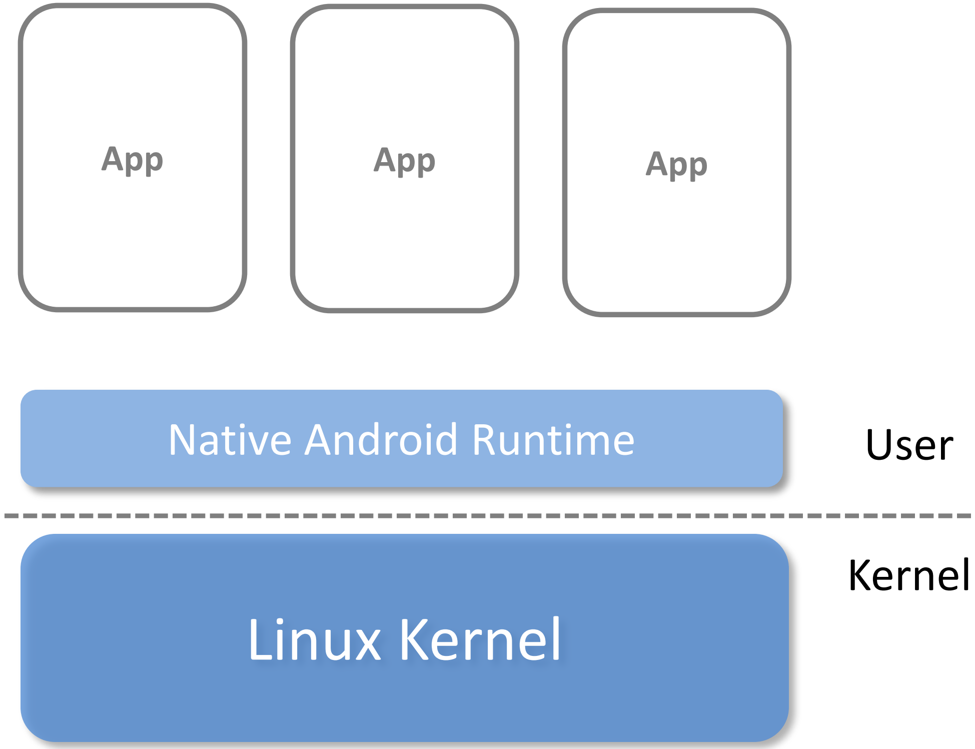
Client-side Solutions

- Android app sandbox
- Security app
- In-app reference monitor

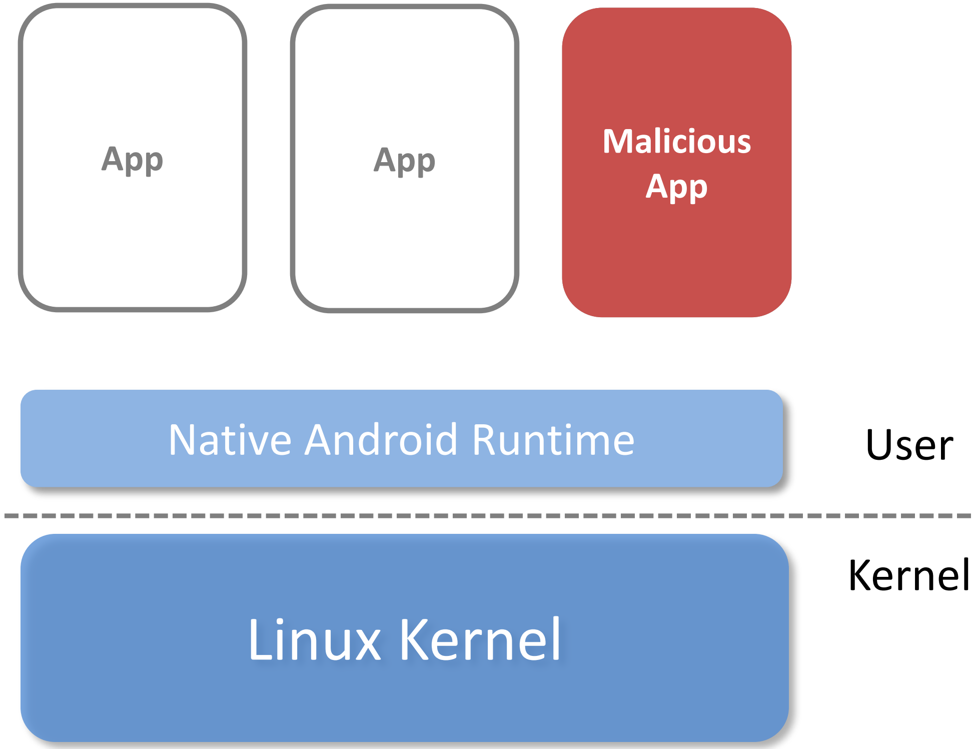
AirBag

- A light-weight solution to effectively isolate untrusted apps

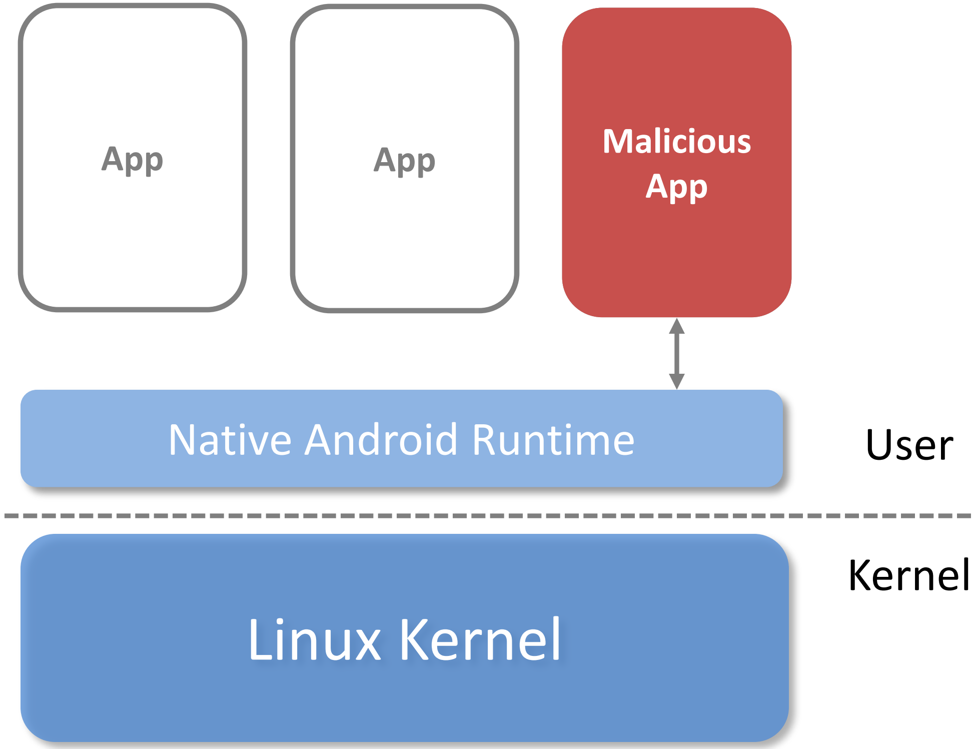
System Design



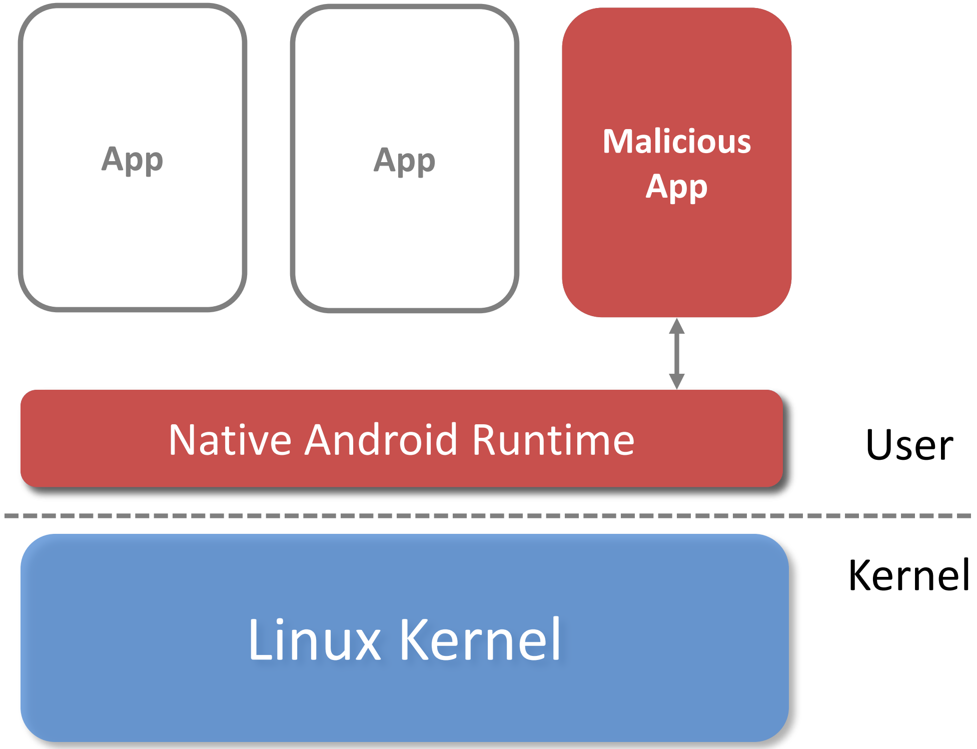
System Design



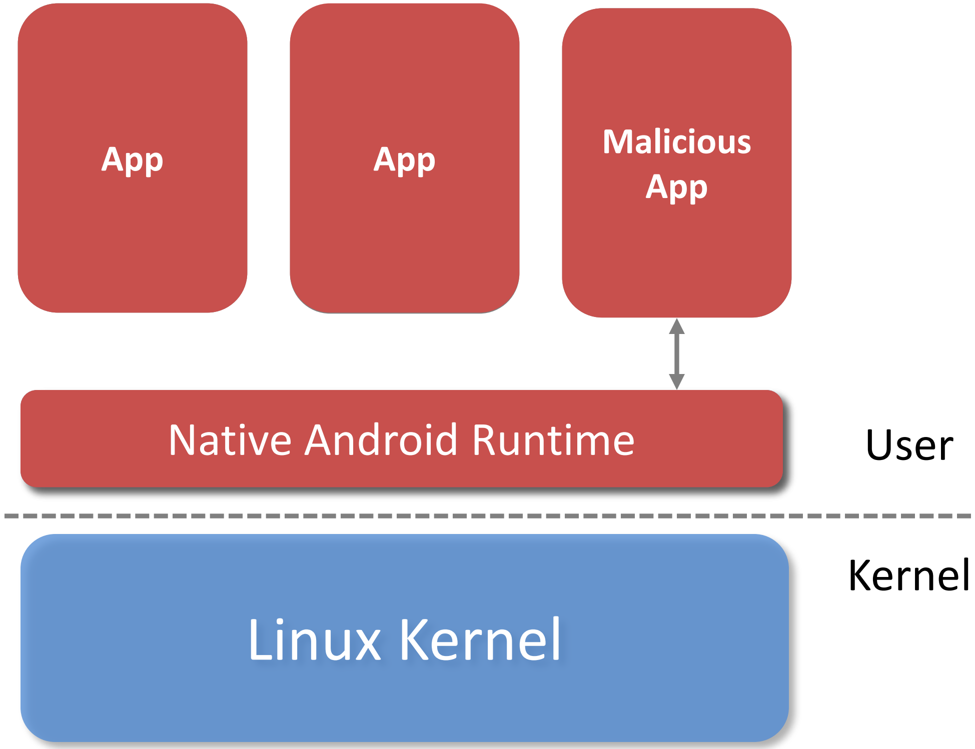
System Design



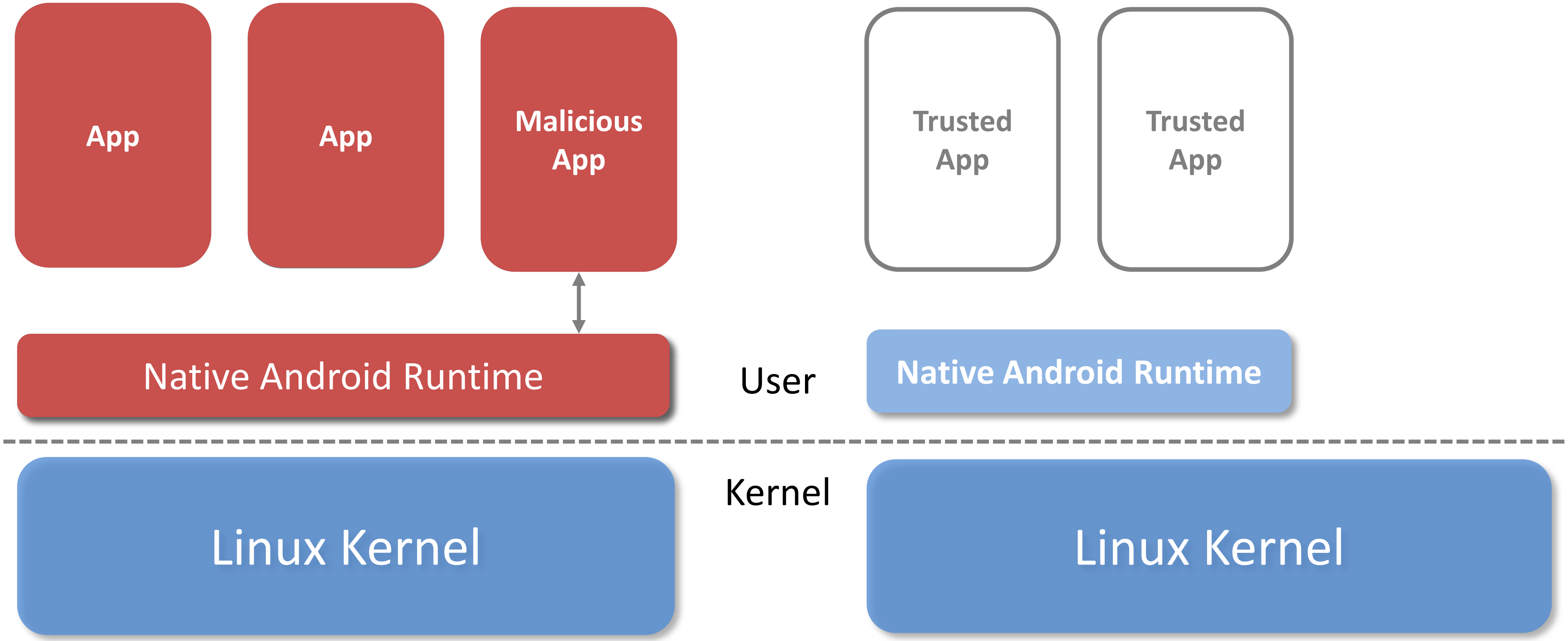
System Design



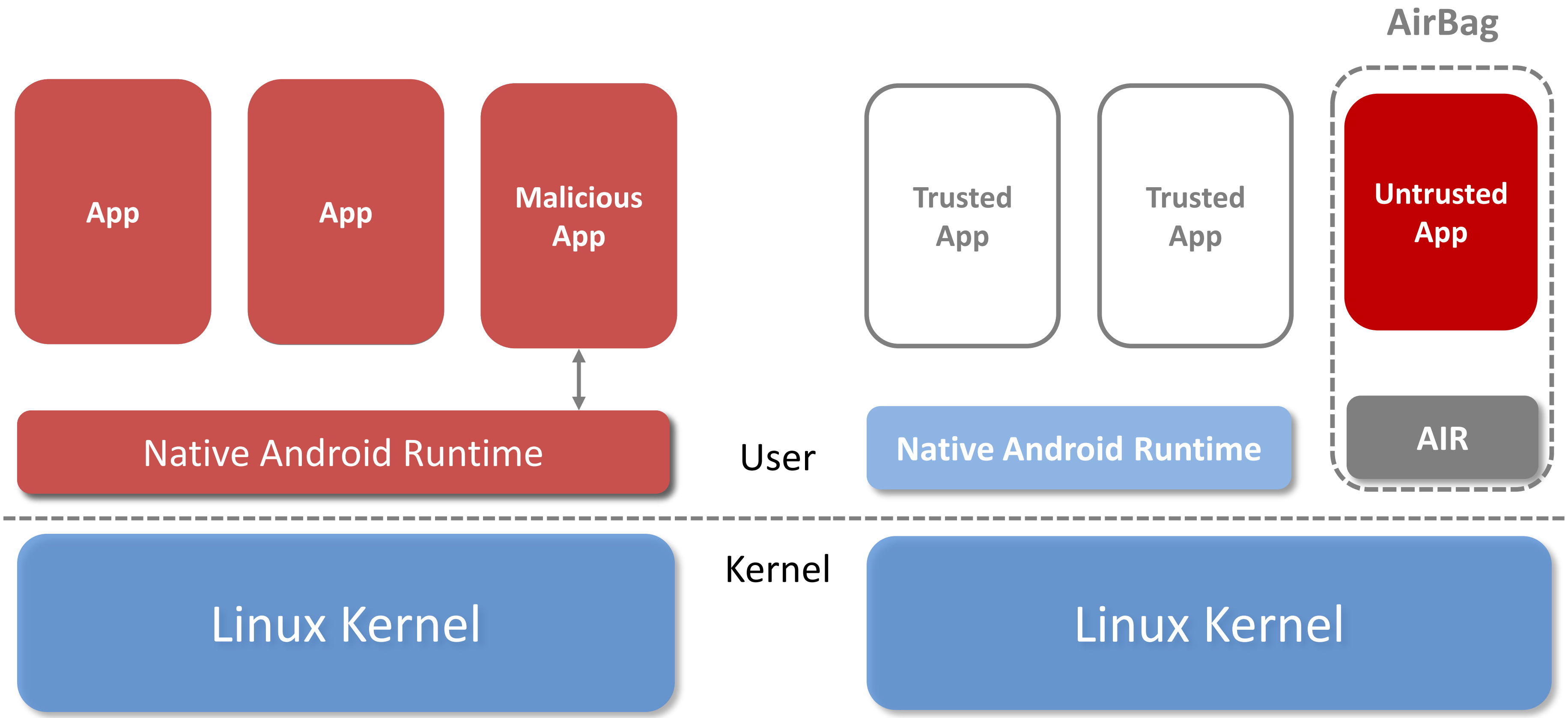
System Design



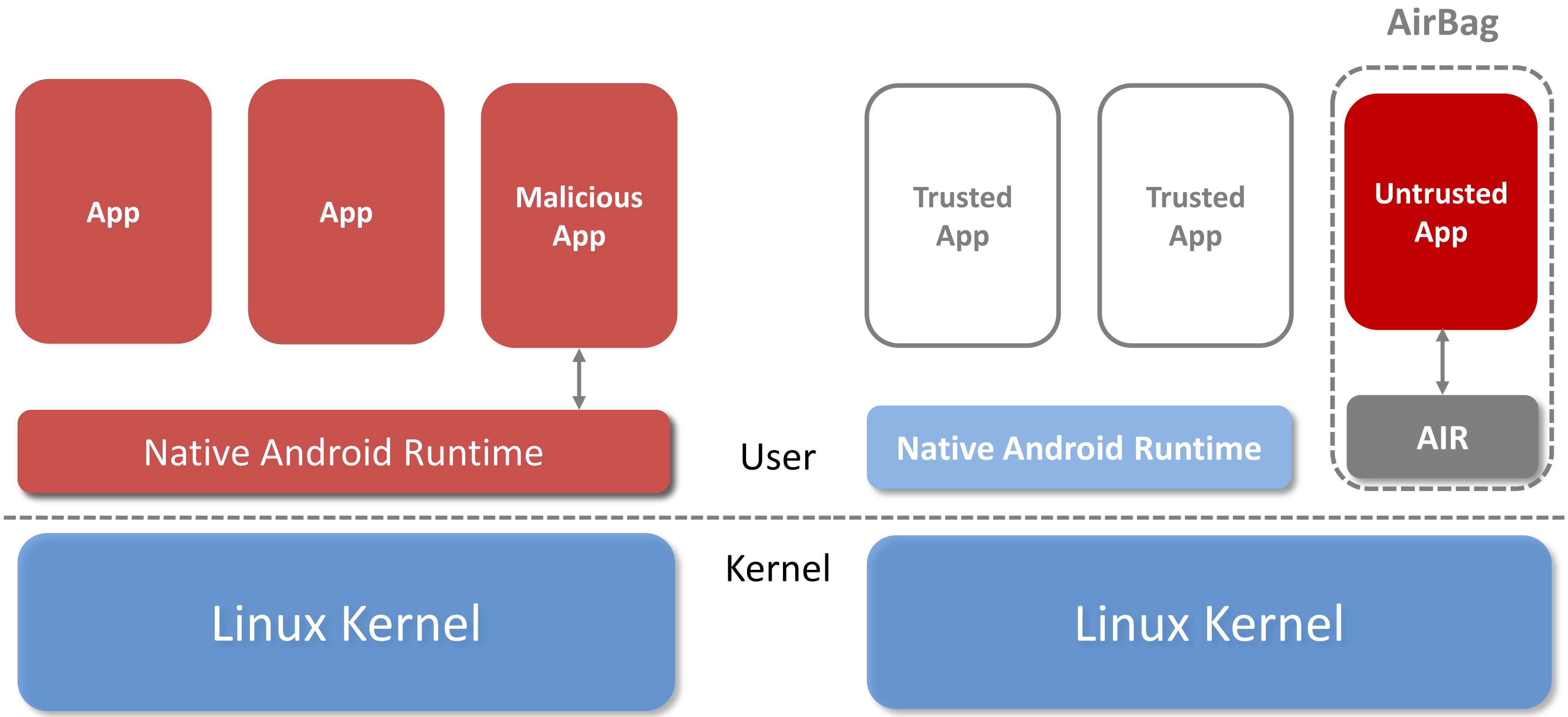
System Design



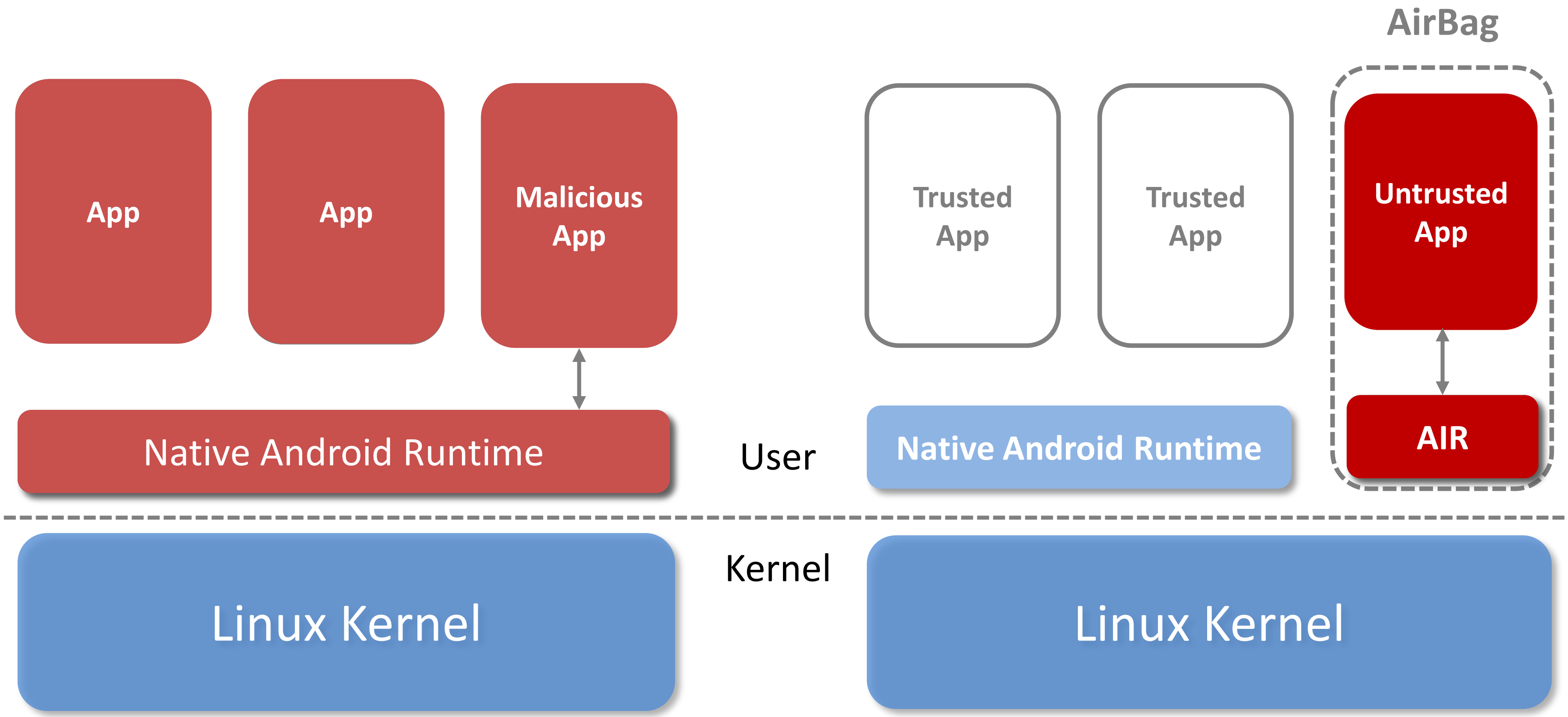
System Design



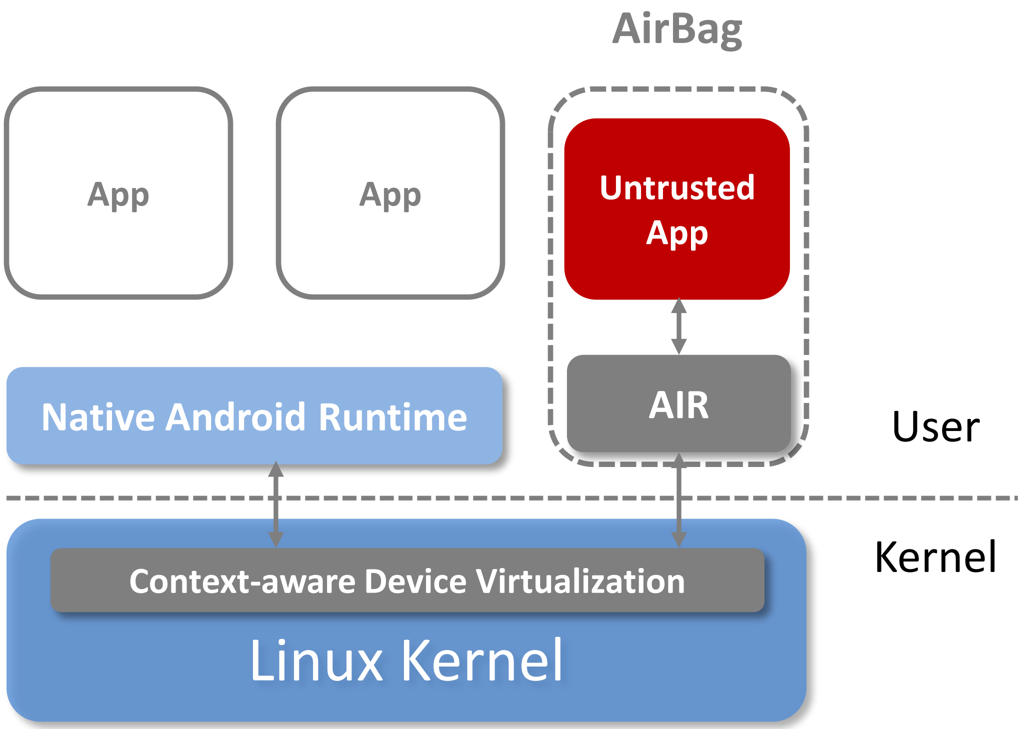
System Design



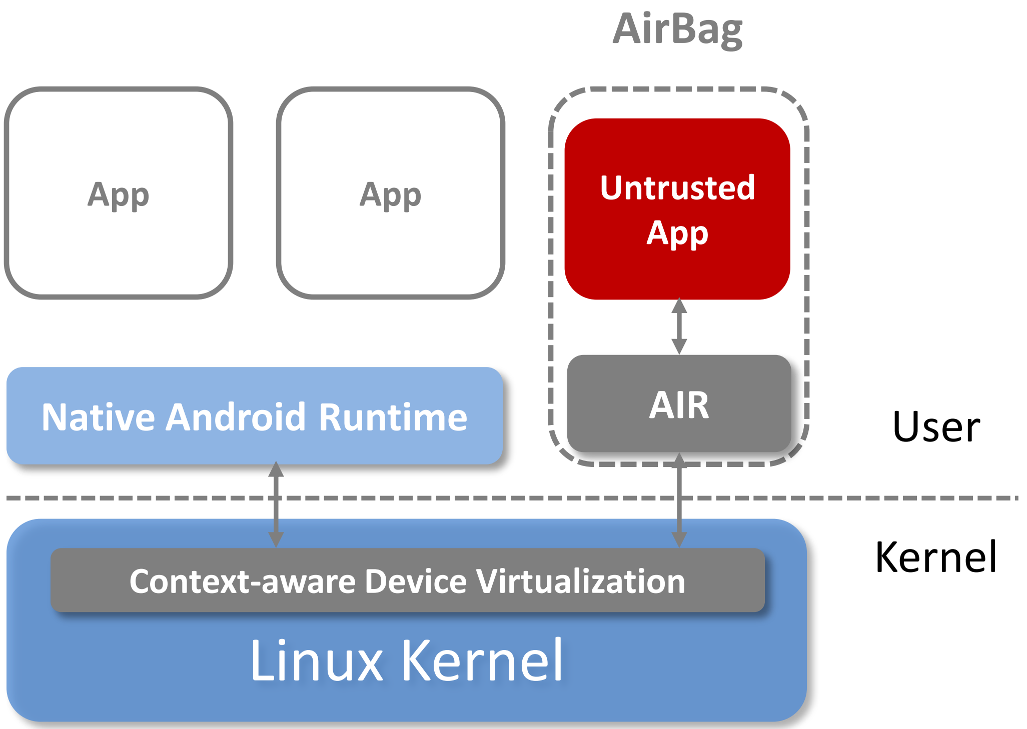
System Design



Key Techniques

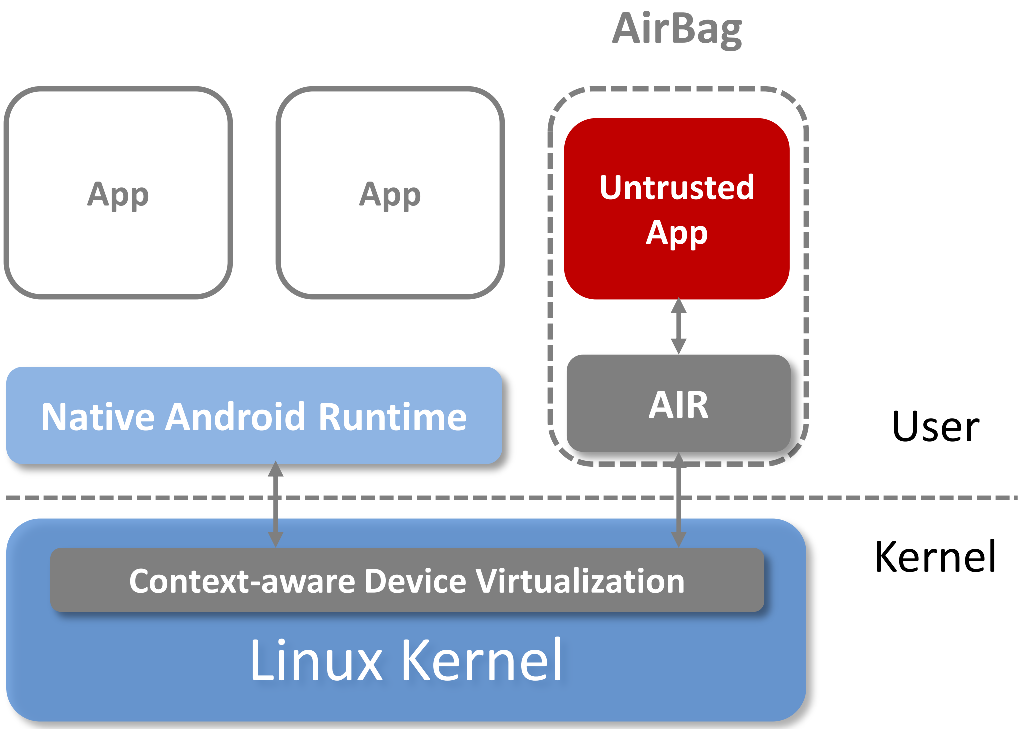


Key Techniques



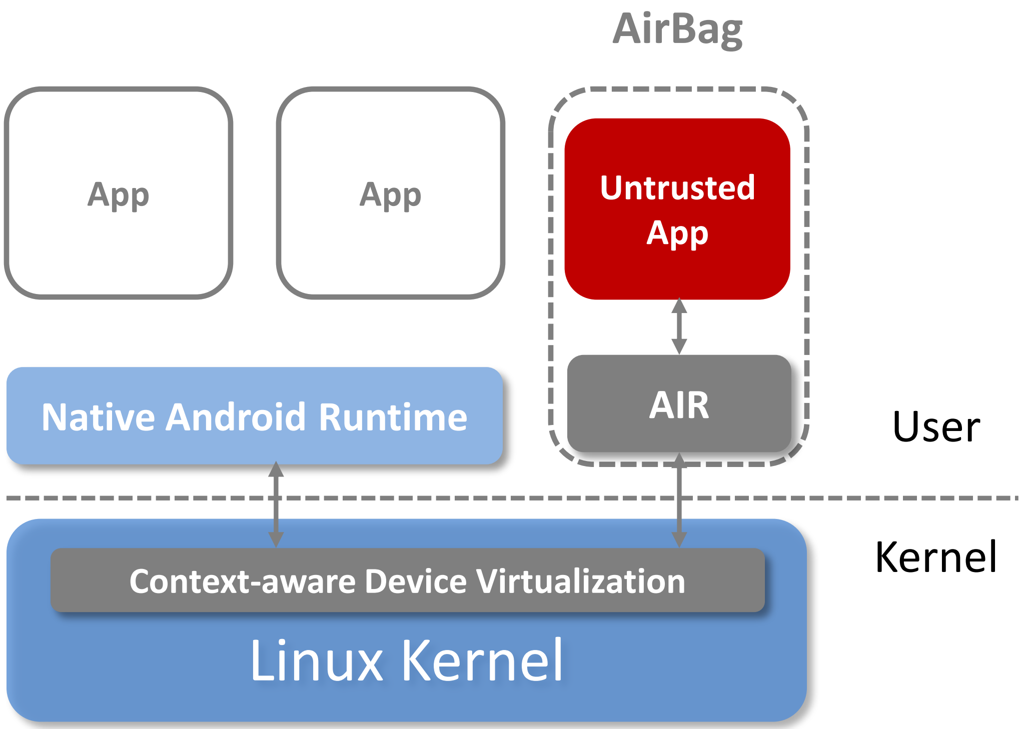
- Decoupled app isolation runtime (AIR)

Key Techniques



- Decoupled app isolation runtime (AIR)
- Namespace and filesystem isolation

Key Techniques



- Decoupled app isolation runtime (AIR)
- Namespace and filesystem isolation
- Context-aware device virtualization

App Isolation Runtime (AIR)

- Separated (and customized) Android runtime for untrusted apps
- Benefits
  - Isolation: compromised AIR does not affect native Android runtime
  - Customization: different running modes
  - Privacy-awareness: prevent stealthy actions

Namespace and Filesystem Isolation

- Separated name space
  - Benefit: apps inside AirBag cannot interact with outside ones
- Separated filesystem: all modifications are inside AirBag
  - Benefit: does not affect original Android system
  - Bonus: easy to provide “restore to default” feature

Context-aware Device Virtualization

- Multiplexing system resources between AIR and native Android runtime

Implementation

Device	Kernel	AIR based on
Google Nexus One	2.6.35.7	Cyanogenmod 7.1.0 Stable Release
Google Nexus 7	3.1.10	Cyanogenmod 9 Nightly Build
Samsung Galaxy S3	3.0.8	Cyanogenmod 9.1.0 Stable Release

Porting for each device is done within one week!

- Three Android devices with different kernel versions
- Less than 2,000 lines of kernel patch

Context-aware Device Virtualization

Device	Description
Audio	Audio Playback and Capture
Framebuffer	Display Output
GPU	Graphics Processor
Input	Touchscreen and Buttons
IPC	Binder IPC Framework
pmem	Physical Memory Allocator
Networking	WiFi Network Interface
Power	Suspend/Resume
RTC	Real Time Clock
Sensors	Temperature, Accelerometer, GPS
Telephony	Cellular Radio

Context-aware Device Virtualization

Device	Description
Audio	Audio Playback and Capture
Framebuffer	Display Output
GPU	Graphics Processor
Input	Touchscreen and Buttons
IPC	Binder IPC Framework
pmem	Physical Memory Allocator
Networking	WiFi Network Interface
Power	Suspend/Resume
RTC	Real Time Clock
Sensors	Temperature, Accelerometer, GPS
Telephony	Cellular Radio

Basic devices to bring up AirBag

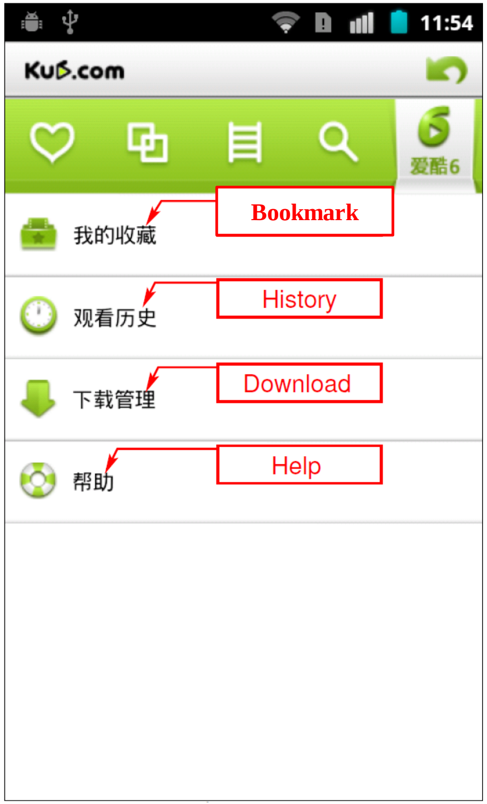
Input

- Keeping the namespace info while registering evdev
- Dispatching input events to the active runtime

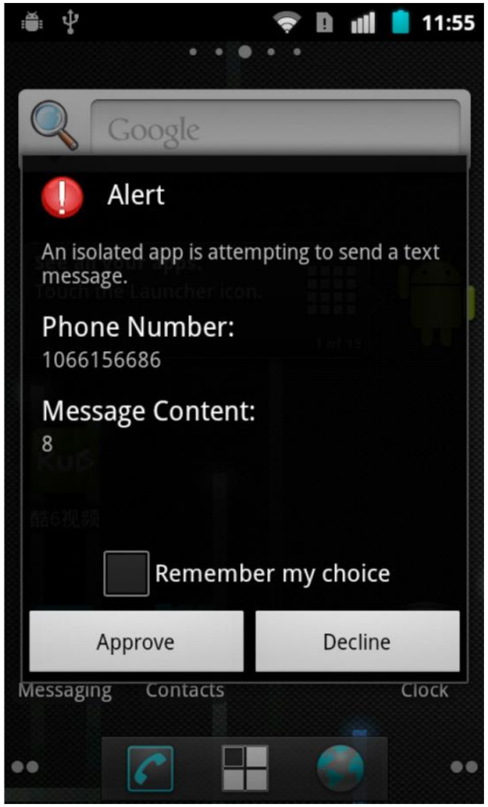
Evaluation

- Dataset: malware samples from 20 families
- Results: malicious operations are isolated

Case Study: HippoSMS



Infected Video Browser running inside AirBag



Alert

An isolated app is attempting to send a text message.

Phone Number:
1066156686

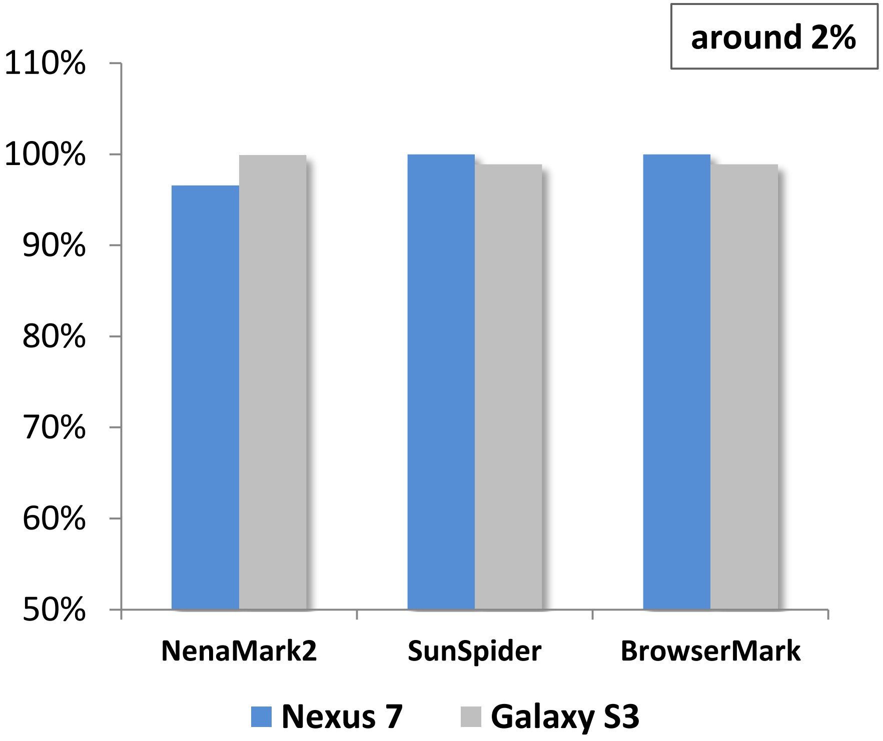
Message Content:
8

□ Remember my choice

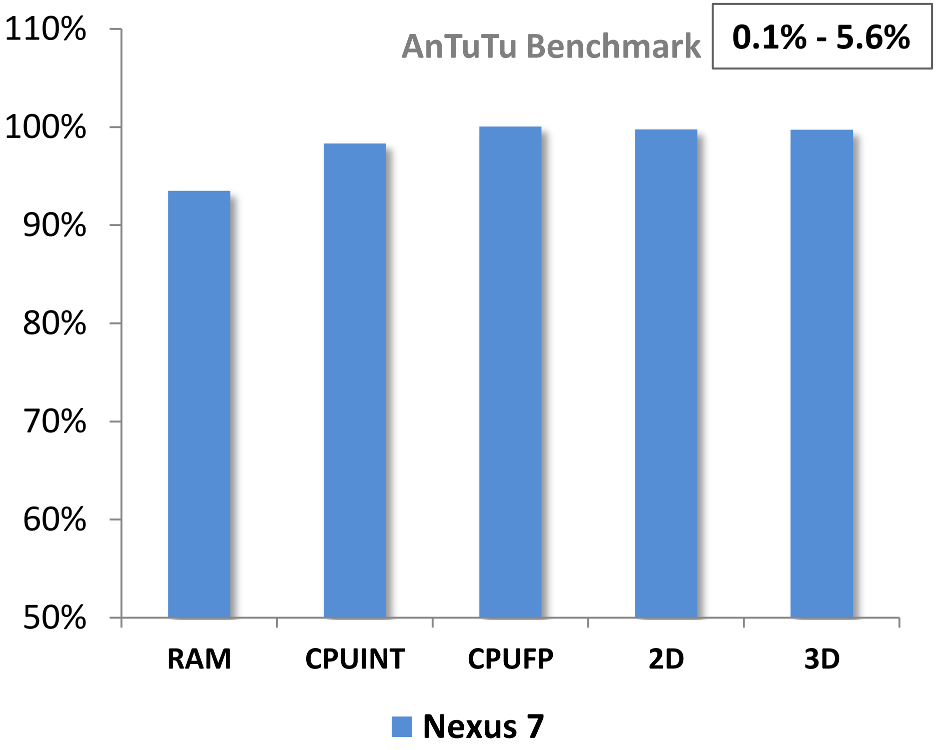
Approve Decline

A pop-up alert on background SMS behavior

Performance Overhead



Benchmark	Version	Type
NenaMark2	2.3	GPU
SunSpider	0.9.1	CPU/IO
BrowserMark	2.0	CPU/IO



Benchmark	Version	Type
AnTuTu	2.8.3	Combination

Computer Science NC STATE UNIVERSITY

Power & Memory

- Power consumption

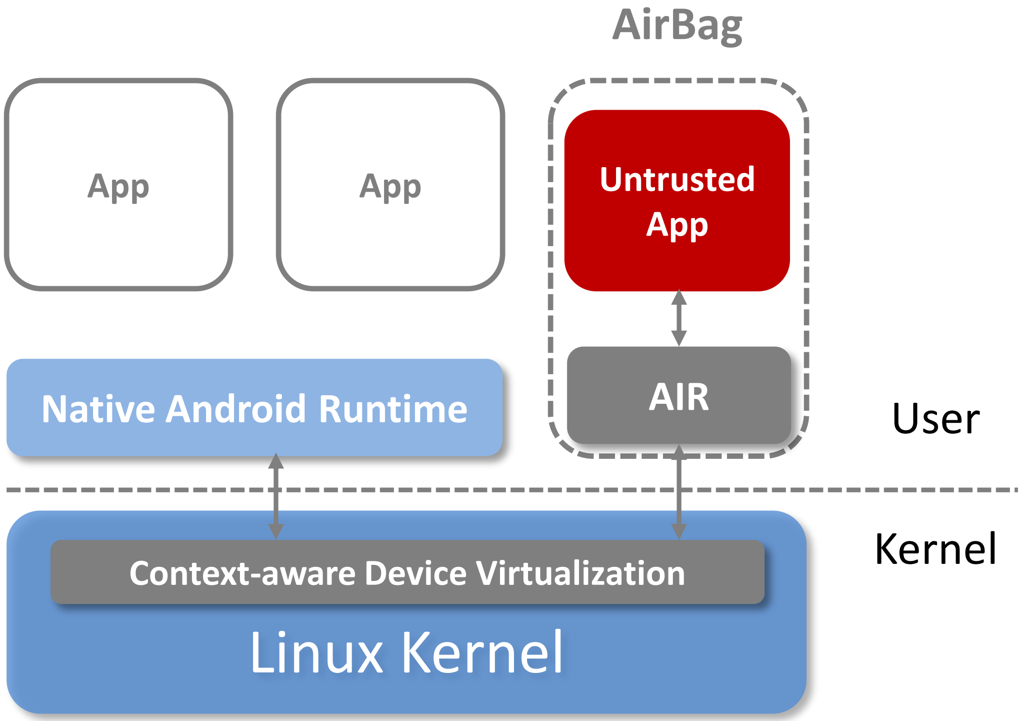
	Stock Nexus 7 (battery level)	Nexus 7 with AirBag (battery level)
Idle for 24hrs	91%	89%
Playing music for 24hrs	66%	63%

- Memory use

	Stock Nexus 7 (in-use memory)	Nexus 7 with AirBag (in-use memory)
Idle for 4hrs	59.31%	60.87%
Playing music for 4hrs	60.25%	63.70%

Conclusion

- AirBag: a light-weight solution to effectively and efficiently isolate untrusted apps



Q & A

Yajin Zhou
http://yajin.org

North Carolina State University

National University of Singapore