CISPA
Center for IT-Security, Privacy
and Accountability

UNIVERSITÄT
DES
SAARLANDES

Boxify: Full-fledged App Sandboxing for Stock Android

Michael Backes, Sven Bugiel, Christian Hammer,
Oliver Schranz, **Philipp von Styp-Rekowsky**

24th USENIX Security Symposium

SPONSORED BY THE
Federal Ministry
of Education
and Research

max planck institut
informatik

German
Research Center
for Artificial
Intelligence

Max
Planck
Institute
for
Software Systems

Motivation

FlaskDroid
[SEC'13]

AirBag
[NDSS'14]

Apex
[ASIACCS'10]

Cells
[SOSP'11]

Dr. Android & Mr. Hide
[SPSM'12]

TaintDroid
[OSDI'10]

AppGuard
[TACAS'13]

L4Android
[SPSM'11]

MOSES
[SACMAT'12]

ASM
[SEC'15]

I-ARM-Droid
[MoST'12]

CRePE
[ISC'10]

DroidForce
[ARES'14]

TrustDroid
[SPSM'11]

Aurasium
[SEC'12]

RetroSkeleton
[MobiSys'13]

Motivation

FlaskDroid
[SEC‘13]

Cells
[SOSP‘11]

Dr. Android & Mr. Hide
[SPSM‘12]

TaintDroid
[OSDI‘10]

L4Android
[SPSM‘11]

AppGuard
[TACAS‘13]

RetroSkeleton
[MobiSys‘13]

CRePE
[ISC‘10]

Apex
[ASIACCS‘10]

I-ARM-Droid
[MoST‘12]

MOSES
[SACMAT‘12]

AirBag
[NDSS‘14]

DroidForce
[ARES‘14]

TrustDroid
[SPSM‘11]

ASM
[SEC‘15]

Aurasium
[SEC‘12]

Motivation

FlaskDroid [SEC‘13]

Cells [SOSP‘11]

TaintDroid [OSDI‘10]

L4Android [SPSM‘11]

CRePE [ISC‘10]

Apex [ASIACCS‘10]

MOSES [SACMAT‘12]

AirBag [NDSS‘14]

TrustDroid [SPSM‘11]

ASM [SEC‘15]

OS Extensions

Dr. Android & Mr. Hide [SPSM‘12]

AppGuard [TACAS‘13]

RetroSkeleton [MobiSys‘13]

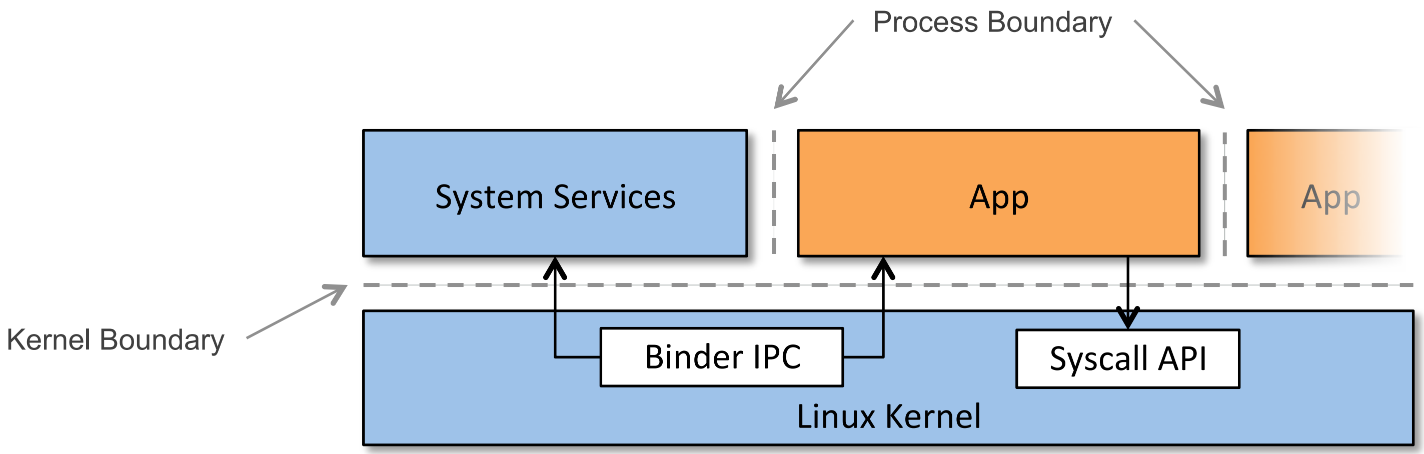
I-ARM-Droid [MoST‘12]

DroidForce [ARES‘14]

Aurasium [SEC‘12]

Application Layer Solutions

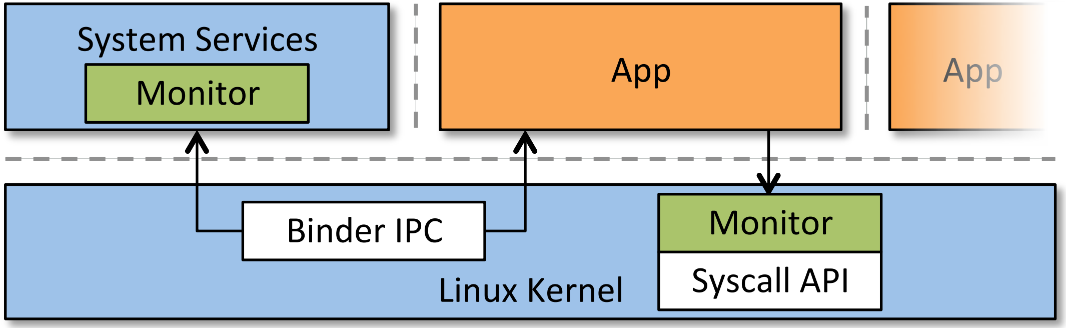
Android OS Extensions



Android OS Extensions

✓ Strong security

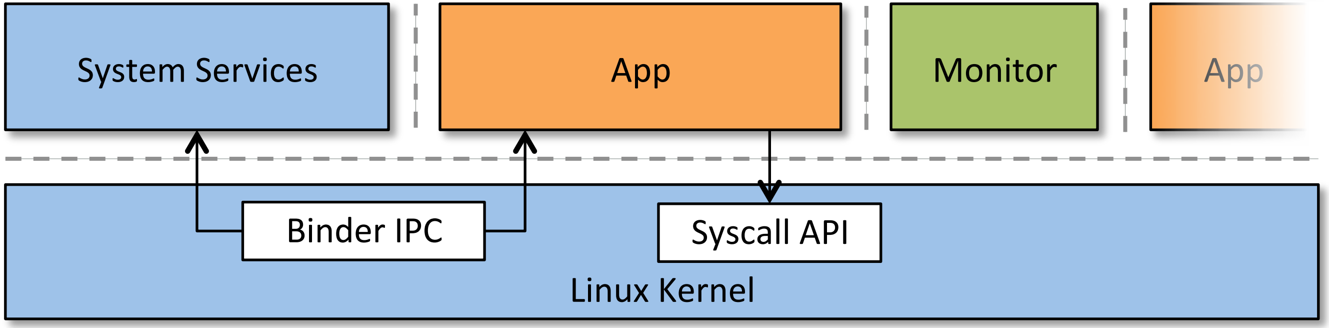
✗ Hard to deploy



Application Layer Solutions

✓ Easy to deploy

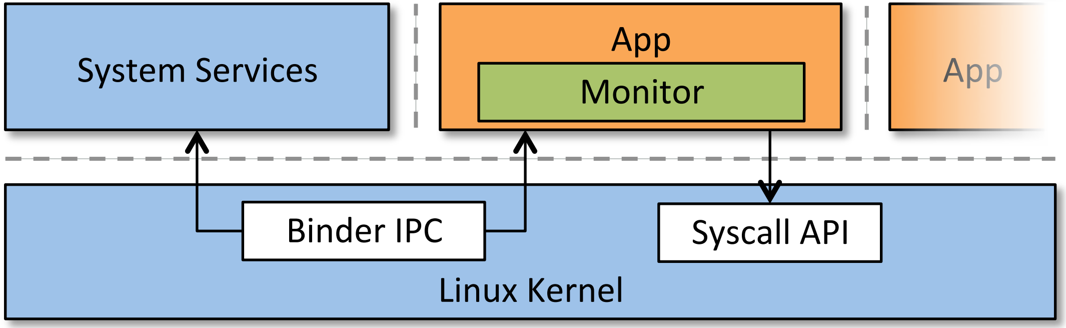
✗ No app monitoring possible



Inlined Reference Monitor

✓ Easy to deploy

✗ Weak security



Goal

OS Extensions

✖ Hard to deploy

✔ Strong security

Application Layer Solutions

✔ Easy to deploy

✖ Weak security

Goal

OS Extensions	Our Goal	Application Layer Solutions
✖ Hard to deploy	✔ Easy to deploy	✔ Easy to deploy
✔ Strong security	✔ Strong security	✖ Weak security

Objectives

Monitor and constrain untrusted applications

✓ **Easy to deploy**

- No firmware modification / root
- No application modification

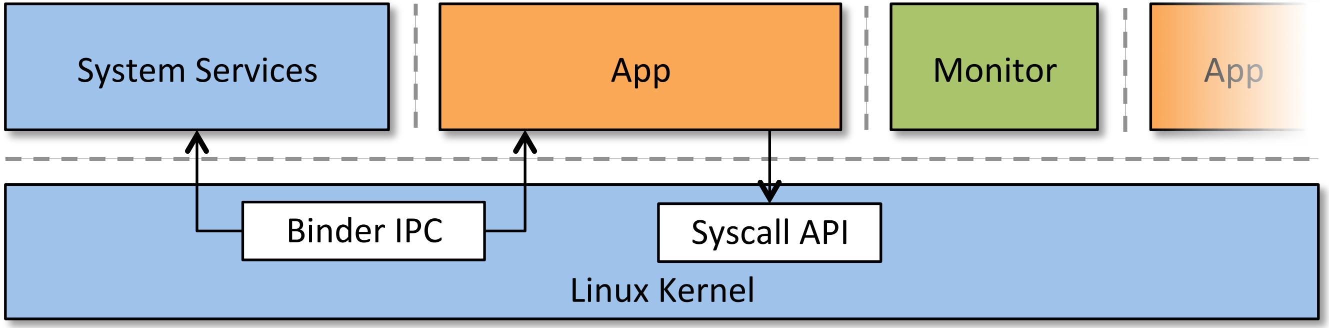
✓ **Strong security**

- Protected reference monitor
- Fail-safe defaults

Approach (1)

Objective: No firmware modification / root

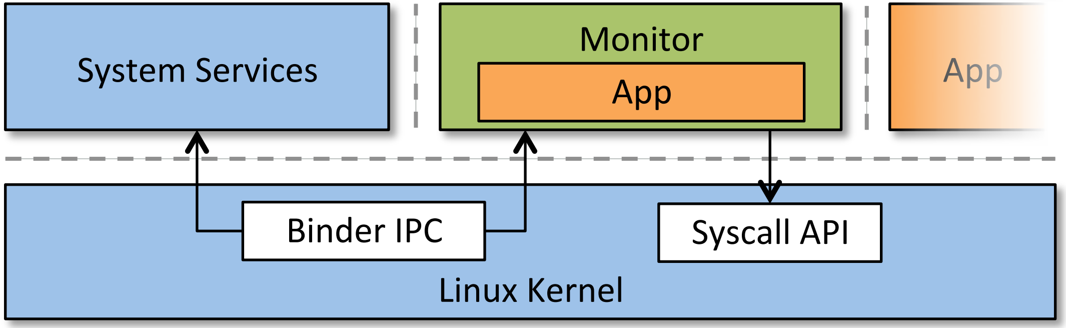
Solution: Regular user-space application



Approach (2)

Objective: No application modification

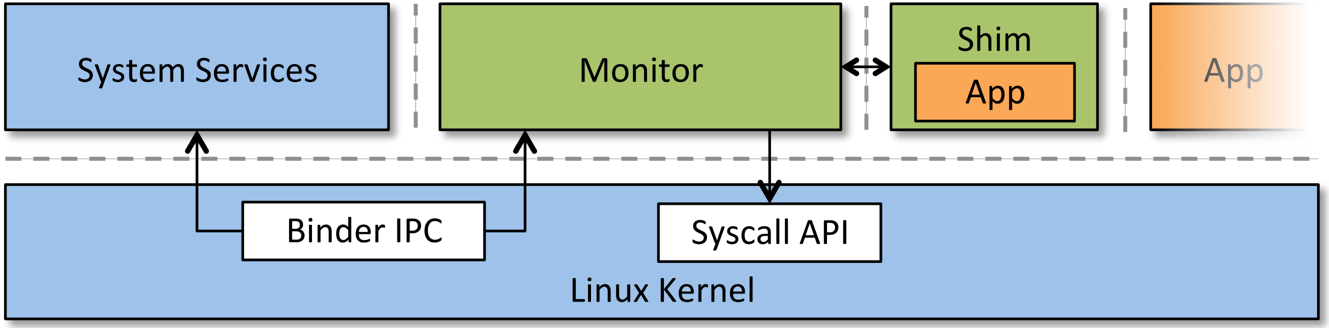
Solution: Application virtualization



Approach (3)

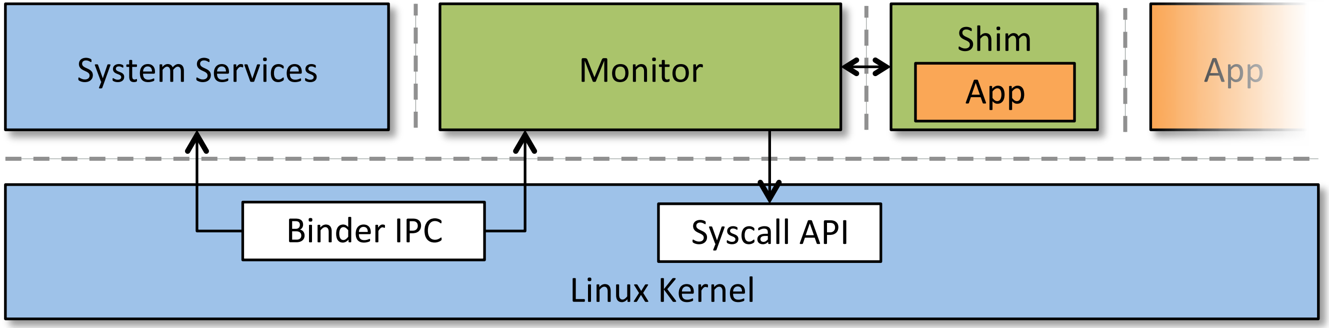
Objective: Protected reference monitor

Solution: Separate process



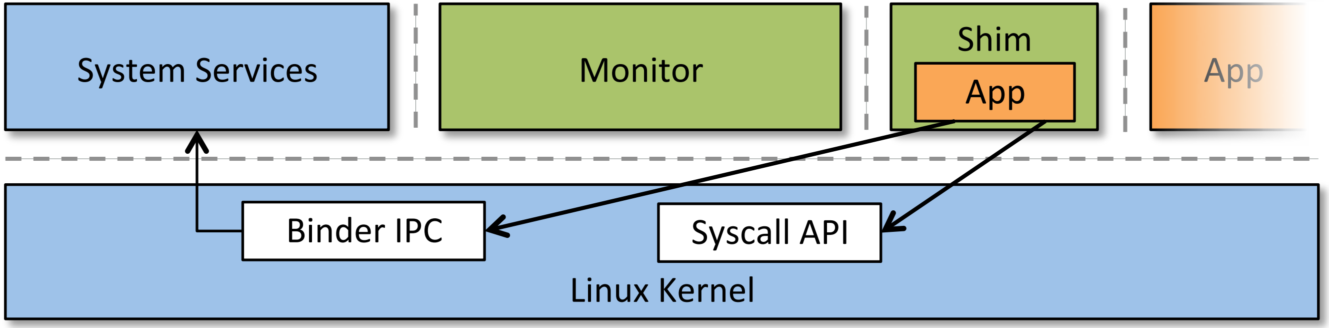
Approach (4)

Objective: Fail-safe defaults



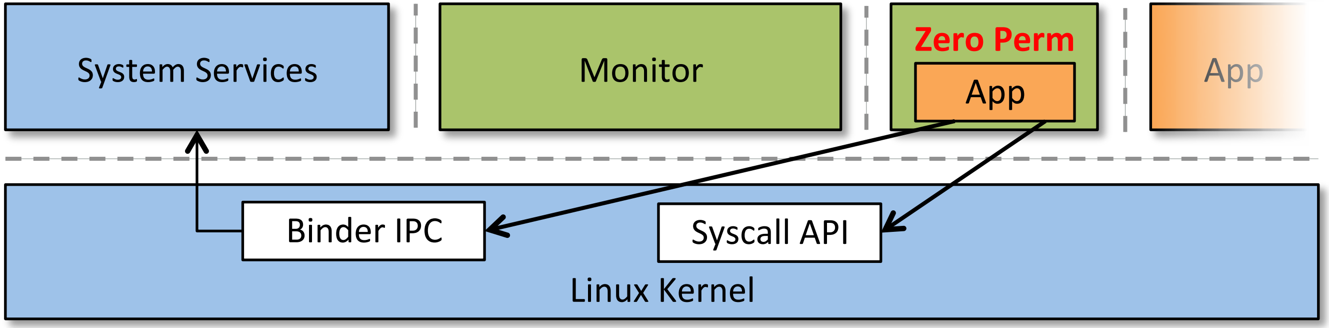
Approach (4)

Objective: Fail-safe defaults



Approach (4)

Objective: Fail-safe defaults



Approach (4)

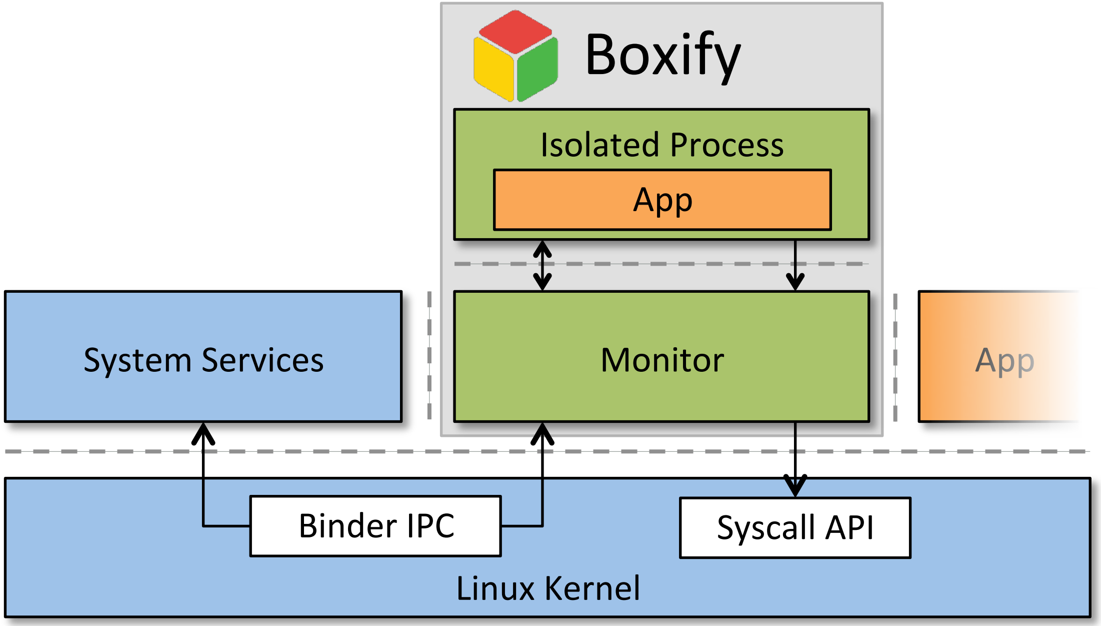
Objective: Fail-safe defaults

Solution: Isolated process

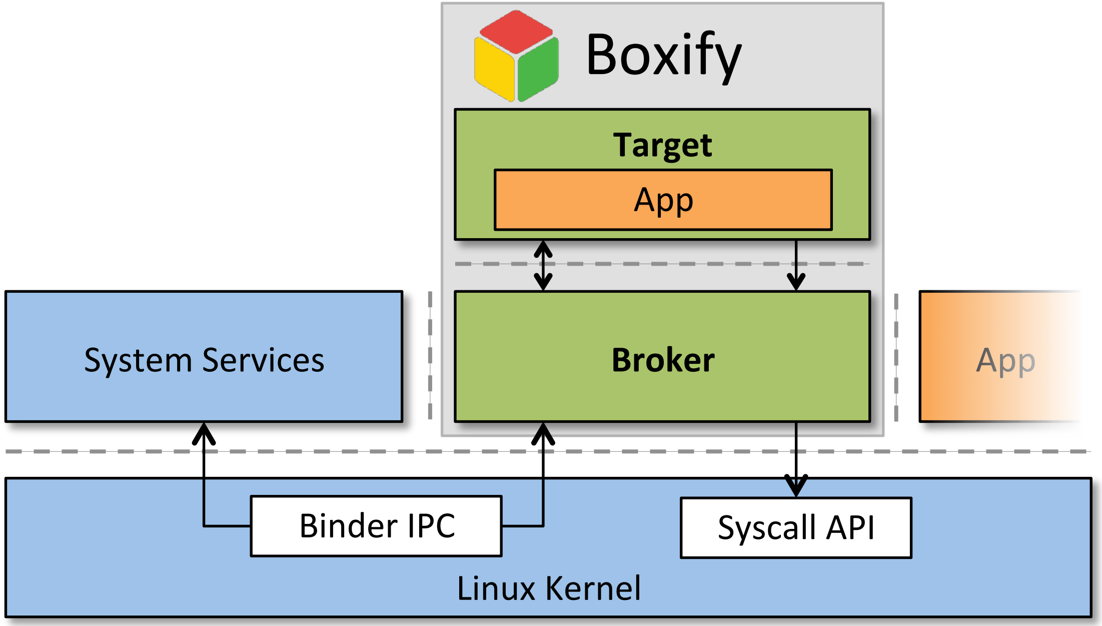
Isolated Process

- Allows *service components* to run isolated from the rest of the application
- Isolated processes
  - Have zero permissions
  - Have no access to system services
  - Run with a distinct, transient UID
  - Cannot write to the filesystem

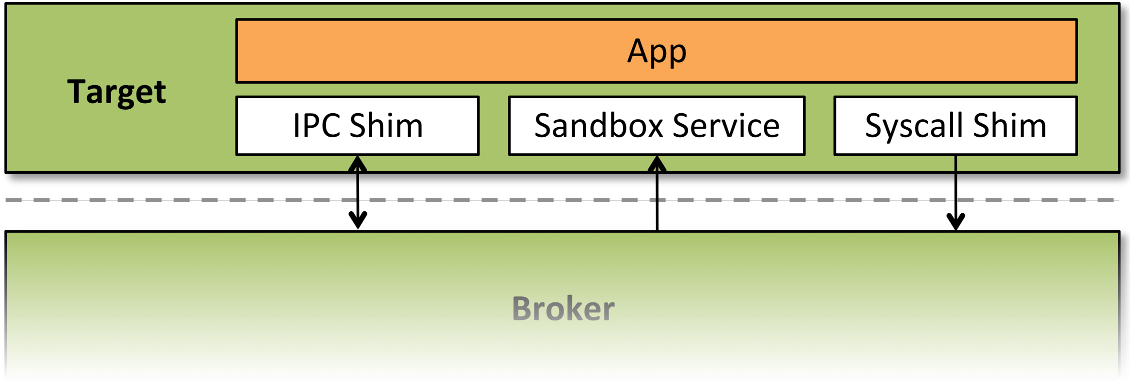
Architecture



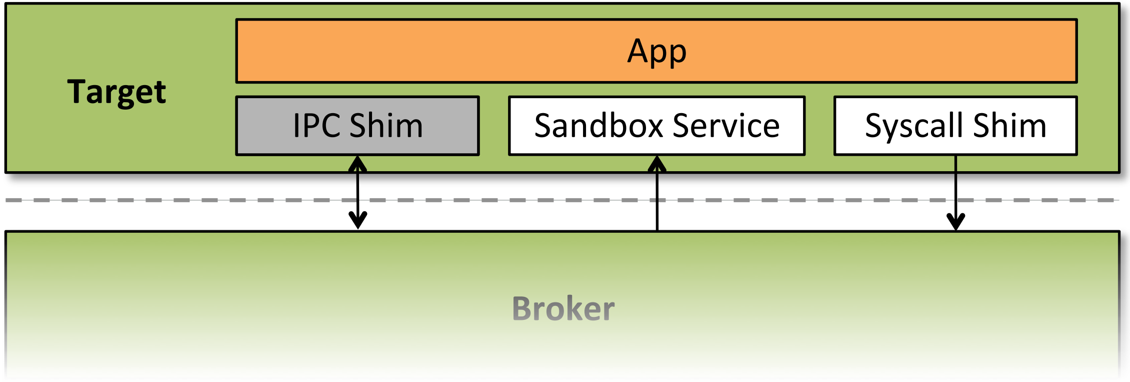
Architecture



Target

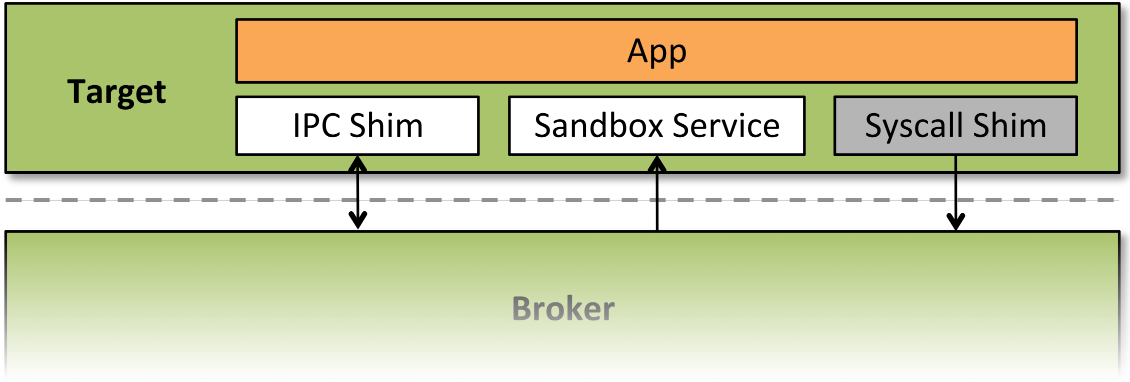


Target



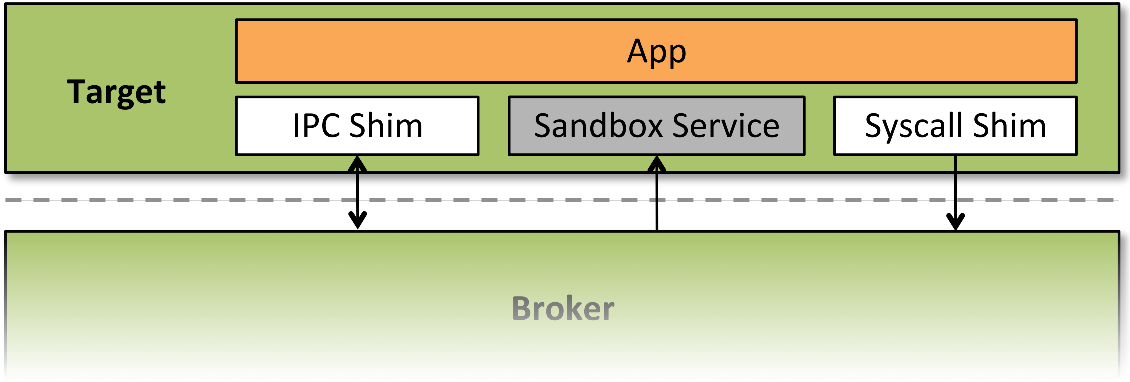
Divert Binder IPC to Broker

Target



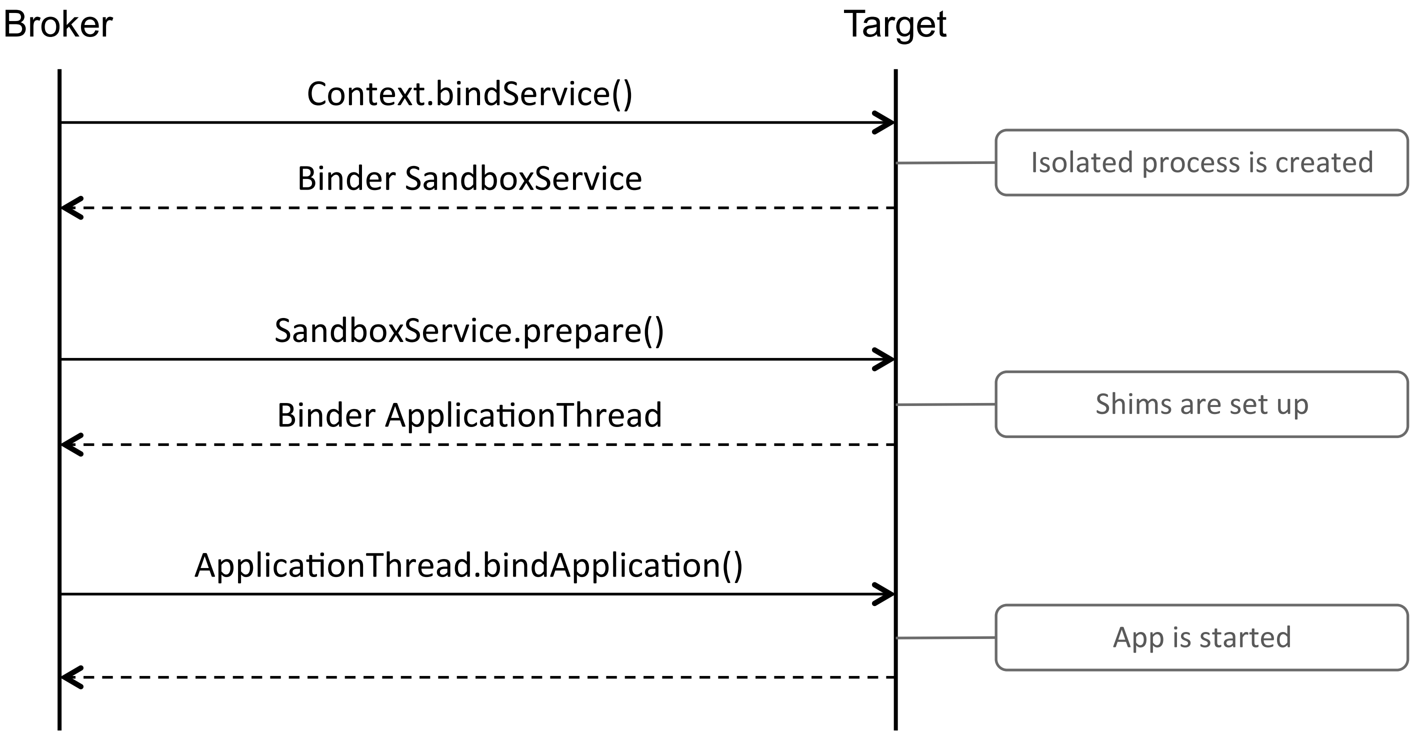
Divert Syscalls to Broker

Target

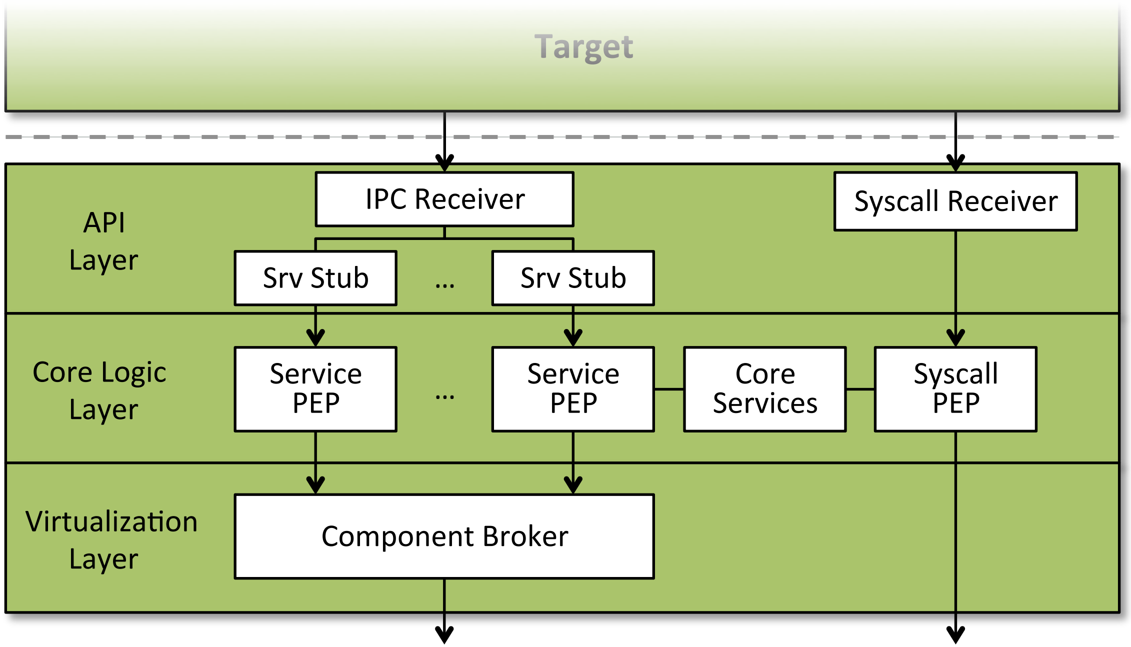


Control channel for loading/terminating apps

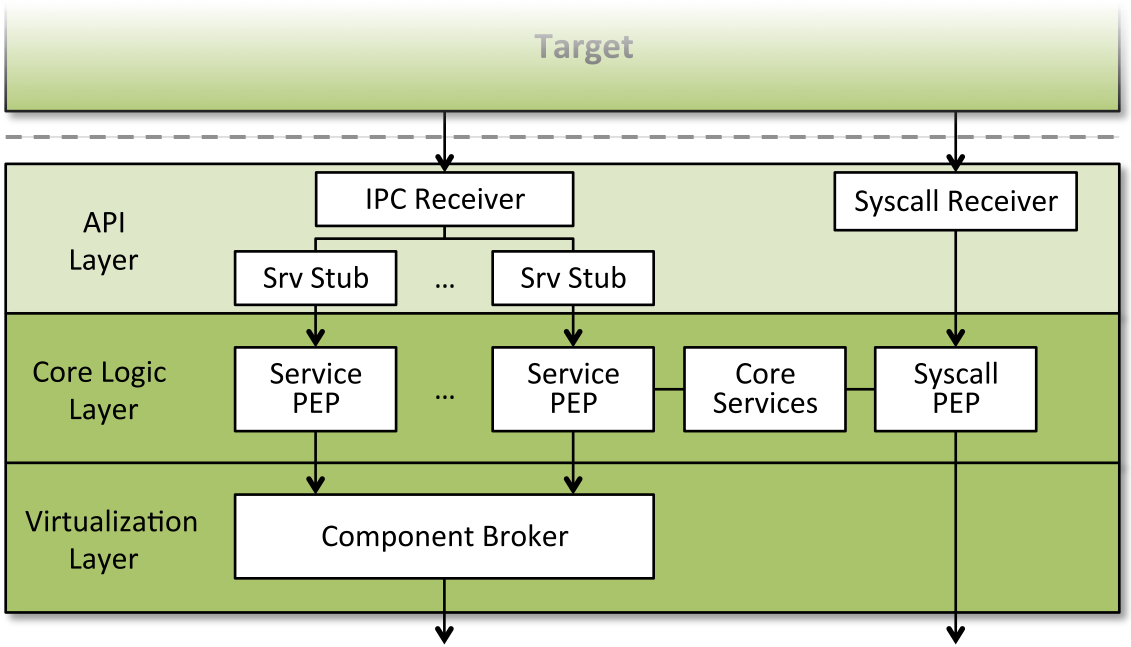
Loading an app



Broker

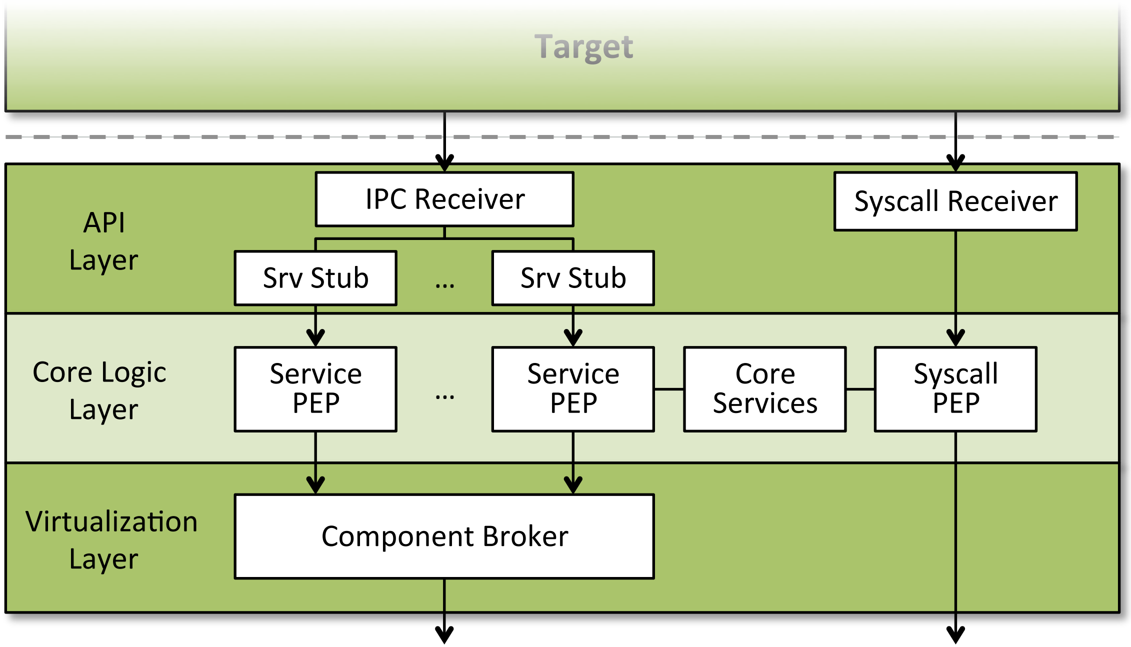

Target
API Layer
IPC Receiver
Syscall Receiver
Srv Stub
…
Srv Stub
Core Logic Layer
Service PEP
…
Service PEP
Core Services
Syscall PEP
Virtualization Layer
Component Broker

API Layer



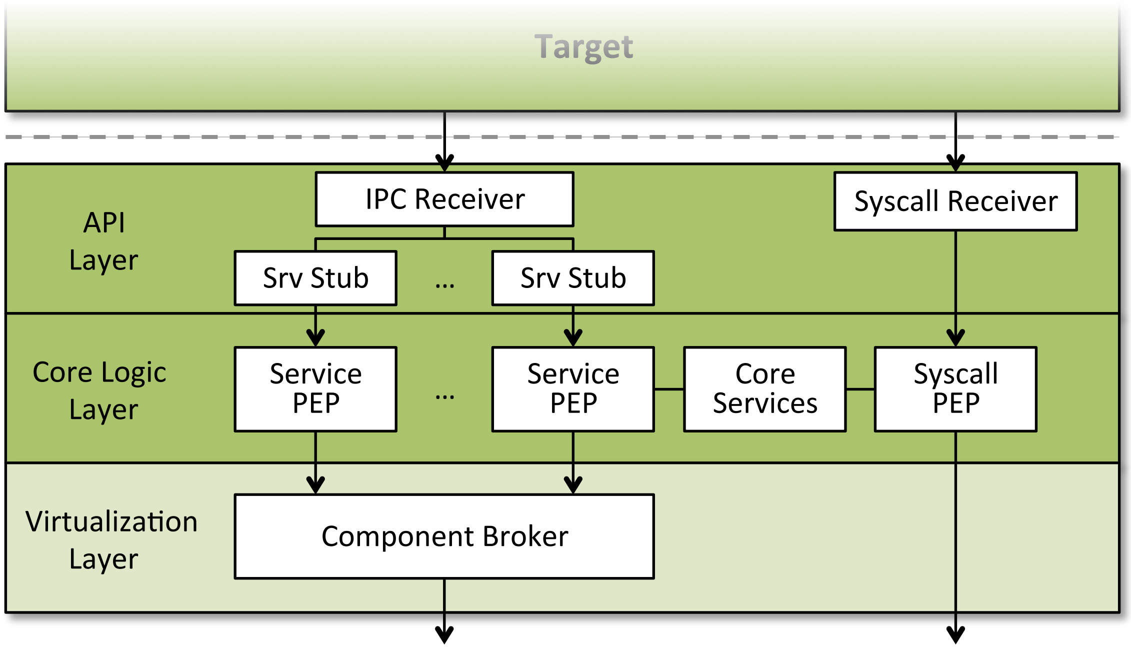
Establish compatibility across Android versions

Core Logic Layer



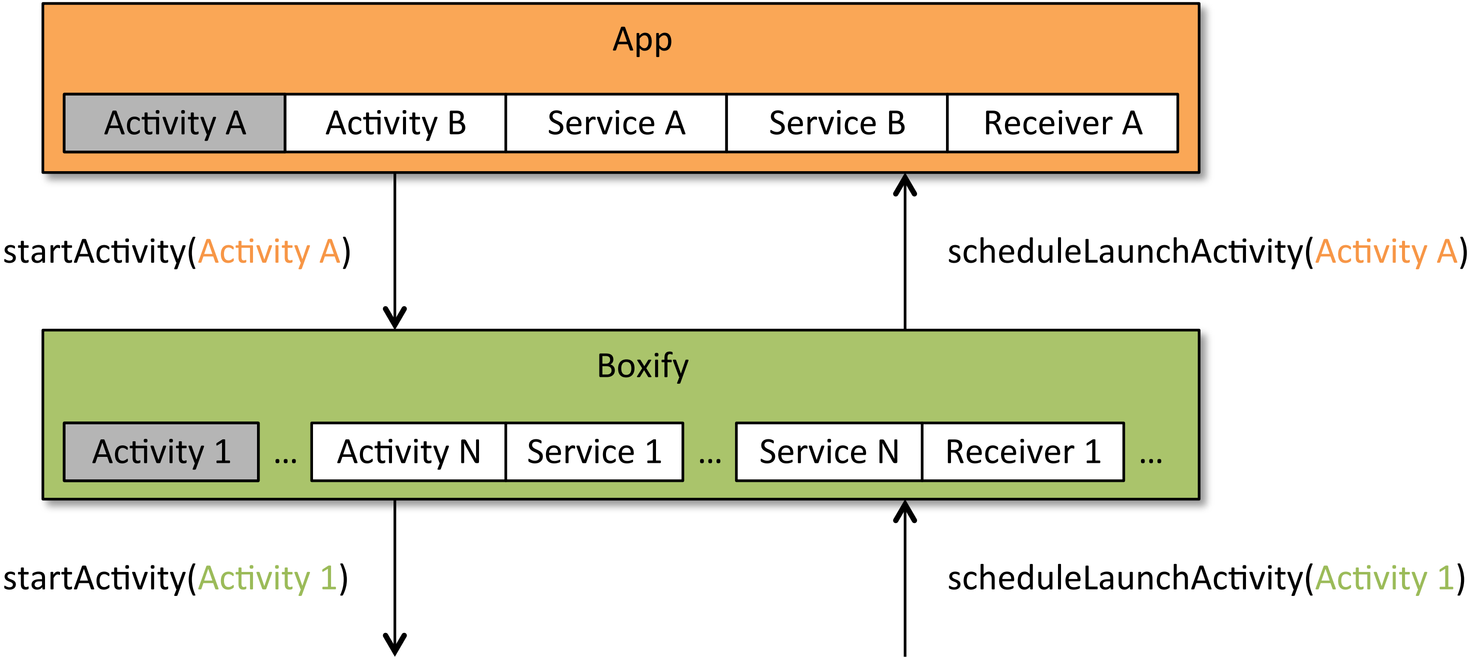
Baseline enforcement & virtual system services

Virtualization Layer



Translate between Boxify and Android system

Virtualization Layer

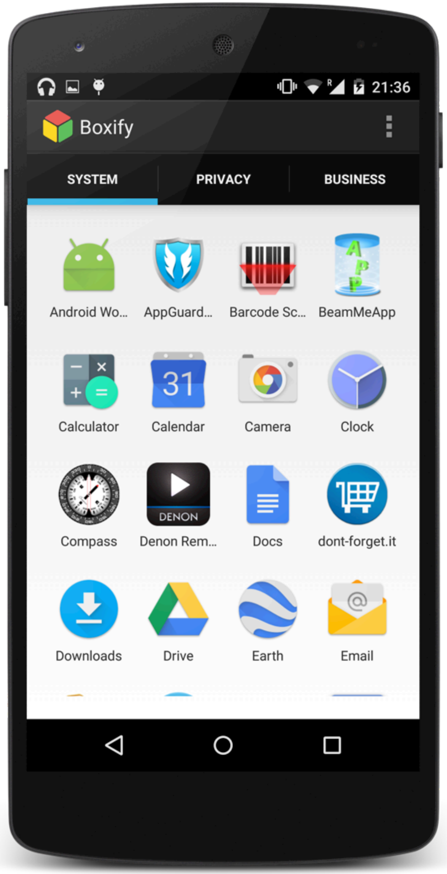


App
Activity A
Activity B
Service A
Service B
Receiver A
startActivity(Activity A)
scheduleLaunchActivity(Activity A)
Boxify
Activity 1
…
Activity N
Service 1
…
Service N
Receiver 1
…
startActivity(Activity 1)
scheduleLaunchActivity(Activity 1)

System Integration

- Launching apps
  - Dedicated Activity

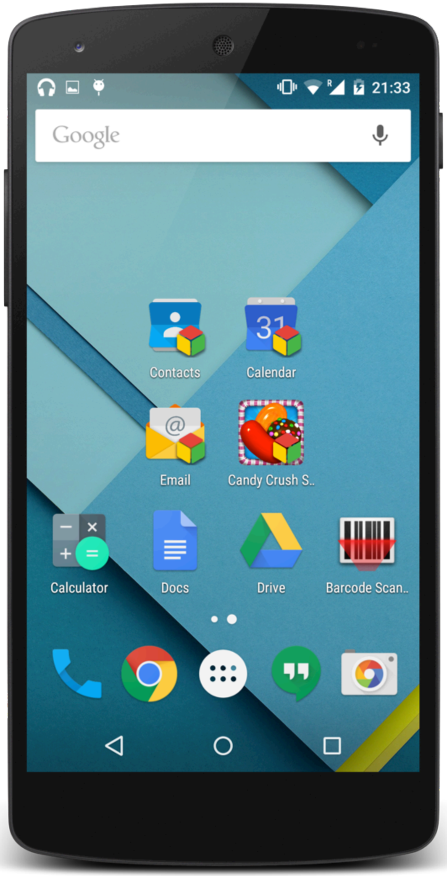
- Installing/Updating apps



System Integration

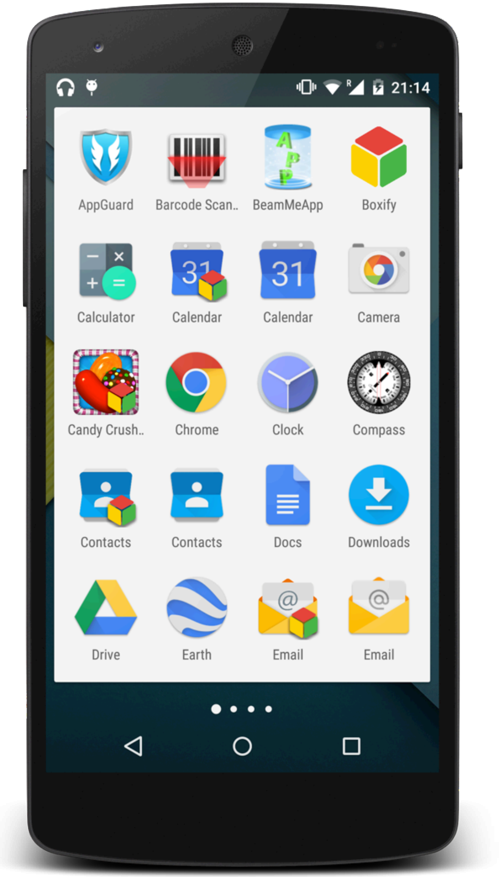
- Launching apps
  - Dedicated Activity
  - Shortcuts on Home Screen

- Installing/Updating apps



System Integration

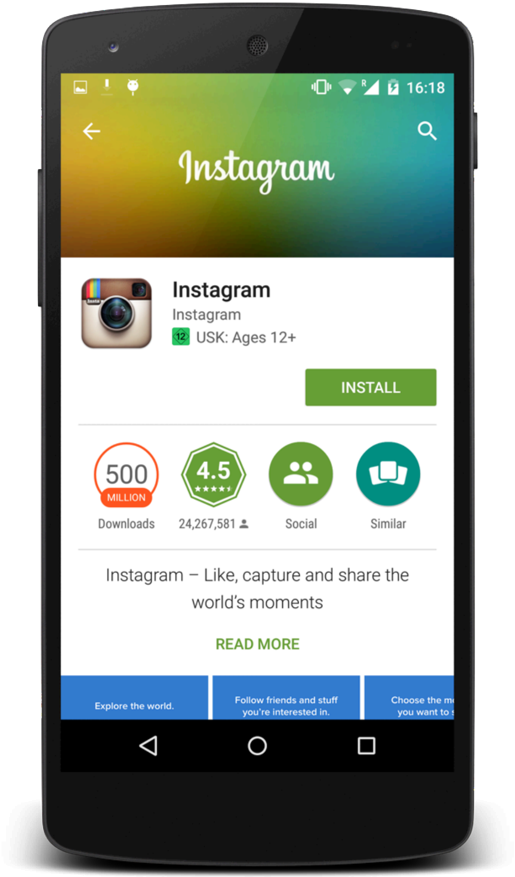
- Launching apps
  - Dedicated Activity
  - Shortcuts on Home Screen
  - Virtualized Launcher
- Installing/Updating apps



System Integration

- Launching apps
  - Dedicated Activity
  - Shortcuts on Home Screen
  - Virtualized Launcher

- Installing/Updating apps
  - Directly via App Stores



Instagram
Instagram
USK: Ages 12+

Instagram – Like, capture and share the world's moments

Performance

Middleware Microbenchmark

API Call	Native	On Boxify	Overhead
Open Camera	103.24 ms	104.48 ms	1.24 ms (1.2%)
Query Contacts	7.63 ms	8.55 ms	0.92 ms (12.0%)
Insert Contacts	66.49 ms	67.51 ms	1.02 ms (1.5%)
Delete Contacts	75.86 ms	76.81 ms	0.95 ms (0.9%)

Performance

Syscall Microbenchmark

System Call	Native	On Boxify	Overhead
`create`	47.2 µs	162.4 µs	115.2 µs
`open`	9.5 µs	122.7 µs	113.2 µs
`remove`	49.5 µs	159.6 µs	110.1 µs
`mkdir`	88.4 µs	199.4 µs	111.0 µs

Performance

Benchmark Tools

Tool	Native	On Boxify	Loss
CF Bench	16082 Pts	15376 Pts	4.3%
Geekbench	1649 Pts	1621 Pts	1.6%
PassMark	3674 Pts	3497 Pts	4.8%
Quadrant	7820 Pts	7532 Pts	3.6%

Discussion & Limitations

- Cancels Android‘s own access control checks
- Violates *Principle of Least Privilege*
- Full kernel attack surface available
- Presence of Boxify detectable

Use Cases

- Instantiate OS extensions at application layer
  - Fine-grained access control
  - Information flow control
  - Dual-persona, BYOD
  - Dynamic analysis
  - Automated testing
  - Xposed
  - …

Conclusion

- Lightweight application virtualization for stock Android
- No root or app modification required
- Low runtime performance overhead
- Wide range of applications

Thank you!