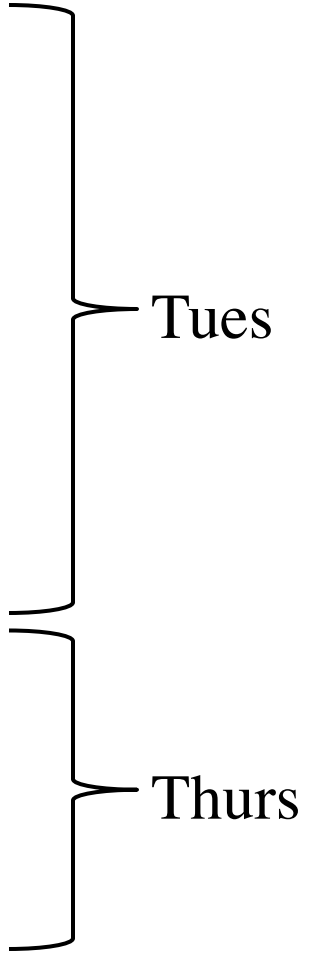
- **Diogo Mónica,**
-
-
-

-
-
  -
-
-
-
  -
  -
-
  -
  -


Tues
Thurs

ANDROID

-
  -
  -
  -
-
-

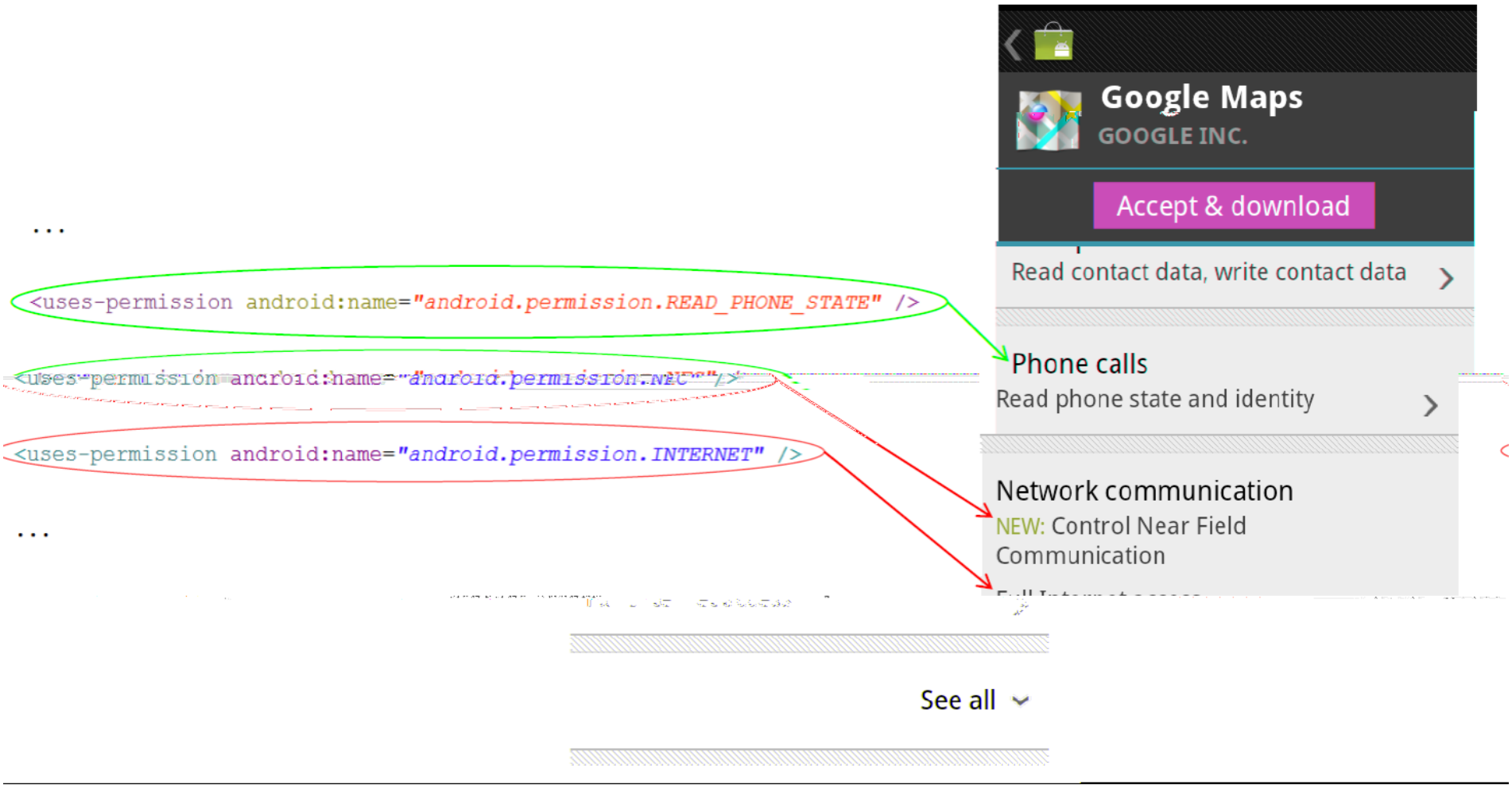
-
-
  -
-
  -
  -


Android Market


Google play

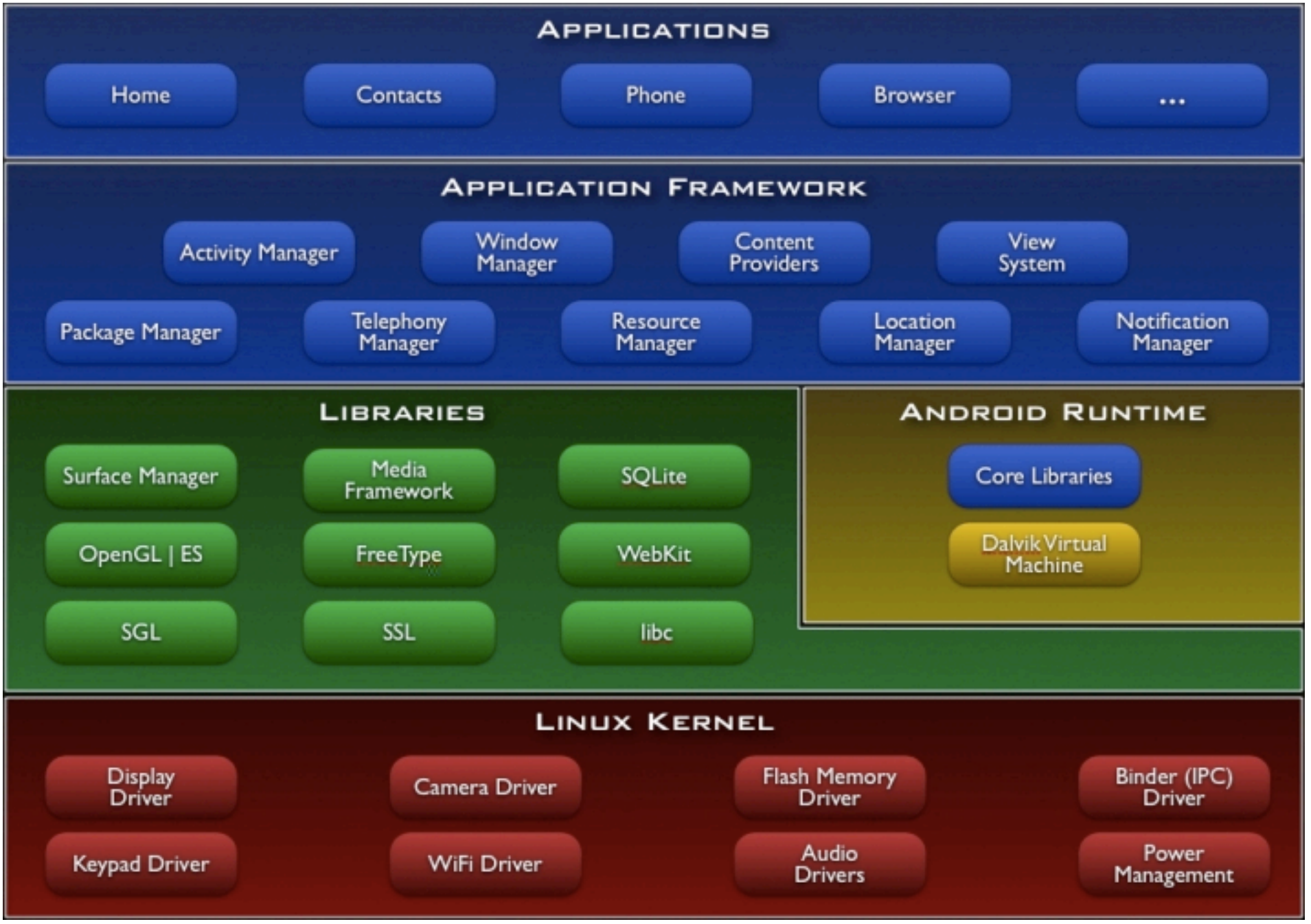
ANDROID PLATFORM

-
-
  -
  -
  -
  -

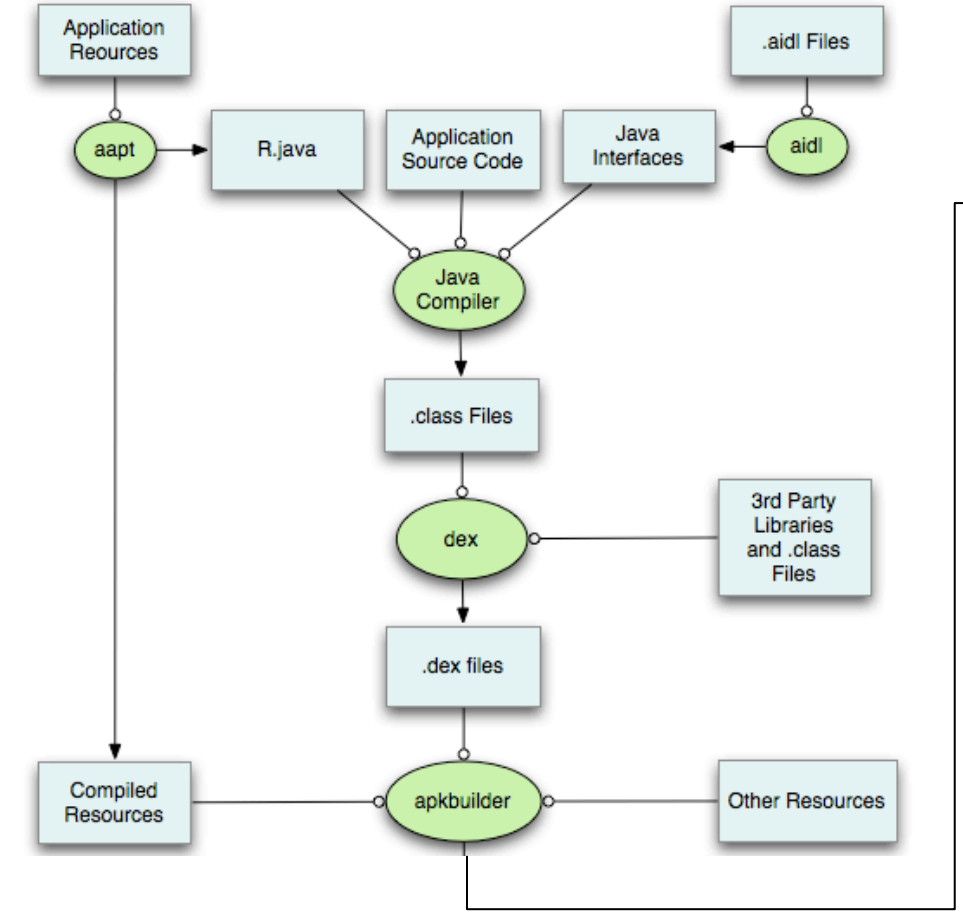


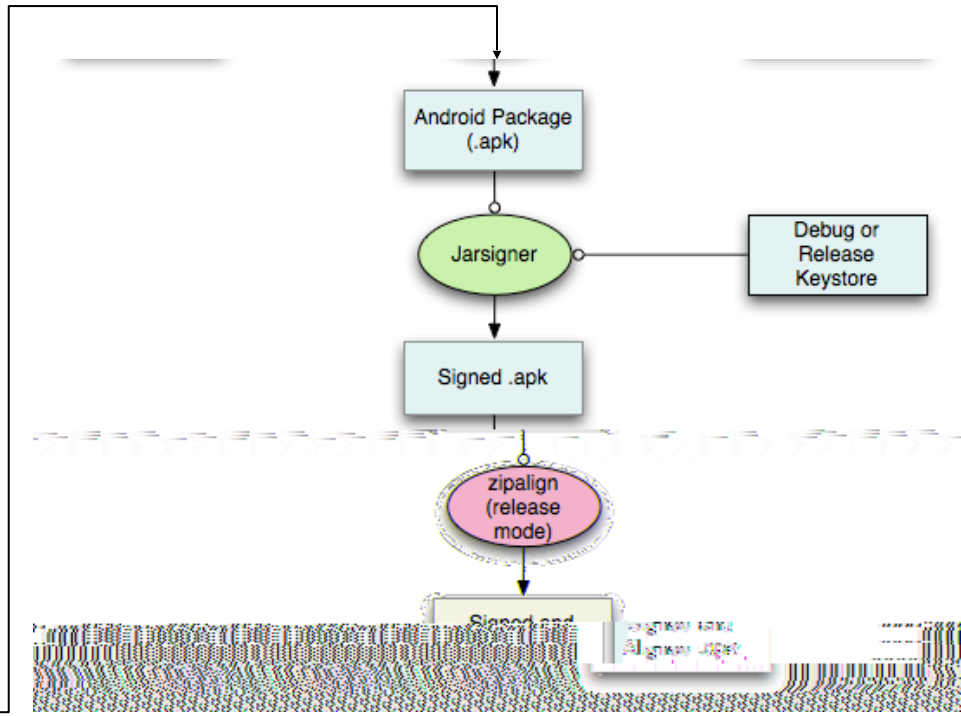
https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

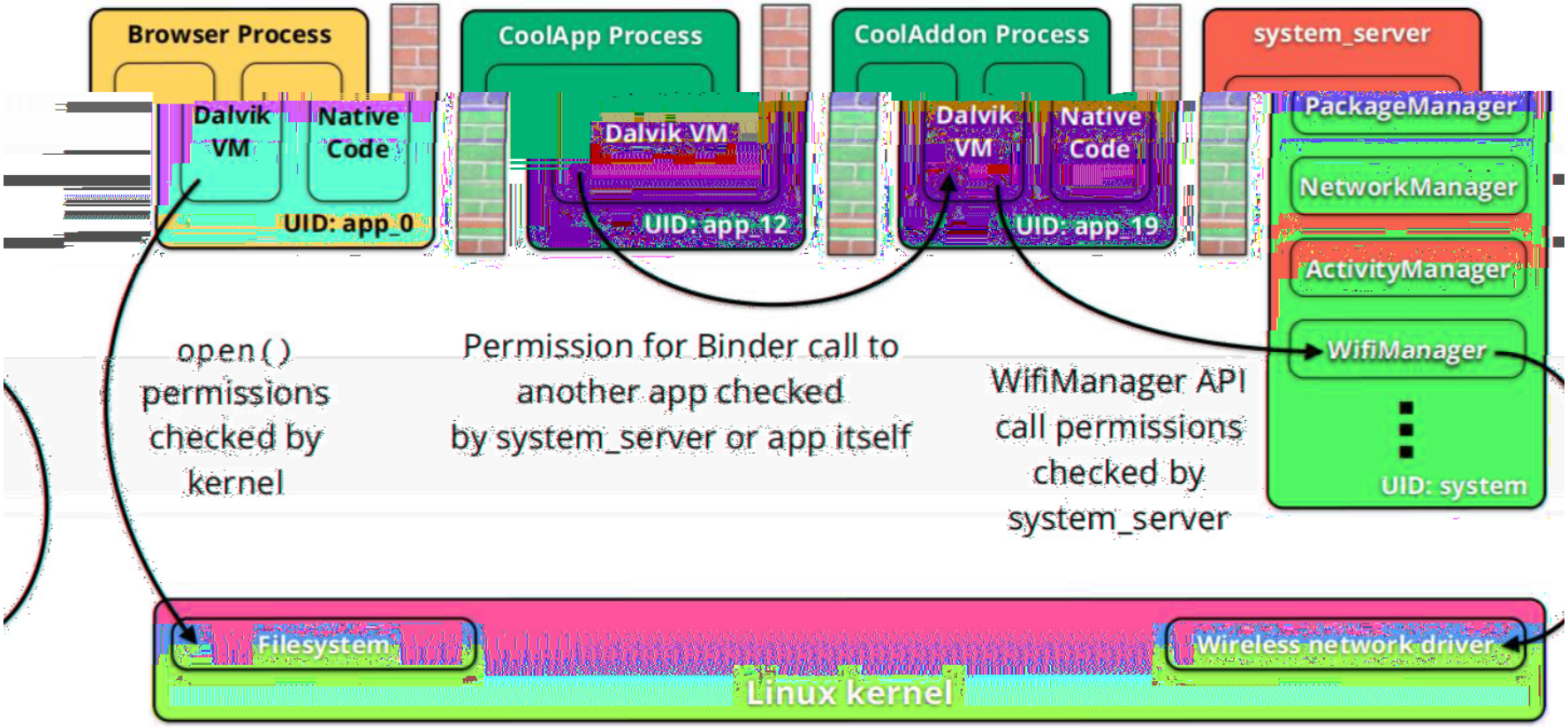
ANDROID PLATFORM


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

ANDROID PLATFORM

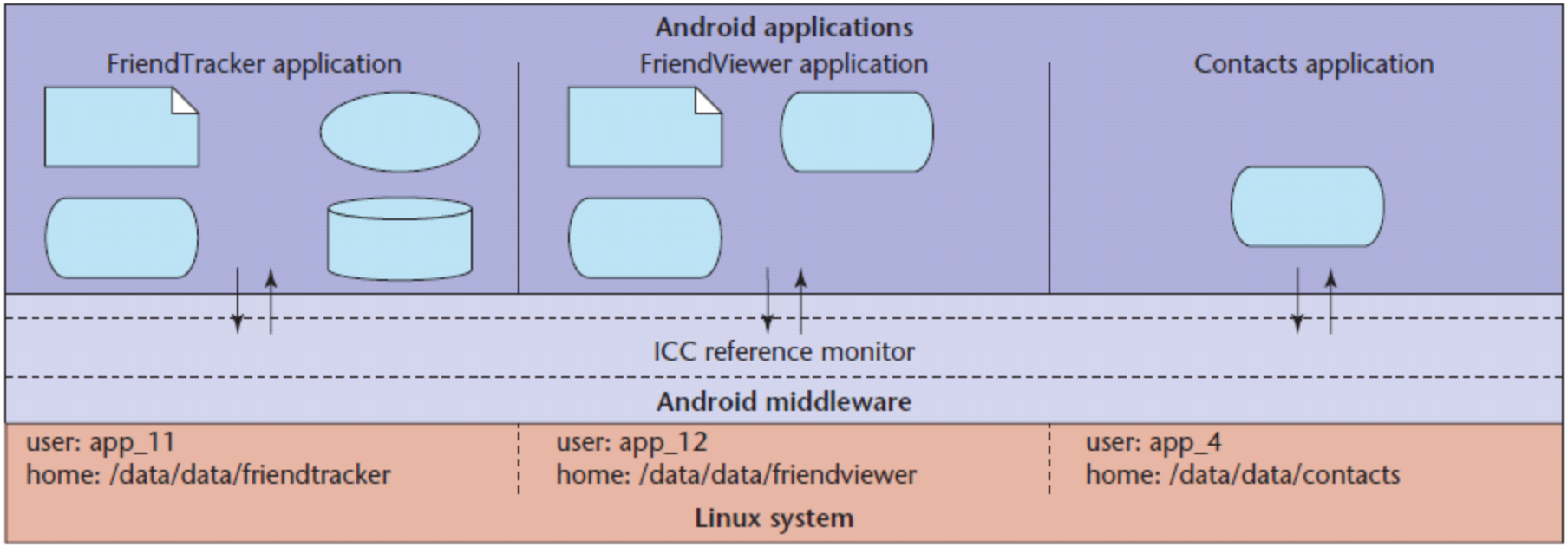

Application Reources
.aidl Files
aapt
R.java
Application Source Code
Java Interfaces
aidl
Java Compiler
.class Files
dex
3rd Party Libraries and .class Files
.dex files
Compiled Resources
apkbuilder
Other Resources


Android Package (.apk)
Jarsigner
Debug or Release Keystore
Signed .apk
zipalign (release mode)



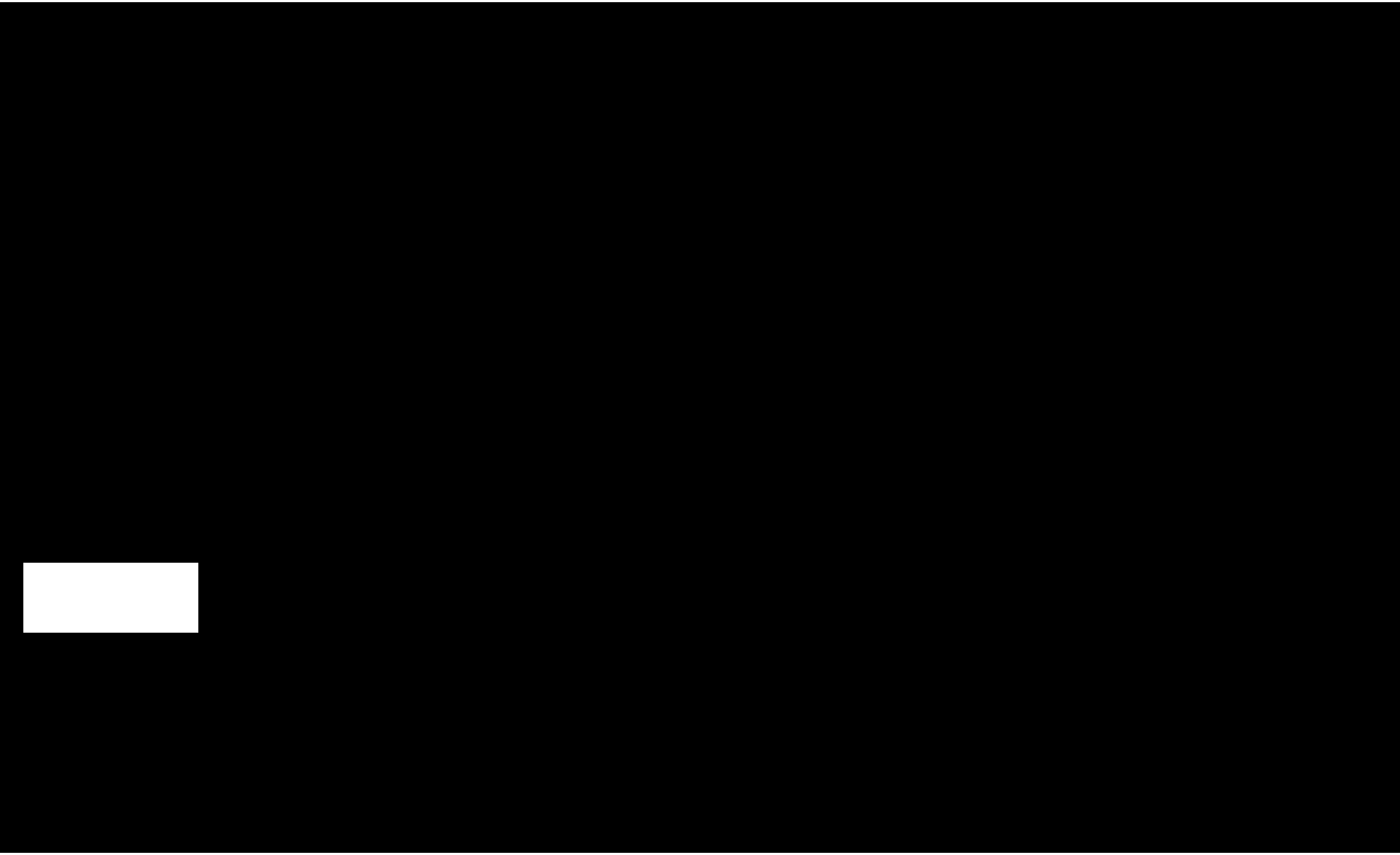
https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

-
-
  -
  -
  -
  -
-
  -
  -

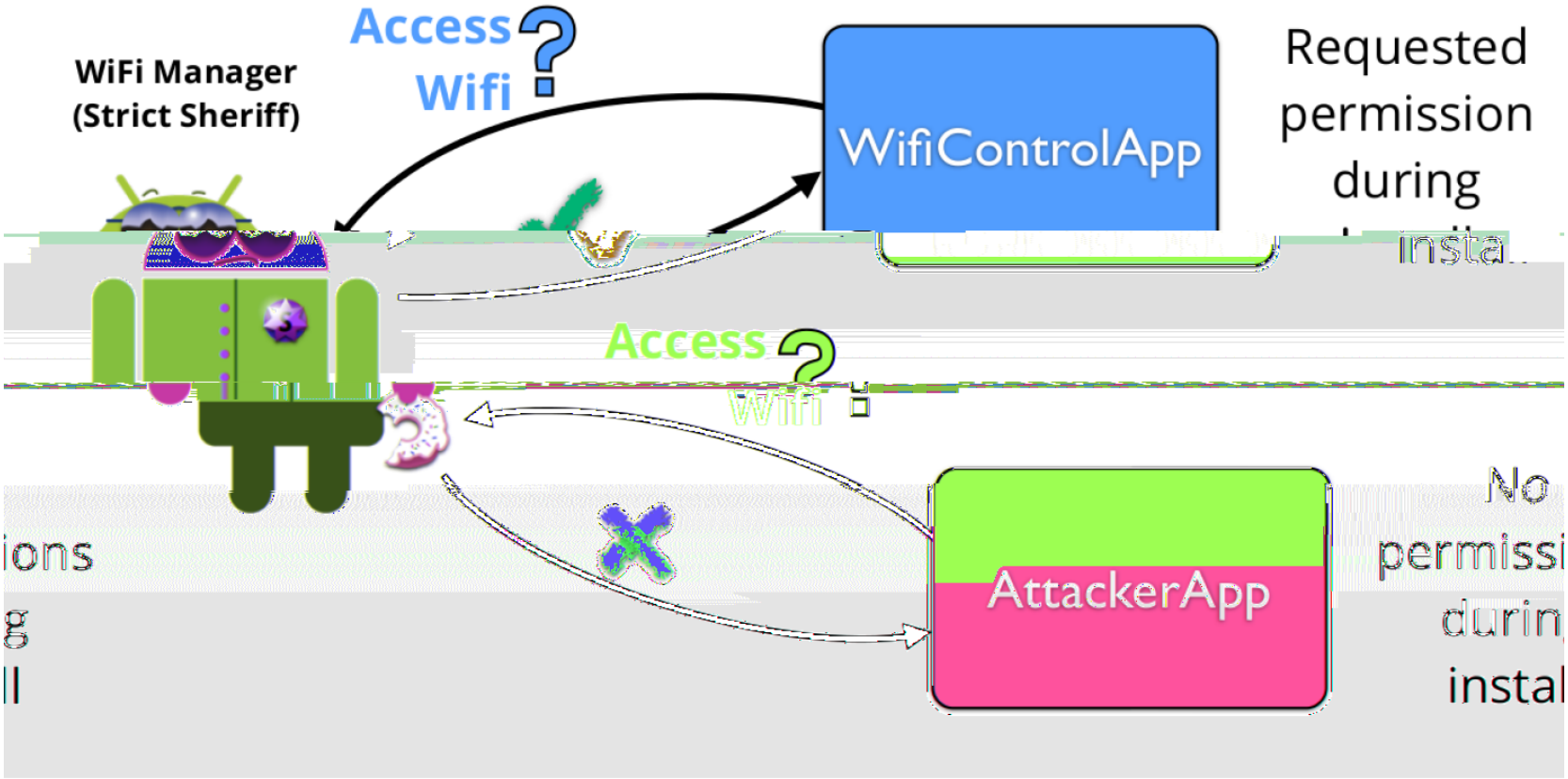


-
  -
  -

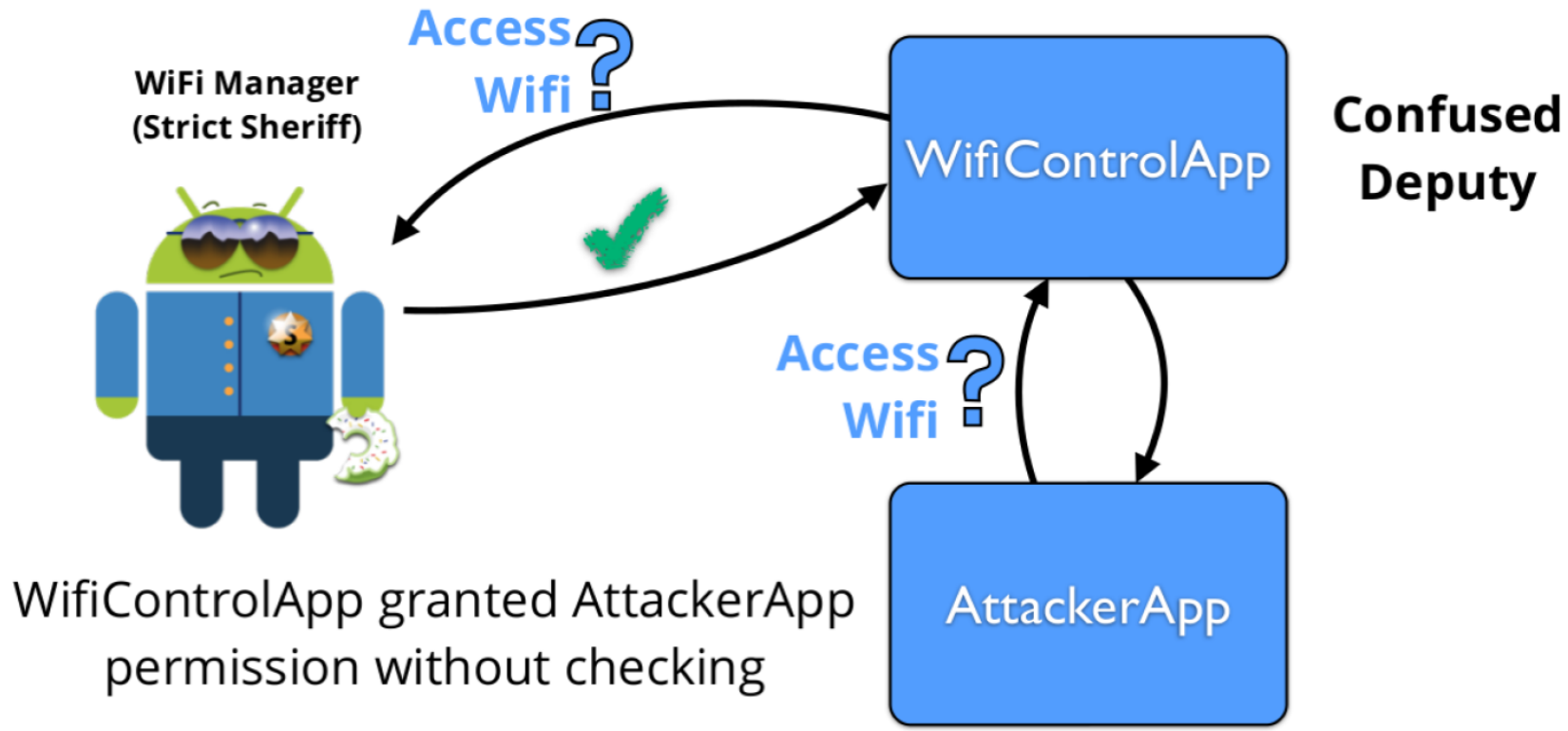
Source: Penn State group Android security paper



Source: Penn State group, Android security tutorial

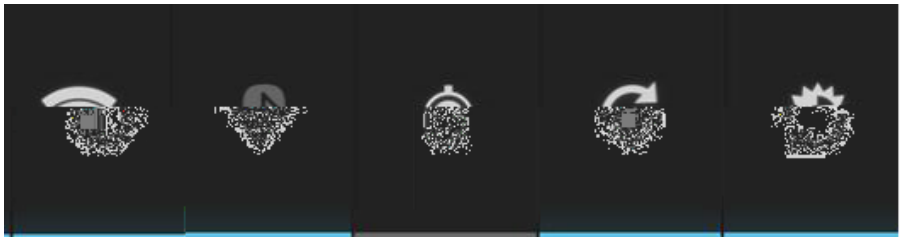


https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf



https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

-
-
  -
  -
  -
-
  -

- 
-
-
-

https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

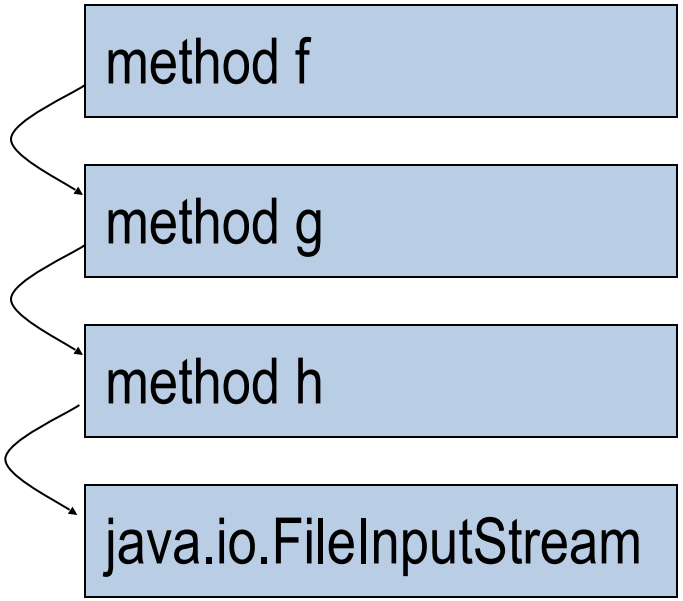
Version	Codename	API	Distribution
1.6	**Donut**	**4**	**0.10%**
2.1	**Eclair**	**7**	**1.50%**
2.2	**Froyo**	**8**	**3.20%**
2.3 - 2.3.2	Gingerbread	9	0.10%
2.3.3 - 2.3.7		10	36.40%
3.2	Honeycomb	13	0.10%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	25.60%
4.1.x	**Jelly Bean**	16	29.00%
4.2.x		**17**	**4.00%**

-
-

https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

-
  -
    -
    - *protection domain*
  -
    -
    -
  -
    -
    -

-
  -
  -
    -


method f
method g
method h
java.io.FileInputStream

ANDROID MALWARE

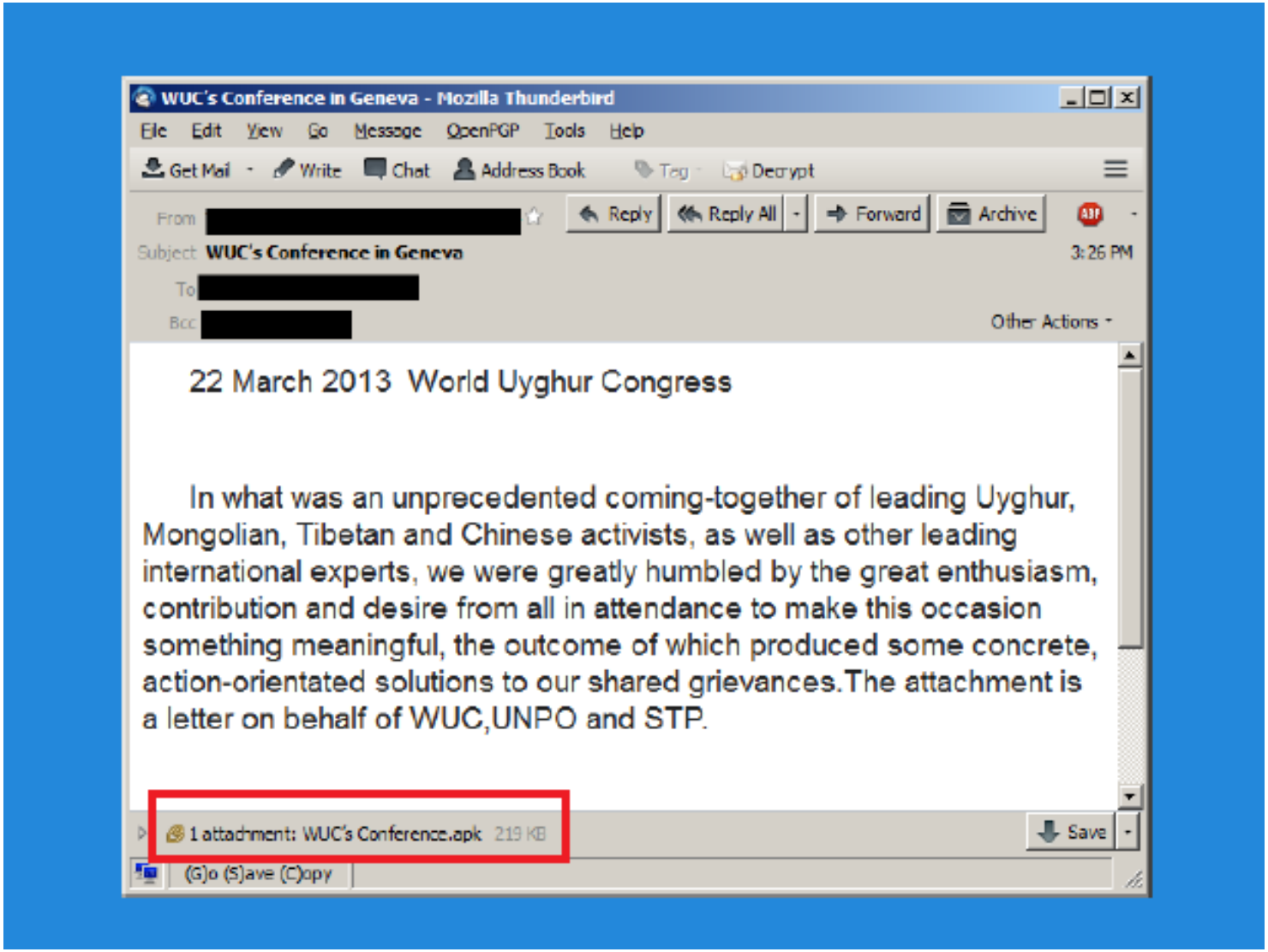
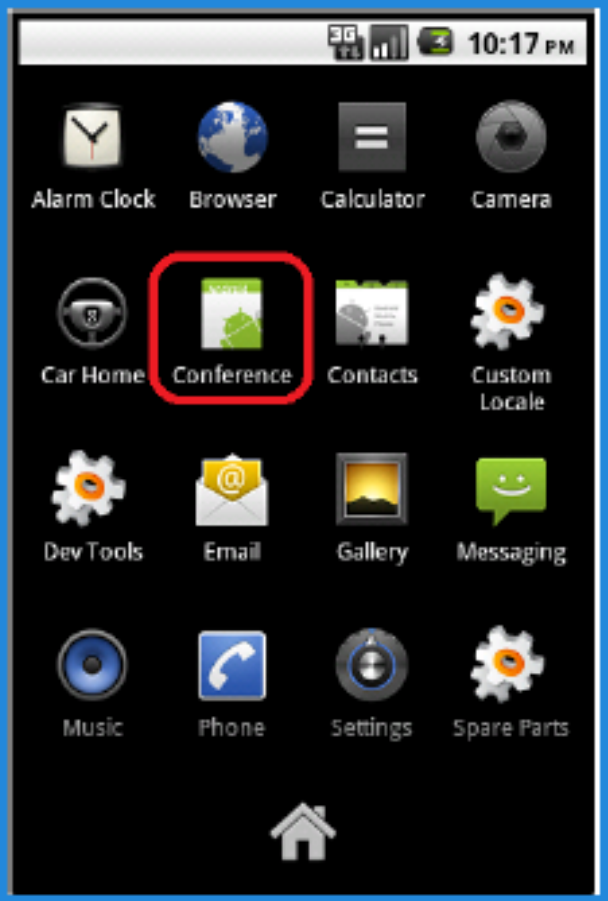


Image: Kaspersky Labs, https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack, March 26th, 2013



WUC's Conference in Geneva

On behalf of all at the Word Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia In what was an unprecedented

Image: Kaspersky Labs, https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack, March 26th, 2013

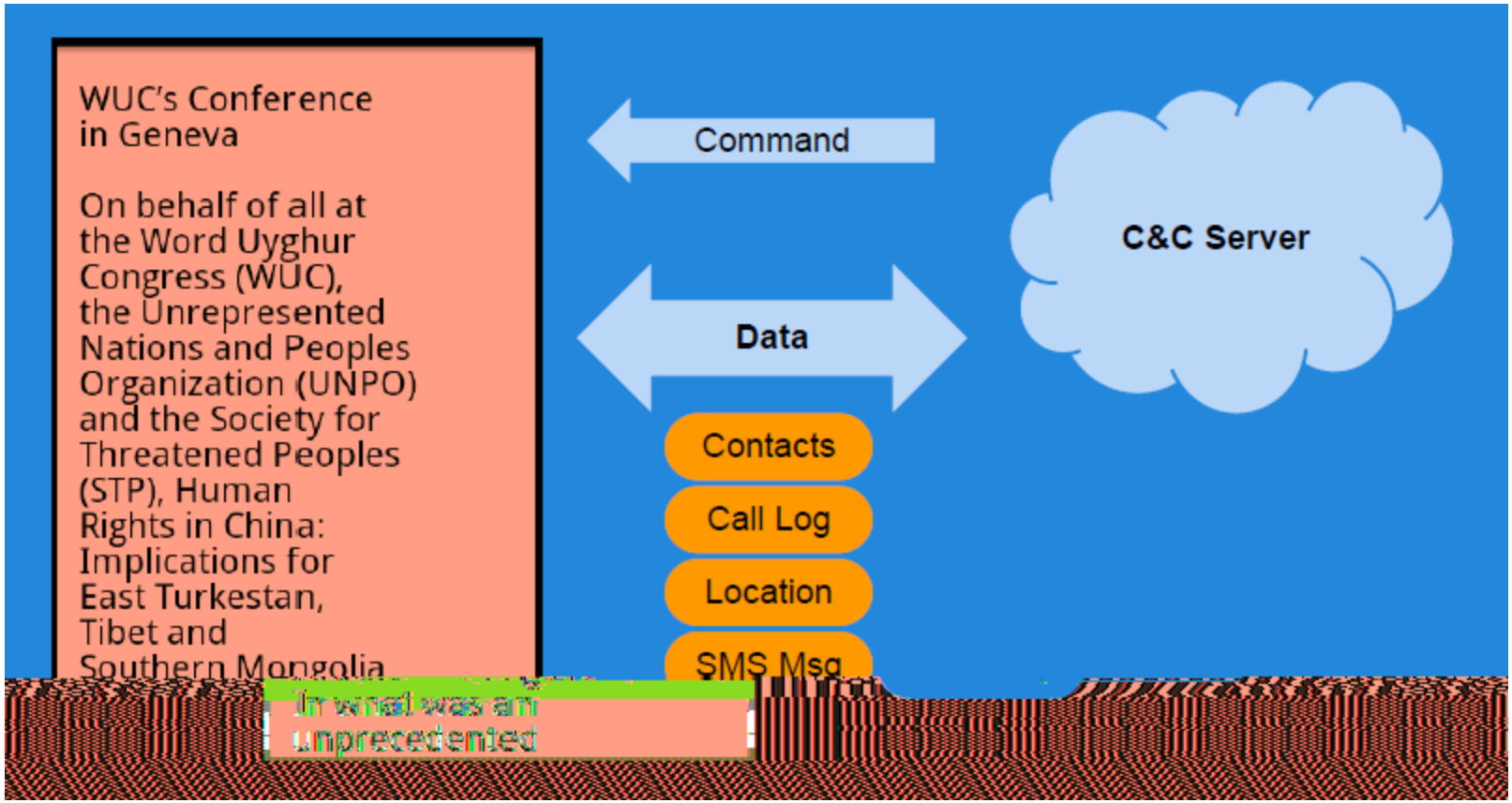
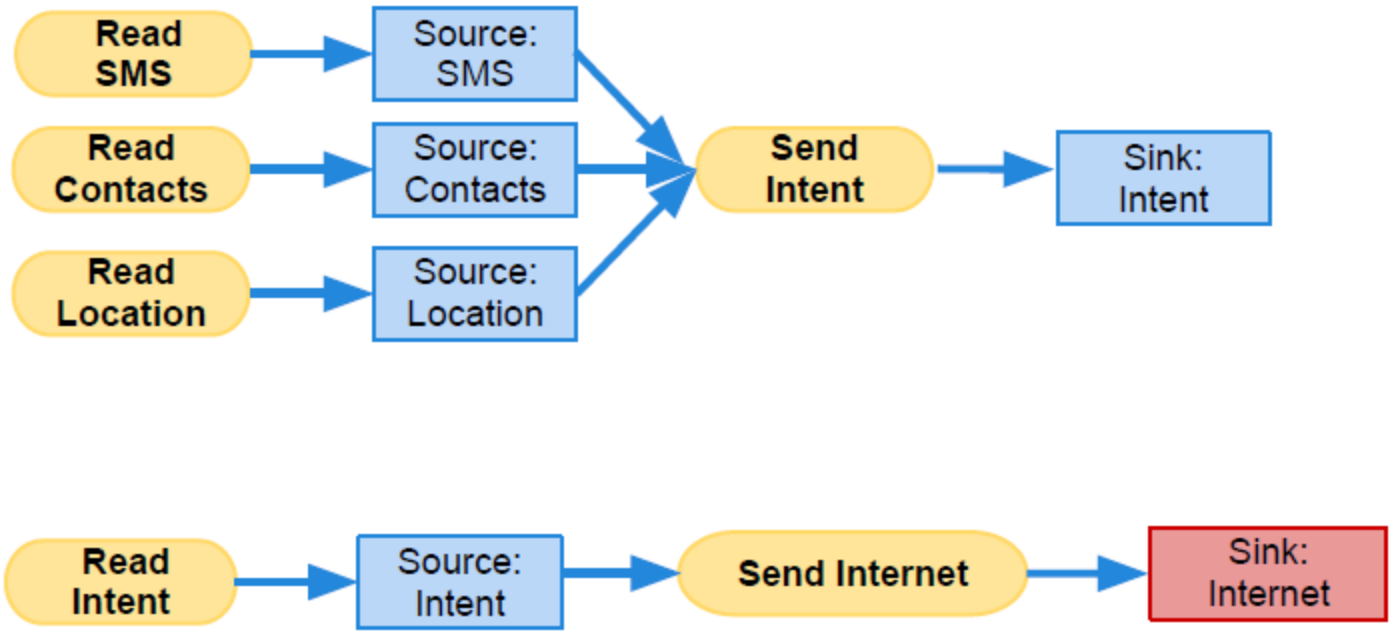


Image: Kaspersky Labs, https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack, March 26th, 2013

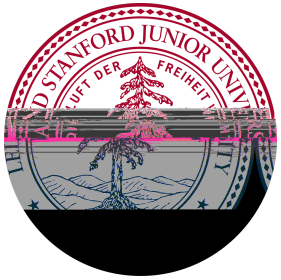
Chuli source-to-sink flows

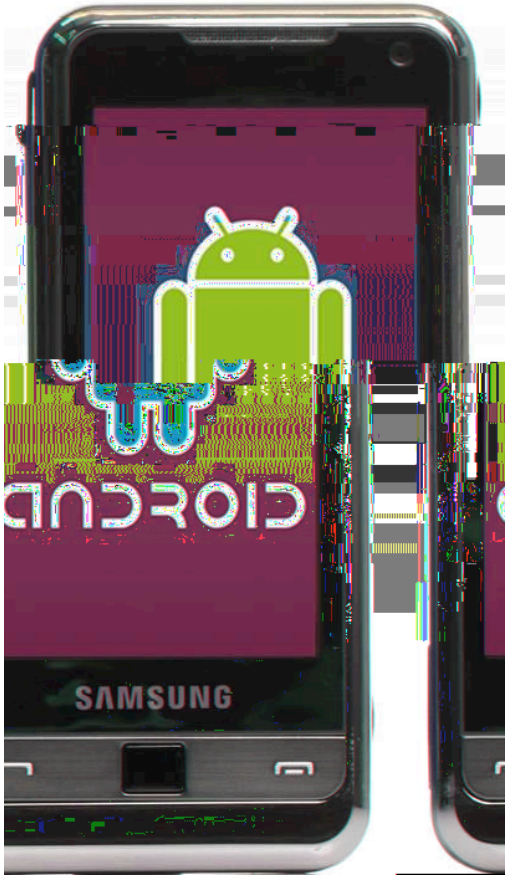


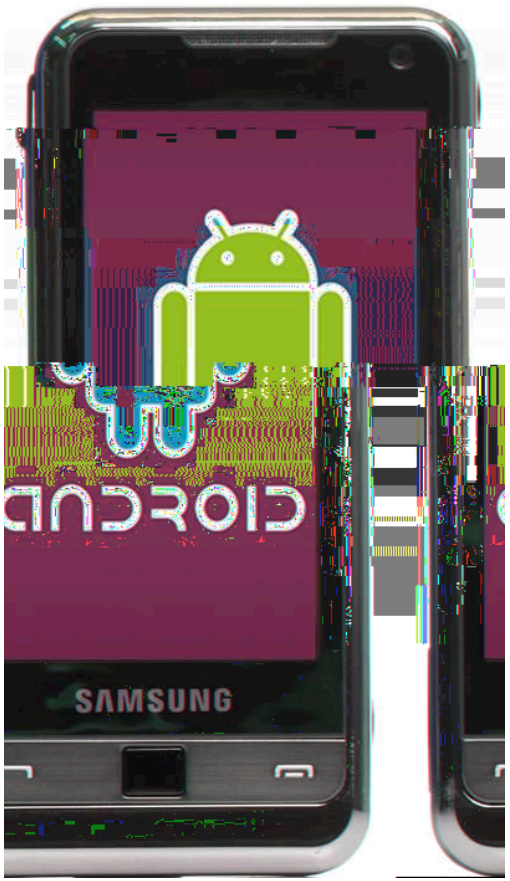
ANDROID WEB APPS

A Large-Scale Study of Mobile Web App Security

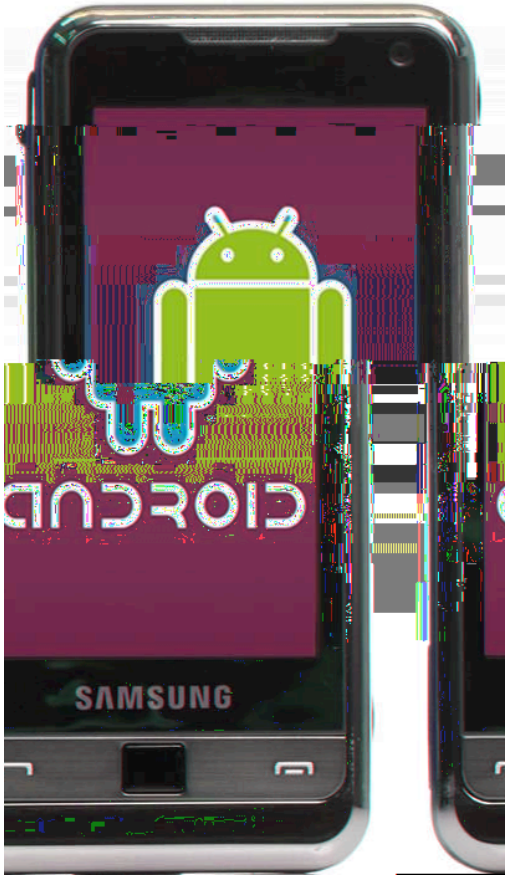
Patrick Mutchler, Adam Doupe,
John Mitchell, Chris Kruegel, Giovanni Vigna




SAMSUNG


android
SAMSUNG


No Service
12:44 PM
Monday
15
Messages
Calendar
Photos
Camera
Videos
Weather
Passbook
Notes
Reminders
Clock
Stocks
Newsstand
iTunes
App Store
Game Center
Settings
Speed Test
Sensorly
Maps
Phone
Mail
Safari
Music

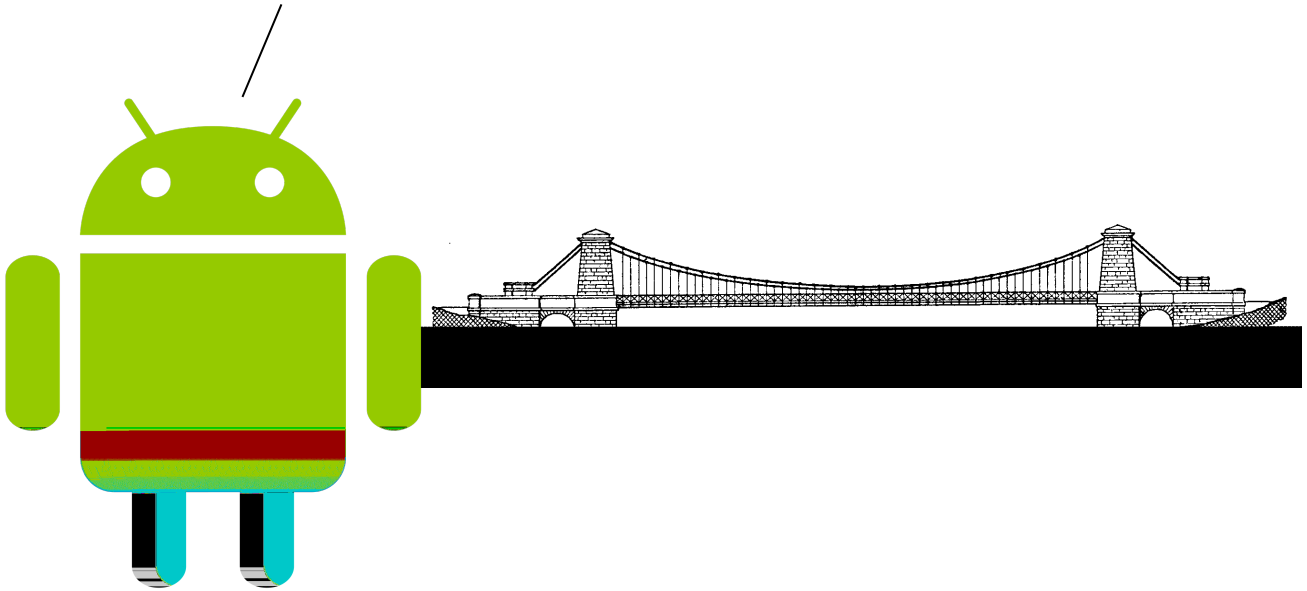

android
SAMSUNG


No Service
12:44 PM
Monday
15
Messages
Calendar
Photos
Camera
Videos
Weather
Passbook
Notes
Reminders
Clock
Stocks
Newsstand
iTunes
App Store
Game Center
Settings
Speed Test
Sensorly
Maps
Phone
Mail
Safari
Music

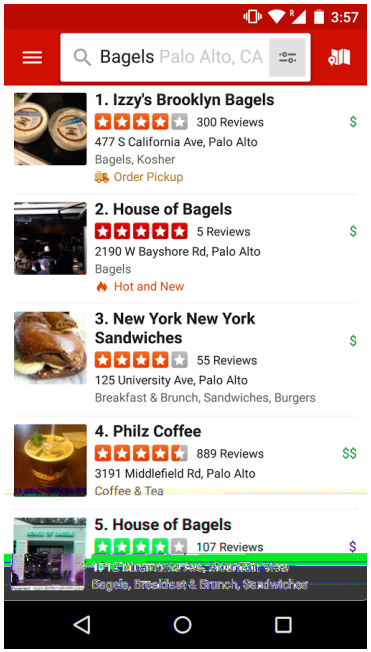

4G
12:38
4
Phone
1
9
SEATTLE SOUNDERS FC
Photos

- Mobile web app: embeds a fully functional web browser as a UI element

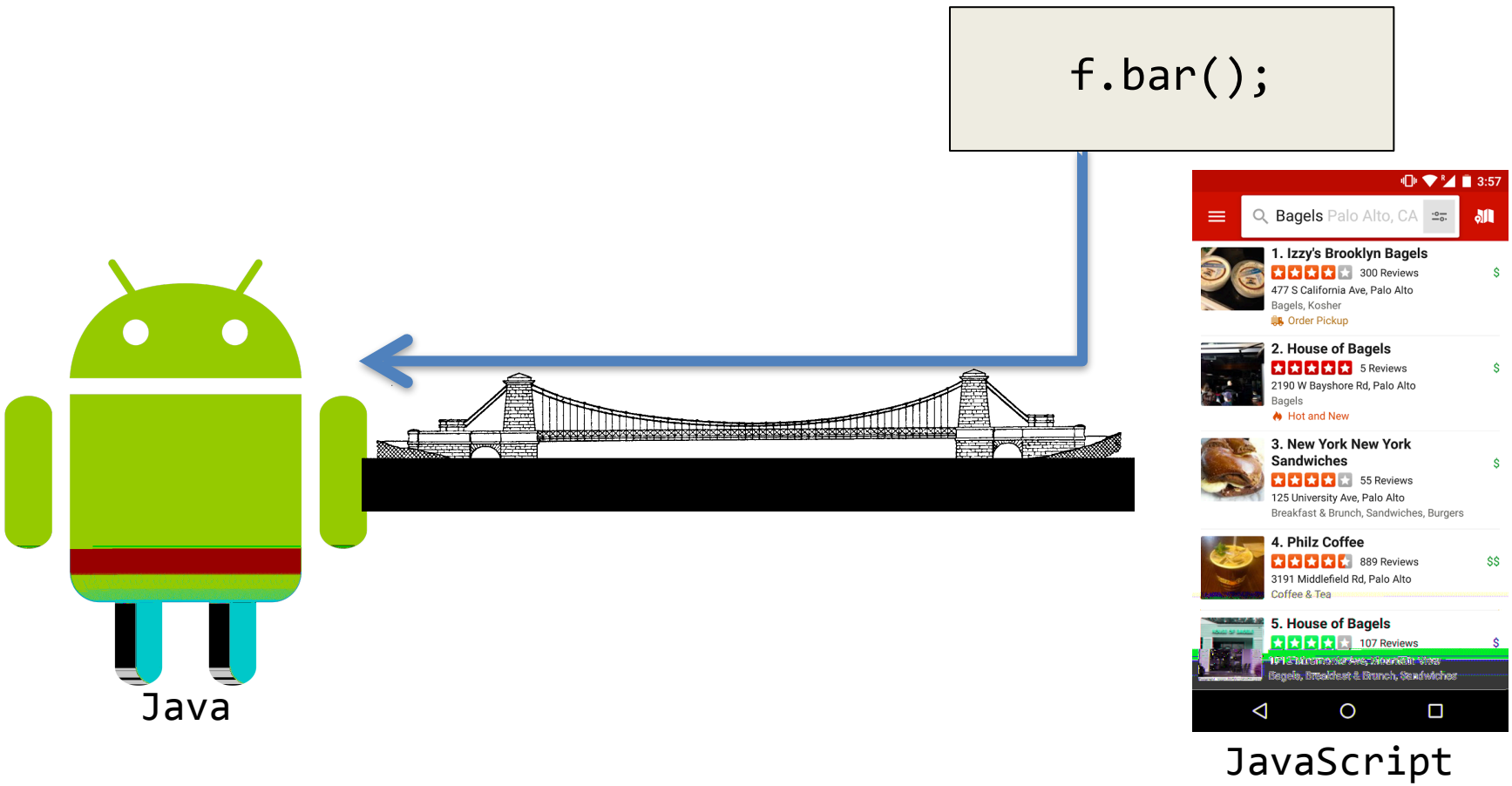
```
Obj foo = new Object();
addJavascriptInterface(foo, ‘f’);
```



Java

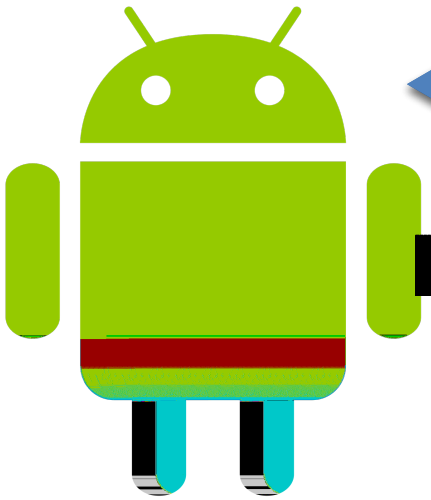


JavaScript

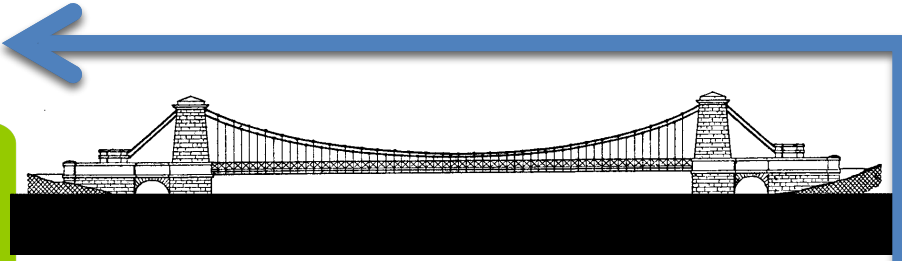

f.bar();
Java
Bagels Palo Alto, CA
1. Izzy's Brooklyn Bagels
300 Reviews
$
477 S California Ave, Palo Alto
Bagels, Kosher
Order Pickup
2. House of Bagels
5 Reviews
$
2190 W Bayshore Rd, Palo Alto
Bagels
Hot and New
3. New York New York Sandwiches
55 Reviews
$
125 University Ave, Palo Alto
Breakfast & Brunch, Sandwiches, Burgers
4. Philz Coffee
889 Reviews
$$
3191 Middlefield Rd, Palo Alto
Coffee & Tea
5. House of Bagels
107 Reviews
$
Bagels, Breakfast & Brunch, Sandwiches
JavaScript

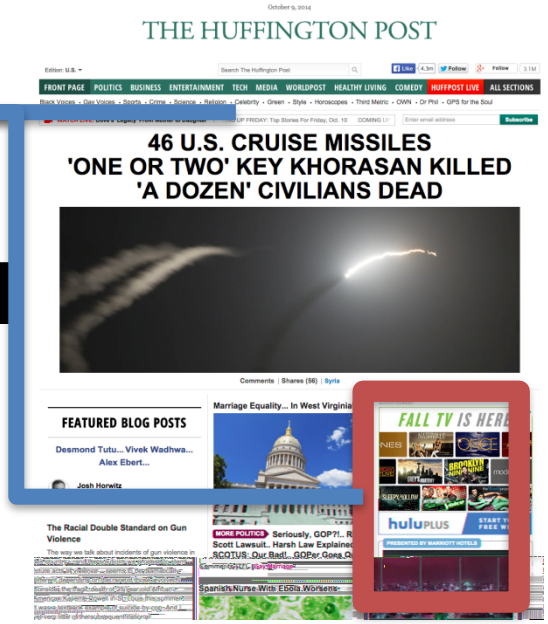

October 9, 2014
THE HUFFINGTON POST
Edition: U.S.
Search The Huffington Post
Like 4.3m
Follow
Follow 3.1M
FRONT PAGE POLITICS BUSINESS ENTERTAINMENT TECH MEDIA WORLDPOST HEALTHY LIVING COMEDY HUFFPOST LIVE ALL SECTIONS
Black Voices • Gay Voices • Sports • Crime • Science • Religion • Celebrity • Green • Style • Horoscopes • Third Metric • OWN • Dr Phil • GPS for the Soul
WATCH LIVE: Dove's 'Legacy' From Mother to Daughter
COMING UP FRIDAY: Top Stories For Friday, Oct. 10
COMING UP
Enter email address
Subscribe
46 U.S. CRUISE MISSILES
'ONE OR TWO' KEY KHORASAN KILLED
'A DOZEN' CIVILIANS DEAD
Isolated in Browser
Comments | Shares (56) | Syria
FEATURED BLOG POSTS
Desmond Tutu... Vivek Wadhwa...
Alex Ebert...
Josh Horwitz
The Racial Double Standard on Gun Violence
The way we talk about incidents of gun violence in this country -- and the solutions we propose to stem future acts of violence -- seems to be dramatically different depending on the race of those involved. Consider the tragic death of 25 year-old African-American Kajama Powell in St. Louis this summer.
Marriage Equality... In West Virginia
MORE POLITICS Seriously, GOP?!.. R
Scott Lawsuit.. Harsh Law Explaine
SCOTUS: Our Bad!.. GOPer Goes Q
et
Comments (77) | Gay Marriage
Spanish Nurse With Ebola Worsens
FALL TV IS HERE
NASHVILLE
ONCE
GREY'S ANATOMY
BROOKLYN NINE-NINE
SLEEPY HOLLOW
the Mindy project
PRESENTED BY MARRIOTT HOTELS

```
f.bar();
```



Java





JavaScript

-
-
-
-

1. Loading untrusted web content
2. Leaking URLs to foreign apps
3. Exposing state changing navigation to foreign apps

1. Loading untrusted web content

2. Leaking URLs to foreign apps

3. Exposing state changing navigation to foreign apps

“You should restrict the web-pages that can load inside your WebView with a whitelist.”

- Facebook

“…only loading content from trusted sources into WebView will help protect users.”

- Adrian Ludwig, Google

1. Navigate to untrusted content

```
// In app code
myWebView.loadUrl(“foo.com”);
```

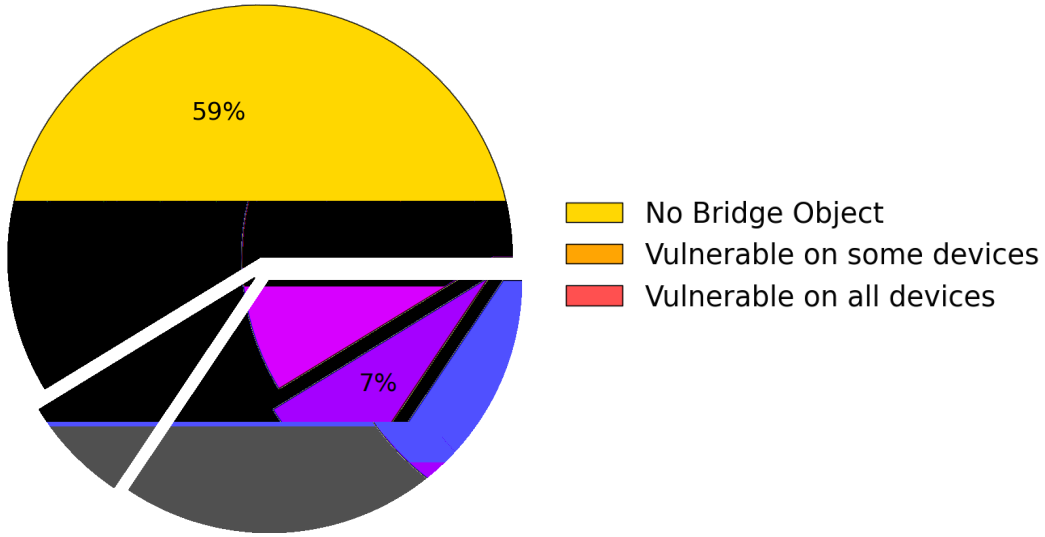
```
// In app code
myWebView.load(“foo.com”);

<!-- In HTML -->
<a href=“foo.com”>click!</a>
```

```
// In app code
myWebView.load(“foo.com”);

<!-- In HTML -->
<a href=“foo.com”>click!</a>

<!-- More HTML -->
<iframe src=“foo.com”/>
```

```
// In app code
myWebView.loadUrl(“foo.com”);

<!-- In HTML -->
<a href=“foo.com”>click!</a>

<!-- More HTML -->
<iframe src=“foo.com”/>

// In JavaScript
window.location = “foo.com”;
```

```
public boolean shouldOverrideUrlLoading(
        WebView view, String url){

    // False -> Load URL in WebView
    // True  -> Prevent the URL load


}
```

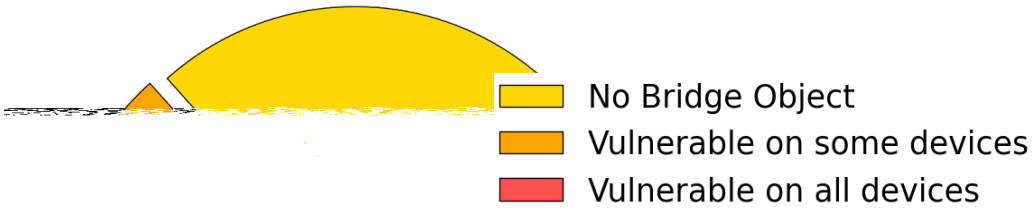
```
public boolean shouldOverrideUrlLoading(
        WebView view, String url){

    String host = new URL(url).getHost();
    if(host.equals(“stanford.edu”))
        return false;
    log(“Overrode URL: ” + url);
    return true;
}
```


59%
7%
No Bridge Object
Vulnerable on some devices
Vulnerable on all devices

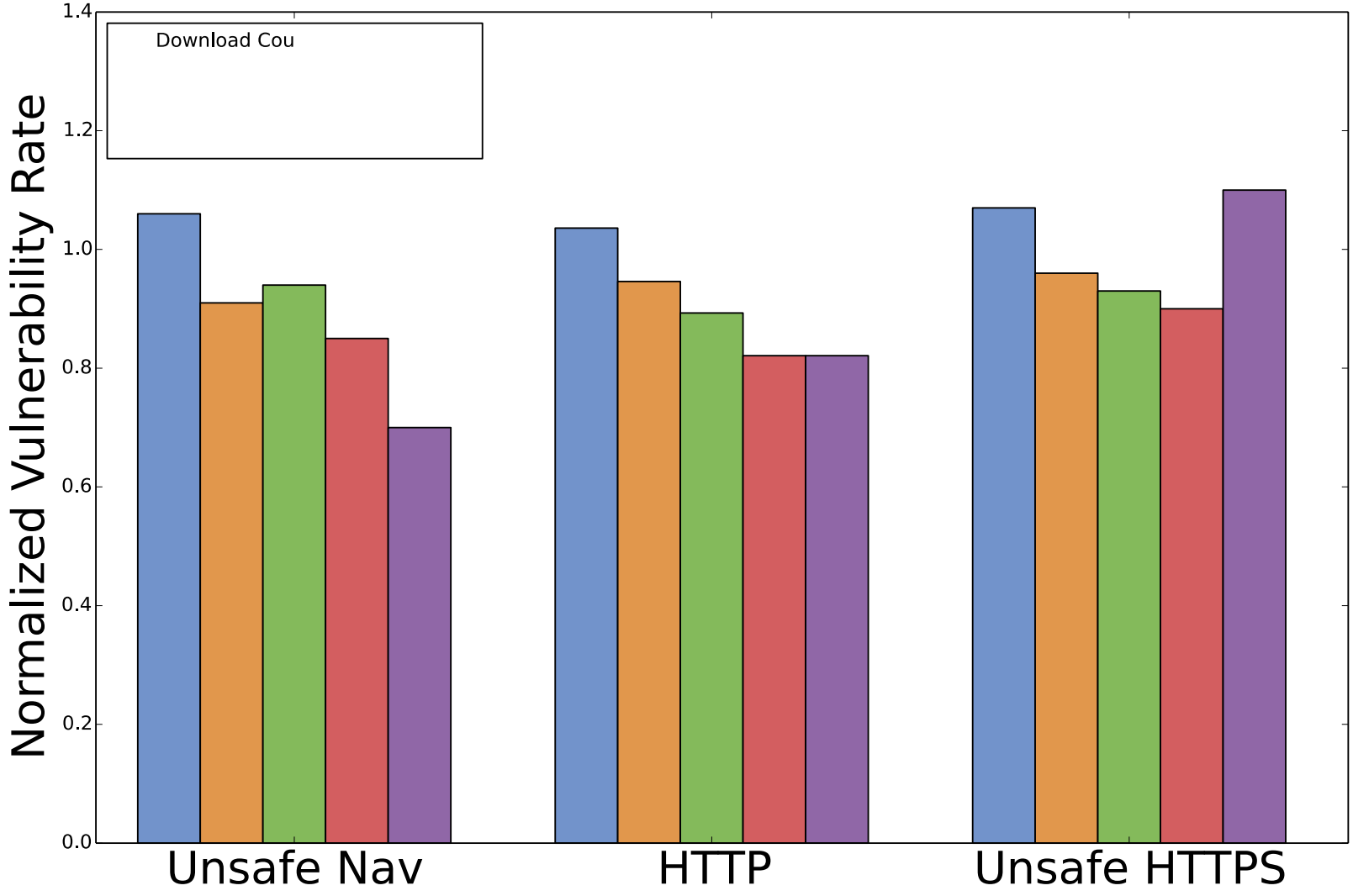
onReceivedSslError

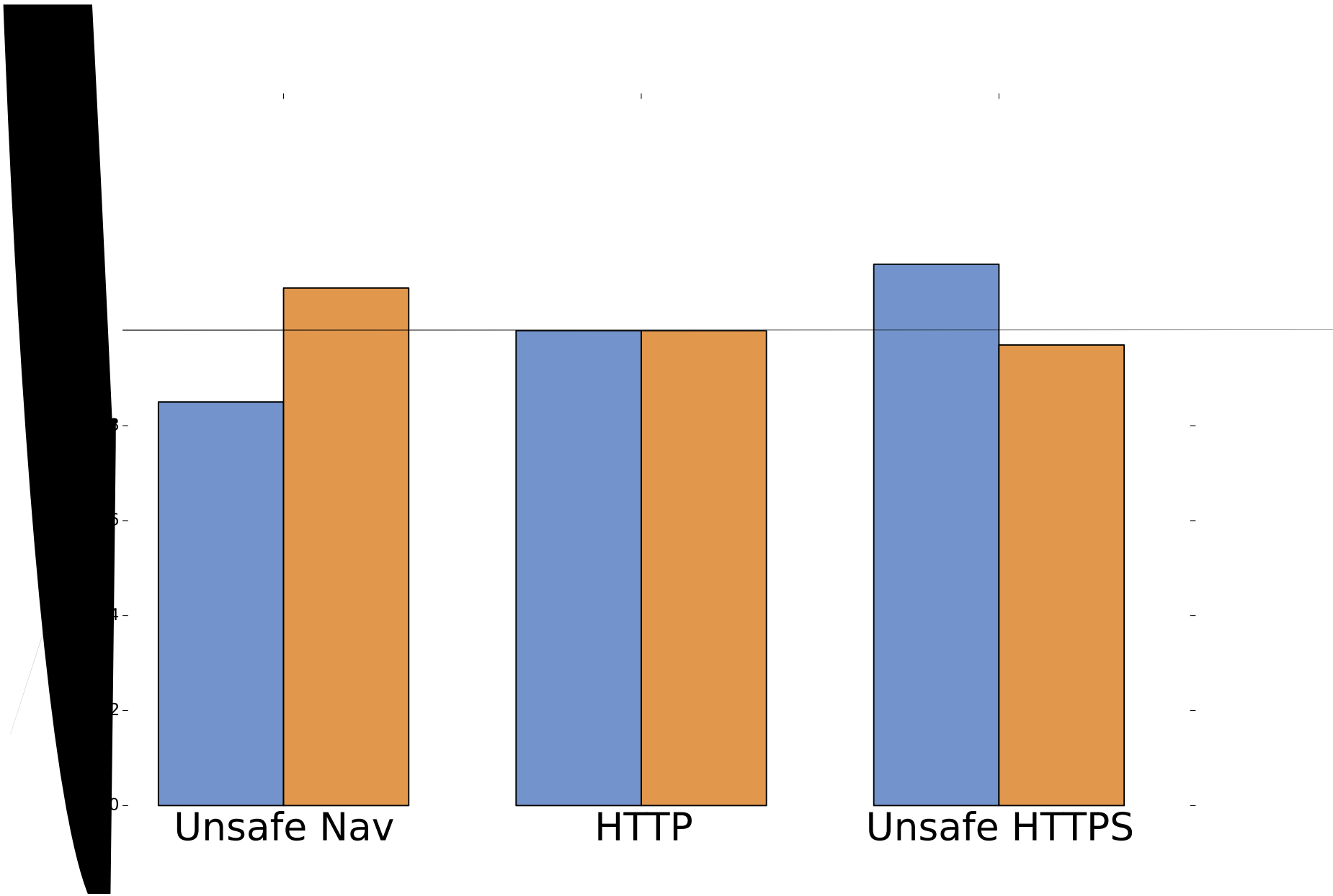
1. handler.proceed()
2. handler.cancel()
3. view.loadUrl(...)

- `onReceivedSslError`
- **must**



Vulnerability	% Relevant	% Vulnerable
Unsafe Nav	15	34
HTTP	40	56
Unsafe HTTPS	27	29


Download Cou
Normalized Vulnerability Rate
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
Unsafe Nav
HTTP
Unsafe HTTPS


Unsafe Nav
HTTP
Unsafe HTTPS

Libraries

29%
unsafe nav

51%
HTTP

53%
unsafe HTTPS

Mobile Web App Feature	% Apps
JavaScript Enabled	97
JavaScript Bridge	36
shouldOverrideUrlLoading	94
shouldInterceptRequest	47
onReceivedSslError	27
postUrl	2
Custom URL Patterns	10

Vuln	% Relevant	% Vulnerable
Unsafe Navigation	15	34
Unsafe Retrieval	40	56
Unsafe SSL	27	29
Exposed POST	2	7
Leaky URL	10	16

Takeaways

- Apps must not load untrusted content into WebViews
- Able to identify violating apps using static analysis
- Vulnerabilities are present in the entire app ecosystem

ANDROID VERSIONING

Target Fragmentation in Android Apps

Patrick Mutchler
John Mitchell

Yeganeh Safaei
Adam Doupe

Takeaways

Android apps can run using outdated OS behavior

- The large majority of Android apps do this
- Including popular and well maintained apps

Outdated security code invisibly permeates the app ecosystem

- “Patched” security vulnerabilities still exist in the wild
- “Risky by default” behavior is widespread

Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences

Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences

6.0

.

- Android Developer Reference

6.0 ***and your app's target SDK is 6.0 or higher***

.

- Android Developer Reference

`targetSdkVersion`, ***may enable compatibility behaviors***

.

- Android Developer Reference

Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences

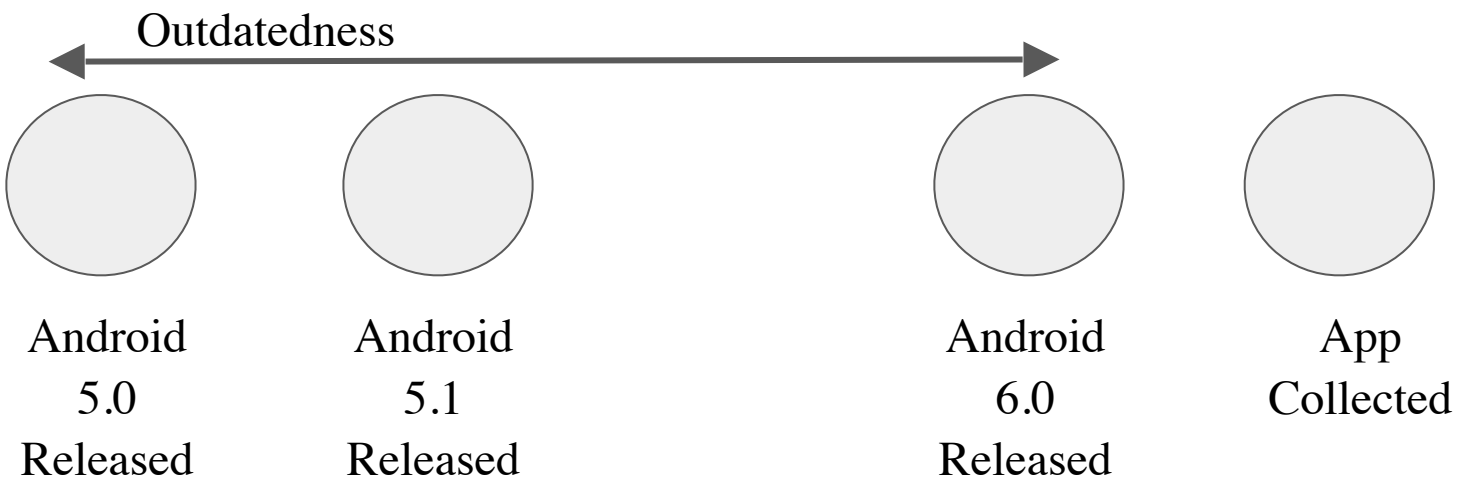
Dataset

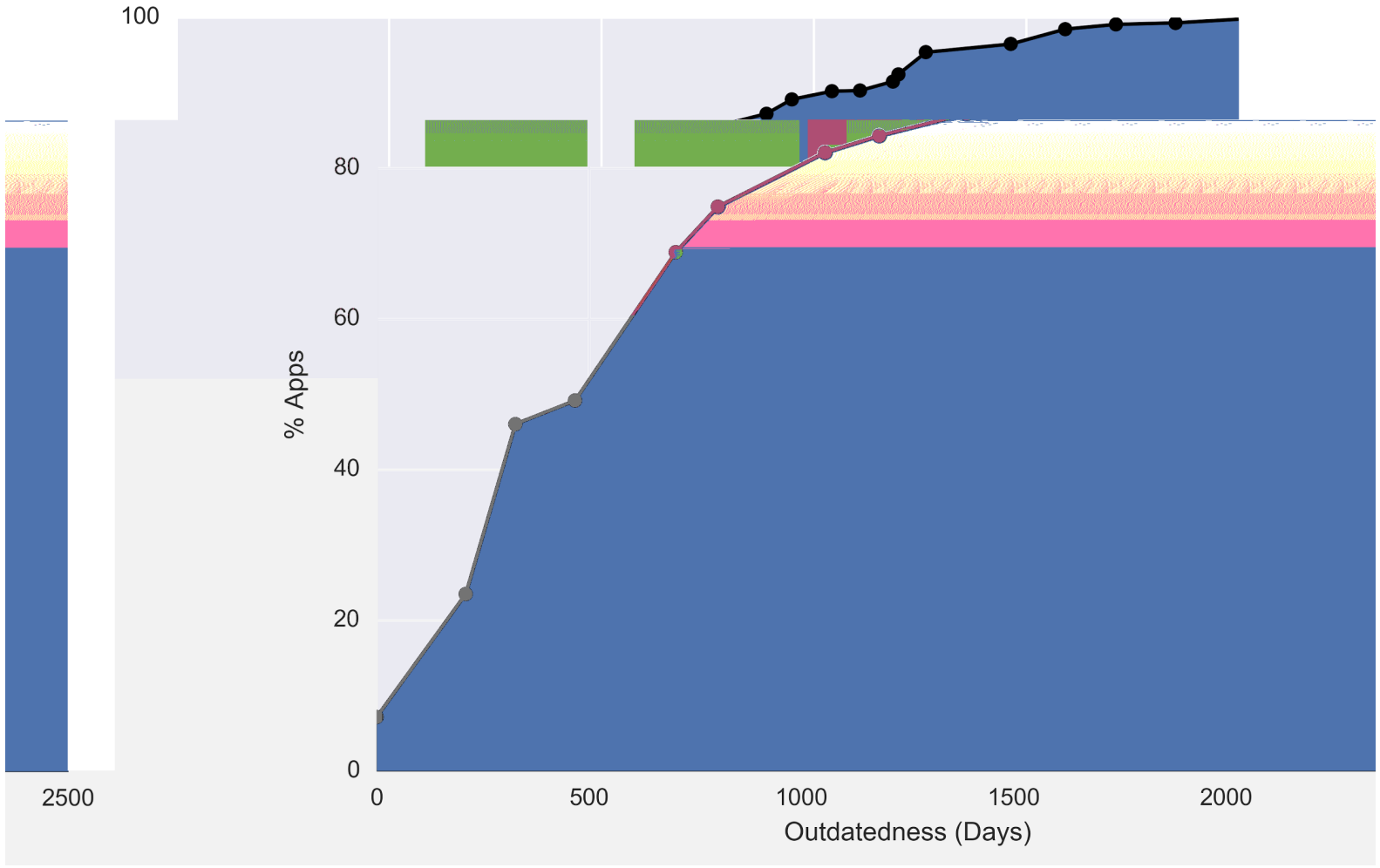
1,232,696 Android Apps

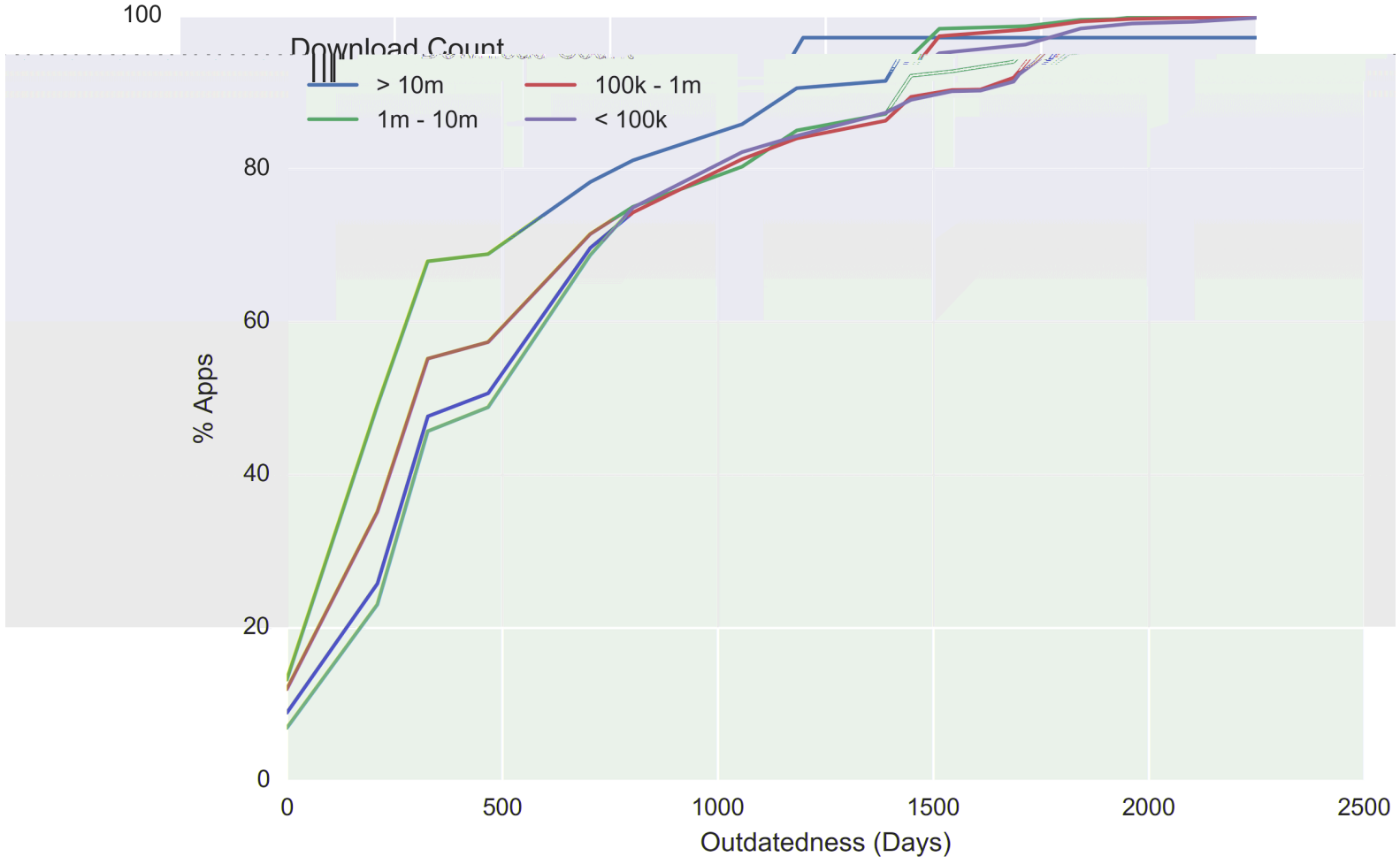
Popularity, Category, Update, and Developer metadata

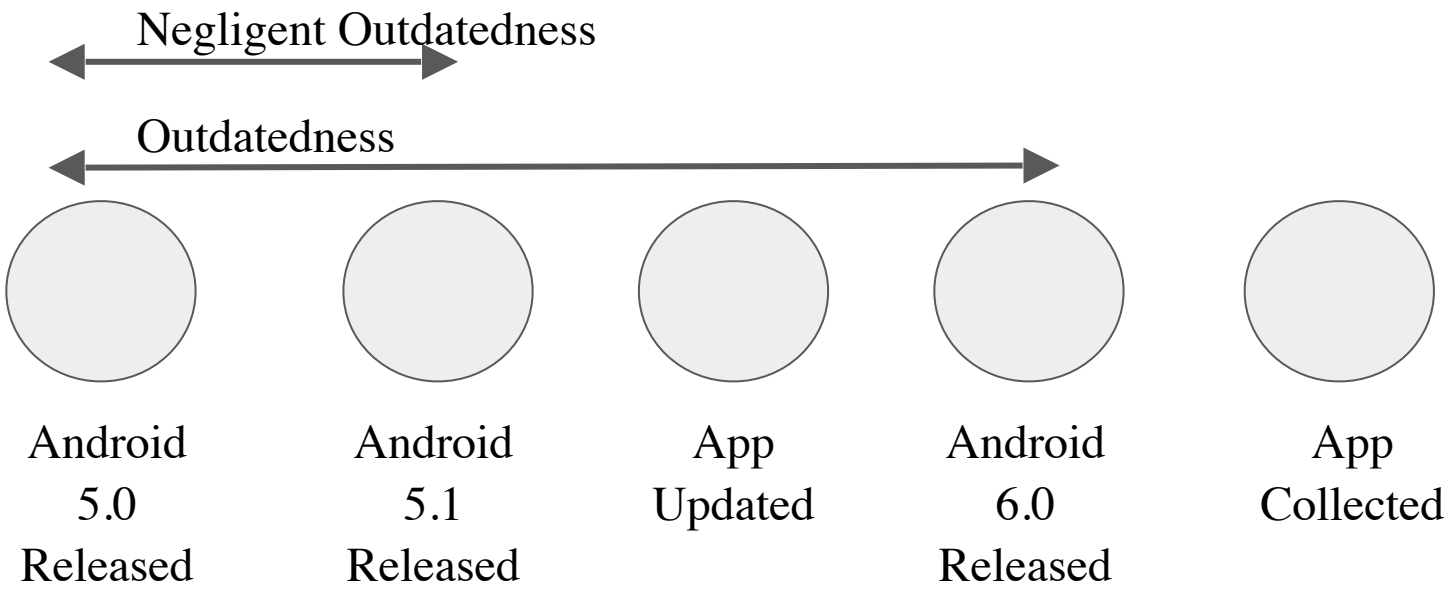
Collected between May 2012 and Dec 2015

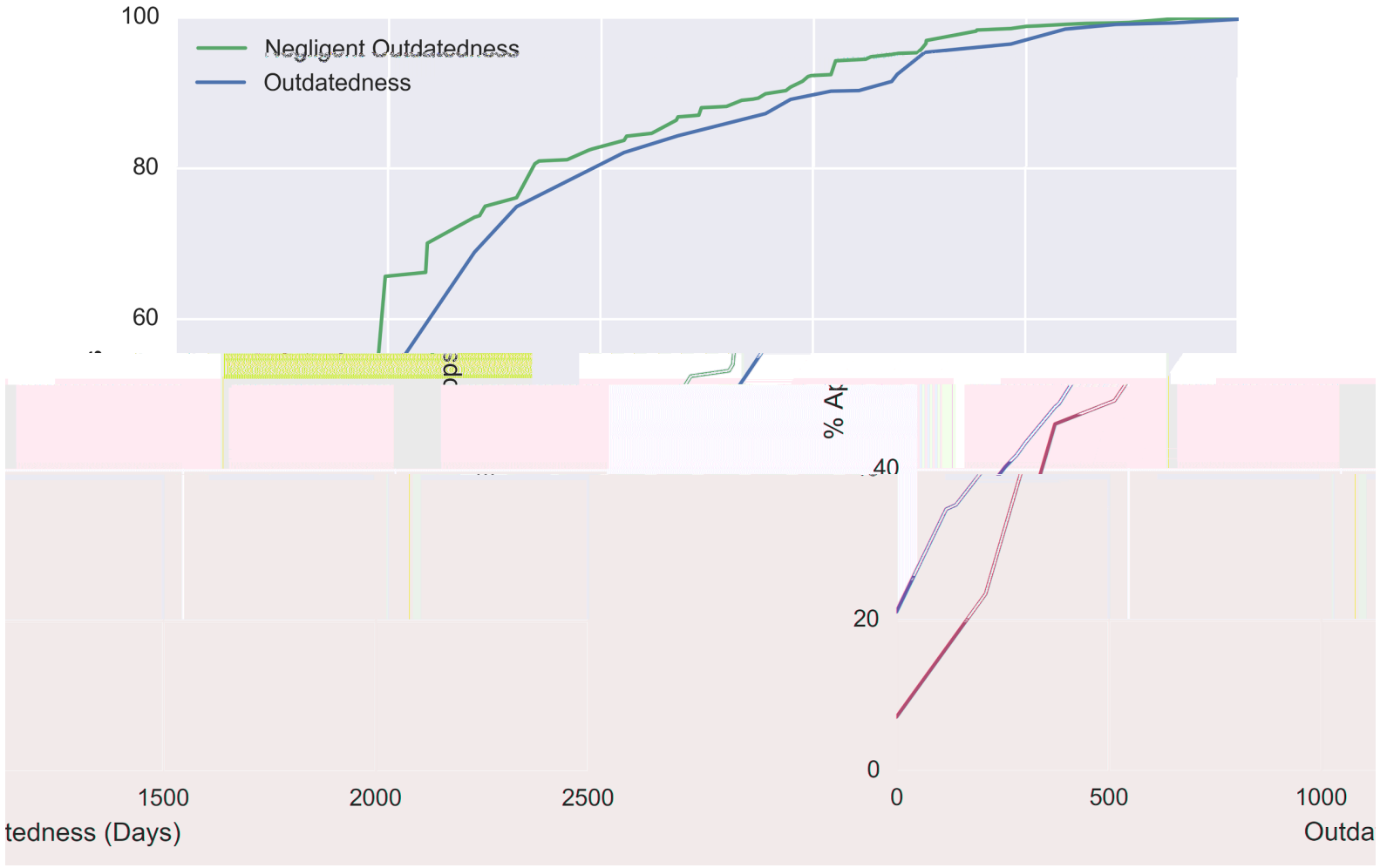
Broken into five datasets by collection date


Outdatedness
Android 5.0 Released
Android 5.1 Released
Android 6.0 Released
App Collected


100
80
60
40
20
0
% Apps
2500
0
500
1000
1500
2000
Outdatedness (Days)


Download Count
> 10m
1m - 10m
100k - 1m
< 100k
100
80
60
40
20
0
% Apps
0
500
1000
1500
2000
2500
Outdatedness (Days)


Negligent Outdatedness
Outdatedness
Android 5.0 Released
Android 5.1 Released
App Updated
Android 6.0 Released
App Collected


100
80
60
Negligent Outdatedness
Outdatedness
40
20
0
1500
2000
2500
0
500
1000
tedness (Days)
Outda

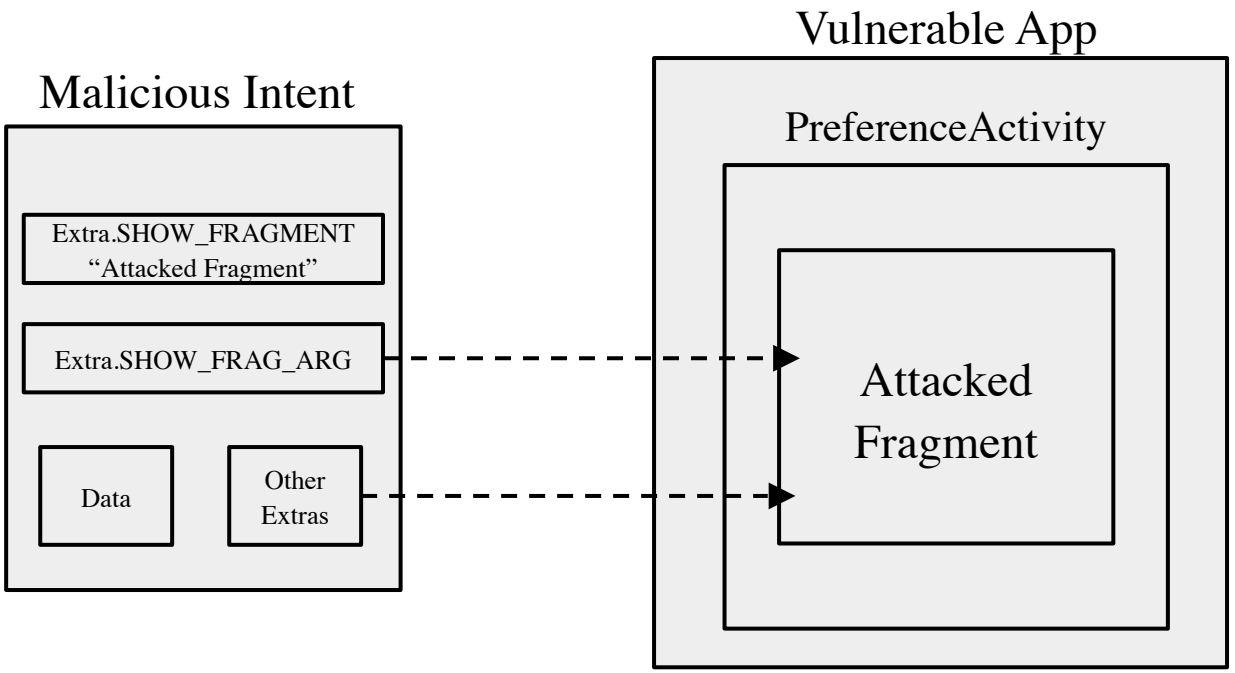
Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences

Fragment Injection



A malicious application can invoke any exported class and supply it with an : : Intent extra in order to make it load an arbitrary class.

securityintelligence.com/new-vulnerability-android-framework-fragment-injection/

Fragment Injection

Fixed in Android 4.4

Developers implement to authorize fragments

Fragment Injection

Vulnerable if:

- Targets 4.3 or lower (31%)
- Some class inherits from (4.8%)
- That class is exported (1.1%)
- That class does not override (0.55%)

4.2% of apps vulnerable if no fix was ever implemented

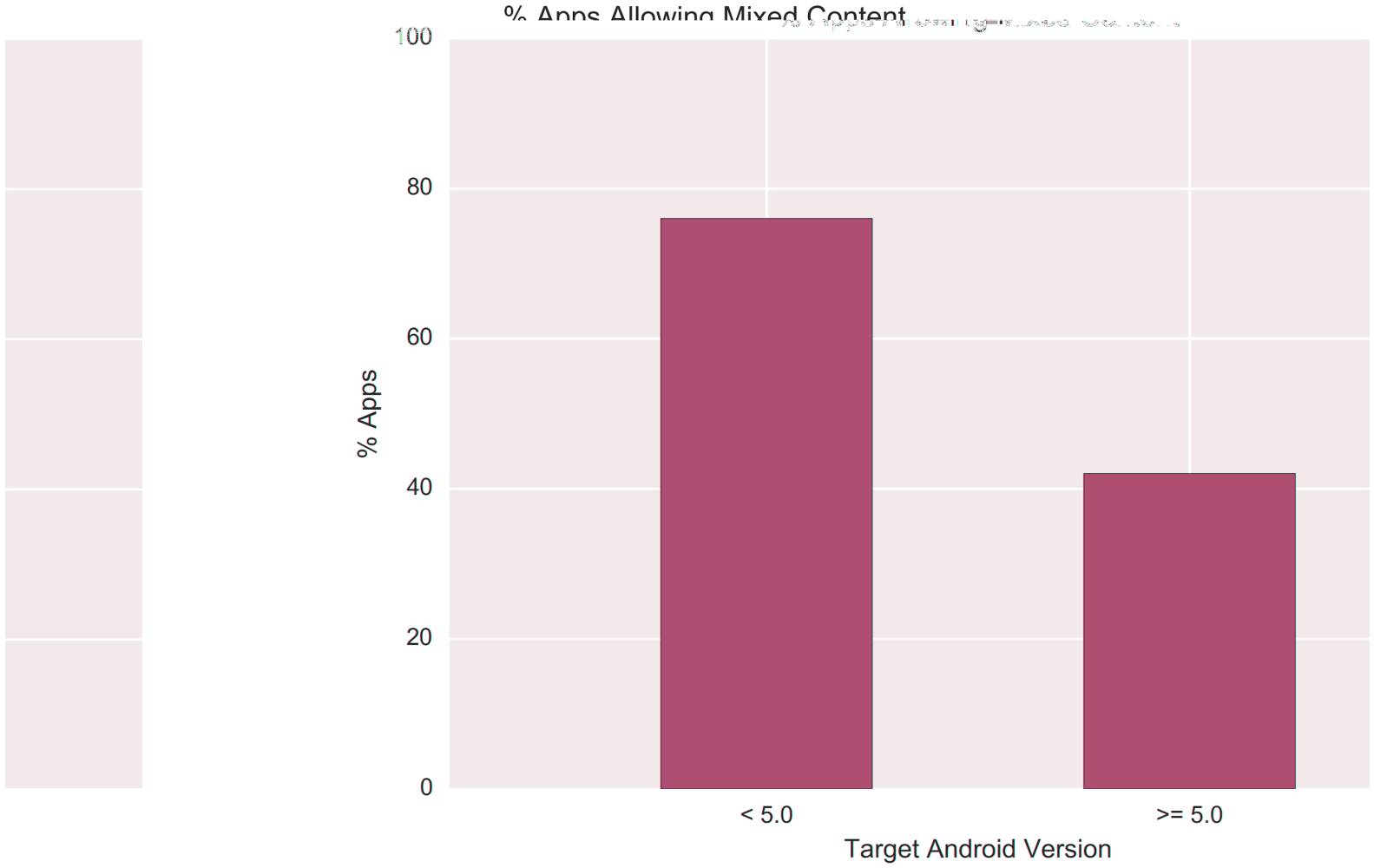
Mixed Content in WebView

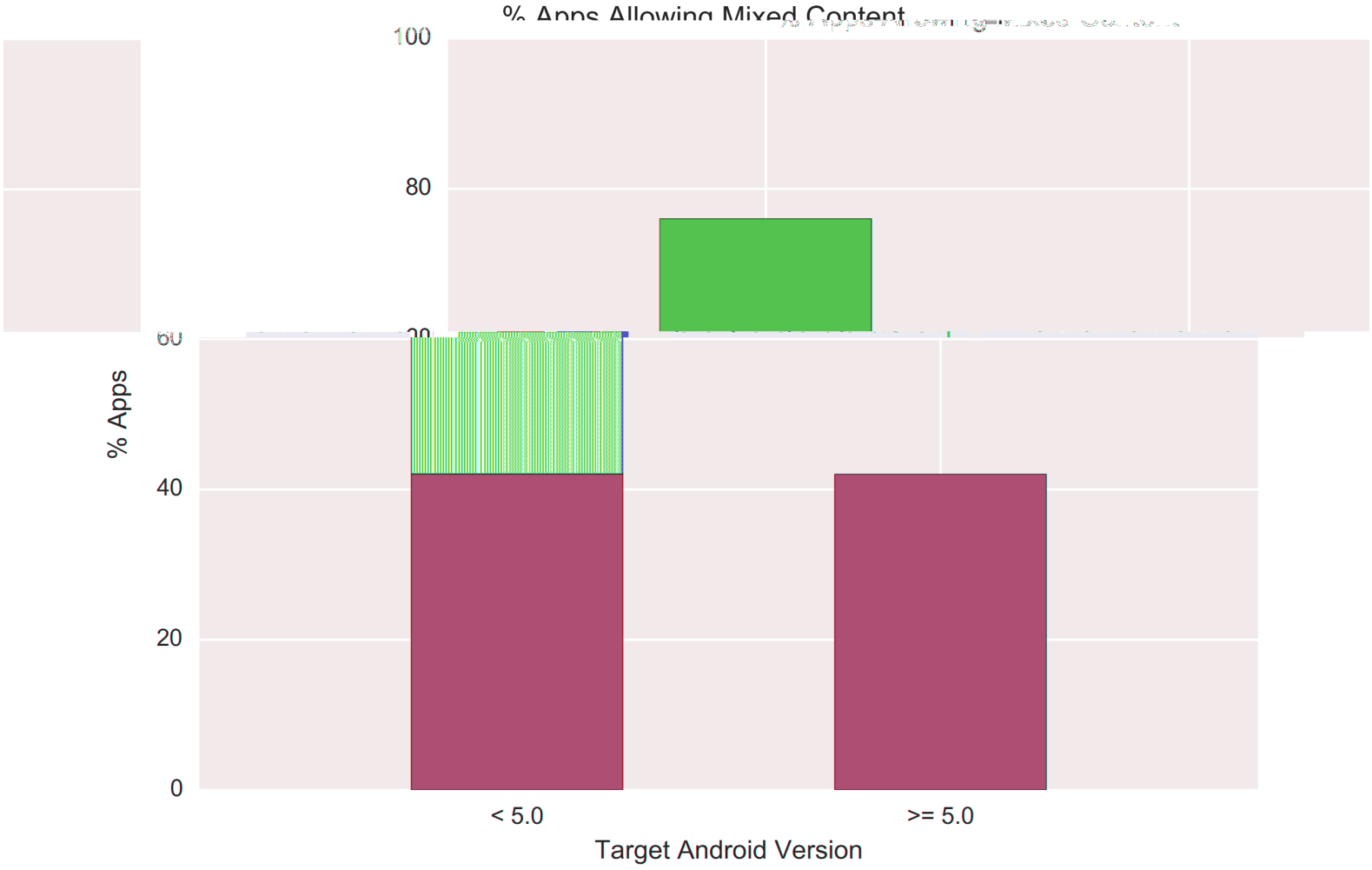
Mixed Content in WebView

Major web browsers block Mixed Content

In Android 5.0, WebViews block Mixed Content by default

Can override default with

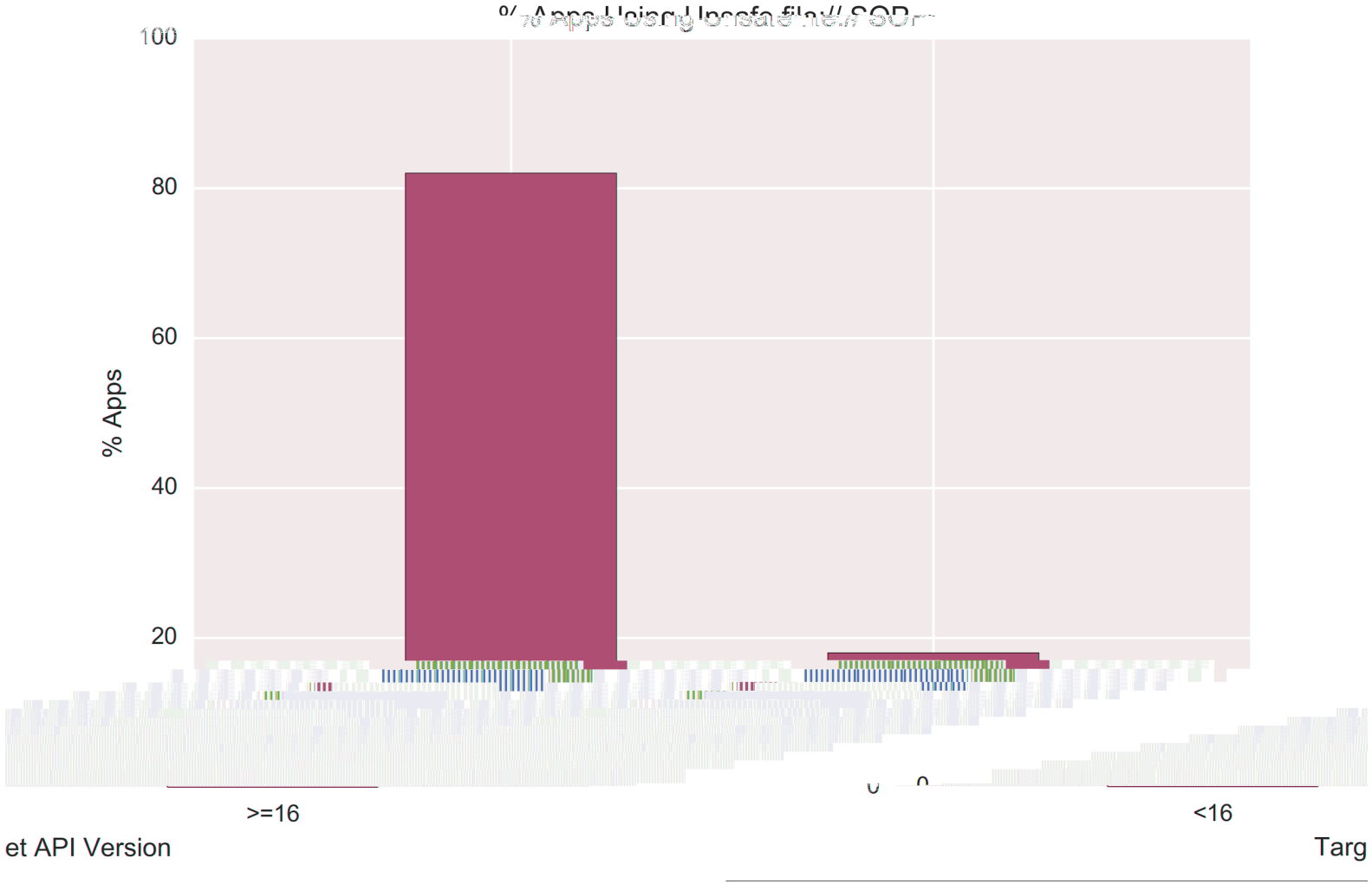

% Apps Allowing Mixed Content
100
80
60
40
20
0
% Apps
< 5.0
>= 5.0
Target Android Version

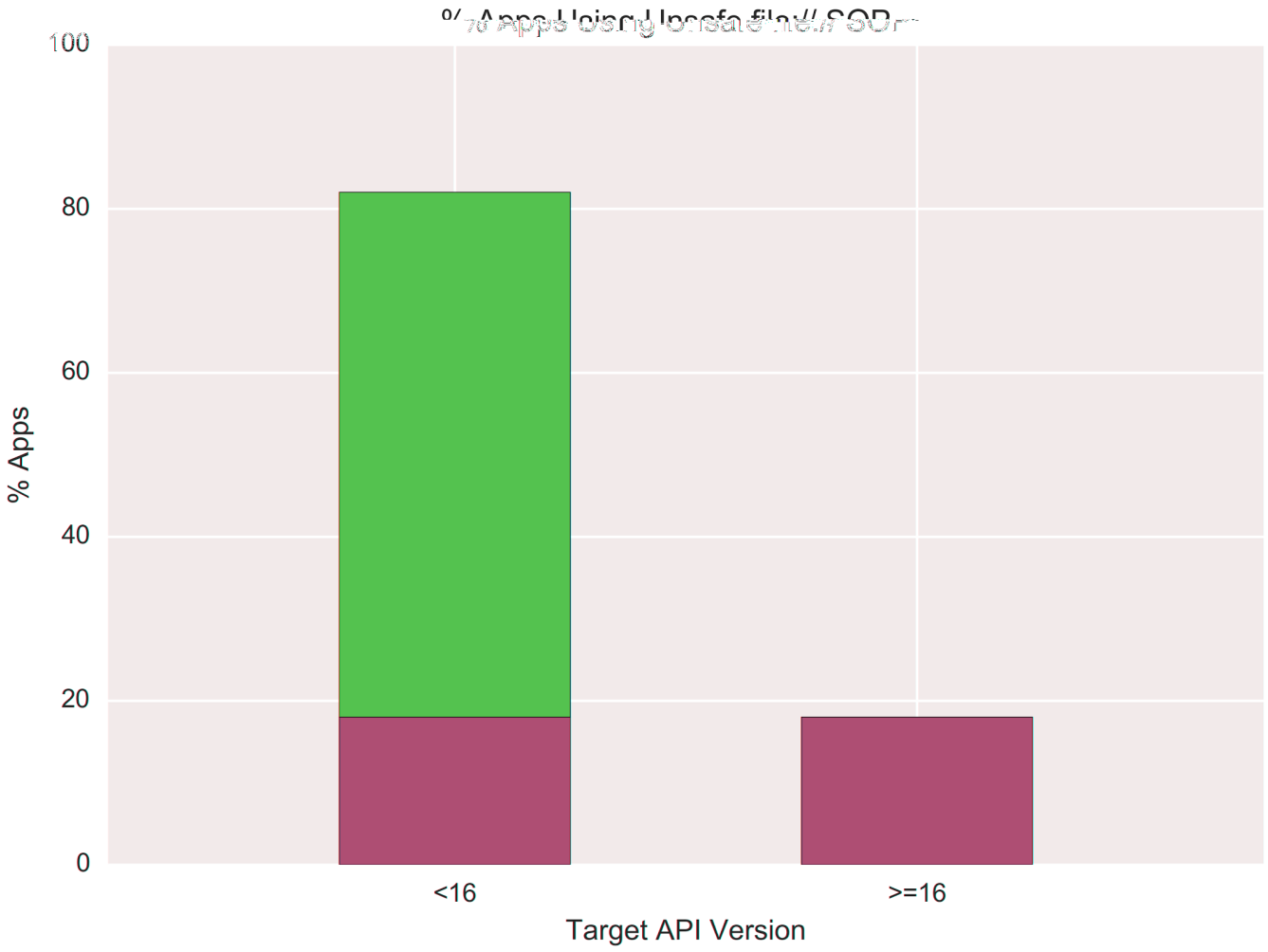

% Apps Allowing Mixed Content
100
80
60
40
20
0
% Apps
< 5.0
>= 5.0
Target Android Version

SOP for URLs in WebView

Android 4.1 separate URLs are treated as unique origins

Can override with


% Apps
100
80
60
40
20
>=16
<16
et API Version
Targ


100
80
60
40
20
0
% Apps
<16
>=16
Target API Version

Summary of Target Fragmentation

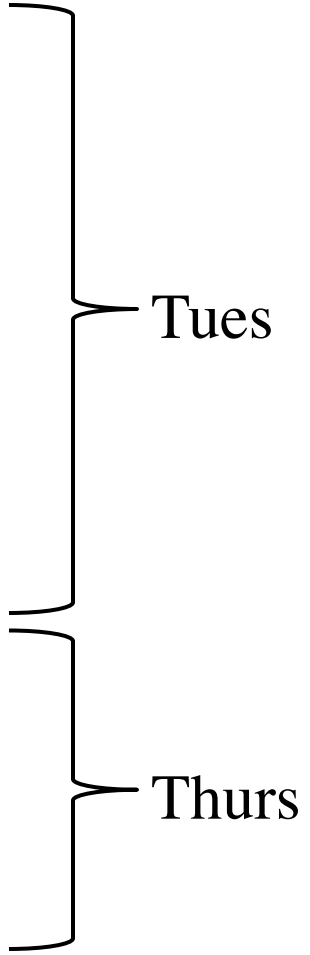
Android apps can run using outdated OS behavior

- The large majority of Android apps do this
- Including popular and well maintained apps

Outdated security code invisibly permeates the app ecosystem

- “Patched” security vulnerabilities still exist in the wild
- “Risky by default” behavior is widespread

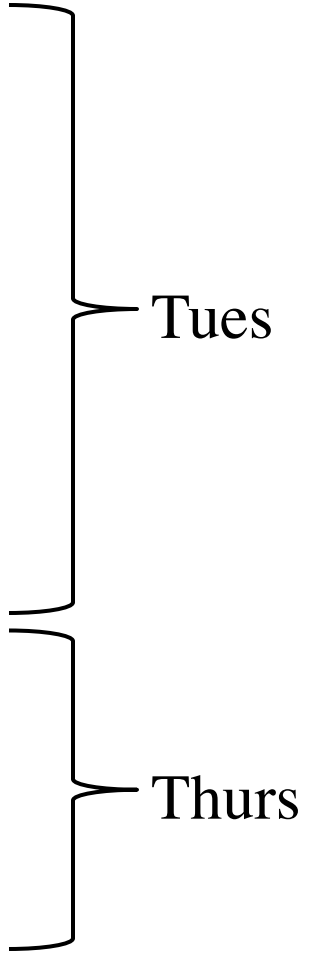
-
-
  -
-
-
-
  -
  -
-
  -
  -


Tues
Thurs

	iOS	Android	Windows

	iOS	Android	Windows

-
-
  -
-
-
-
  -
  -
-
  -
  -


Tues
Thurs