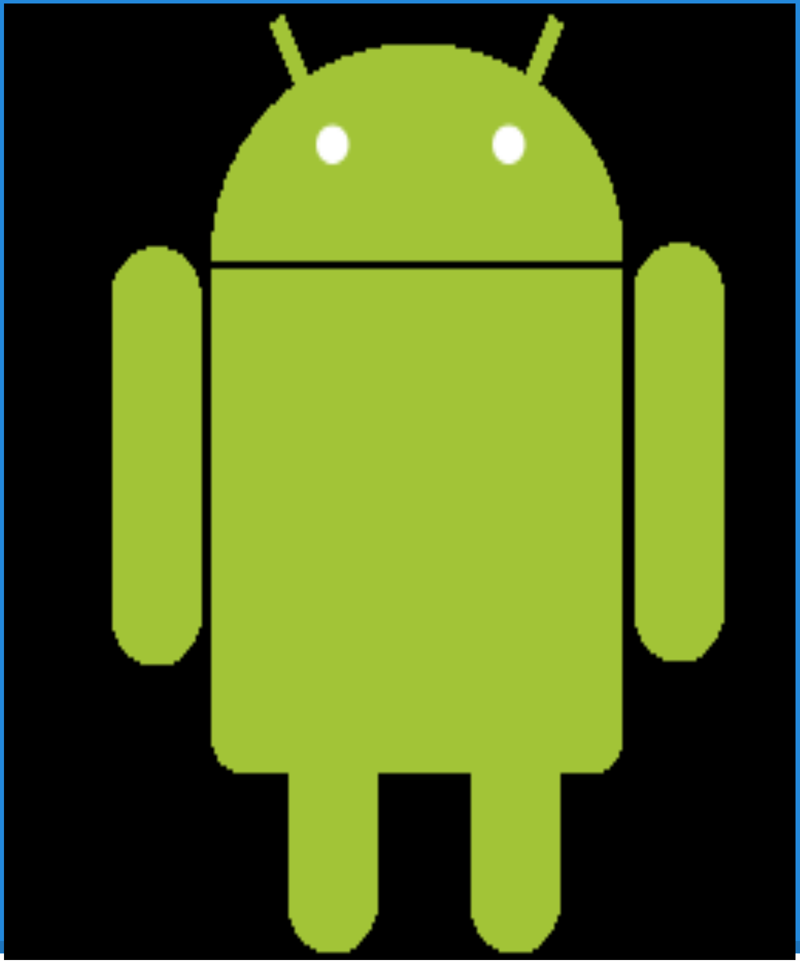
CS155: Android Malware



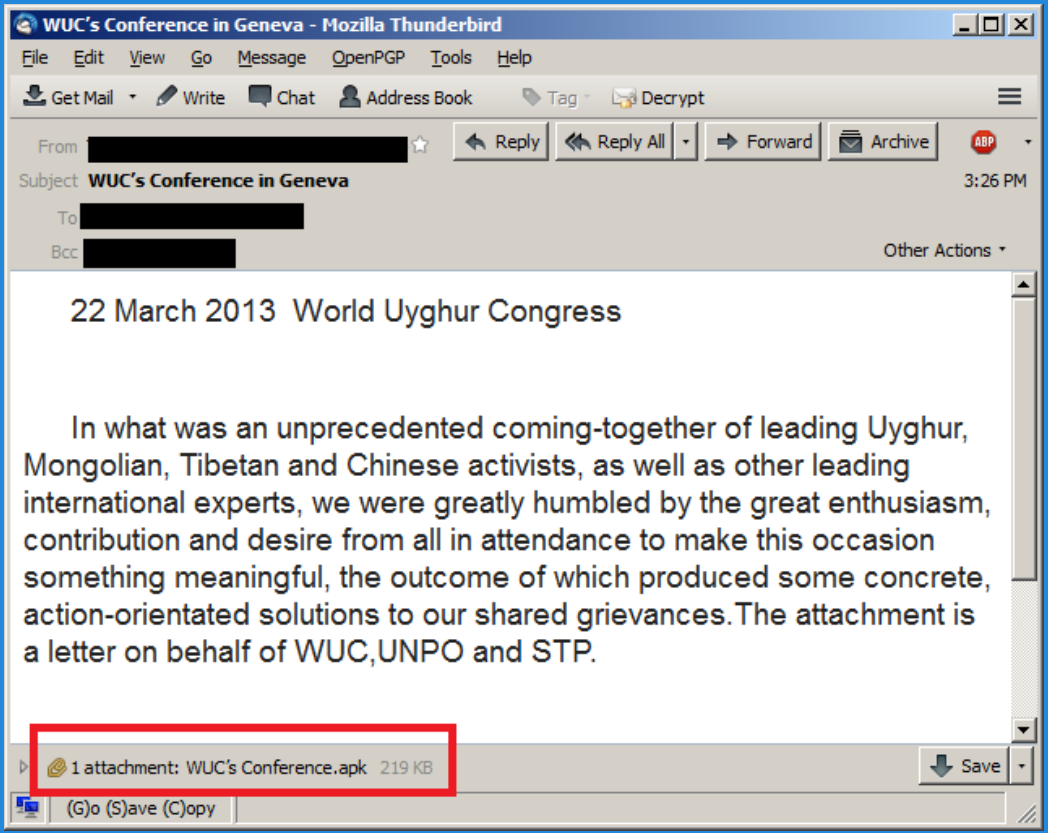
Jason Franklin Ph.D.
Research Associate and Visiting Lecturer

Save the Dalai Lama!

Start

It's March 24th, 2013...

You're a Tibetan activist named Alice



From [redacted]

Subject **WUC's Conference in Geneva**

3:26 PM

To [redacted]

Bcc [redacted]

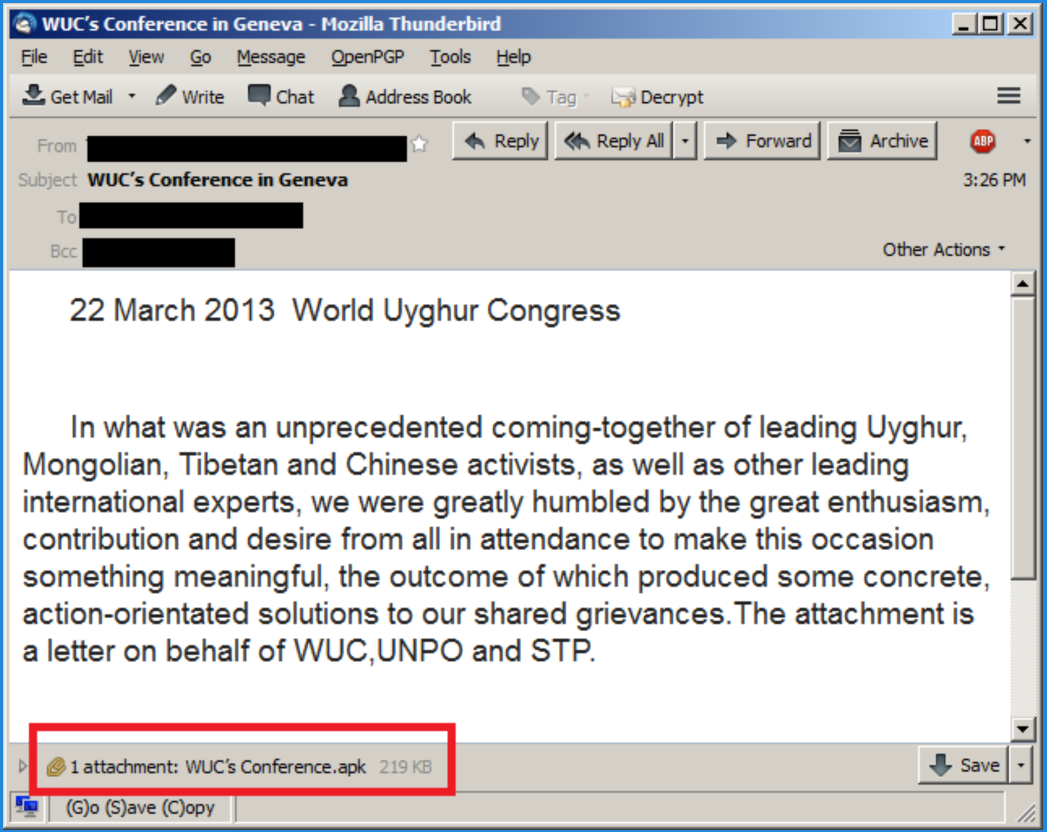
22 March 2013 World Uyghur Congress

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-orientated solutions to our shared grievances.The attachment is a letter on behalf of WUC,UNPO and STP.

1 attachment: WUC's Conference.apk 219 KB

You receive an email from a fellow activist, Bob

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


WUC's Conference in Geneva - Mozilla Thunderbird
File Edit View Go Message OpenPGP Tools Help
Get Mail Write Chat Address Book Tag Decrypt
Reply Reply All Forward Archive
Other Actions
Save
(G)o (S)ave (C)opy

From [redacted]

Subject WUC's Conference in Geneva 3:26 PM

To [redacted]

Bcc [redacted]

22 March 2013 World Uyghur Congress

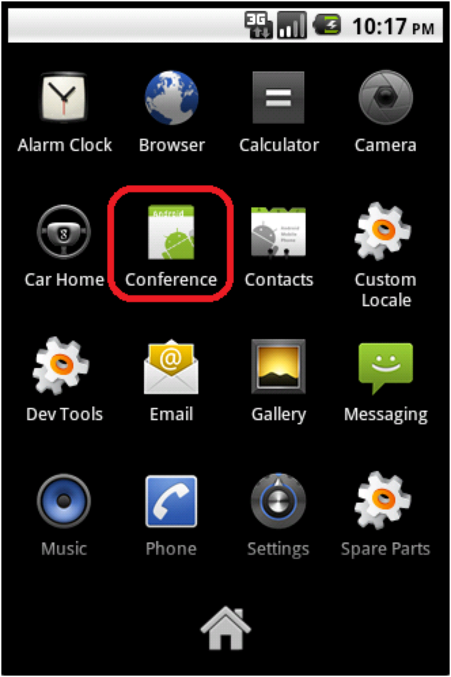
In what was an unprecedented coming-together of leading Uyghur, Mongolian, Tibetan and Chinese activists, as well as other leading international experts, we were greatly humbled by the great enthusiasm, contribution and desire from all in attendance to make this occasion something meaningful, the outcome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

1 attachment: WUC's Conference.apk 219 KB

Attached to the email is an Android application

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

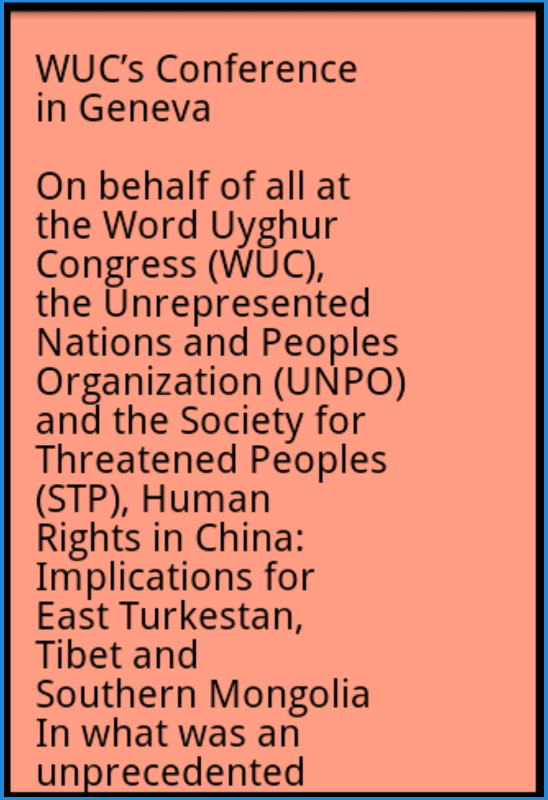
You install the android app...



Now it's running on your android device

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

Everything seems fine...



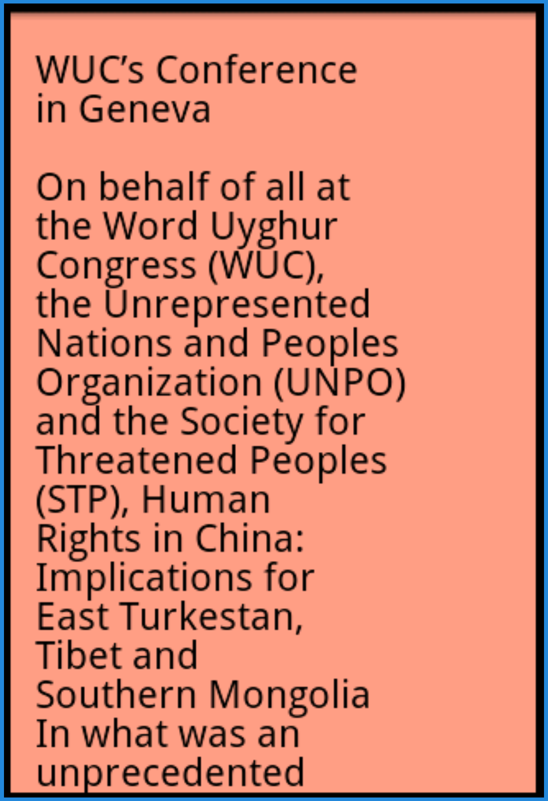
WUC's Conference
in Geneva

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

However, things are not as they appear

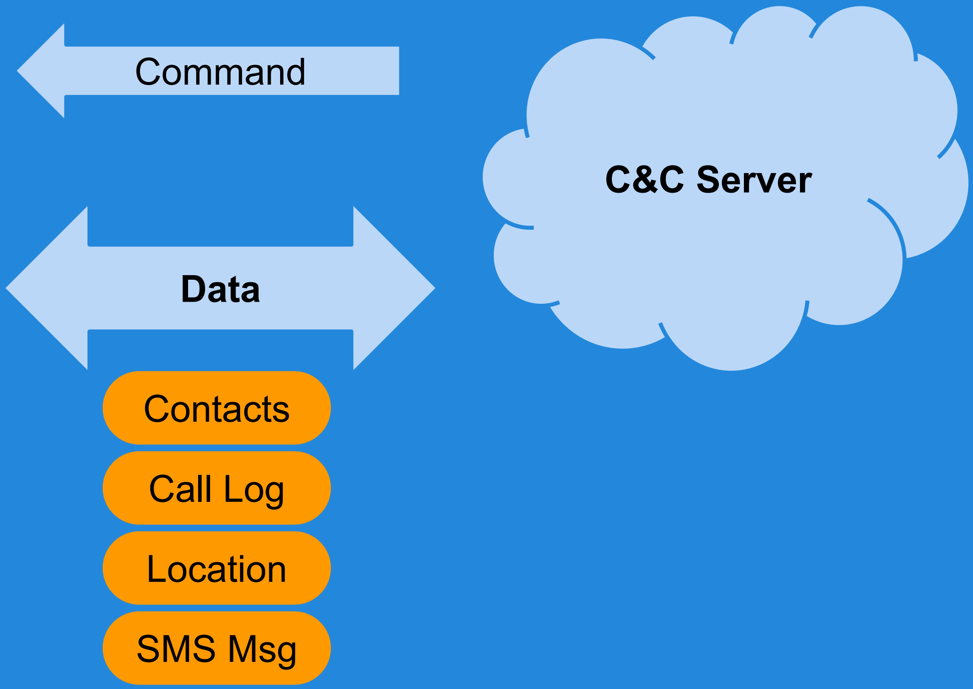
Image: Kaspersky Labs, https://www.securelist.com/en/blog/208194186/Android_Trojan_Found_in_Targeted_Attack, March 26th, 2013

Background behaviors



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



Malware's behaviors triggered by C&C server (chuli)

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

Save the Dalai Lama!

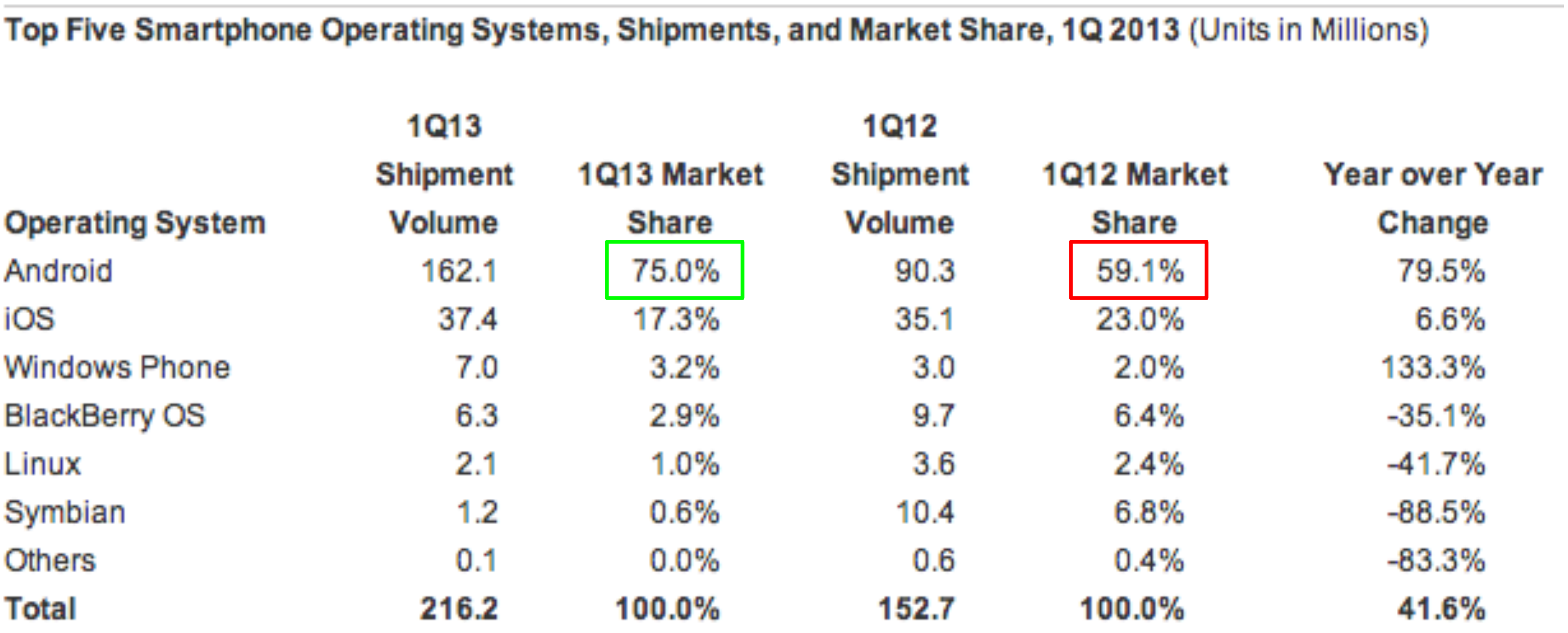
GAME OVER

Save the Dalai Lama!

First, study Android!

Play Again?

Android Market Share (1Q12/1Q13)



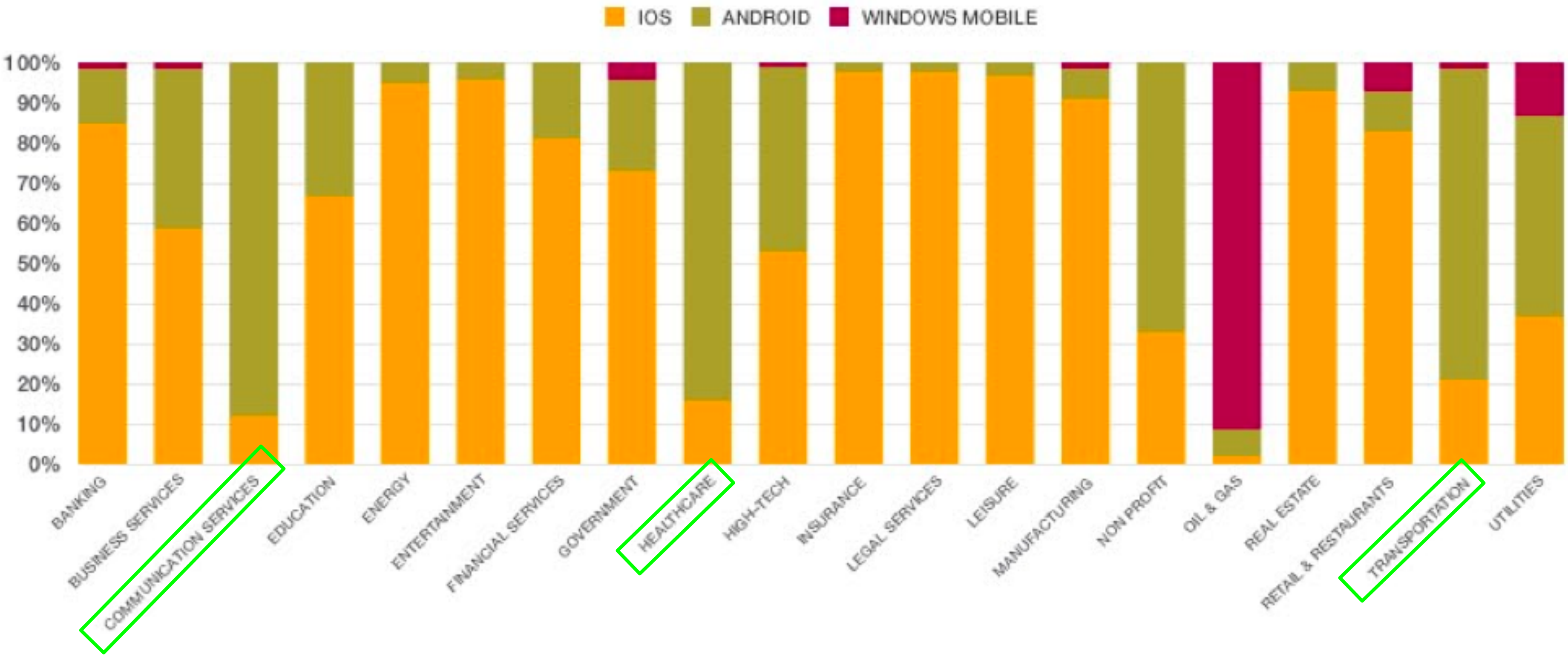
Top Five Smartphone Operating Systems, Shipments, and Market Share, 1Q 2013 (Units in Millions)

Operating System	1Q13 Shipment Volume	1Q13 Market Share	1Q12 Shipment Volume	1Q12 Market Share	Year over Year Change
Android	162.1	75.0%	90.3	59.1%	79.5%
iOS	37.4	17.3%	35.1	23.0%	6.6%
Windows Phone	7.0	3.2%	3.0	2.0%	133.3%
BlackBerry OS	6.3	2.9%	9.7	6.4%	-35.1%
Linux	2.1	1.0%	3.6	2.4%	-41.7%
Symbian	1.2	0.6%	10.4	6.8%	-88.5%
Others	0.1	0.0%	0.6	0.4%	-83.3%
Total	**216.2**	**100.0%**	**152.7**	**100.0%**	**41.6%**

Image: IDC

Enterprise Adoption

Top Vertical Industries' Device Adoption by OS



Source: Citrix

Centralized Application Distribution

# of apps: 50,000+ as of Oct 2012 [2]

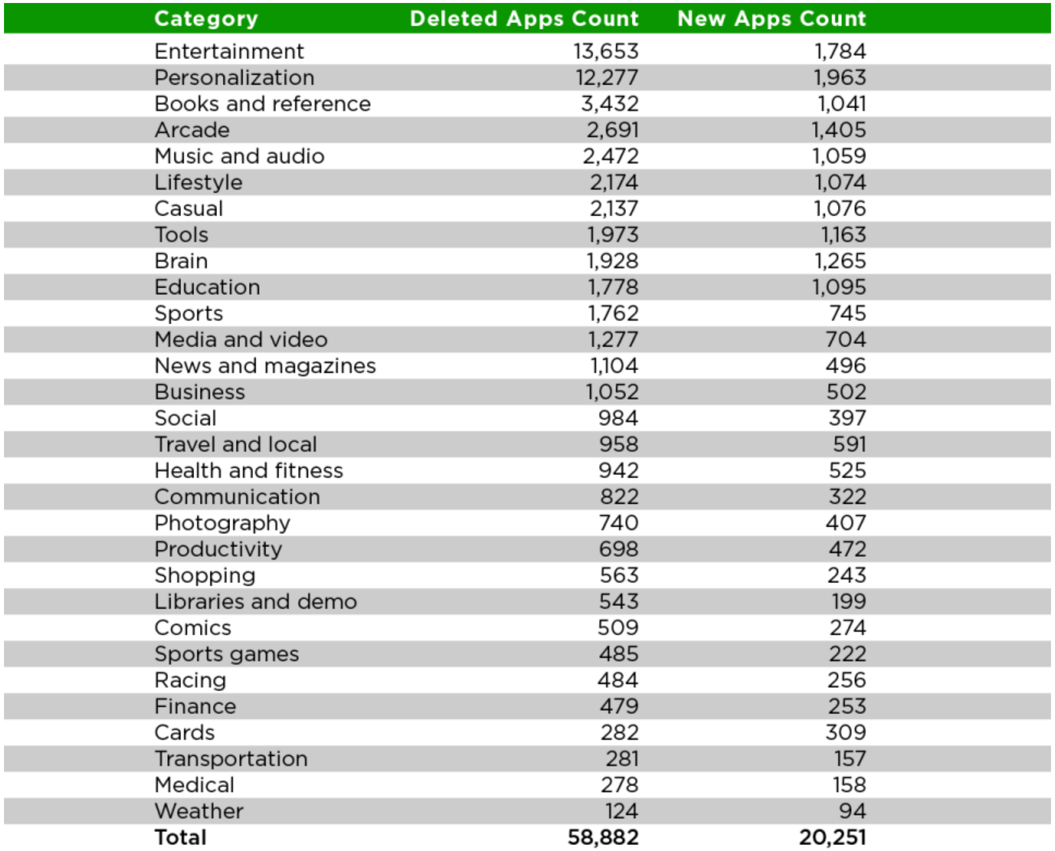
# of apps: 800,000 as of Feb 2013 [1]

[1]. http://en.wikipedia.org/wiki/Google_Play

[2]. http://www.theverge.com/2012/9/6/3296612/amazon-appstore-for-android-50000-app-count-september-2012

App Stores Enable Curation

- Google removes 60,000 apps
  - non-compliant, malicious, low quality, spammy



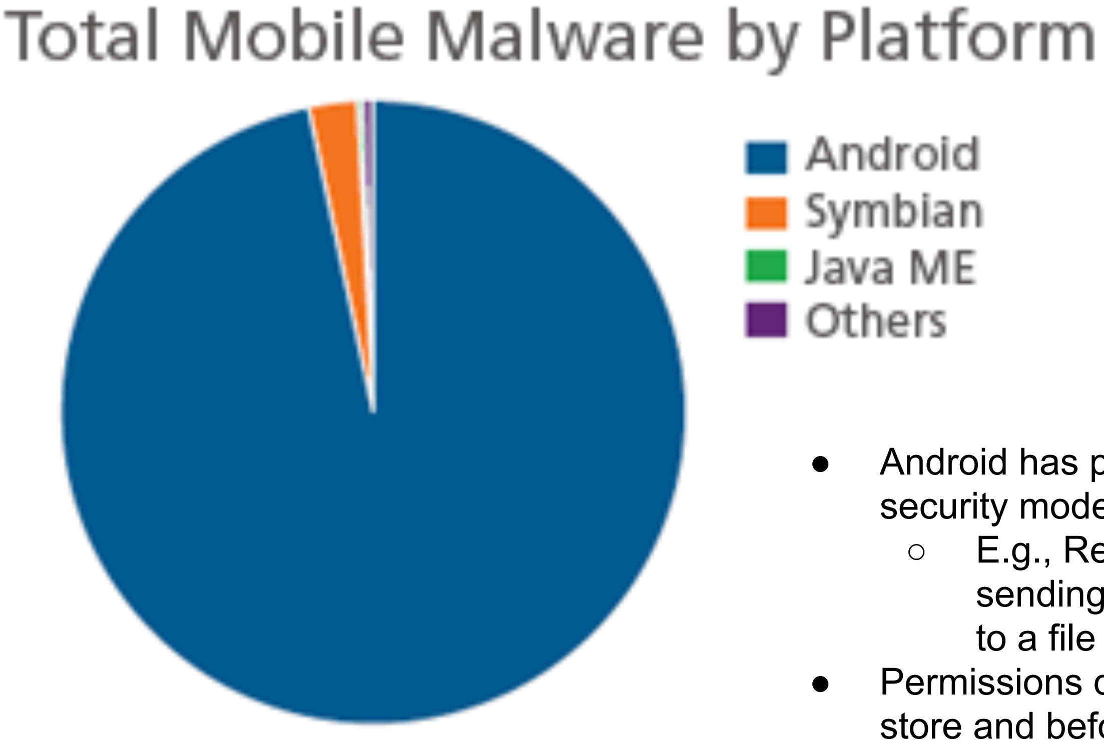
Category	Deleted Apps Count	New Apps Count
Entertainment	13,653	1,784
Personalization	12,277	1,963
Books and reference	3,432	1,041
Arcade	2,691	1,405
Music and audio	2,472	1,059
Lifestyle	2,174	1,074
Casual	2,137	1,076
Tools	1,973	1,163
Brain	1,928	1,265
Education	1,778	1,095
Sports	1,762	745
Media and video	1,277	704
News and magazines	1,104	496
Business	1,052	502
Social	984	397
Travel and local	958	591
Health and fitness	942	525
Communication	822	322
Photography	740	407
Productivity	698	472
Shopping	563	243
Libraries and demo	543	199
Comics	509	274
Sports games	485	222
Racing	484	256
Finance	479	253
Cards	282	309
Transportation	281	157
Medical	278	158
Weather	124	94
Total	**58,882**	**20,251**

[1]. http://techcrunch.com/2013/04/08/nearly-60k-low-quality-apps-booted-from-google-play-store-in-february-points-to-increased-spam-fighting/

App Store Promise

Centralization + Curation = Safety

Reality



- Android has permission based security model
  - E.g., Reading user data, sending to internet, writing to a file all require perms
- Permissions displayed in app store and before install
- User expected to remain vigilant
  - Common failure point

Source: McAfee, Feb. 2013
http://www.mcafee.com/us/security-awareness/articles/mobile-malware-growth-continuing-2013.aspx

Malware Trends

- Q1 2012: 5,000 malicious apps detected

- Q2 2012: 10,000 malicious apps detected
  - In 1 month

- 17 malicious apps downloaded 700k times

[1]. http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-behind-the-android-menace-malicious-apps/

Malware Author's Goals - $$$

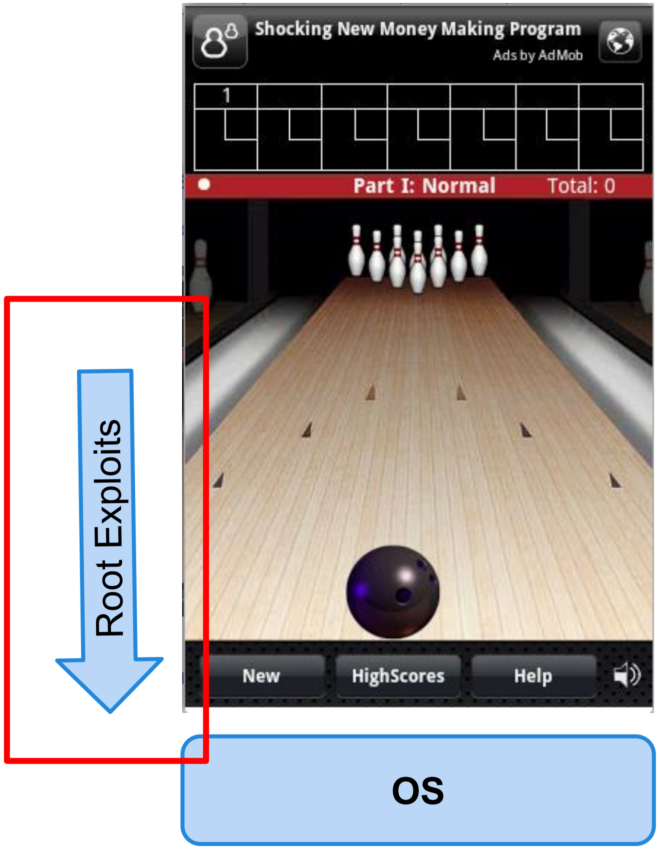
- Immediate monetization
  - Abuse premium-service (48%)
    - Send premium SMS in background
  - Display Ads (22%)
  - Data Theft (21%)
  - Click Fraud (7%)

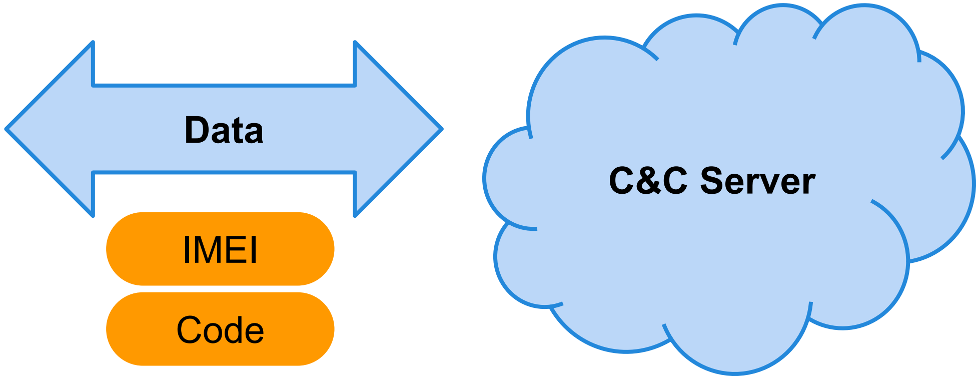
- Investment in platform
  - Remote control (19%)
  - Root exploit (11%)

[1]. http://blog.trendmicro.com/trendlabs-security-intelligence/infographic-behind-the-android-menace-malicious-apps/

Noteworthy Malware - DroidDream

- Malware hidden in repackaged apps (in Google Play)
  - App functionality drives downloads
- Malware may require additional permissions
- Users unknowingly install app despite permissions
- After install, app can leak data in background
  - Android security model requires user vigilance





Honest Developers Break Rules Too

"**Permissions changed** in the latest update to read my phone number. **Totally unacceptable** for a puzzle game. Uninstalling." [1]

"**Uninstalling** due to the added permissions**."** [1]

"Why suddenly Read phone state permission?" [1]

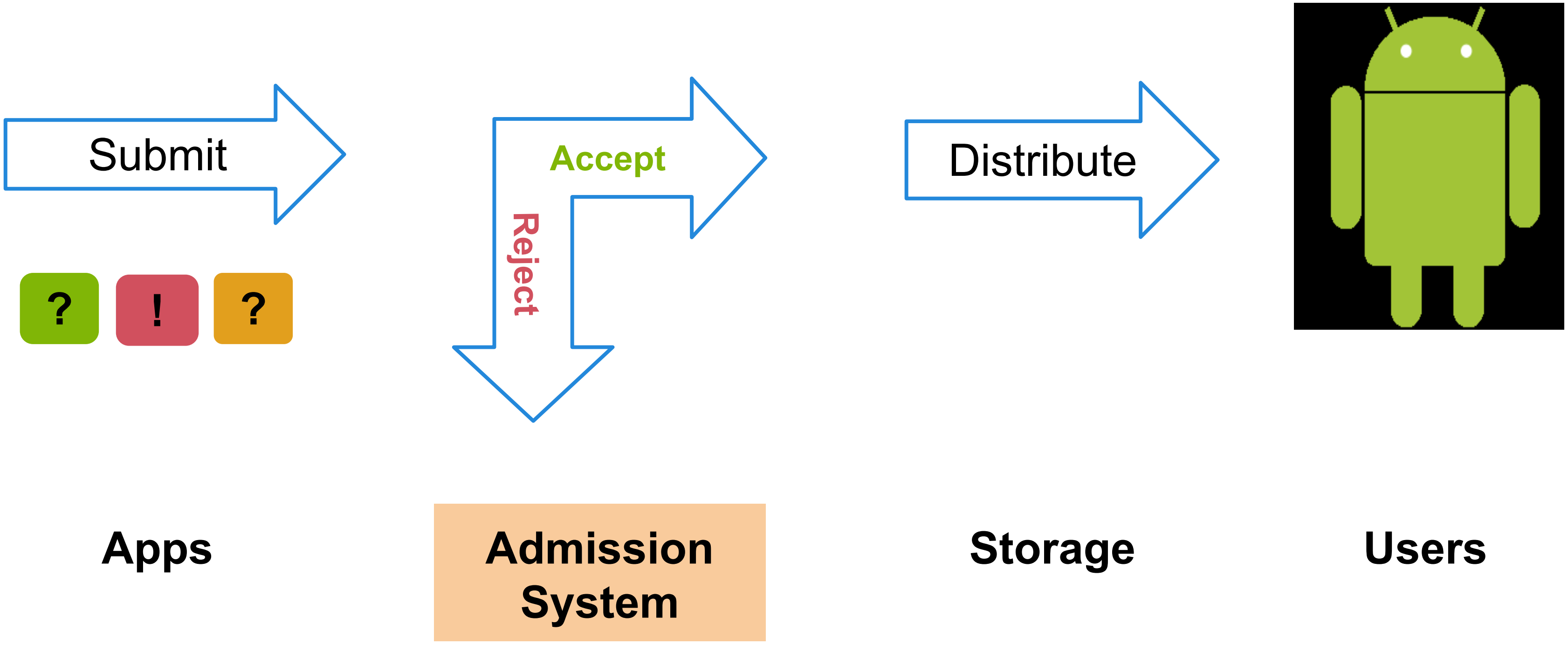
"Simple and challenging game but with new update there is too many Permissions for a simple game, will not be updating and once completed all levels I will be deleting it." [1]

[1] Oh, My Brain! Block Buzzle by mToy, https://play.google.com/store/apps/details?id=biz.mtoy.blockpuzzle&feature=related_apps#?t=W251bGwsMSwxLDEwOSwiYml6Lm10b3kuYmxvY2twdXp6bGUiXQ..

Save the Dalai Lama!

Focus on the App Store!

Architecture of an App Store



Submit

? ! ?

Accept

Reject

Distribute

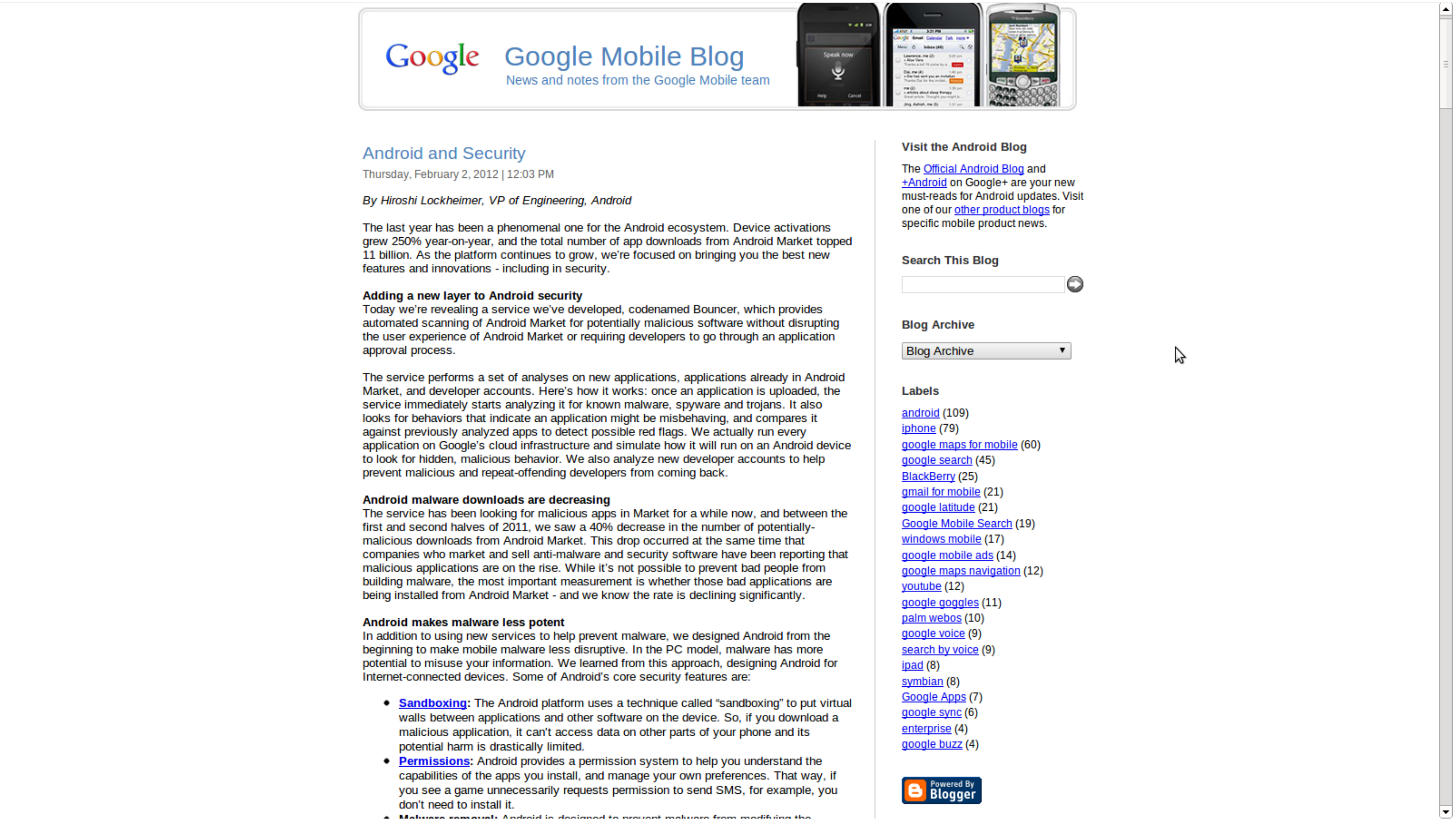
Apps

Admission System

Storage

Users
]

Admission System - Google Bouncer



Google Mobile Blog
News and notes from the Google Mobile team

Android and Security

Thursday, February 2, 2012 | 12:03 PM

By Hiroshi Lockheimer, VP of Engineering, Android

The last year has been a phenomenal one for the Android ecosystem. Device activations grew 250% year-on-year, and the total number of app downloads from Android Market topped 11 billion. As the platform continues to grow, we're focused on bringing you the best new features and innovations - including in security.

Adding a new layer to Android security
Today we're revealing a service we've developed, codenamed Bouncer, which provides automated scanning of Android Market for potentially malicious software without disrupting the user experience of Android Market or requiring developers to go through an application approval process.

The service performs a set of analyses on new applications, applications already in Android Market, and developer accounts. Here's how it works: once an application is uploaded, the service immediately starts analyzing it for known malware, spyware and trojans. It also looks for behaviors that indicate an application might be misbehaving, and compares it against previously analyzed apps to detect possible red flags. We actually run every application on Google's cloud infrastructure and simulate how it will run on an Android device to look for hidden, malicious behavior. We also analyze new developer accounts to help prevent malicious and repeat-offending developers from coming back.

Android malware downloads are decreasing
The service has been looking for malicious apps in Market for a while now, and between the first and second halves of 2011, we saw a 40% decrease in the number of potentially-malicious downloads from Android Market. This drop occurred at the same time that companies who market and sell anti-malware and security software have been reporting that malicious applications are on the rise. While it's not possible to prevent bad people from building malware, the most important measurement is whether those bad applications are being installed from Android Market - and we know the rate is declining significantly.

Android makes malware less potent
In addition to using new services to help prevent malware, we designed Android from the beginning to make mobile malware less disruptive. In the PC model, malware has more potential to misuse your information. We learned from this approach, designing Android for Internet-connected devices. Some of Android's core security features are:

- **Sandboxing**: The Android platform uses a technique called "sandboxing" to put virtual walls between applications and other software on the device. So, if you download a malicious application, it can't access data on other parts of your phone and its potential harm is drastically limited.
- **Permissions**: Android provides a permission system to help you understand the capabilities of the apps you install, and manage your own preferences. That way, if you see a game unnecessarily requests permission to send SMS, for example, you don't need to install it.
- **Malware removal:** Android is designed to prevent malware from modifying the

Visit the Android Blog

The Official Android Blog and +Android on Google+ are your new must-reads for Android updates. Visit one of our other product blogs for specific mobile product news.

Search This Blog

Blog Archive

Blog Archive ▼

Labels

android (109)
iphone (79)
google maps for mobile (60)
google search (45)
BlackBerry (25)
gmail for mobile (21)
google latitude (21)
Google Mobile Search (19)
windows mobile (17)
google mobile ads (14)
google maps navigation (12)
youtube (12)
google goggles (11)
palm webos (10)
google voice (9)
search by voice (9)
ipad (8)
symbian (8)
Google Apps (7)
google sync (6)
enterprise (4)
google buzz (4)

Powered By Blogger

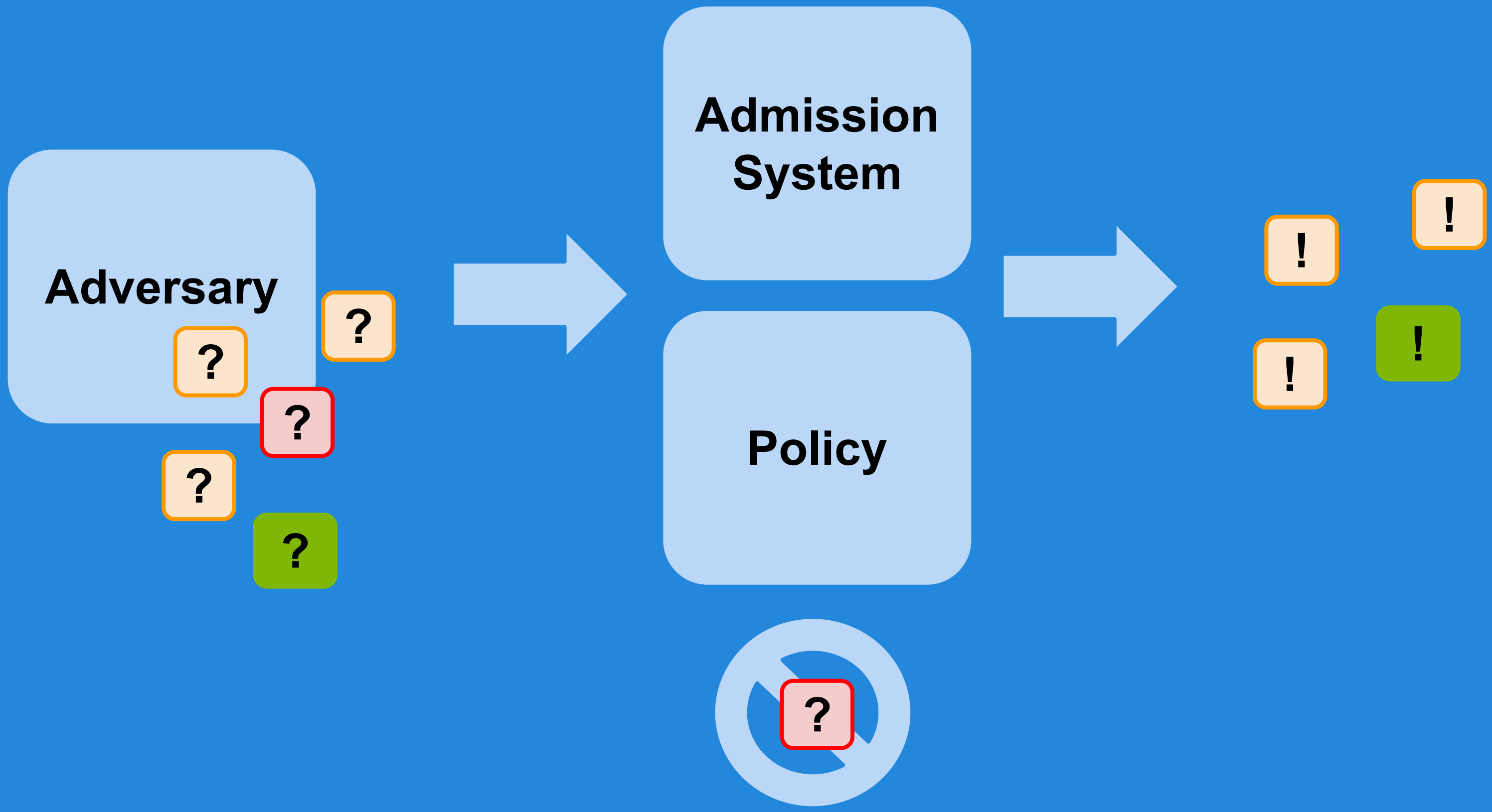
Inside Google Bouncer (Unofficial)

- Performs set of analyses on new app
  - Analysis details not provided
- Run app for 5 minutes in emulator
  - Dynamic analysis
- Simulate how app will run on Android device
  - Input generation problem
- Look for hidden, malicious behavior
  - Apply set of (undefined) heuristics + policies
- Few official statements, details sparse
  - Why? Prevent circumvention? Competitive reasons?
  - Risk/reward to openness

Save the Dalai Lama!

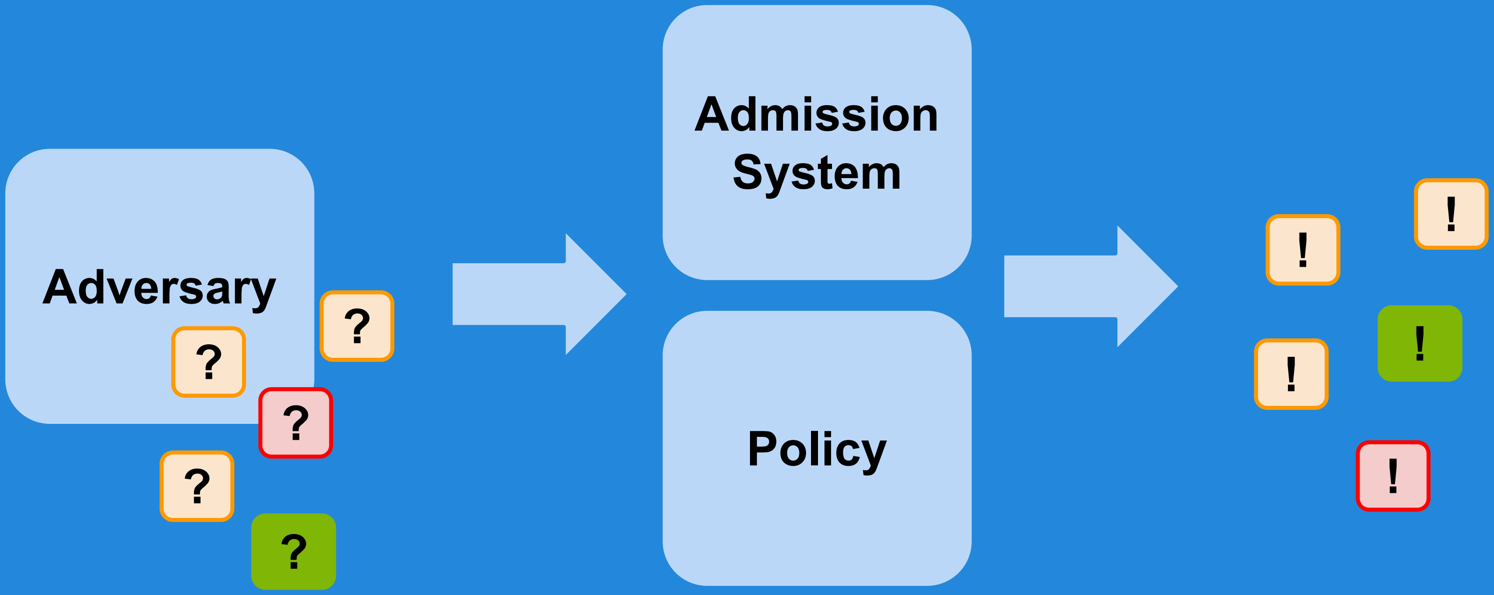
The admission system is the key!

Malware detection game



Defender's Goal: Correctly classify programs

Adversary



Adversary's Goal: Violate policy in undetectable way

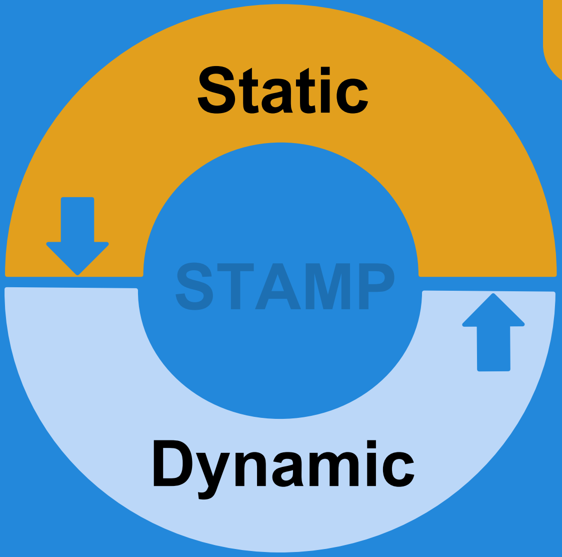
Policies

- State acceptable/unacceptable behaviors
    - **Data Theft:** What personal data can leave device?
        - User impact: Data privacy (data-out)
    - **Device Control:** Exploit OS etc.
        - User impact: device integrity (data-in)
    - **Service Misuse:** Premium SMS
        - User impact: $
    - **Spam:** How many/which type of ads?
        - User impact: time
    - **Others**
        - No comprehensive taxonomy

Admission System

Static Analysis

More behaviors, fewer details



Dynamic (Runtime) Analysis

Fewer behaviors, more details

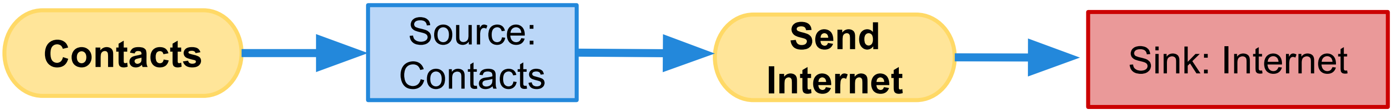
Static and Dynamic Analysis

- Static analysis
  - No code execution
  - Benefit: Can certify programs (100% coverage)
  - Challenge: Scalability and false positives

- Dynamic analysis
  - Monitor program execution at runtime
  - Benefit: No false positives
  - Challenge: Input generation to achieve coverage (false negatives)

Flow Policies

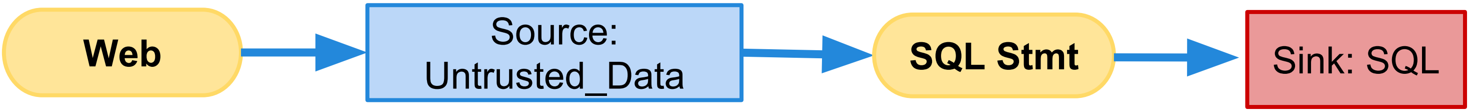
- Data theft



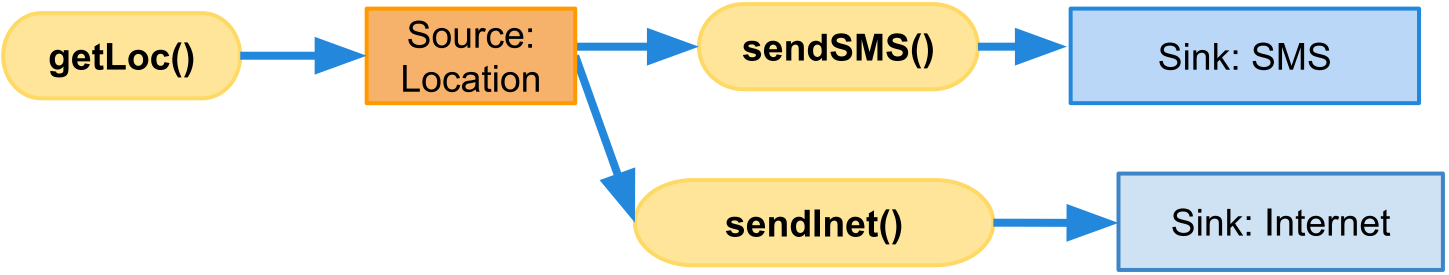
- Privacy policies
  - Avoid liability, protect consumer privacy

Privacy Policy
This app collects your:
Contacts
Phone Number
Address

- Injection vulnerabilities



Static Data Flow Analysis



- Identify source-to-sink flows (a.k.a. data theft)
  - Sources: Location, Calendar, Contacts, Device ID etc.
  - Sinks: Internet, SMS, Disk, etc.

Data Flow Analysis

```
p = ...
t = foo(p);
q = t;
```

Code example

Whether data stored in program variable *p* *may* flow to program variable *q*?

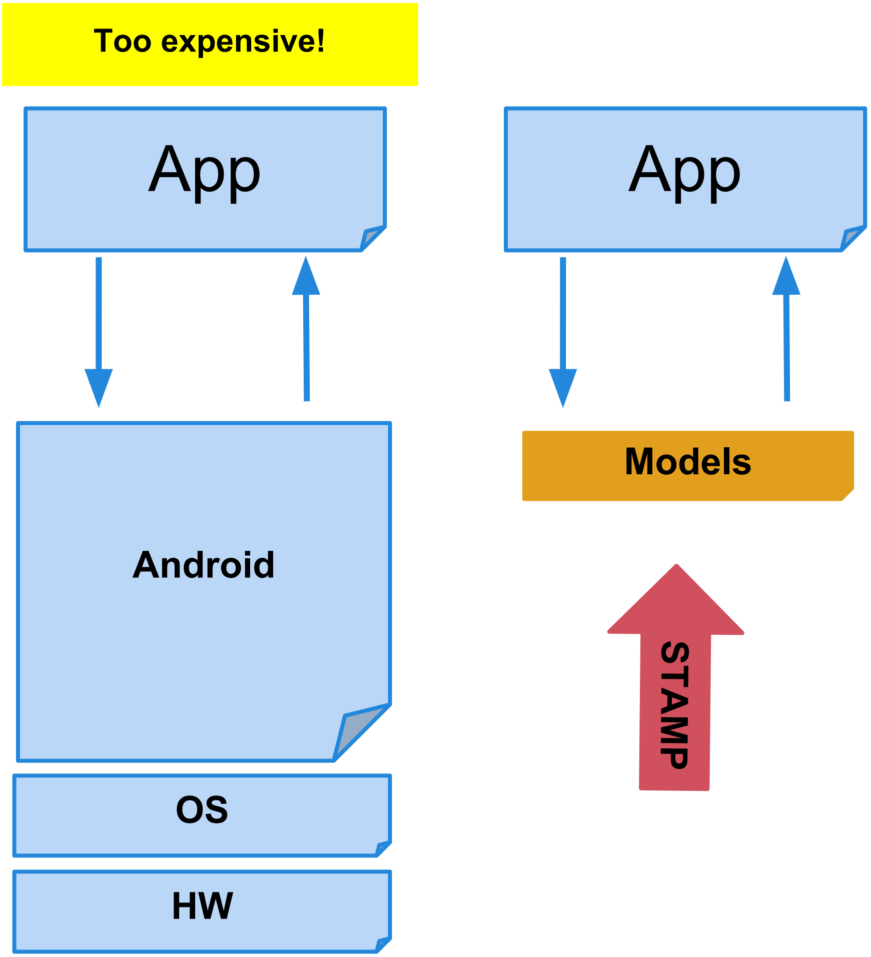
Detection of Private-data Leak

```
p = getDeviceId();
t = foo(p);
q = t;
sendSMS(q);
```

Code example

Whether the device id *may be* leaked through SMS?

Detection system tradeoffs



- Reimplement Android/Java
  - Add sources and sinks
  - 20k methods to inspect
- Whole-program analysis
  - High coverage
  - Low false positive rate

Save the Dalai Lama!

I’m bored.

Tracking Sensitive Data

```
android.Telephony.TelephonyManager: String getDeviceId()
```

```
@STAMP(SRC ="$DEVICEID", SINK ="@return")
```

Sources

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

30+ types of sensitive data

Save the Dalai Lama!

zzzzzzz
MATEO

Sinks

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

10+ types of exit points

Flows

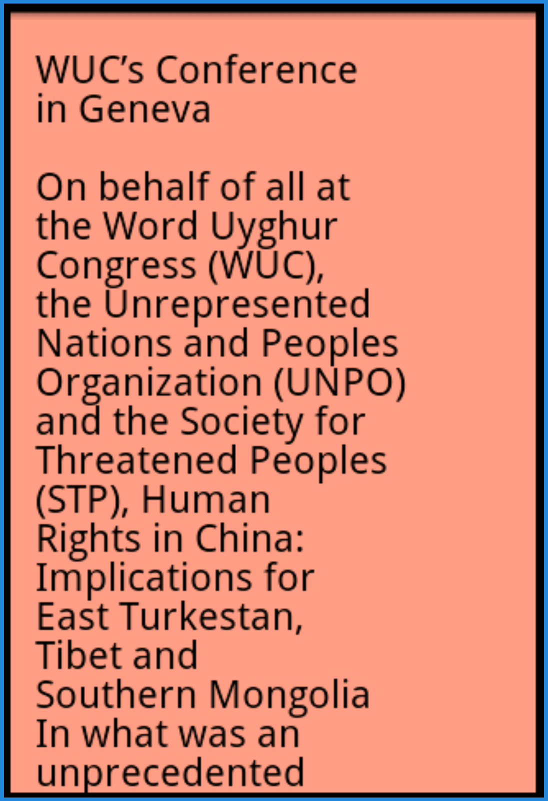
396 Flow Types

Detectable Flows = Sources x Sink

Save the Dalai Lama!

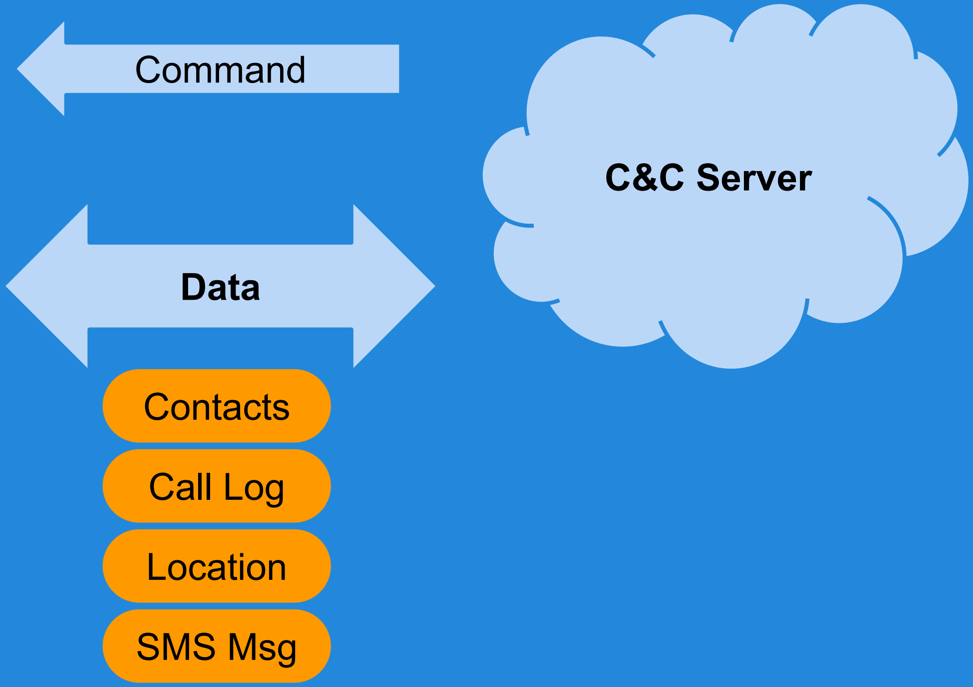
Start

Detecting background behaviors



WUC's Conference
in Geneva

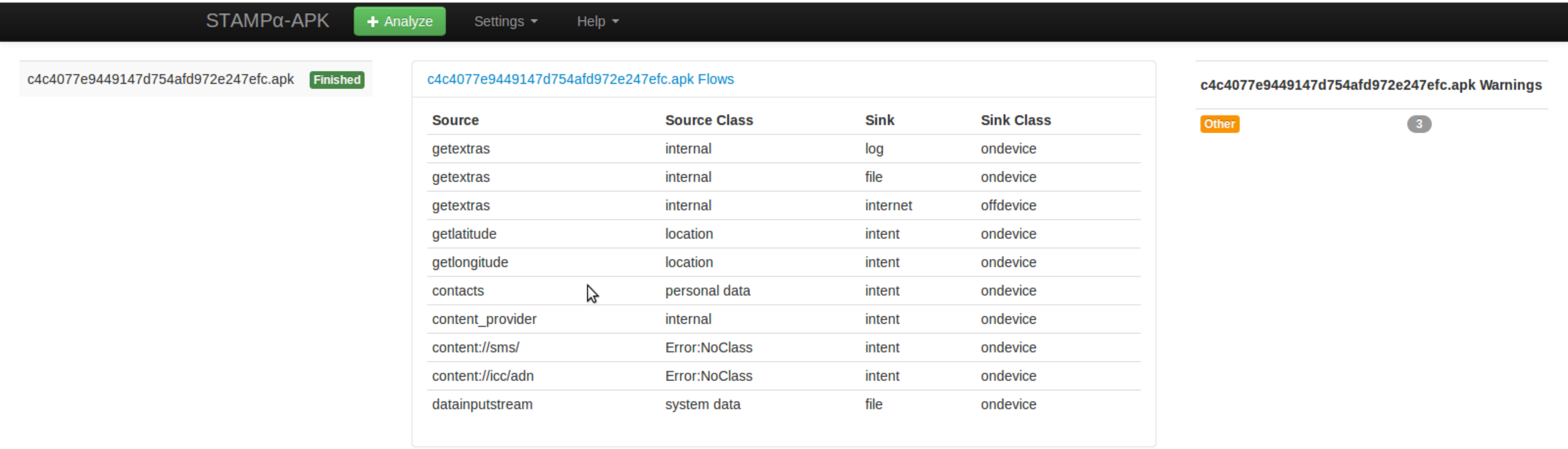
On behalf of all at the Word Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia In what was an unprecedented



Sensitive data leaving device is source-to-sink flow

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

Stamp Source-to-sink Flows



c4c4077e9449147d754afd972e247efc.apk Finished

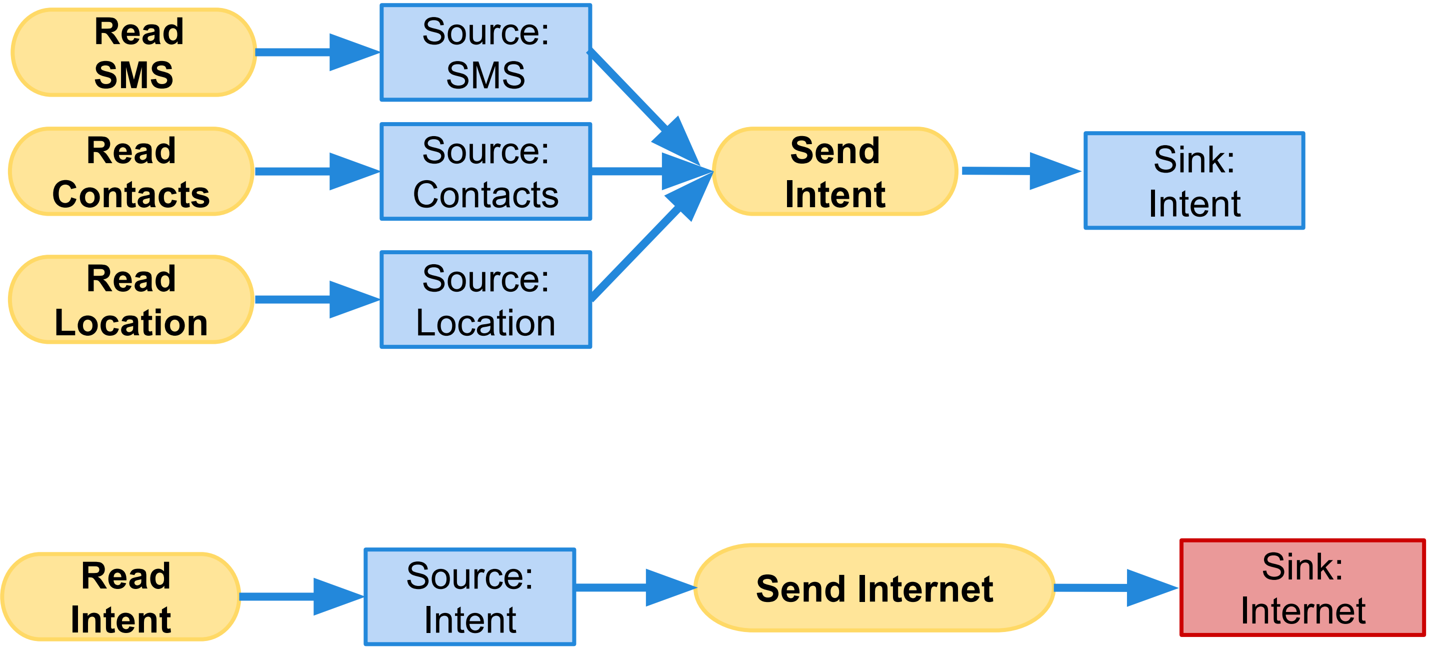
c4c4077e9449147d754afd972e247efc.apk Flows

Source	Source Class	Sink	Sink Class
getextras	internal	log	ondevice
getextras	internal	file	ondevice
getextras	internal	internet	offdevice
getlatitude	location	intent	ondevice
getlongitude	location	intent	ondevice
contacts	personal data	intent	ondevice
content_provider	internal	intent	ondevice
content://sms/	Error:NoClass	intent	ondevice
content://icc/adn	Error:NoClass	intent	ondevice
datainputstream	system data	file	ondevice

c4c4077e9449147d754afd972e247efc.apk Warnings

Other	3

Chuli Source-to-sink Flows



You Saved the Dalai Lama!

Save the Dalai Lama!

Can you help me with something else?

Start

Privacy Policy

This app collects your:

Contacts
Phone Number
Address

Let's look at an example of a privacy-violating program

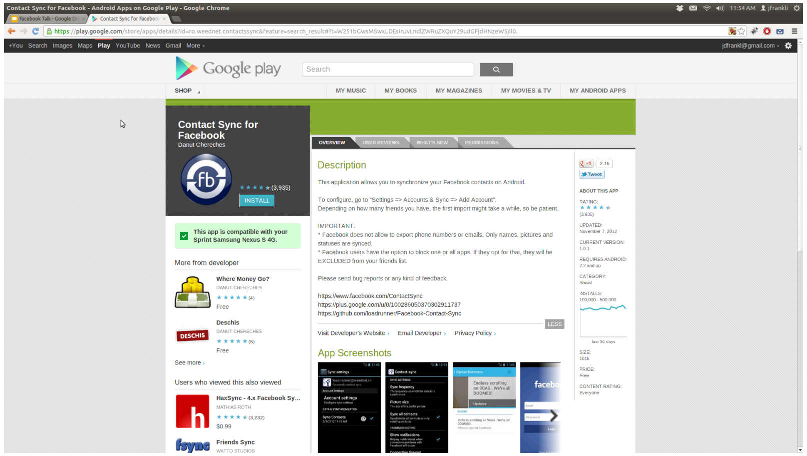
Facebook Contact Sync

Contact Sync for Facebook (unofficial)

Description:

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

Privacy Policy: (page not found)



Contact Sync for Facebook
Danut Chereches
★★★★★ (3,935)

☑ This app is compatible with your Sprint Samsung Nexus S 4G.

More from developer

Where Money Go?
DANUT CHERECHES
★★★★★ (4)
Free

Deschis
DANUT CHERECHES
★★★★★ (6)
Free

See more ›

Users who viewed this also viewed

HaxSync - 4.x Facebook Sy...
MATHIAS ROTH
★★★★★ (3,232)
$0.99

Friends Sync
WATTO STUDIOS

Description

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

To configure, go to "Settings => Accounts & Sync => Add Account".
Depending on how many friends you have, the first import might take a while, so be patient.

IMPORTANT:
* Facebook does not allow 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.

Please send bug reports or any kind of feedback.

https://www.facebook.com/ContactSync
https://plus.google.com/u/0/100286050370302911737
https://github.com/loadrunner/Facebook-Contact-Sync

Visit Developer's Website › Email Developer › Privacy Policy ›

App Screenshots

ABOUT THIS APP

RATING:
★★★★★
(3,935)

UPDATED:
November 7, 2012

CURRENT VERSION:
1.0.1

REQUIRES ANDROID:
2.2 and up

CATEGORY:
Social

INSTALLS:
100,000 - 500,000

SIZE:
101k

PRICE:
Free

CONTENT RATING:
Everyone

Unknowns

Does this app have hidden behaviors?

Does it steal my Facebook data?

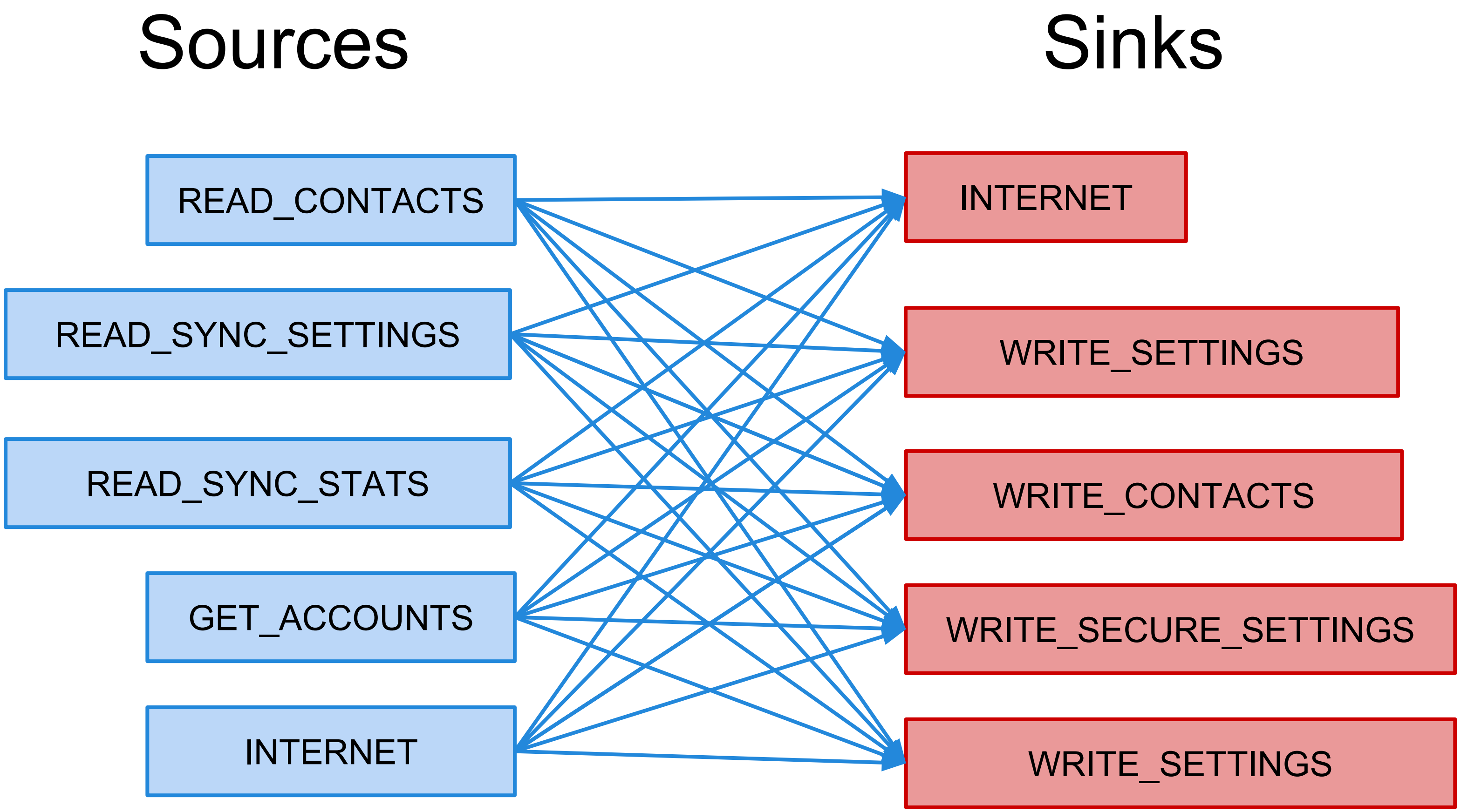
Does it have vulnerabilities?

Does it steal my contacts?

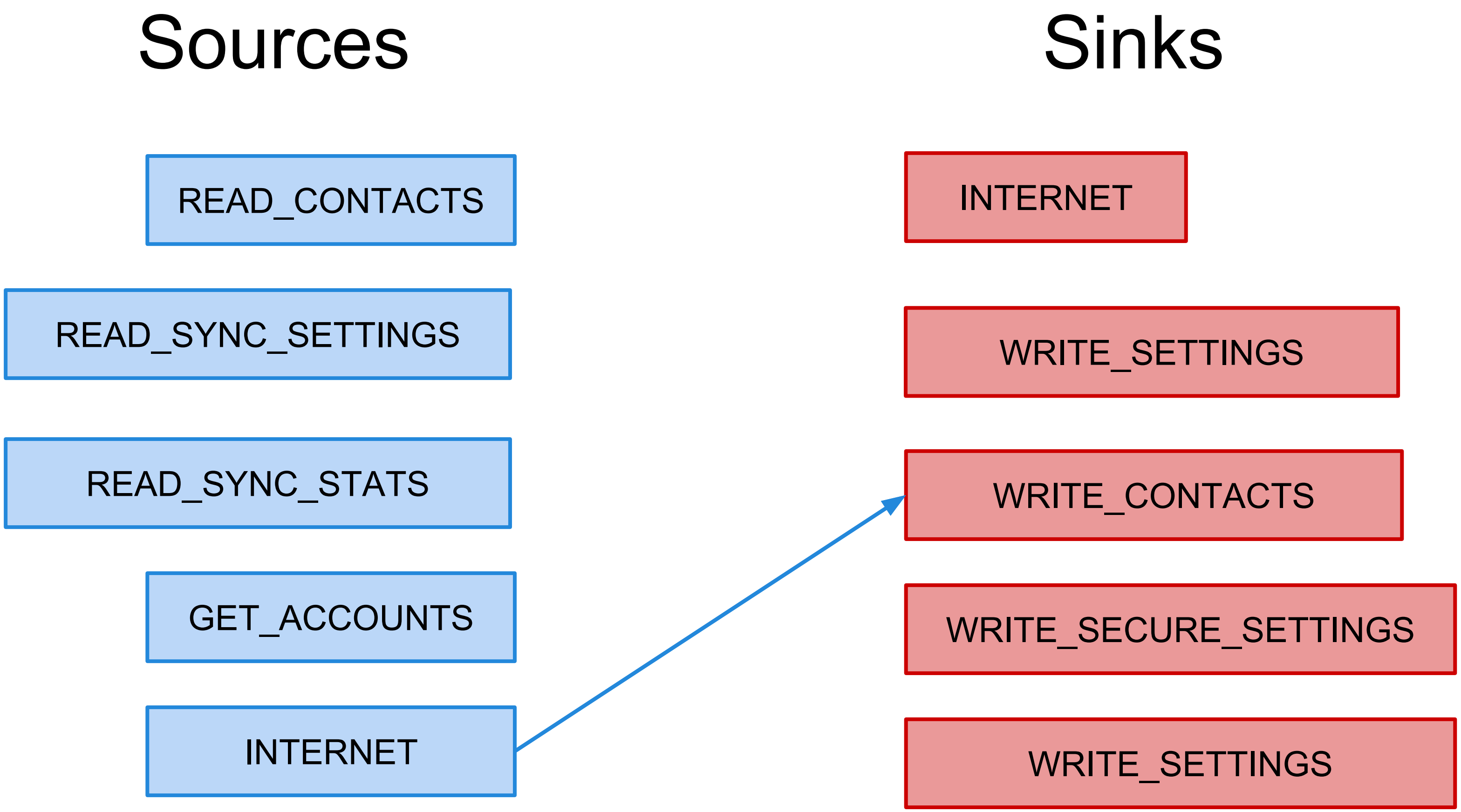
What you get today

Category	**Permission**	**Description**
Your Accounts	AUTHENTICATE_ACCOUNTS	Act as an account authenticator
	MANAGE_ACCOUNTS	Manage accounts list
	USE_CREDENTIALS	Use authentication credentials
Network Communication	**INTERNET**	**Full Internet access**
	ACCESS_NETWORK_STATE	View network state
Your Personal Information	**READ_CONTACTS**	**Read contact data**
	WRITE_CONTACTS	Write contact data
System Tools	WRITE_SETTINGS	Modify global system settings
	WRITE_SYNC_SETTINGS	Write sync settings (e.g. Contact sync)
	READ_SYNC_SETTINGS	Read whether sync is enabled
	READ_SYNC_STATS	Read history of syncs
Your Accounts	GET_ACCOUNTS	Discover known accounts
Extra/Custom	WRITE_SECURE_SETTINGS	Modify secure system settings

Potential Flows



Acceptable Flows



Sources

READ_CONTACTS

READ_SYNC_SETTINGS

READ_SYNC_STATS

GET_ACCOUNTS

INTERNET

Sinks

INTERNET

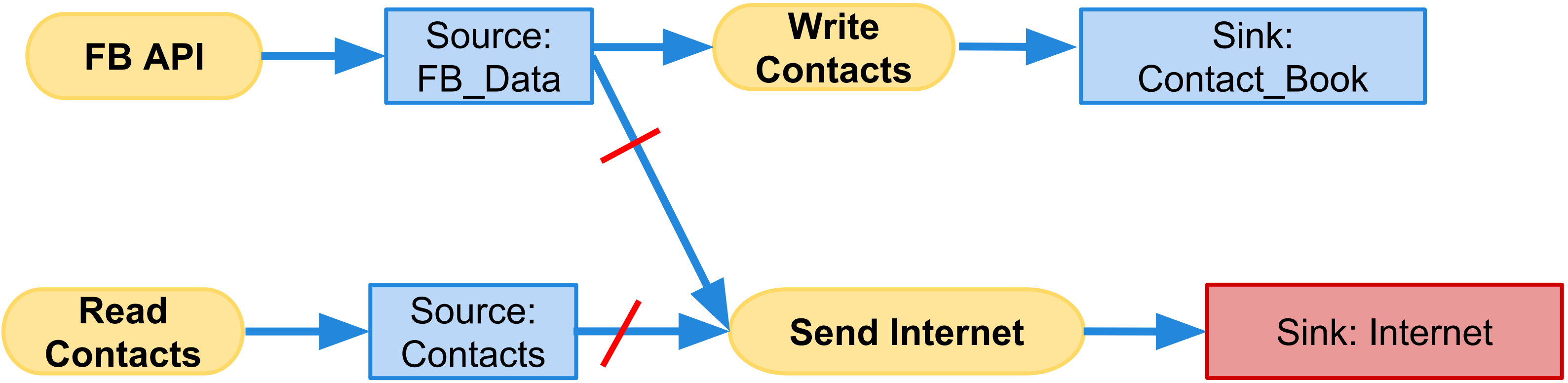
WRITE_SETTINGS

WRITE_CONTACTS

WRITE_SECURE_SETTINGS

WRITE_SETTINGS

Certification



- Red slashes designate absence of flow
- All flows were within expected specification
    - No hidden behaviors

You Saved the Dalai Lama!

Review

- Described Android malware problem
  - Chuli, DroidDream, data collection incentives
- Google Bouncer deployed to detect malware
  - Dynamic analysis - input generation problem
- Defined malware detection game
  - Adversary, Detection System, Policy
- Stamp detection system
  - Static analysis - scalability/false positives
- Privacy analysis
  - Mandatory notification of data collection

You Saved the Dalai Lama!

Questions?

Questions?

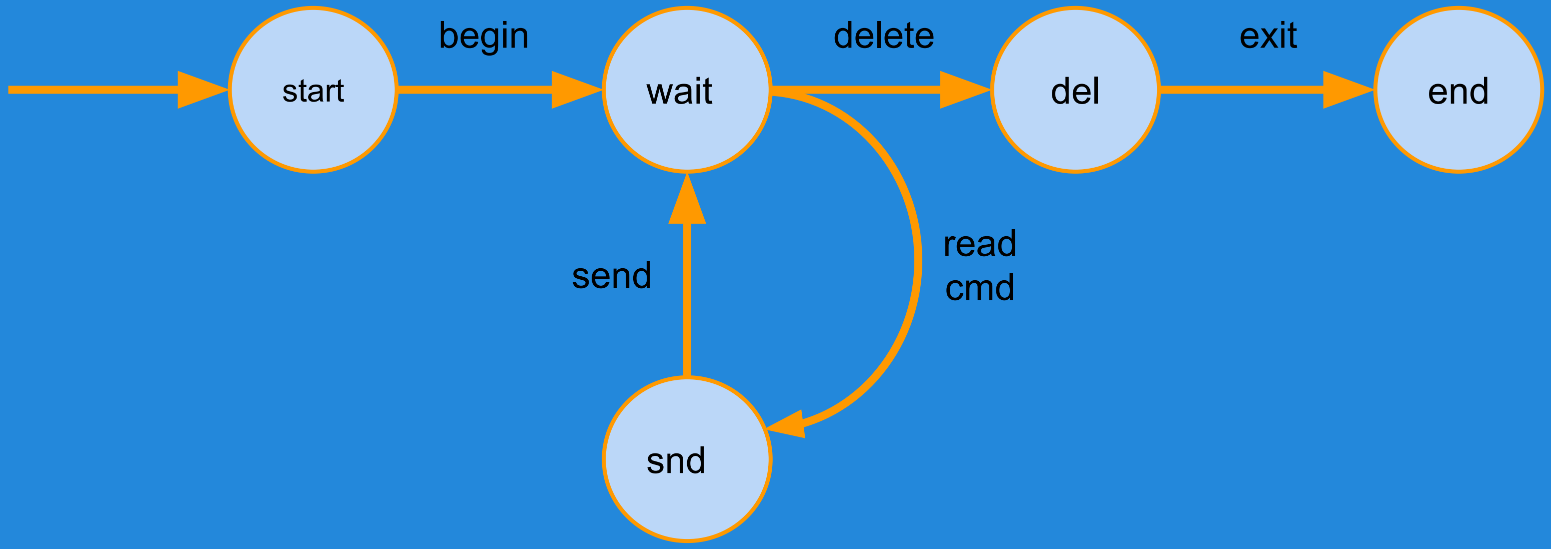
Jason Franklin, Ph.D.

jfrankli@cs.stanford.edu

Credits:

Alex Aiken, Saswat Anand, John Mitchell

Abstract Program Execution



States: mapping of variable names to values
Transitions: relation on pairs of states
Traces: sequence of states or state,transition pairs

Opportunity

Centralization + Certification = Safety

Free

Beyond testing

Policies,
Procedures,
Best practices,
Verification

Broadly defined

Cost,
Legal Compliance,
Performance,
Privacy,
Security