Shining the Light on Flashlight and the Security of Thousands of Mobile Apps

Theodora Titonis, Vice President Mobile, Veracode

Professional Techniques – T13

AGENDA

- The Mobile Security Stack
- Recent Attacks on Each Layer
- Securing the Application Layer
- Examples of Risky and Malicious Apps
- Shining the Light on Flashlight Apps
- What can we do
- Questions

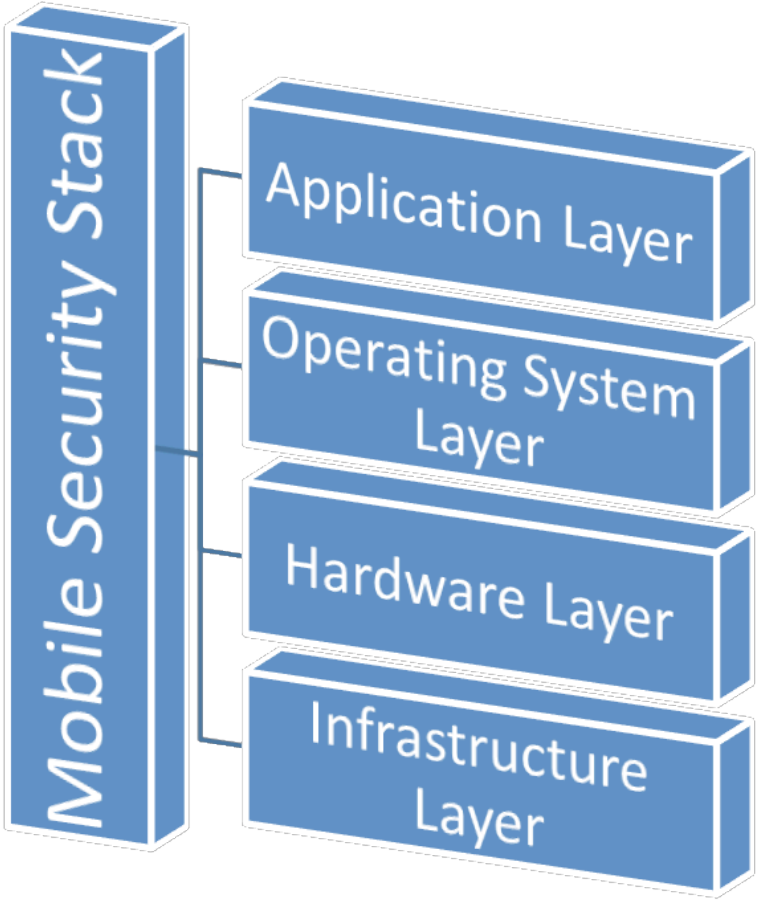
THE MOBILE SECURITY STACK

CYBERSECURITY

The protection of electronic information and communications systems and the data contained within those systems.

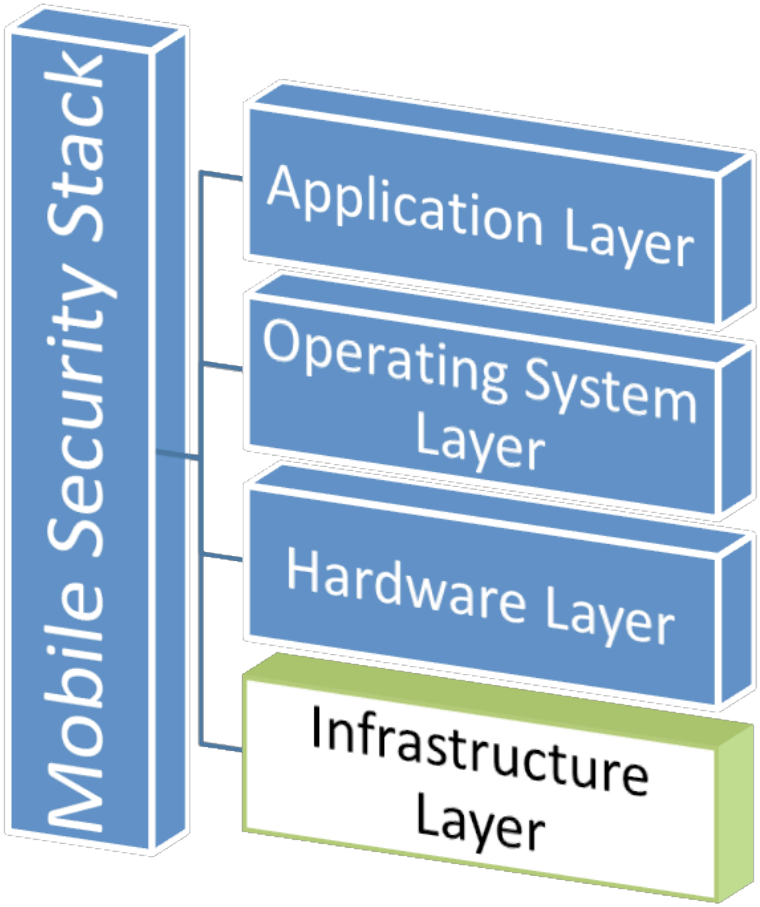
MOBILE SECURITY STACK

- Well-defined layers
- An abstraction based model
- Allows for focus on specific area of concern/expertise
- Results in a comprehensive approach



INFRASTRUCTURE

- Supports all other layers
- Owned by the mobile carrier
- Encompasses protocols like LTE, GPS, SMS, MMS, VOIP
- Vulnerabilities effective across multiple carriers



INFRASTRUCTURE

Los Angeles Times | ARTICLE COLLECTIONS

← Back to Original Article

VoIP phone hackers pose public safety threat

Hospitals, 911 call centers and other public safety agencies can be shut down by hackers

July 18, 2013 | By Paresh Dave

The demand stunned the hospital employee. She had picked up the emergency room's phc doctor. But instead, an unfamiliar male greeted her by name and then threatened to paral him hundreds of dollars.

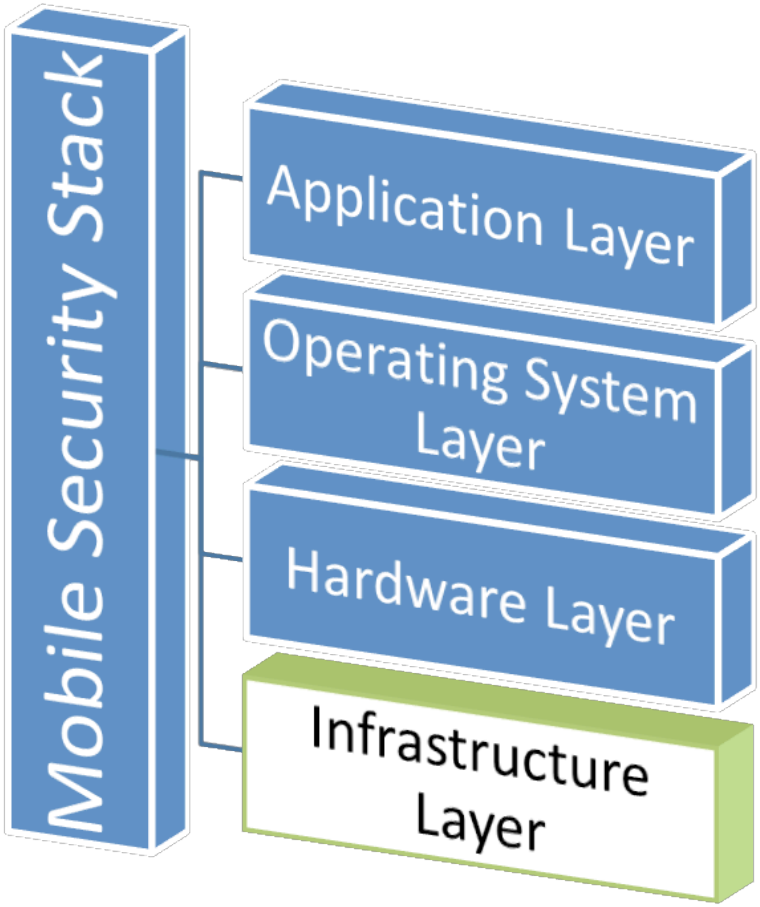
Shortly after the worker hung up on the caller, the ER's six phone lines went dead. For nea families calling the San Diego hospital heard nothing but busy signals.

The hospital had become a victim of an extortionist who, probably using not much more tl handedly generated enough calls to tie up the lines.

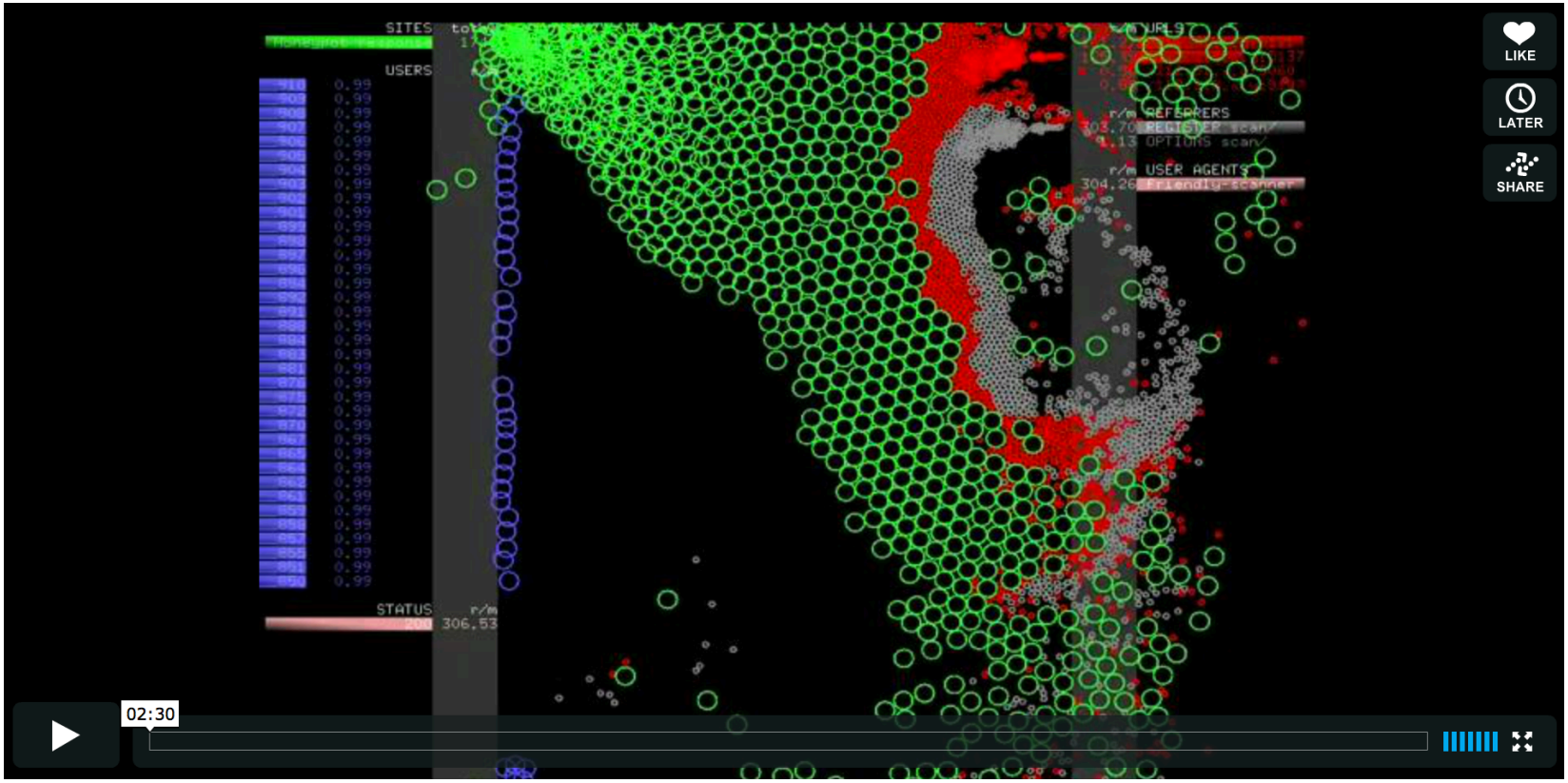
Distributed denial-of-service attacks — taking a website down by forcing thousands of con visit and overwhelm it — has been a favored choice of hackers since the advent of the Inte

Now, scammers are inundating phone lines by exploiting vulnerabilities in the burgeoning system.

The frequency of such attacks is alarming security experts and law enforcement officials, v tool of scammers, it could easily be adopted by malicious hackers and terrorists to knock c 911 call centers.

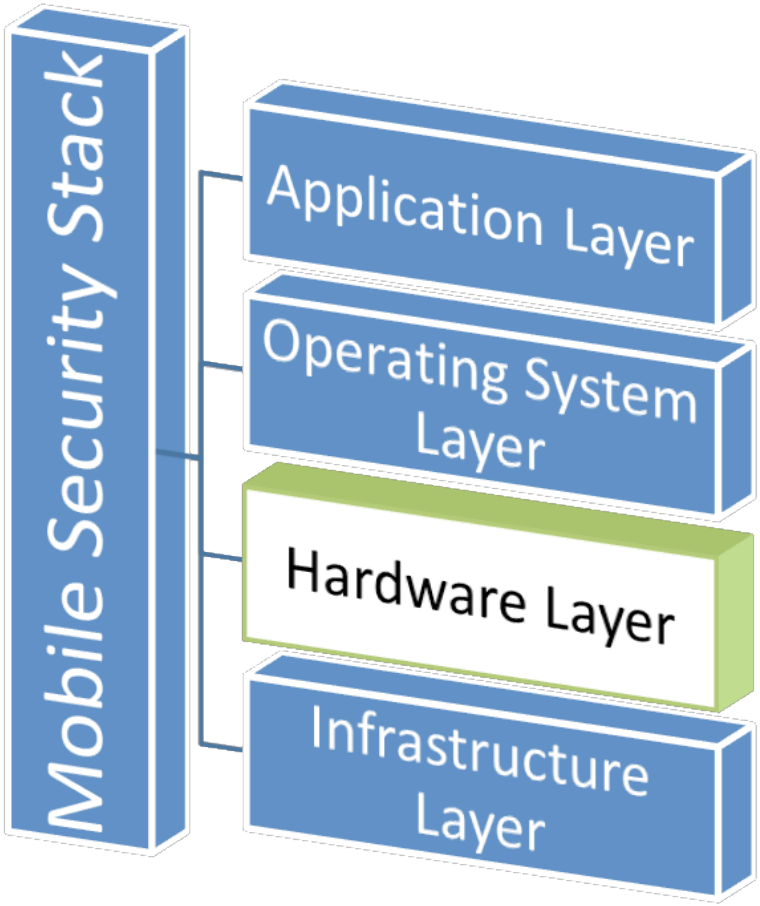


INFRASTRUCTURE



HARDWARE

- Smartphone or Tablet
- Firmware
- Maintained by manufacturer
- Carrier pushes upgrades
- Infrastructure interfaces with firmware to pass data
- Accessible to the operating system for device control



HARDWARE

CRN

Android Phone Hack Bypasses Samsung Galaxy Note 2 Lock Screen

By Robert Westervelt, CRN 4:39 PM EST Mon. Mar. 04, 2013

A hacking technique demonstrating a way to bypass the device lock screen feature on Android smartphones has been discovered.

The security flaw was discovered on Android 4.1.2 and demonstrated on a Samsung Galaxy Note 2 smartphone. Terence Eden, a mobile enthusiast, posted the smartphone lock bypass technique on his personal blog.

The bypass could potentially enable someone to make a phone call, record from the microphone, play music or interact with a server. The attacker could also view the calendar or emails if a widget displays them on the home screen, Eden said.

[**Related:** Apple Vs. Android: Which Smartphone Platform Is Safer?]

The video demonstrates the hack on the stock firmware, which Samsung recently pushed out to users. Hitting the home screen button briefly displays the home screen, enabling a user to view it and potentially run apps by quickly tapping on them.

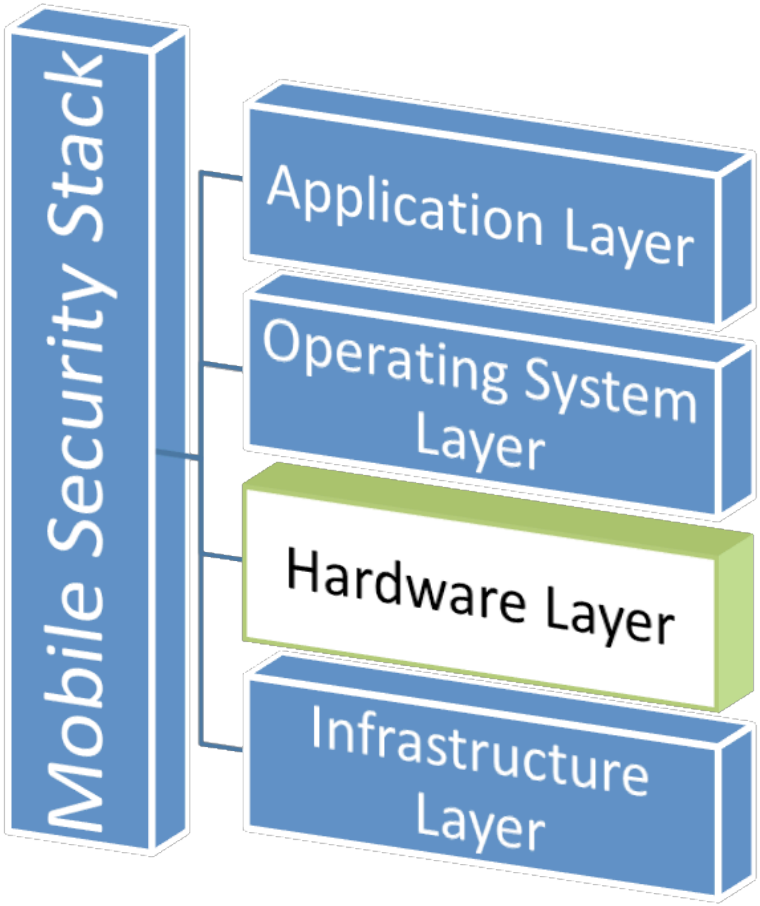
"This is a reasonably small vulnerability," Eden said in the video demonstration. "If the person has direct-dial on there, you will be able to dial it."

Eden said he released details about the bypass because it has a number of limitations. To make a phone call, the direct dial widget needs to be on the device's home screen. Attempting to run an app will send it immediately into the background, he wrote.

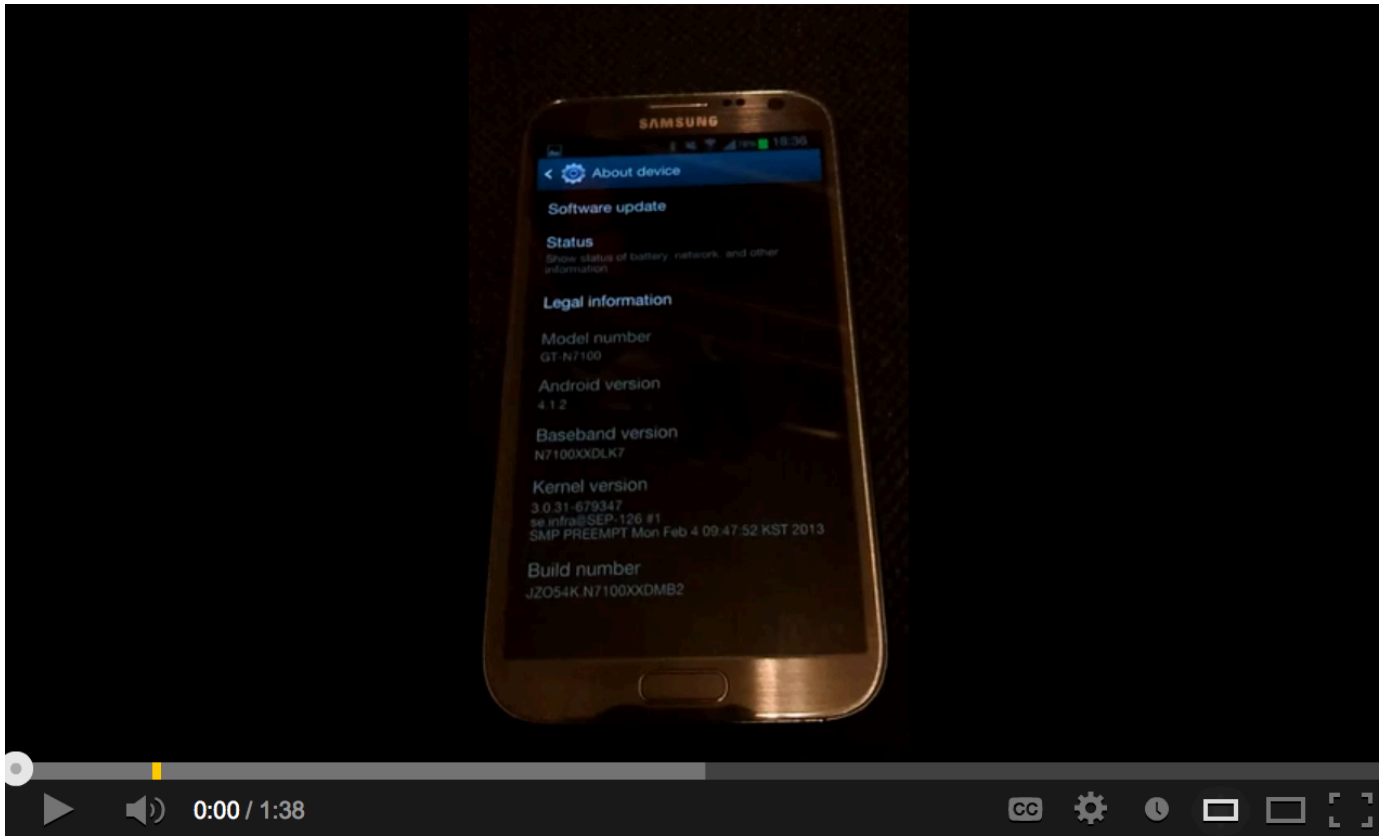
"Rapidly tapping the home button will -- depending on your launcher -- allow you to see what is on every home screen," wrote Eden. "Using an external video camera you should be able to clearly see all the user's calendar & email widgets if they have enabled them."

Last month, Apple rushed out a security update for iPhones, fixing a coding error that enabled users to bypass the pass code features on the smartphones. The flaw was similar to a previous one in the iPhone, which was reintroduced by developers into the phone firmware during the coding process. The iPhone hack was slightly more serious, enabling users to get around a security code to make a call, access voicemail, view or modify contacts and browse photos.

Both the Android and Apple bypasses appear to be fairly low-level hacks, said Cameron Camp, a security researcher at Bratislava, Slovakia-based security firm ESET. The real issue, according to Cameron, is the lengthy time it takes for Google to get an update out to impacted device owners. A security fix issued by Google would have to go upstream to handset manufacturers and then to carriers who will release a fix to device owners.



HARDWARE


SAMSUNG
About device
Software update
Status
Legal information
Model number
GT-N7100
Android version
4.1.2
Baseband version
N7100XXDLK7
Kernel version
3.0.31-679347
se.infra@SEP-126 #1
SMP PREEMPT Mon Feb 4 09:47:52 KST 2013
Build number
JZO54K.N7100XXDMB2
0:00 / 1:38

HARDWARE

ZDNet

White Papers | Hot Topics | Downloads | Reviews | Newsletters

US Edition | Virtualization | BYOD | SMB | Data Center | CXO | Windows 8 | Apple

MUST READ: *15 most wanted features in the next iPhon*

Topic: Security *Discover* *Follow via:*

Researchers reveal how to hack an iPhone in 60 seconds

Summary: *Three Georgia Tech hackers have disclosed how to hack iPhones and iPads with malware in under sixty seconds using a "malicious charger." UPDATED.*

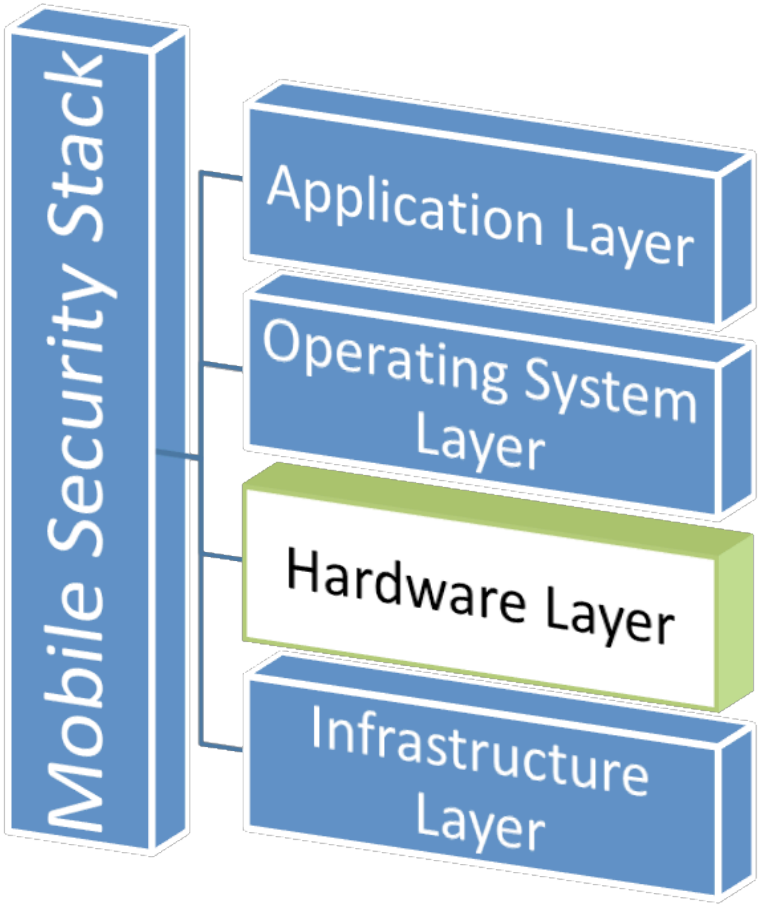
By Violet Blue for Zero Day | July 31, 2013 -- 22:05 GMT (15:05 PDT)
Follow @violetblue

Three Georgia Tech hackers have revealed how to hack iPhones and iPads with malware imitating ordinary apps in under sixty seconds using a "malicious charger."

Today at a Black Hat USA 2013 press conference, the researchers revealed for the first time exactly how the USB charger they built can compromise iOS devices in less than a minute.

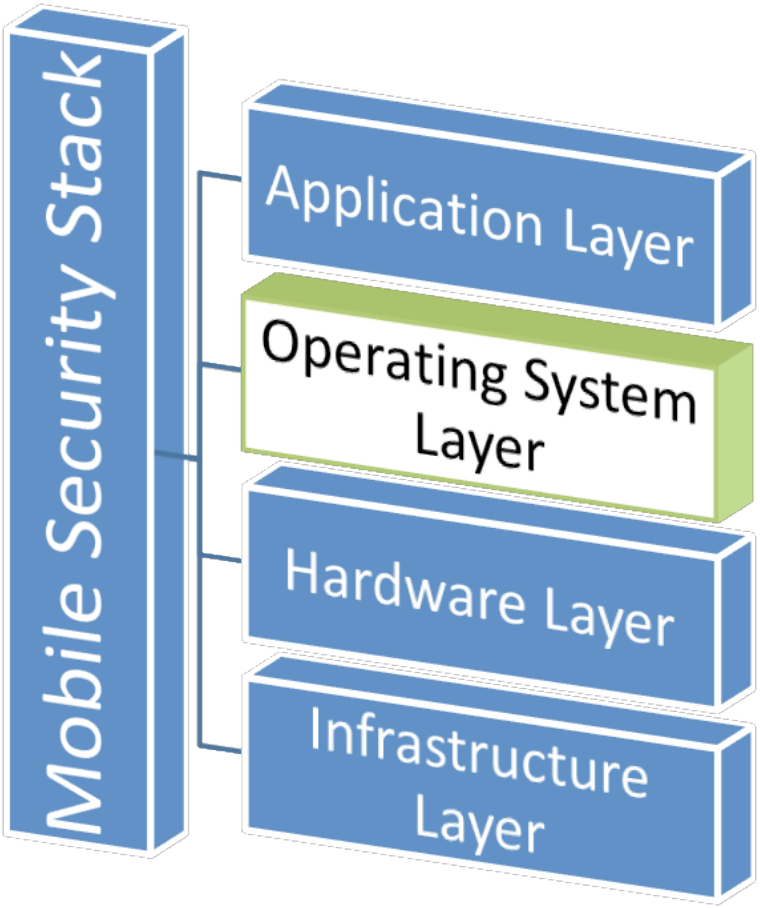
Billy Lau, Yeongjin Jang and Chengyu Song showed how they made an ordinary looking charger into a malicious vector for transmitting malware using an open source BeagleBoard, available for $125 (similar to a Raspberry Pi).

For the demonstration, the researchers used an iPhone. They plugged in the phone, and when the passcode was entered, the sign-code attack began.



OPERATING SYSTEM

- The software running on the device
- Apple's iOS and Google's Android
- Allows communication between the hardware and application layers
- Provides access to it's resources by publishing Application Programming Interfaces (APIs)



OPERATING SYSTEM

PC | REVIEWS | NEWS & OPINIONS | DOWNLOADS | BUSINESS | DAILY DEALS

SecurityWatch with Neil Rubenking

Top Categories

Security Software
Hacking
Privacy
Social Media
Top Threats

SEE ALL »

Trending Tags

malware
vulnerabilities
vulnerability
patch
antivirus
apple
adobe

SEE ALL »

Follow

More Blogs

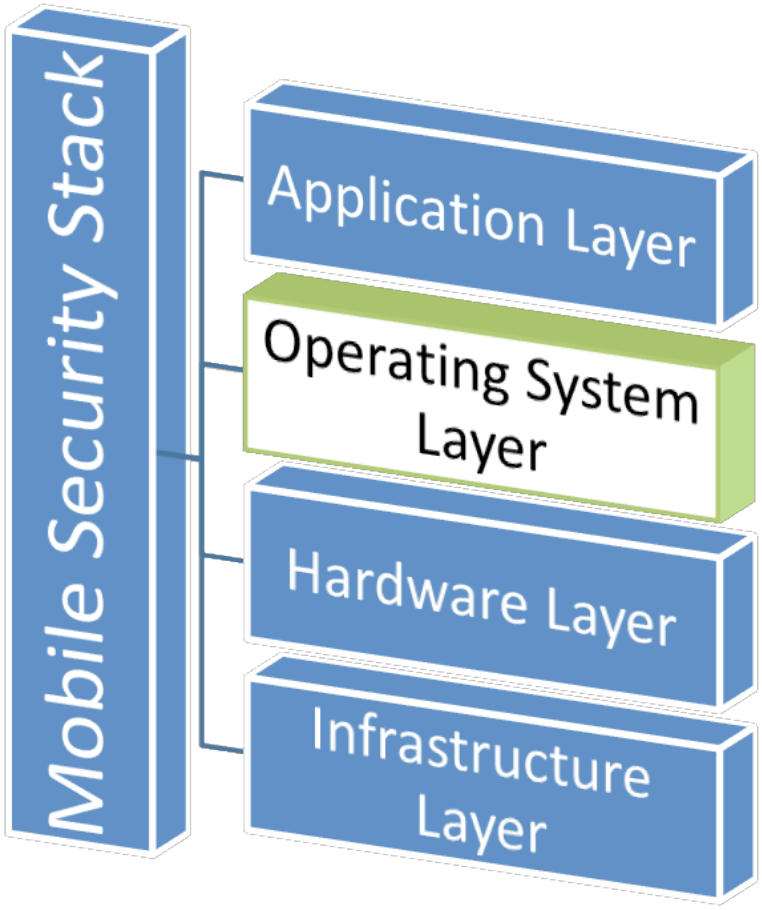
Forward Thinking

Black Hat: Multiple "Master Key" Vulnerabilities Afflict Android

Aug 01, 2013 5:31 PM EST | [num] Comments

By Neil J. Rubenking

It all started as a prank, explained Bluebox Security's Jeff Forristal. The Bluebox team wanted to create a hacked version of the FourSquare app that would make it seem like you're somewhere odd, like Antarctica. Alas, Google Maps rejected requests from the tweaked app. Pursuing ways around that problem led the team to the weakness they dubbed "Master Key". "This topic has already been covered," said Forristall. "It leaked. It's been out for a few weeks. But actually there's more than one master key, so this talk grew from one bug to four."



OPERATING SYSTEM

Forbes | New Posts | Most Popular NFL's Richest Teams | Lists Top Innovative Companies | Vid Vegas

Adrian Kingsley-Hughes, Contributor
I write about hardware and software YOU need to know about.
+ Follow (141)

TECH | 2/18/2013 @ 4:00PM | 4,512 views

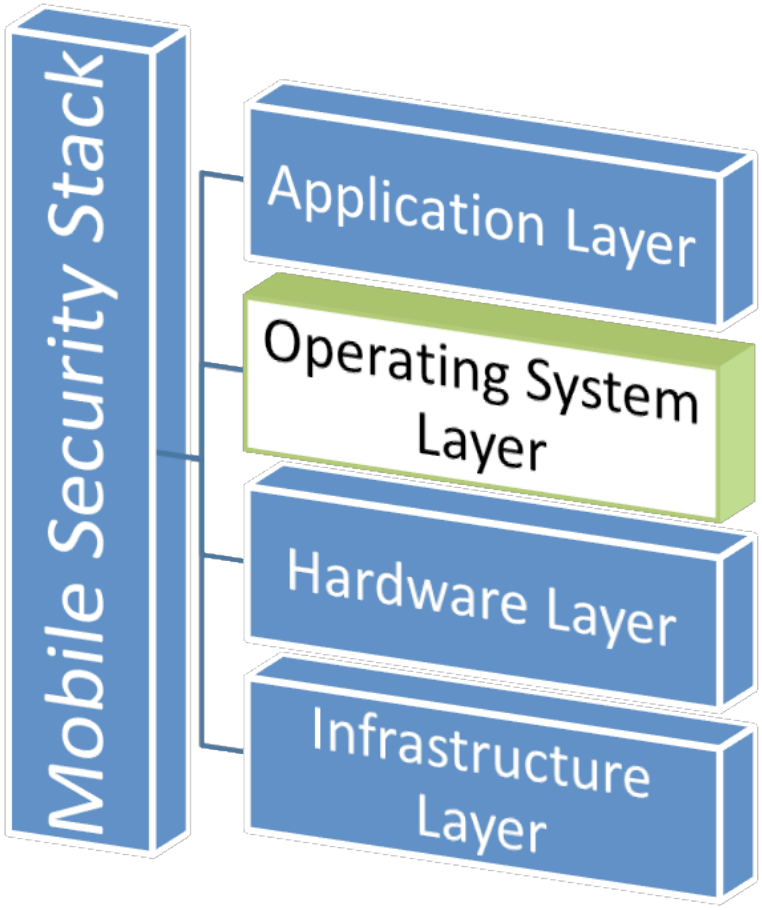
New iOS Lock Screen Vulnerability Uncovered

+ Comment Now + Follow Comments

Hot on the heels of a vulnerability that gave snoopers the ability to bypass the iPhone's passcode in iOS 6 and make calls, view and modify contacts, and even access to photos via the Contacts app, is a new one that allows the entire contents of the handset to by synced with iTunes.

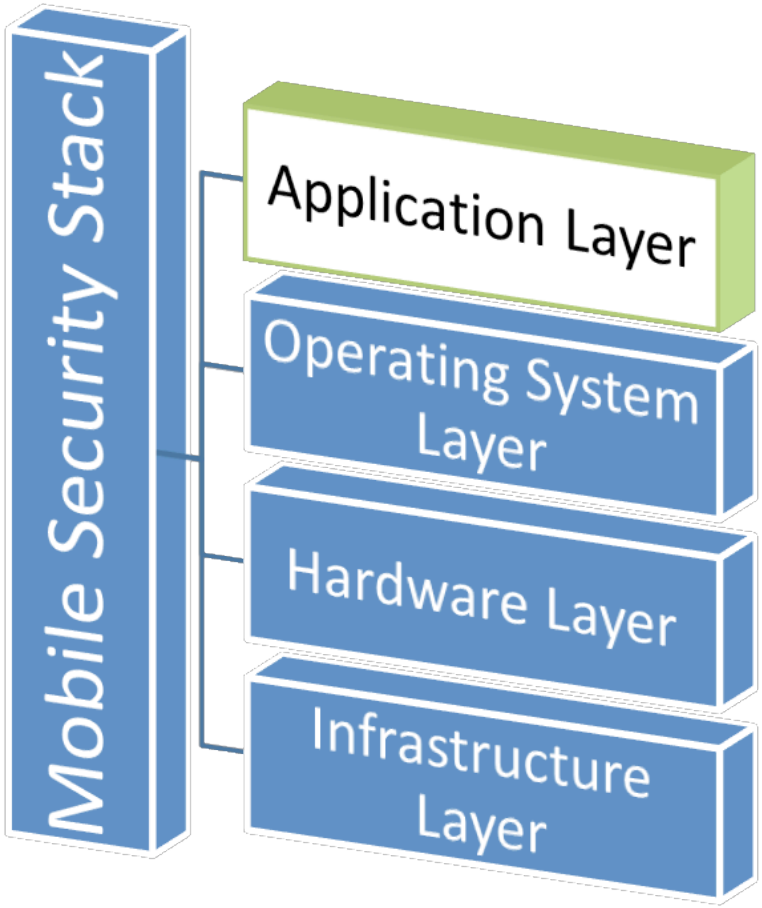
"The vulnerability is located in the main login module of the mobile iOS device [applies to iPhone or iPad] when processing to use the screenshot function in combination with the emergency call and power button," said Vulnerability Lab, who initially discovered the flaw.

The vulnerability allows anyone with physical access to the iOS device the ability to easily bypass the passcode lock and use a USB cable to get access to the data stored on the iPhone or iPad from a Mac or PC.



APPLICATION

- More app downloads than stars in our galaxy by 2017
- Software that the end-user directly interfaces with
- Utilizes the API's provide by the operating system (OS)
- Interfaces with the cloud or device through the OS



APPLICATION

Android app malware rates jump 40 percent

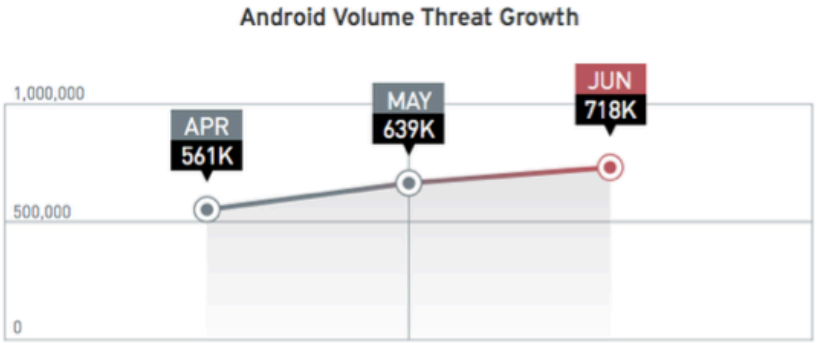
Summary: *A new report released by Trend Micro says that mobile malware rates are skyrocketing.*

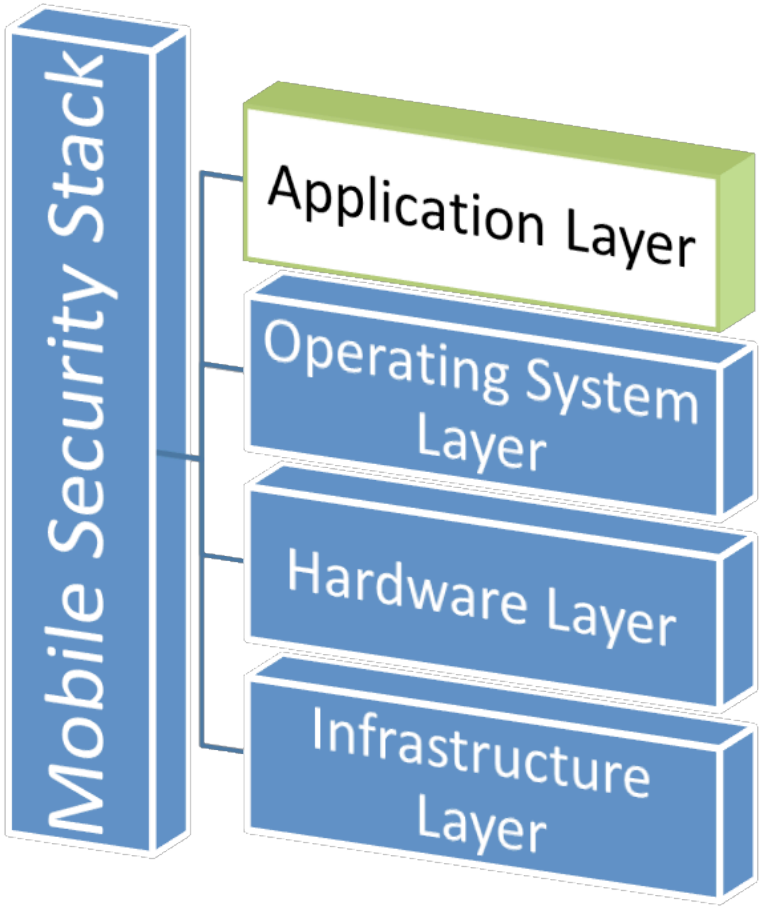
By Charlie Osborne for Zero Day | August 7, 2013 -- 10:00 GMT (03:00 PDT)
Follow @ZDNetCharlie

Mobile malware in the Android ecosystem has grown by over 40 percent in the past few months, researchers say.

A new report issued by Trend Micro (.pdf) says that high-risk, malicious app rates on the Google Android operating system rose to 718,000 at the end of the second quarter in comparison to 509,000 in the first quarter of this year.

The number of malicious Android apps in circulation surged by over 350,000 in this time period -- which originally took three years to reach when Google's Android operating system became established.





APPLICATION

COMMUNICATIONS NEWS

2 COMMENTS

Remotely Assembled Malware Blows Past Apple's Screening Process

Research unmasks a weakness of Apple's App Store: new apps apparently are run for only a few seconds before approval.

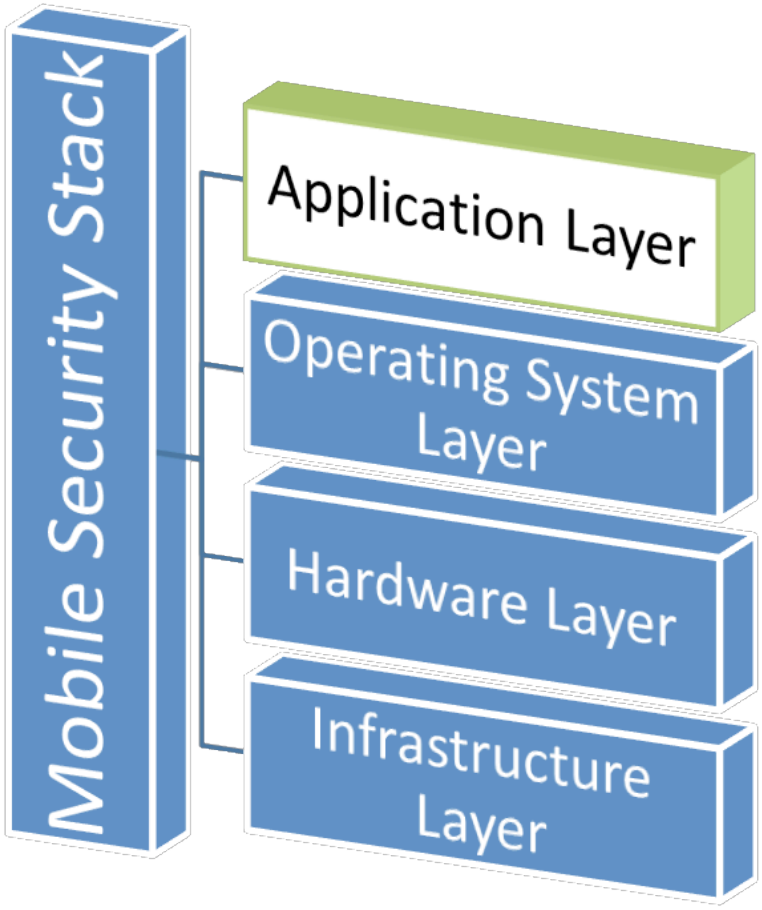
By David Talbot on August 15, 2013

Mystery has long shrouded how Apple vets iPhone, iPad, and iPod apps for safety. Now, researchers who managed to get a malicious app up for sale in the App Store have determined that the company's review process runs at least some programs for only a few seconds before giving the green light.

This wasn't long enough for Apple to notice that an app that purported to offer news from Georgia Tech contained code fragments that later assembled themselves into a malicious digital creature. This

WHY IT MATTERS

More than 600 million devices with Apple's iOS have been sold.



SECURING THE APPLICATION LAYER

APPLICATION

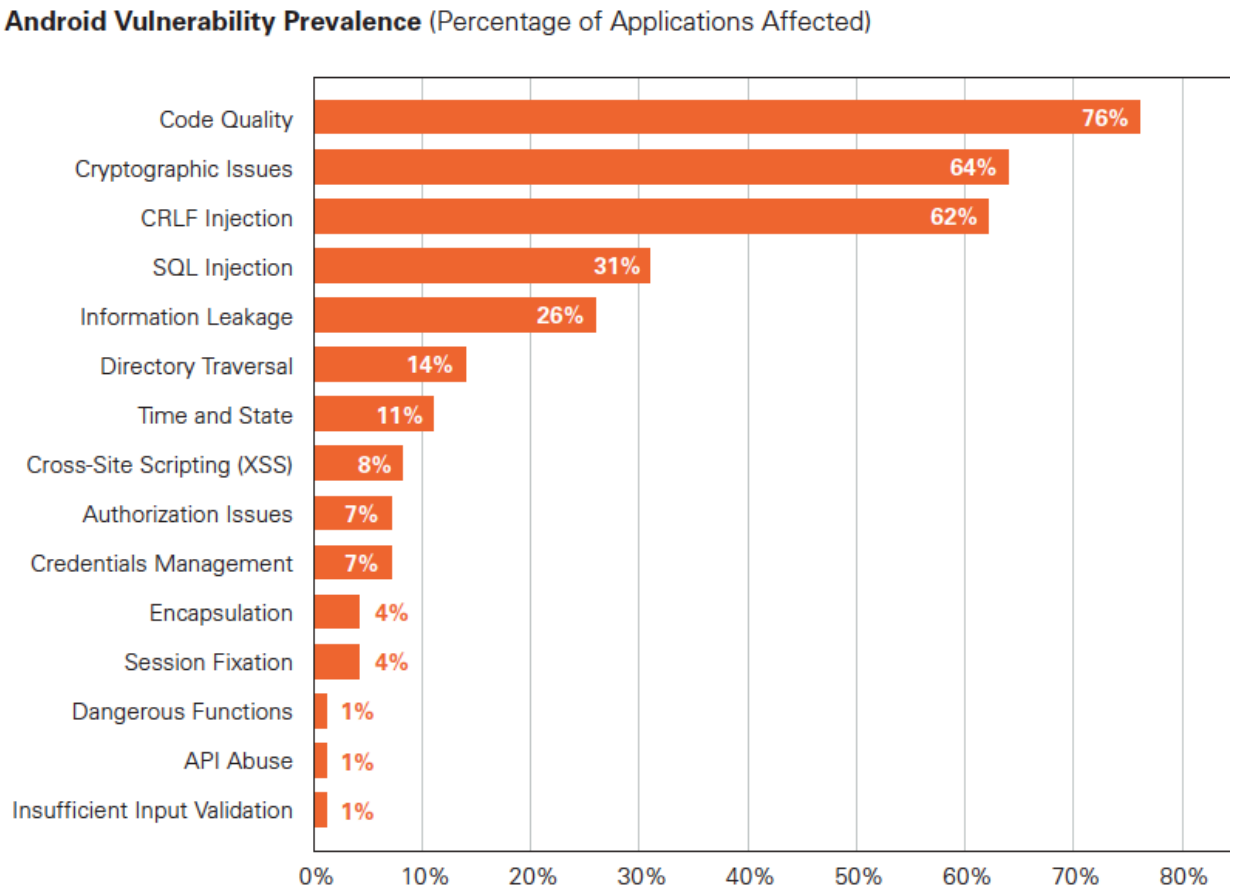
Insecure apps are the leading cause of security breaches and data loss.

VULNERABILITIES

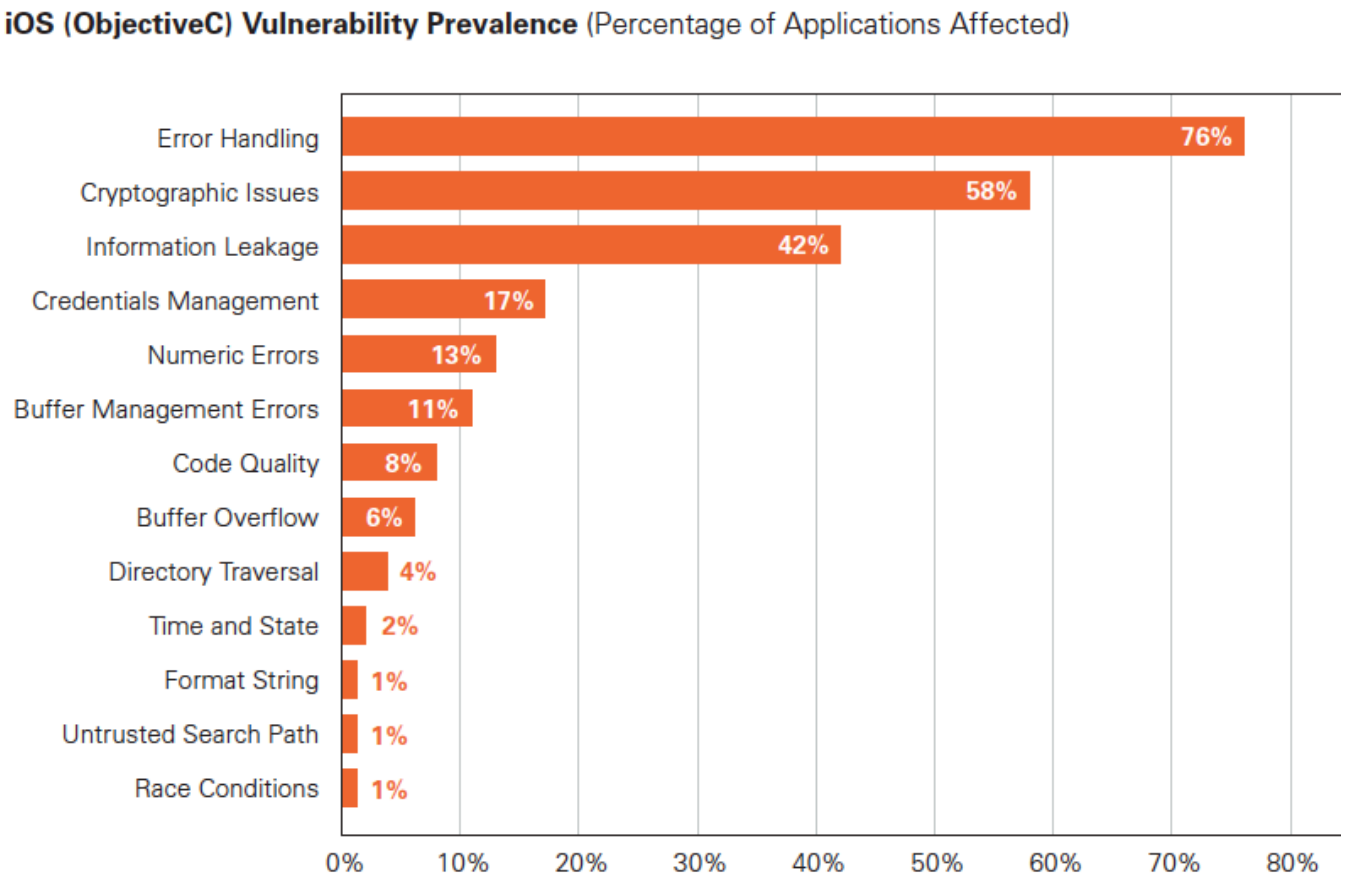
Vulnerability Distribution for Mobile Platforms (Share of Total Vulnerabilities Found)

Android		iOS	
CRLF Injection	37%	Information Leakage	62%
Cryptographic Issues	33%	Error Handling	20%
Information Leakage	10%	Cryptographic Issues	7%
SQL Injection	9%	Directory Traversal	6%
Time and State	4%	Buffer Management Errors	3%

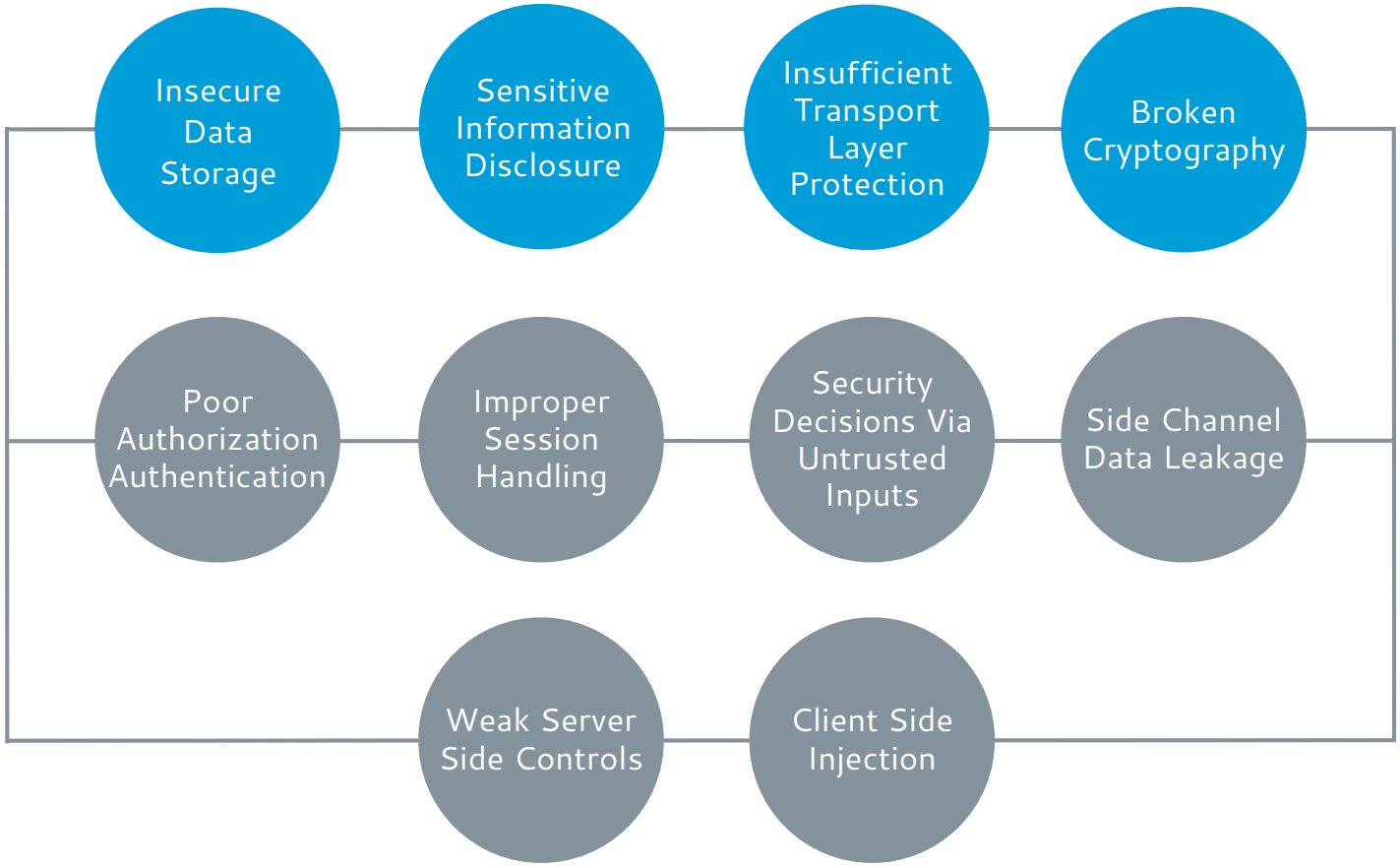
ANDROID VULNERABILITIES



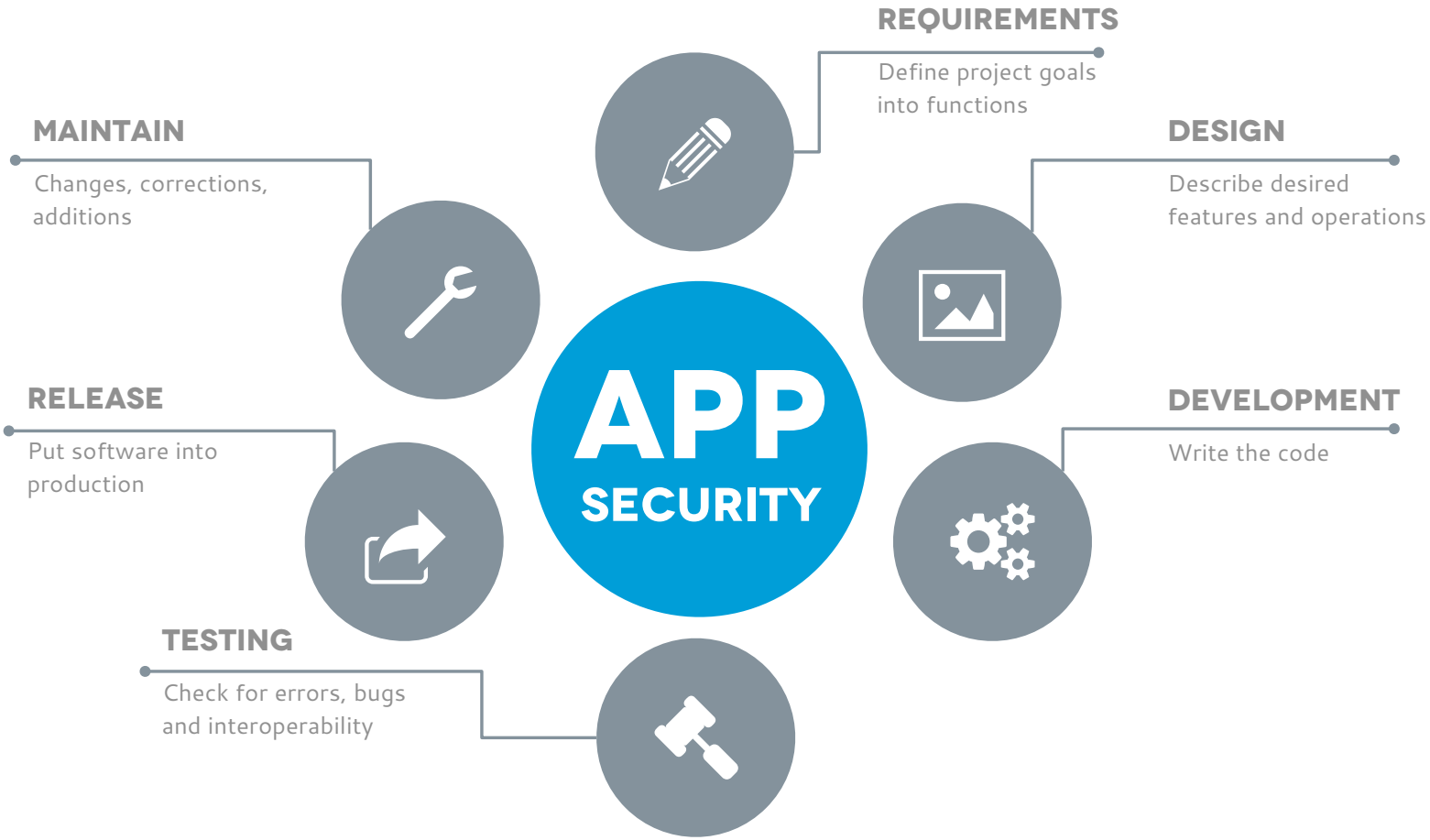
iOS VULNERABILITIES



OWASP MOBILE TOP 10



APP DEVELOPMENT LIFECYCLE

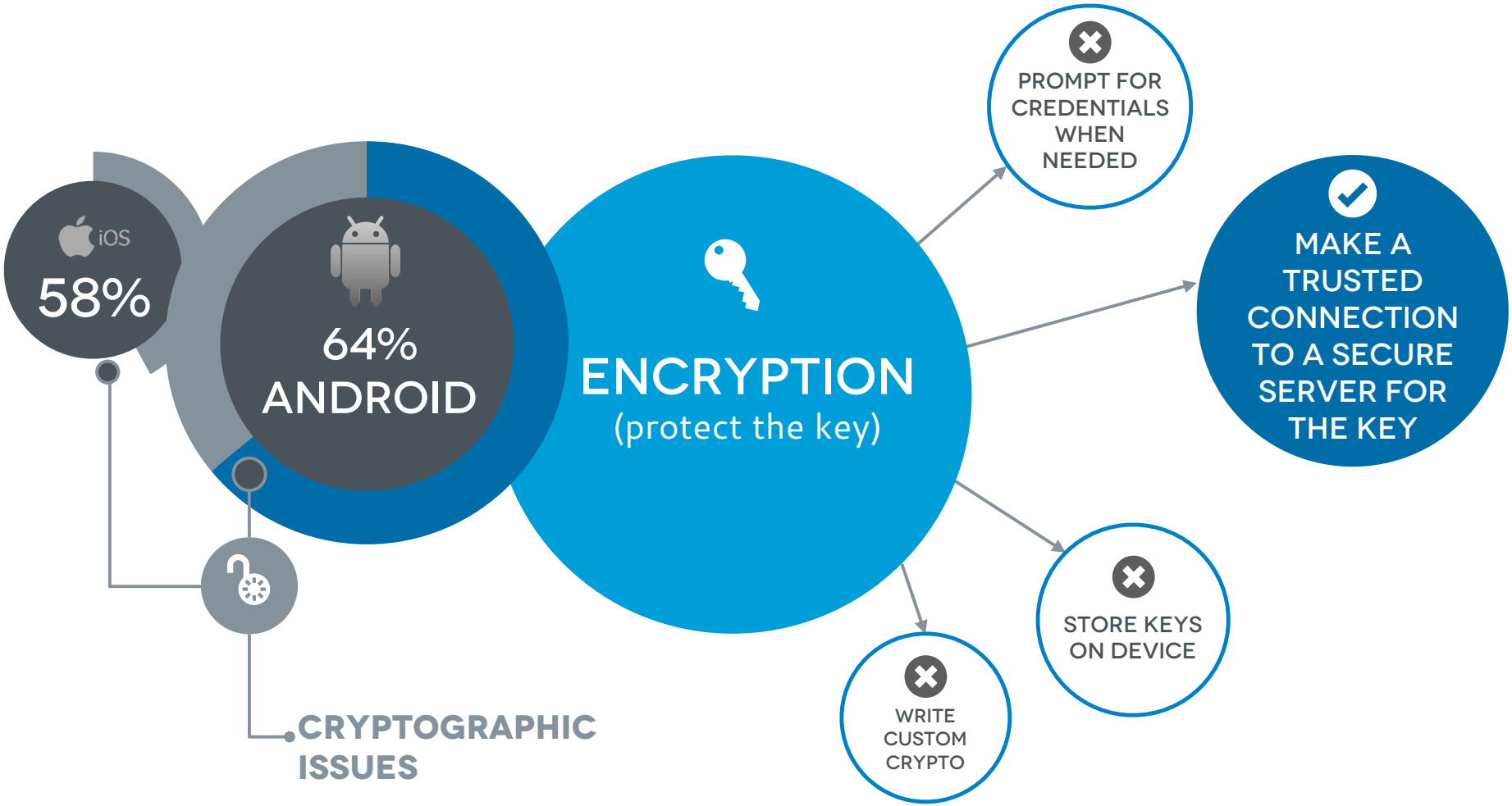


INSECURE DATA STORAGE

The basic security architecture, access controls and isolation provided to files and databases may be adequate for non-sensitive data

There are **NO** good ways,
native to Android,
to store sensitive data
on the device

PROPER USE OF ENCRYPTION



PROTECT SENSITIVE DATA

1. Take a user-supplied
2. Derive 256-bit AES key from password
3. Encrypt and decrypt data at will

STORE DATA ANYWHERE

Once we encrypt the data we can store it in a file, in a database, even on the SD card

DO NOT STORE KEY

Keep the symmetric key from compromise by NOT storing it anywhere at anytime

```
String password = ...;
String PBE_ALGORITHM = "PBEWithSHA256And256BitAES-CBC-BC";
String CIPHER_ALGORITHM = "AES/CBC/PKCS5Padding";
int NUM_OF_ITERATIONS = 1000;
int KEY_SIZE = 256;
byte[] salt = "abababababababababab".getBytes();
byte[] iv = "1234567890abcdef".getBytes();
String clearText = ...; // This is the value to be encrypted.
byte[] encryptedText;
byte[] decryptedText;
try
{
  PBEKeySpec pbeKeySpec = new PBEKeySpec(password.toCharArray(),
  salt, NUM_OF_ITERATIONS, KEY_SIZE);
  SecretKeyFactory keyFactory = SecretKeyFactory.getInstance(PBE_ALGORITHM);
  SecretKey tempKey = keyFactory.generateSecret(pbeKeySpec);
  SecretKey secretKey = new SecretKeySpec(tempKey.getEncoded(), "AES");
  IvParameterSpec ivSpec = new IvParameterSpec(iv);
  Cipher encCipher = Cipher.getInstance(CIPHER_ALGORITHM);
  encCipher.init(Cipher.ENCRYPT_MODE, secretKey, ivSpec);
  Cipher decCipher = Cipher.getInstance(CIPHER_ALGORITHM);
  decCipher.init(Cipher.DECRYPT_MODE, secretKey, ivSpec);
  encryptedText = encCipher.doFinal(clearText.getBytes());
  decryptedText = decCipher.doFinal(encryptedText);
  String sameAsClearText = new String(decryptedText);
}
  catch (Exception e)
{
...
}
```

RISKY AND MALICIOUS APPS

MOBILE ENTERPRISE

APP PRODUCER

By 2015, mobile application development projects will outnumber native PC projects by

4-to-1*

APP CONSUMER

62%

of companies to allow BYOD by year's end[1]

93%

of companies face challenges adopting BYOD policies[2]

*Gartner Top Predictions for IT Organizations and Users, 2012 and Beyond

[1]http://www.zdnet.com/unavoidable-62-percent-of-companies-to-allow-byod-by-years-end-7000010703

[2]http://www.net-security.org/secworld.php?id=15006

MOBILE ENTERPRISE

APP PRODUCER

Mobile SDLC:

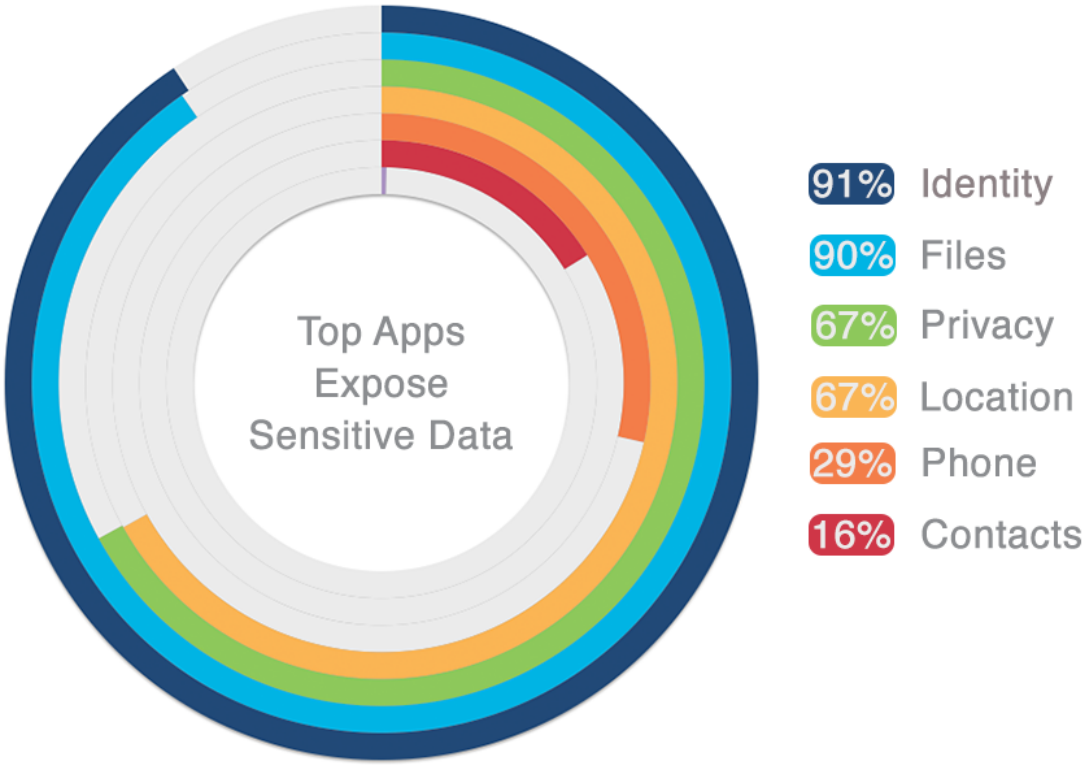
- **Volume:** 10-100s of apps
- **Speed:** New apps every quarter
- **Choice:** Developer driven

APP CONSUMER

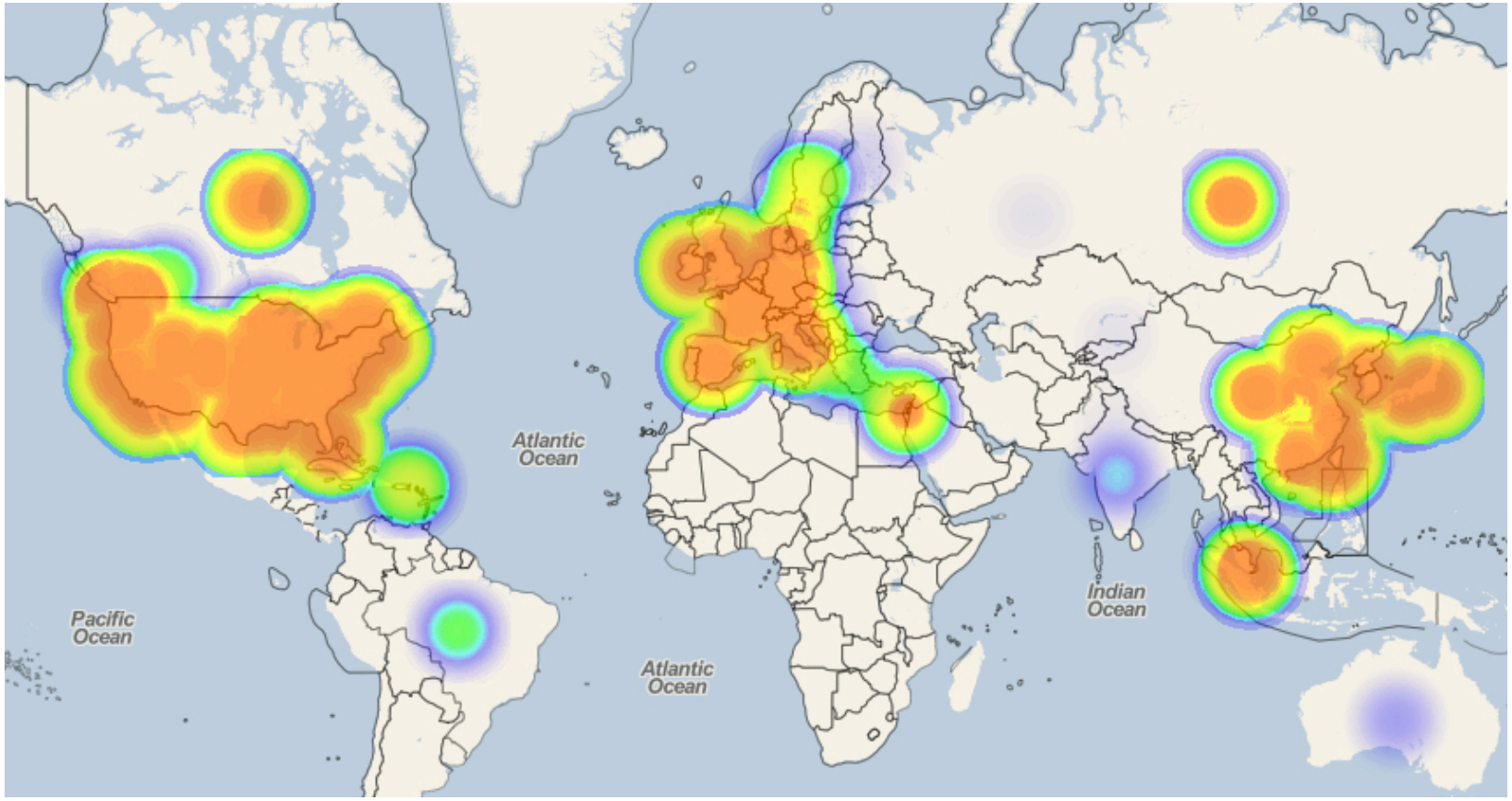
BYOD (or BYOA):

- **Volume:** Thousands of apps
- **Speed:** New apps every day
- **Choice:** Employee Driven

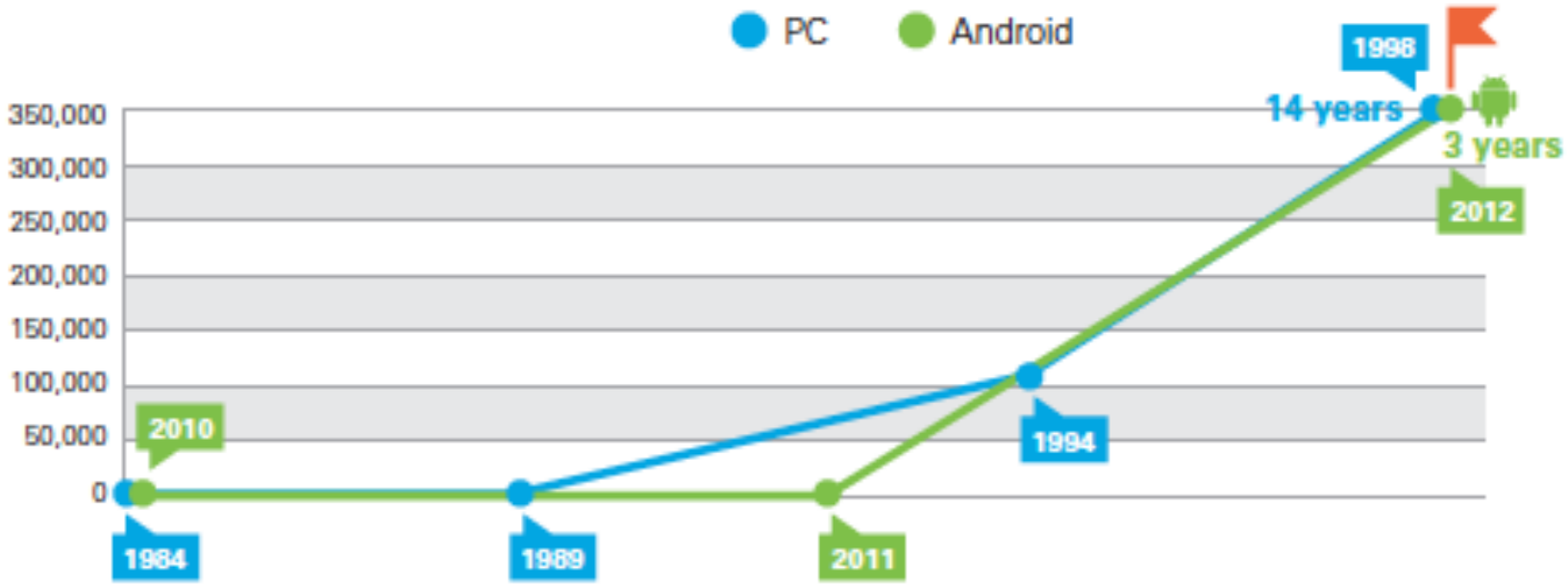
RISKY ANDROID APPS



RISKY AND MALICIOUS ANDROID APPS



GROWTH OF MALICOUS ANDROID APPS

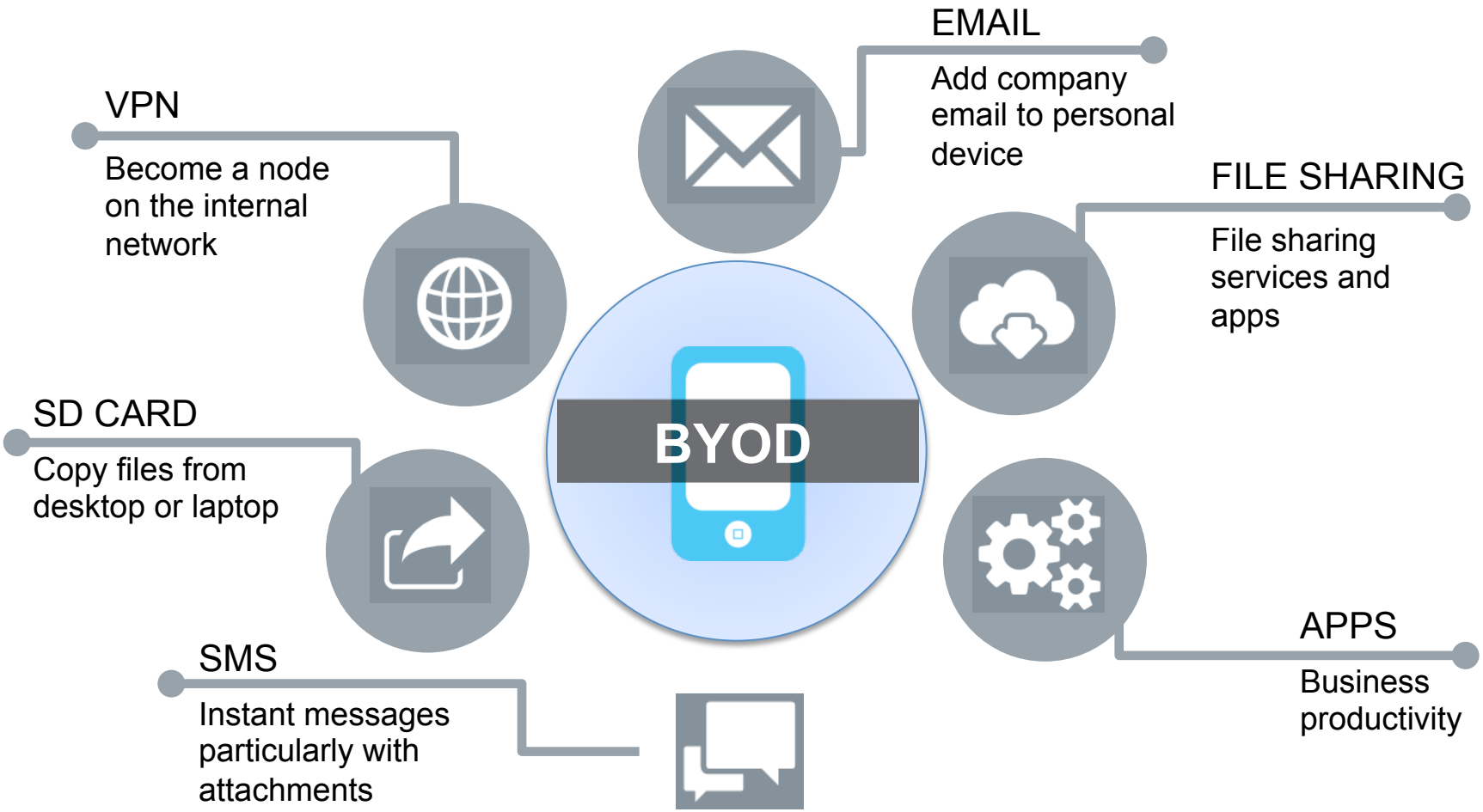


DATA LOSS

94% of companies said lost information was their biggest concern in a mobile security incident.

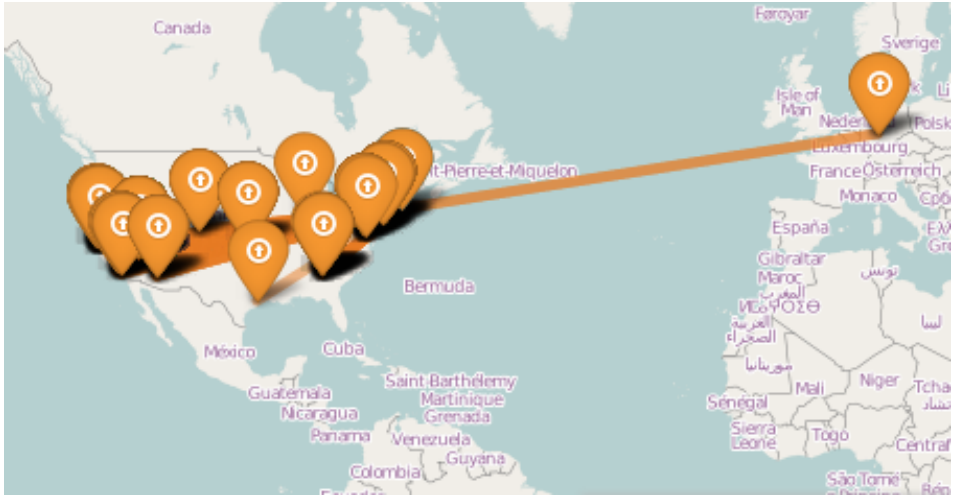
http://www.net-security.org/secworld.php?id=15006

SENSITIVE DATA LANDS ON EMPLOYEE DEVICES



SENSITIVE DATA LEAVES EMPLOYEE DEVICES

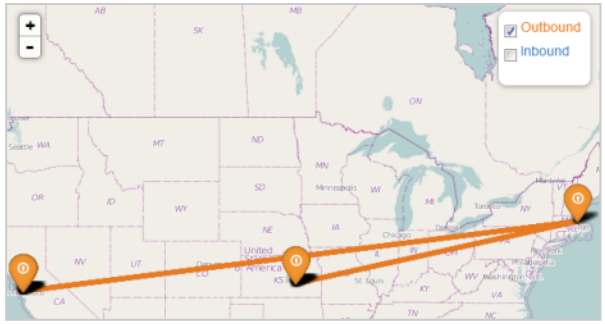
- System Logs
- Unique Device Identification
- Device Type Information
- Carrier Information
- Device Location
- Examine Root File System



BATTERY SAVER APP

10 million downloads

Risk Info	
Rating	5
Label	Suspicious



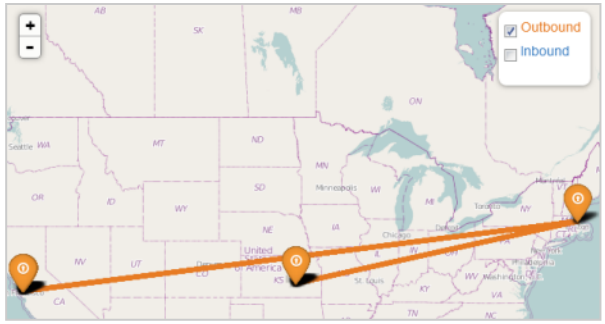
Category	Code Item
SMS	Receive SMS Messages Contains the code required to receive messages via SMS.
Networking	HTTP Upload The app contains the code needed in order to upload resources to a web server.
System Access	Check if Device is Rooted Code exists to determine if the device has been rooted/jailbroken and running in superuser/admin mode.
Sensitive Information	Access Unique Device Identification Information Information like phone number, IMEI, etc.
System Access	Examine Android Account Contains code to examine store accounts through the operating system API. Usernames and other info may be stored here. This is normal but can be hazardous if an app stores password in clear text.

Permissions
android.permission.MODIFY_PHONE_STATE
android.permission.READ_PHONE_STATE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BATTERY_STATS
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.DISABLE_KEYGUARD
android.permission.GET_ACCOUNTS
android.permission.GET_TASKS
android.permission.READ_SYNC_SETTINGS
android.permission.RECEIVE_MMS
android.permission.RECEIVE_SMS
android.permission.RECEIVE_WAP_PUSH
android.permission.SYSTEM_ALERT_WINDOW
android.permission.WAKE_LOCK
android.permission.WRITE_APN_SETTINGS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SECURE_SETTINGS
android.permission.WRITE_SETTINGS
android.permission.WRITE_SYNC_SETTINGS

BATTERY SAVER APP

10 million downloads

Risk Info	
Rating	5
Label	Suspicious



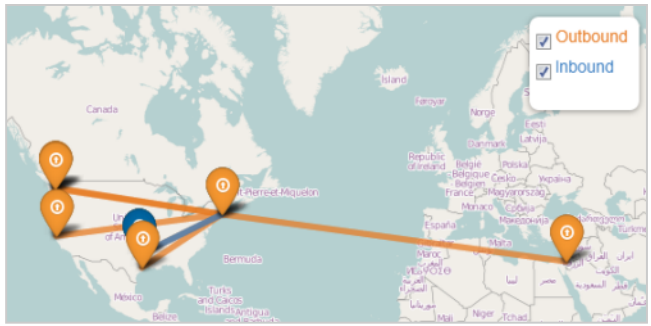
Category	Code Item
SMS	Receive SMS Messages Contains the code required to receive messages via SMS.
Networking	HTTP Upload The app contains the code needed in order to upload resources to a web server.
System Access	Check if Device is Rooted Code exists to determine if the device has been rooted/jailbroken and running in superuser/admin mode.
Sensitive Information	Access Unique Device Identification Information Information like phone number, IMEI, etc.
System Access	Examine Android Account Contains code to examine store accounts through the operating system API. Usernames and other info may be stored here. This is normal but can be hazardous if an app stores password in clear text.

Permissions
android.permission.MODIFY_PHONE_STATE
android.permission.READ_PHONE_STATE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BATTERY_STATS
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.DISABLE_KEYGUARD
android.permission.GET_ACCOUNTS
android.permission.GET_TASKS
android.permission.READ_SYNC_SETTINGS
android.permission.RECEIVE_MMS
android.permission.RECEIVE_SMS
android.permission.RECEIVE_WAP_PUSH
android.permission.SYSTEM_ALERT_WINDOW
android.permission.WAKE_LOCK
android.permission.WRITE_APN_SETTINGS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SECURE_SETTINGS
android.permission.WRITE_SETTINGS
android.permission.WRITE_SYNC_SETTINGS

PHOTO APP

100,000 downloads

Risk Info	
Rating	6
Label	Suspicious



System Access	Check if Device is Rooted Code exists to determine if the device has been rooted/jailbroken and running in superuser/admin mode.
Sensitive Information	Access Unique Device Identification Information Information like phone number, IMEI, etc.
Sensitive Information	Retrieve SIM Card Information Contains code that may reveal the serial number of your SIM card as well as information about the provider network with which it is attached.
Sensitive Information	Retrieve Carrier Information Contains code that may identify and retrieve information about your mobile service prodiver.
Sensitive Information	Examine File System Contains code that may attempt to read the root filesystem, download cache, sd card and/or digital media rights files.
Sensitive Information	Retrieve Information About Device Type Contains code capable of finding the device brand, model and/or version of the operating system.
Sensitive Information	Monitor Device Location Code is present that may track the location of the device based on cellular network and or/gps. This is also aware of when the location changes.

Permissions
android.permission.READ_PHONE_STATE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.INTERNET
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.CAMERA
android.permission.GET_ACCOUNTS
com.android.browser.permission.READ_HISTORY_BOOKMARKS
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS
com.android.launcher.permission.INSTALL_SHORTCUT
com.android.launcher.permission.UNINSTALL_SHORTCUT
com.android.launcher.permission.READ_SETTINGS
com.lge.launcher.permission.INSTALL_SHORTCUT
com.motorola.launcher.permission.INSTALL_SHORTCUT
com.fede.launcher.permission.READ_SETTINGS
org.adw.launcher.permission.READ_SETTINGS
com.motorola.dlauncher.permission.READ_SETTINGS
com.google.android.c2dm.permission.RECEIVE
com.lge.launcher.permission.READ_SETTINGS
com.motorola.dlauncher.permission.INSTALL_SHORTCUT
com.htc.launcher.permission.READ_SETTINGS
com.motorola.launcher.permission.READ_SETTINGS
com.pic.stitch.creater.free.permission.C2D_MESSAGE

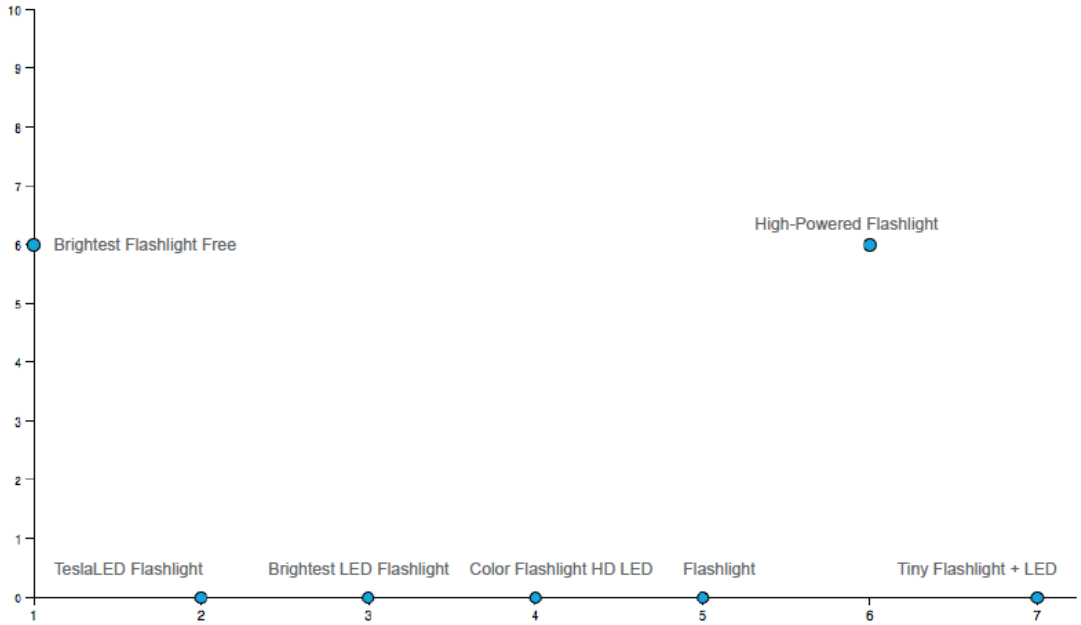
SHINING THE LIGHT ON FLASHLIGHT APPS

FLASHLIGHT APPS

Rank	Platform	App
4	Android	Brightest Flashlight Free ®
58	Android	Flashlight HD LED
65	Android	LED Flashlight
1	Android	Brightest LED Flashlight
3	Android	Brightest LED Flashlight
5	Android	Tiny Flashlight + LED
27	Android	Super Bright Flashlight ®
27	Android	Tiny Flashlight + LED
48	Android	Color Flashlight HD LED
53	Android	Disco Light™ LED Flashlight
73	Android	GPS Speedometer & Flashlight
88	Android	Super Bright Flashlight ®

Rank	Platform	App
2	iOS	Flashlight ?
5	iOS	Flashlight ?
7	iOS	Flashlight ?
8	iOS	Flashlight for iPhone , iPod and iPad
14	iOS	iTorch Flashlight
23	iOS	Flashlight !
25	iOS	Flashlight ?
32	iOS	Magnifying Glass With Light - digital magnifier with flashlight
34	iOS	Light - LED Flashlight
59	iOS	Flashlight ?

FLASHLIGHT APPS

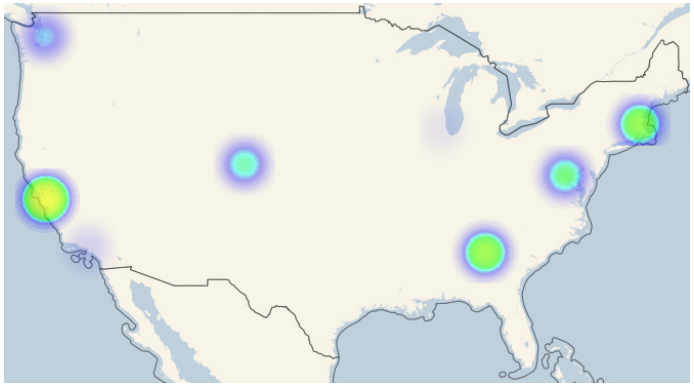


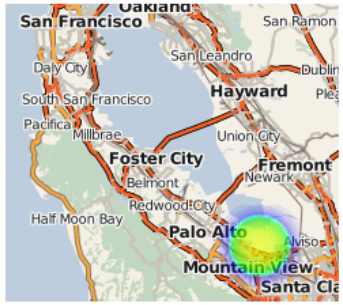
App	Package	Name	Downloads (30 Days)
1	goldenshorestechnologies.brightestflashlight.free	Brightest Flashlight Free™	10,000,000+
2	com.teslacoilsw.flashlight	TeslaLED Flashlight	1,000,000+
3	com.surpax.ledflashlight.panel	Brightest LED Flashlight	1,000,000+
4	com.socialnmobile.hd.flashlight	Color Flashlight HD LED	5,000,000+
5	com.intellectualflame.ledflashlight.washer	Flashlight	10,000,000+
6	com.ihandysoft.ledflashlight.mini	High-Powered Flashlight	1,000,000+
7	com.devuni.flashlight	Tiny Flashlight + LED	100,000,000+

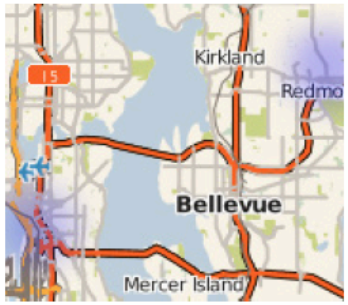
ANTIVIRUS SCANNERS

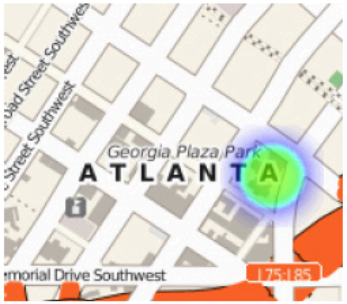
	App						
Scanner	1	2	3	4	5	6	7
AVG	0	0	0	0	0	0	0
Agnitum	0	0	0	0	0	0	0
Identity	0	0	0	0	0	0	0
AntiVir	0	0	0	0	0	0	0
Antiy-AVL	0	0	0	0	0	0	0
Avast	0	0	0	0	0	0	0
BitDefender	0	0	0	0	0	0	0
ByteHero	0	0	0	0	0	0	0
CAT-QuickHeal	0	0	0	0	0	0	0
ClamAV	0	0	0	0	0	0	0
Commtouch	0	0	0	0	0	0	0
Comodo	0	0	0	0	0	0	0
DrWeb	0	0	0	0	0	0	0
ESET-NOD32	0	0	0	0	0	0	0
Emsisoft	0	0	0	0	0	0	0
F-Prot	0	0	0	0	0	0	0
F-Secure	0	0	0	0	0	0	0
Fortinet	0	0	0	0	0	0	0
GData	0	0	0	0	0	0	0
Ikarus	0	0	0	0	0	0	0
Jiangmin	0	0	0	0	0	0	0
K7AntiVirus	0	0	0	0	0	0	0
Kaspersky	0	0	0	0	0	0	0
Kingsoft	0	0	0	0	0	0	0
Malwarebytes	0	0	0	0	0	0	0
McAfee	0	0	0	0	0	0	0
McAfee-GW-Edition	0	0	0	0	0	0	0
MicroWorld-eScan	0	0	0	0	0	0	0
Microsoft	0	0	0	0	0	0	0
NANO-Antivirus	0	0	0	0	0	0	0
Norman	0	0	0	0	0	0	0
PCTools	0	0	0	0	0	0	0
Panda	0	0	0	0	0	0	0
Rising	0	0	0	0	0	0	0
SUPERAntiSpyware	0	0	0	0	0	0	0
Sophos	0	0	0	0	0	0	0
Symantec	0	0	0	0	0	0	0
TheHacker	0	0	0	0	0	0	0
TotalDefense	0	0	0	0	0	0	0
TrendMicro	0	0	0	0	0	0	0
VBA32	0	0	0	0	0	0	0
VIPRE	0	0	0	0	0	0	0
ViRobot	0	0	0	0	0	0	0
eSafe	0	0	0	0	0	0	0
nProtect	0	0	0	0	0	0	0

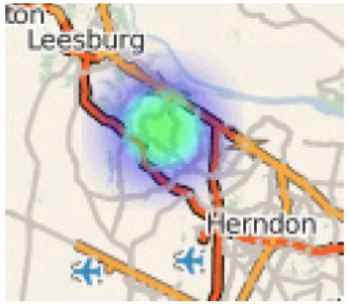
NETWORK ANALYSIS

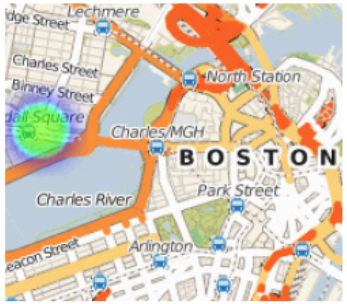












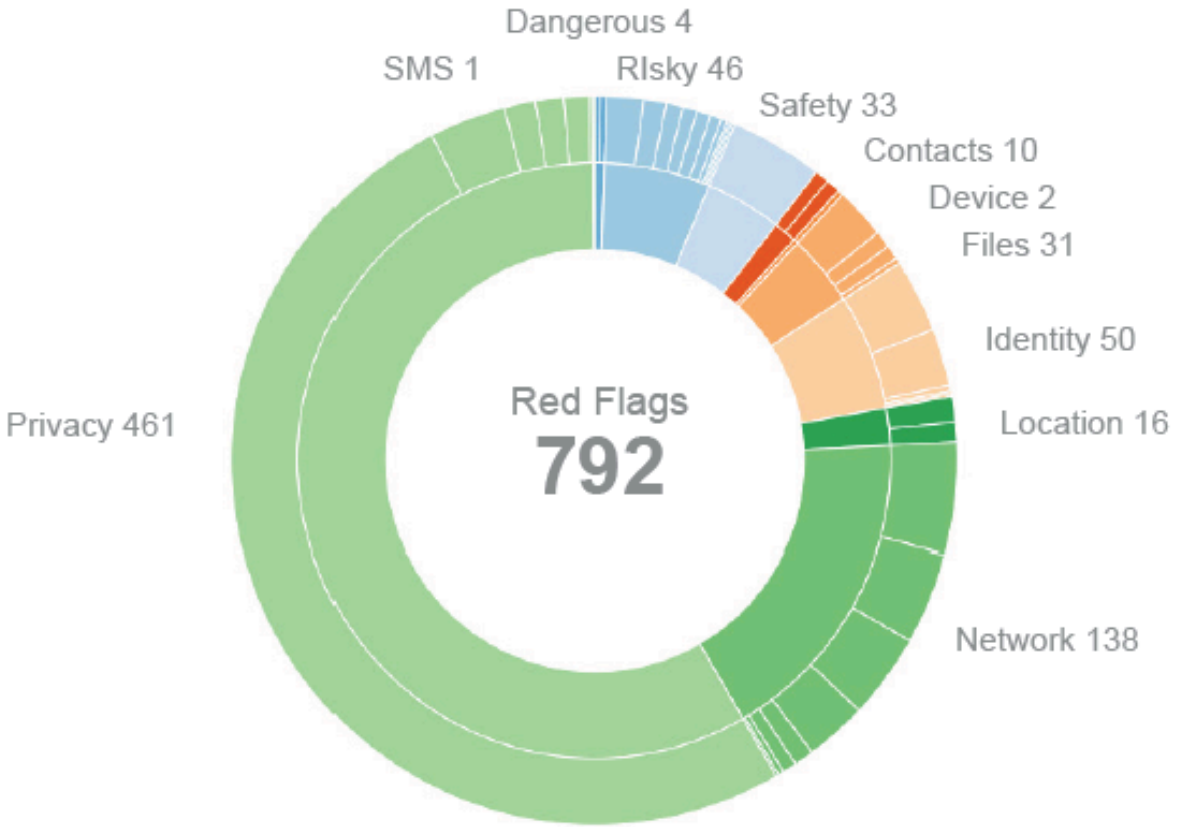
BRIGHTEST FREE

Category	Description
DANGEROUS	SEEK SUPER USER MODE VIA NATIVE JAVA PROCESS
	LAUNCH NATIVE JAVA PROCESS VIA COMMAND LINE
RISKY	RELY ON TIMER AND OR TIME DELAY STRUCTURE
	RETRIEVE SENSITIVE INFORMATION ABOUT YOUR NETWORK PROVIDER
	INTERACTING WITH JAVASCRIPT WEBVIEWS
	HANDLE JAVA OBJECT CLASS REFLECTION
	ENABLING AND OR LOADING JAVASCRIPT ON WEBVIEWS
	TIME DELAY STRUCTURE POSSIBLY ASSOCIATED WITH NETWORK SMS INTERACTION
	HANDLE SECURITY EXCEPTIONS POSSIBLY DUE TO LACK OF PROPER PERMISSION
	READING ANDROID SYSTEM LOGS
	RELYING ON SOMEWHAT DENSE USE OF STRINGS
	MANAGE AND OR ACCEPT CONNECTIONS VIA NETWORK SOCKETS
SAFETY	FINE GRAINED MANAGEMENT OF LIFECYCLE OF ITS ACTIVITIES
CONTACTS	EDIT CONTACT LIST
	MONITOR CONTACT LIST
DEVICE	MONITOR CAMERA INTERFACE
FILES	EXFILTRATE VIA DELETION ON FILESYSTEM
	INQUISITIVE ABOUT SD CARD DIRECTORY CONTENTS
	ACCESS TO YOUR SD CARD
	EXFILTRATE VIA CHANGE TO FILESYSTEM
IDENTITY	RETRIEVE YOUR UNIQUE PHONE IDENTIFIER GSM IMEI
	RETRIEVE INFORMATION ABOUT YOUR DEVICE TYPE
	RETRIEVE YOUR SUBSCRIBER ID GSM IMSI
	DETERMINE IF YOUR DEVICE TYPE IS AN EMULATOR
	RETRIEVE YOUR DEVICE MAC ADDRESS

BRIGHTEST FREE

Category	Description
LOCATION	CHECK YOUR LAST GEOLOCATION
	ACCESS TO YOUR LOCATION VIA GPS COORDINATES
NETWORK	UPLOAD URL RESOURCES VIA HTTP POST
	UNSECURE WEB BROWSING
	DOWNLOAD URL RESOURCES BUT VIA APACHE LIBRARIES
	DOWNLOAD URL RESOURCES
	QUERY LOOKUP URL RESOURCES VIA HTTP GET
	RETRIEVE HTTP STATUS CODE
	START NETWORK SOCKET SERVER
	ALLOW OUTBOUND INBOUND JAVA NET SOCKETS
PRIVACY	CONVENTIONAL AD DELIVERY
	BANNER BASED ADS
	ACCESS TO WELL KNOWN MOBILE AD SERVERS
	MONITOR YOUR NETWORK STATUS
	ACTIVATE FINE GRAIN EVENT MONITORING TO DEVELOPER MEASUREMENTS THIRD PARTY
	LOOK AT YOUR ANDROID ACCOUNT
SMS	SEND SMS MESSAGES

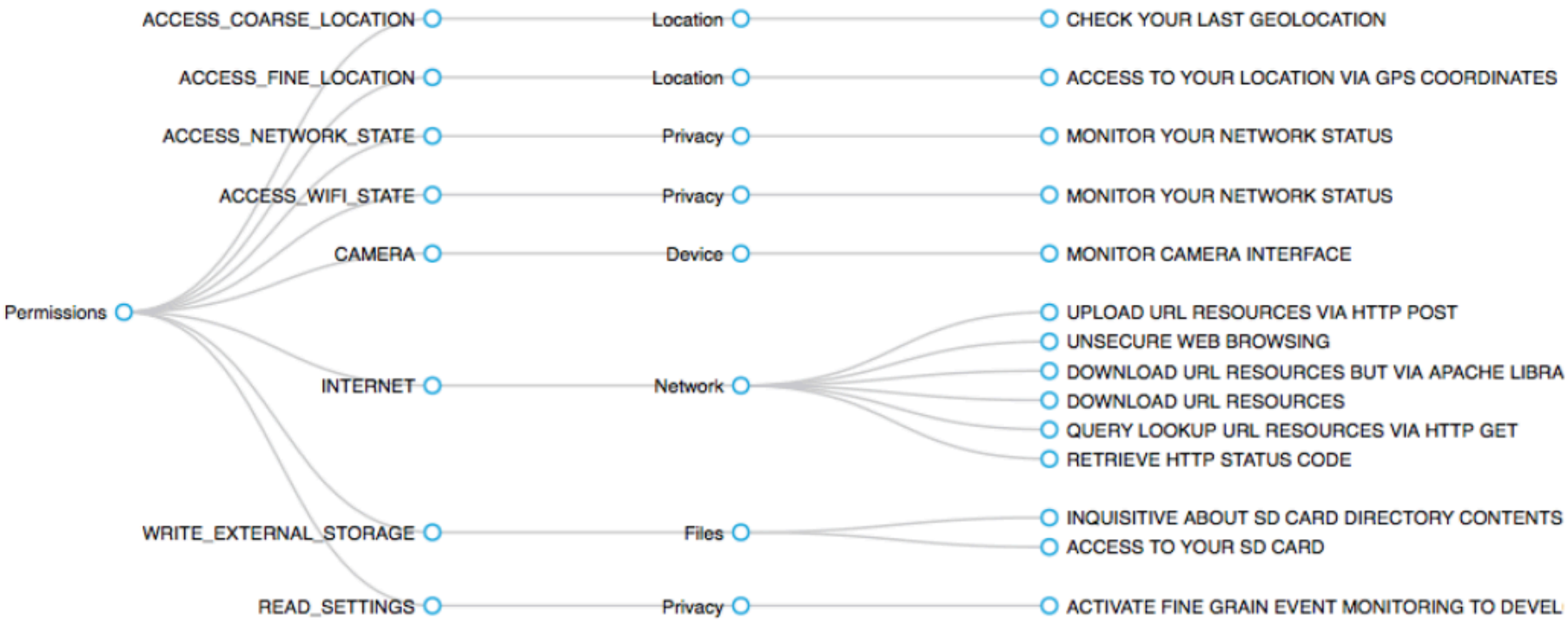
BRIGHTEST FREE



BRIGHTEST FREE

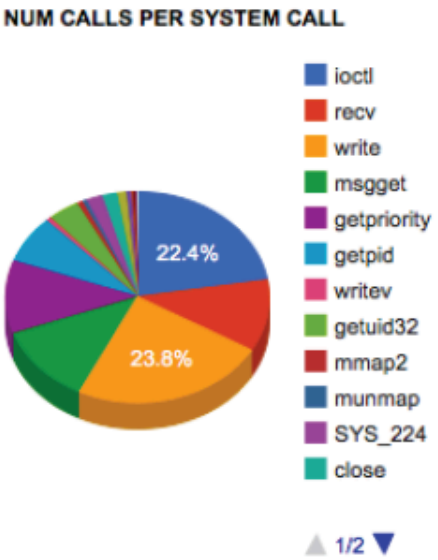
Category	Permission	Category	Permission
LOCATION	android.permission.ACCESS_COARSE_LOCATION	PRIVACY	com.android.launcher.permission.READ_SETTINGS
LOCATION	android.permission.ACCESS_FINE_LOCATION		com.android.launcher.permission.UNINSTALL_SHORTCUT
NETWORK	android.permission.ACCESS_NETWORK_STATE	PRIVACY	com.fede.launcher.permission.READ_SETTINGS
NETWORK	android.permission.ACCESS_WIFI_STATE	PRIVACY	com.htc.launcher.permission.READ_SETTINGS
DEVICE	android.permission.CAMERA		com.lge.launcher.permission.INSTALL_SHORTCUT
	android.permission.FLASHLIGHT	PRIVACY	com.lge.launcher.permission.READ_SETTINGS
NETWORK	android.permission.INTERNET		com.motorola.dlauncher.permission.INSTALL_SHORTCUT
	android.permission.READ_PHONE_STATE	PRIVACY	com.motorola.dlauncher.permission.READ_SETTINGS
	android.permission.STATUS_BAR		com.motorola.launcher.permission.INSTALL_SHORTCUT
	android.permission.WAKE_LOCK	PRIVACY	com.motorola.launcher.permission.READ_SETTINGS
FILES	android.permission.WRITE_EXTERNAL_STORAGE	PRIVACY	org.adw.launcher.permission.READ_SETTINGS
	com.android.launcher.permission.INSTALL_SHORTCUT		

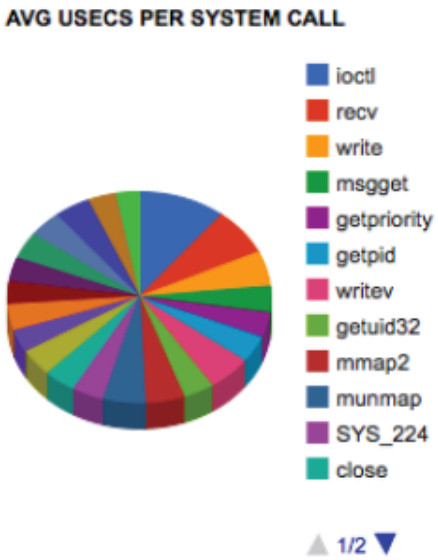
BRIGHTEST FREE



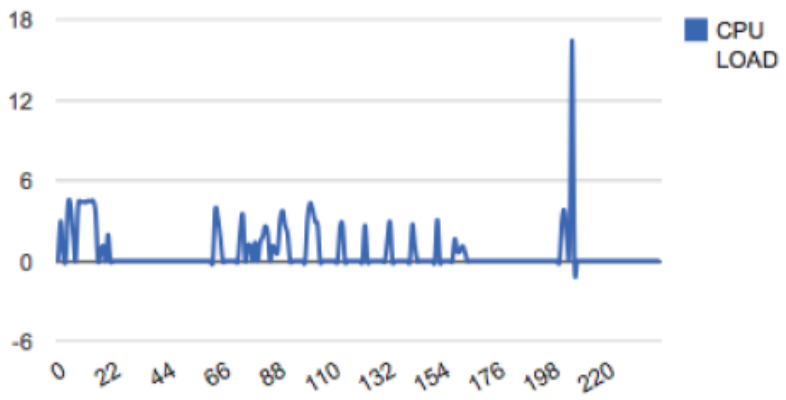
BRIGHTEST FREE

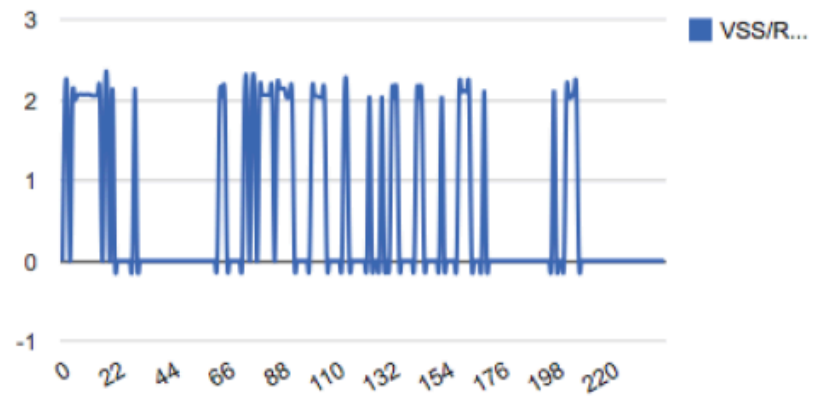
SYSTEM CALL	TOTAL NUMBER	AVERAGE USECS (LOG)
SYS_224	63	4.98
brk	2	4.52
clone	1	5.64
close	59	5.04
dup	17	4.38
fstat64	2	5.31
getpid	230	5.25
getpriority	352	4.85
gettimeofday	1	3.74
getuid32	122	4.84
ioctl	706	13.76
mmap2	22	6.13
mprotect	5	4.74
msgget	383	5.25
munmap	16	6.43
open	36	5.34
pivot_root	2	5.14
read	5	5.20
recv	348	9.31
setpriority	10	4.44
write	750	6.87
writev	21	6.96

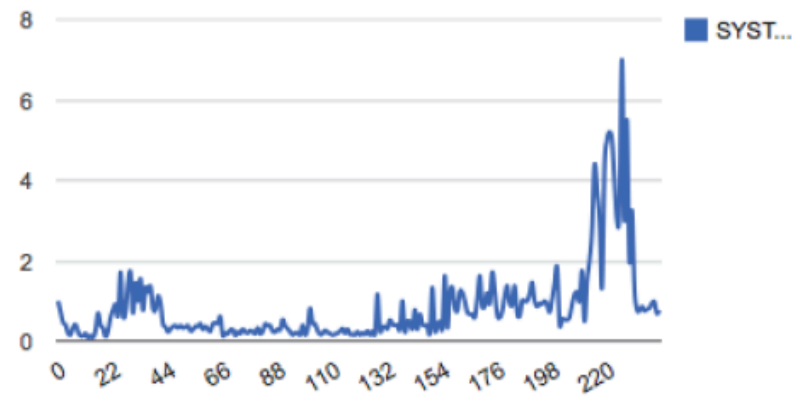


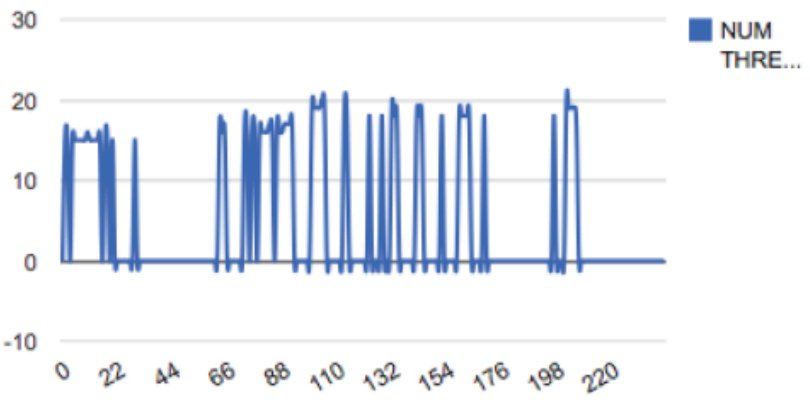


BRIGHTEST FREE



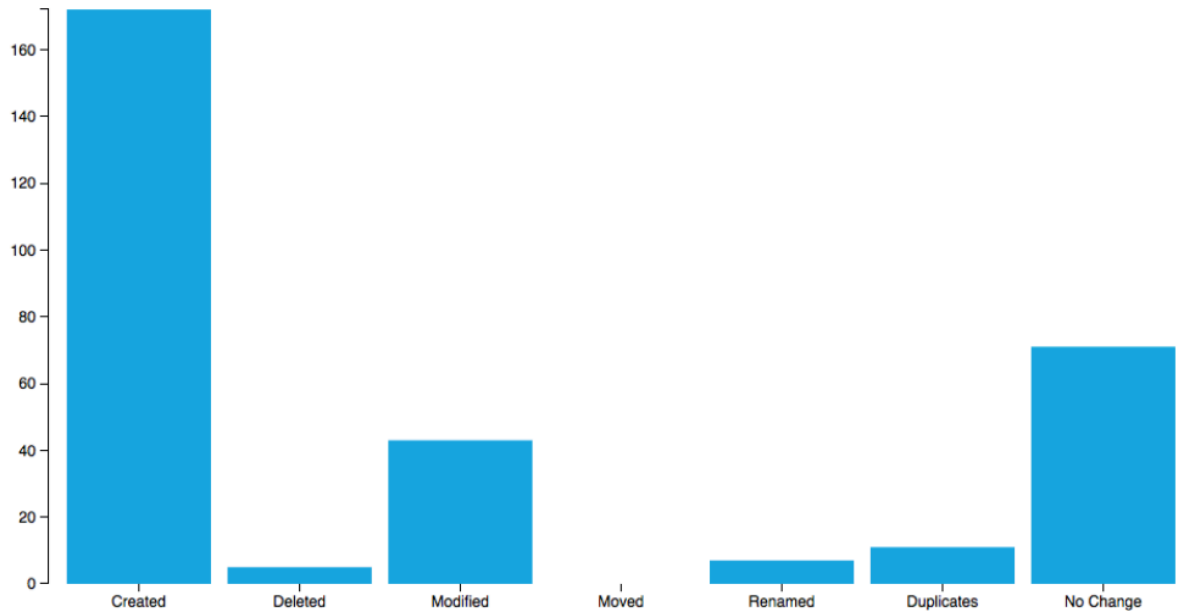






BRIGHTEST FREE

Count	Category
172	Created
5	Deleted
43	Modified
0	Moved
7	Renamed
11	Duplicates
71	No Change



BRIGHTEST FREE

IP Address	Hostname
173.252.101.26	www.facebook.com
206.165.250.101	m.addthisedge.com
107.21.253.152	ads.mobclix.com
184.73.198.91	ads.mobclix.com
173.194.46.3	plusone.google.com
173.194.46.2	plusone.google.com
173.194.46.1	plusone.google.com
173.194.46.0	plusone.google.com
173.194.46.7	plusone.google.com
173.194.46.6	plusone.google.com
54.245.104.37	beacon.krxd.net
173.194.46.4	plusone.google.com
23.23.213.194	ads.mobclix.com
173.194.46.9	plusone.google.com
173.194.46.8	plusone.google.com
50.112.117.233	beacon.krxd.net
23.61.194.203	www.polls.newsvine.com
173.194.46.16	www.google.com
173.194.46.15	ssl.gstatic.com
173.194.46.14	plusone.google.com
173.194.46.12	lh4.googleusercontent.com
173.194.46.11	lh4.googleusercontent.com
173.194.46.10	lh4.googleusercontent.com
23.61.194.209	msnbcmedia.msn.com
174.129.198.92	ads.mobclix.com
173.194.46.19	www.google.com
173.194.46.18	www.google.com

IP Address	Hostname
184.28.96.251	static.chartbeat.com
23.61.194.193	m.static.newsvine.com
207.171.163.4	s.veltimedia.net
23.61.194.195	static.ak.facebook.com
23.61.194.218	b.scorecardresearch.com
199.59.148.86	r.twimg.com
23.61.194.217	analytics.breakingnews.com
23.61.194.210	b.scorecardresearch.com
23.21.171.71	met.adwhirl.com
50.112.99.60	beacon.krxd.net
98.137.88.37	assets.msnbc.msn.com
98.137.88.36	assets.msnbc.msn.com
98.137.88.35	assets.msnbc.msn.com
98.137.88.34	assets.msnbc.msn.com
23.61.194.178	www.polls.newsvine.com
107.22.248.193	a.veltimedia.net
23.61.194.177	www.cdn.newsvine.com
199.59.148.16	r.twimg.com
216.157.12.154	bank06.mi.clicks.mp.mydas.mobi
216.157.12.243	bank56.mi.ads.mp.mydas.mobi
216.157.12.245	bank60.mi.ads.mp.mydas.mobi
216.157.12.244	bank34.mi.ads.mp.mydas.mobi
64.4.21.39	udc.msn.com
216.157.12.249	bank51.mi.clicks.mp.mydas.mobi
23.6.97.224	p.twitter.com
23.61.194.185	b.scorecardresearch.com
23.21.127.160	assets.pinterest.com

BRIGHTEST FREE

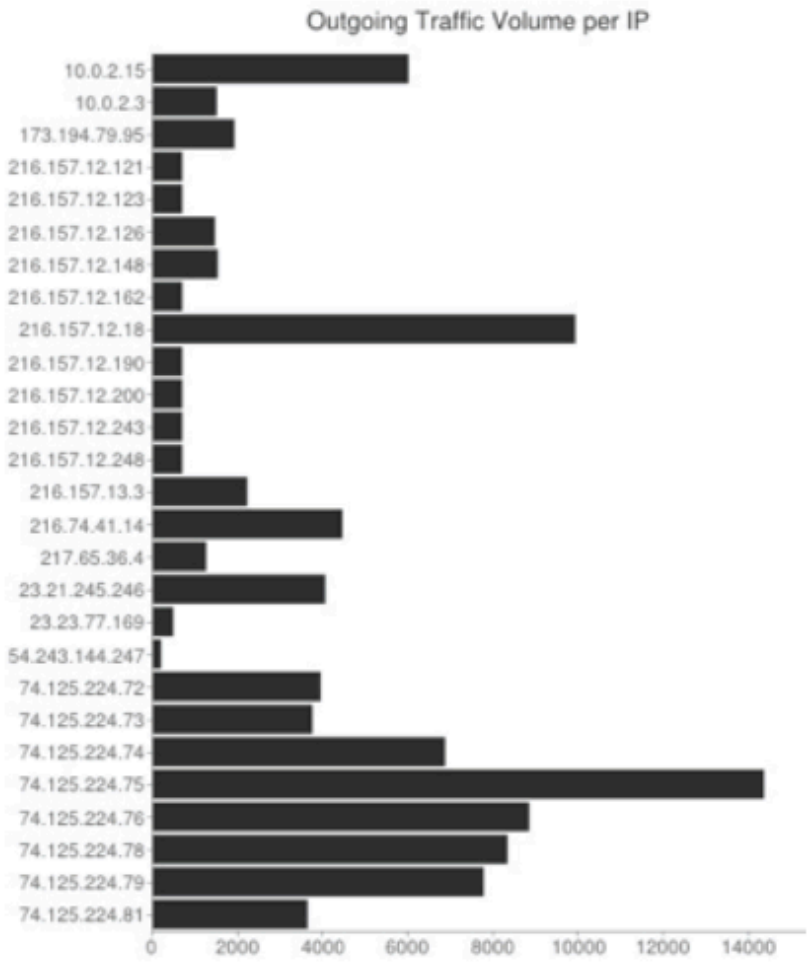
IP Address	Hostname
206.190.60.138	assets.msnbc.msn.com
206.190.60.139	assets.msnbc.msn.com
138.108.7.20	www.google-analytics.com
107.22.159.240	s.mobclix.com
199.59.150.12	r.twimg.com
23.61.194.163	msnbcmedia.msn.com
98.137.88.83	assets.msnbc.msn.com
23.23.76.233	a.veltimedia.net
98.137.88.84	assets.msnbc.msn.com
173.194.46.5	plusone.google.com
216.157.12.121	bank72.mi.ads.mp.mydas.mobi
216.157.12.18	androidsdk.ads.mp.mydas.mobi
107.20.176.85	ads.mobclix.com
174.129.243.85	ping.chartbeat.net
23.21.114.16	widgets.pinterest.com
216.157.12.159	bank11.mi.ads.mp.mydas.mobi
107.22.249.10	a.veltimedia.net
65.55.206.225	home.mobile.msn.com
107.20.164.39	data.mobclix.com
23.21.128.184	ping.chartbeat.net
173.194.46.17	www.google.com
23.23.133.169	met.adwhirl.com
23.61.194.240	analytics.breakingnews.com
72.21.92.20	static.ak.fbcdn.net
23.61.194.248	b.scorecardresearch.com

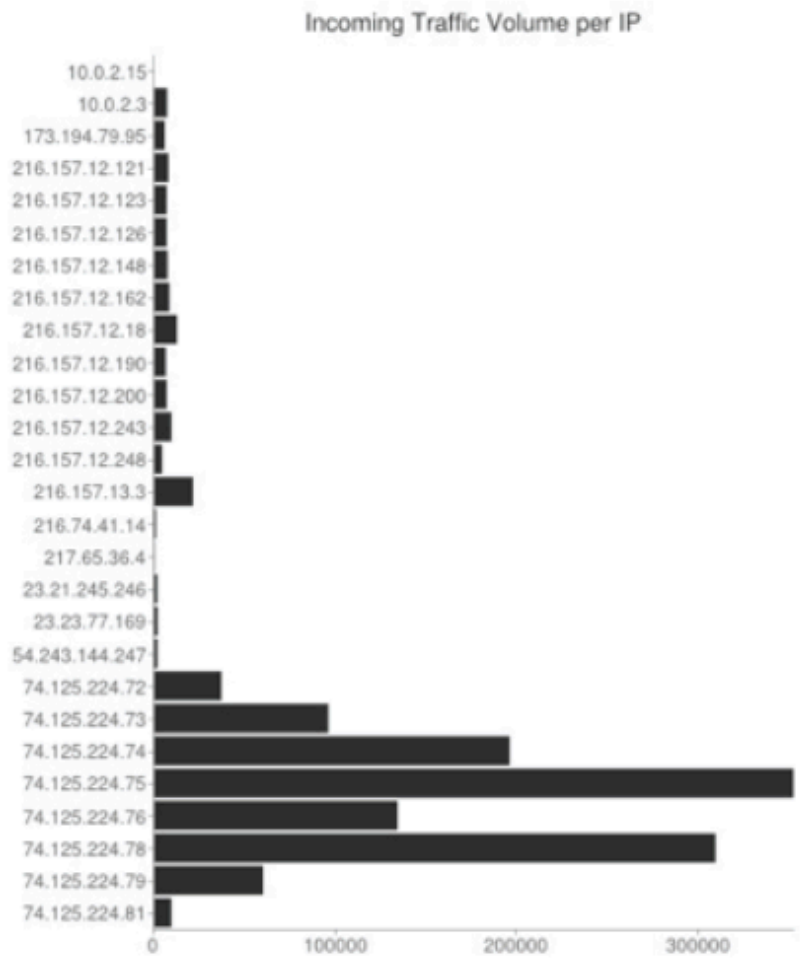
IP Address	Hostname
50.19.108.122	ping.chartbeat.net
23.61.194.251	static.ak.facebook.com
72.21.91.196	s9.addthis.com
23.23.212.172	s.mobclix.com
65.54.161.24	c.msn.com
206.165.250.99	cf.addthis.com
23.56.114.110	s-static.ak.facebook.com
127.0.0.1	ad.doubleclick.net
65.54.71.21	extreme.statics.msn.com
107.21.5.10	hastrk2.com
216.157.12.191	bank28.mi.ads.mp.mydas.mobi
23.61.194.225	m.static.newsvine.com
107.20.247.113	a.veltimedia.net
107.22.249.1	a.veltimedia.net
54.235.196.151	met.adwhirl.com
23.56.127.139	connect.facebook.net
216.157.12.239	bank59.mi.ads.mp.mydas.mobi
157.55.112.138	lib.newsvine.com
216.157.12.128	bank71.mi.ads.mp.mydas.mobi
107.20.146.28	a.veltimedia.net
107.20.164.42	data.mobclix.com
50.16.204.38	ads.mobclix.com
216.74.41.14	data.flurry.com
75.101.145.57	ads.mobclix.com
173.194.46.20	www.google.com

BRIGHTEST FREE

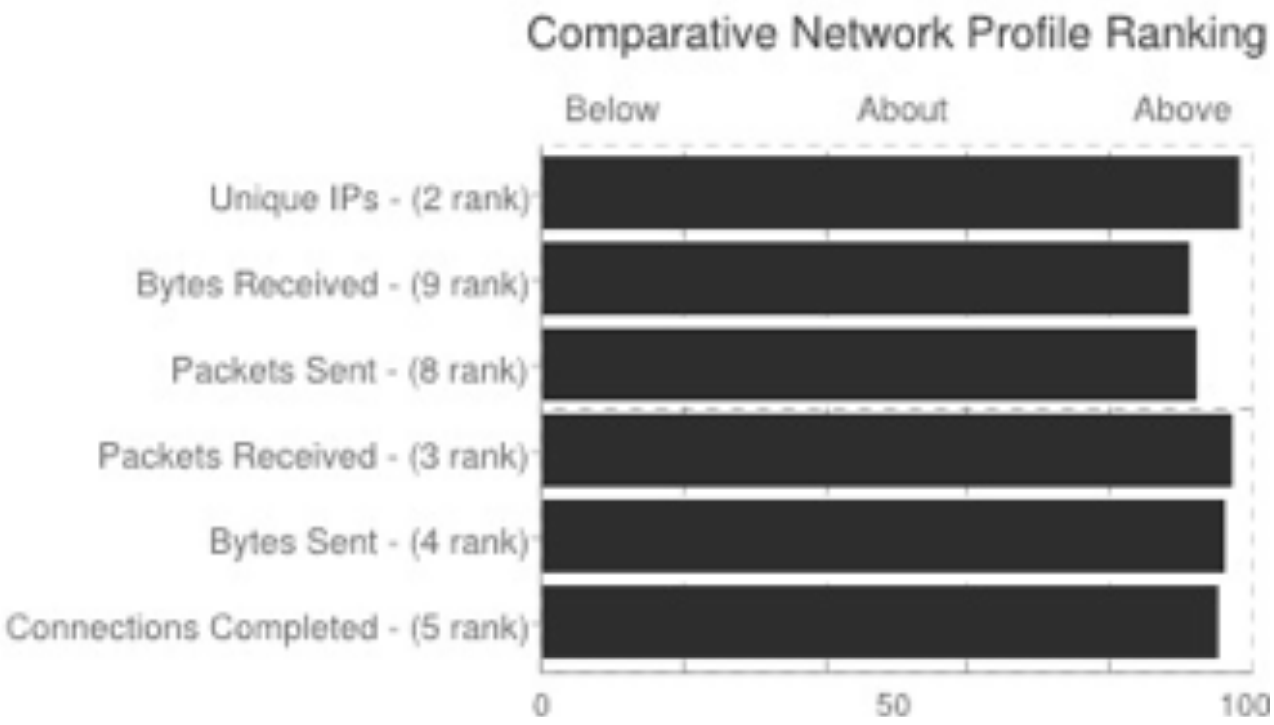
Host/Domain	URLS	Bytes	GeoIP Location
http://platform.twitter.com	2	92650	[23.6.97.224 of network 23.6.97.128/7 in country US]
http://static.chartbeat.com	0	7167	[173.223.52.176 of network 173.223.52.144/13 in country US]
https://lh4.googleusercontent.com	0	1508	
https://play.google.com	2	75273	
https://lh5.ggpht.com	1	4663	
https://lh4.ggpht.com	3	67480	
https://ssl.gstatic.com	5	60859	
https://lh3.ggpht.com	2	41922	
http://assets.msnbc.msn.com	1	16026	[174.35.40.35 of network 174.35.40.3/17 in country US]
https://lh3.googleusercontent.com	0	1287	
http://extreme.statics.msn.com	6	52984	[65.54.71.21 of network 65.54.70.20/14 in country US]
https://wallet.google.com	0	99510	
https://s-static.ak.facebook.com	0	25477	
http://secure-us.imrworldwide.com	0	44	[65.171.135.52 of network 65.171.135.20/19 in country US]
http://msnbcmedia.msn.com	4	35787	[174.35.40.35 of network 174.35.40.3/17 in country US]
http://m.static.newsvine.com	0	1601	[173.223.52.202 of network 173.223.52.130/13 in country US]
https://platform.twitter.com	0	20797	
http://www.cdn.newsvine.com	2	125025	[173.223.52.208 of network 173.223.52.144/13 in country US]
http://cdn.krxd.net	0	64999	[184.28.96.251 of network 184.28.96.24/10 in country US]
http://www.polls.newsvine.com	0	1075	[173.223.52.195 of network 173.223.52.131/13 in country US]
http://p.twitter.com	0	43	[23.6.97.224 of network 23.6.97.128/7 in country US]
http://ping.chartbeat.net	1	86	[54.243.144.145 of network 54.243.144.129/7 in country US]
http://extreme.mobile.msn.com	5	29680	[65.54.71.21 of network 65.54.70.20/14 in country US]
http://s7.addthis.com	0	7019	[72.21.91.196 of network 72.21.91.132/23 in country US]
http://lib.newsvine.com	0	8345	[157.55.112.138 of network 157.55.112.138/15 in country US]
http://ads.mocean.mobi	1	86	[72.21.92.20 of network 72.21.92.20/22 in country US]
https://lib.newsvine.com	0	5430	
https://apis.google.com	1	126106	
https://lh6.ggpht.com	0	10925	
http://cdn.lib.newsvine.com	6	34222	[173.223.52.195 of network 173.223.52.131/13 in country US]

BRIGHTEST FREE





BRIGHTEST FREE



WHAT CAN WE DO

WHAT CAN WE DO

- Make secure coding practices an integral part of your Software Development Lifecycle
- Ensure that apps that you are producing are free from vulnerabilities
- Ensure that third-party libraries used in your apps are free from risky behavior
- Ensure that the apps in your enterprise app store and on your employee devices are free from risky behavior and malicious code

WHAT CAN WE DO

- **Understand** how mobile apps put sensitive data at risk
- **Detect** which mobile apps violate enterprise policy quickly and efficiently
- **Act** intelligently to mitigate risk and protect data

ENTERPRISE ACTION AT CONTROL POINTS

Mobile Device Management (MDM)

Mobile Application Management (MAM)

Enterprise App Stores

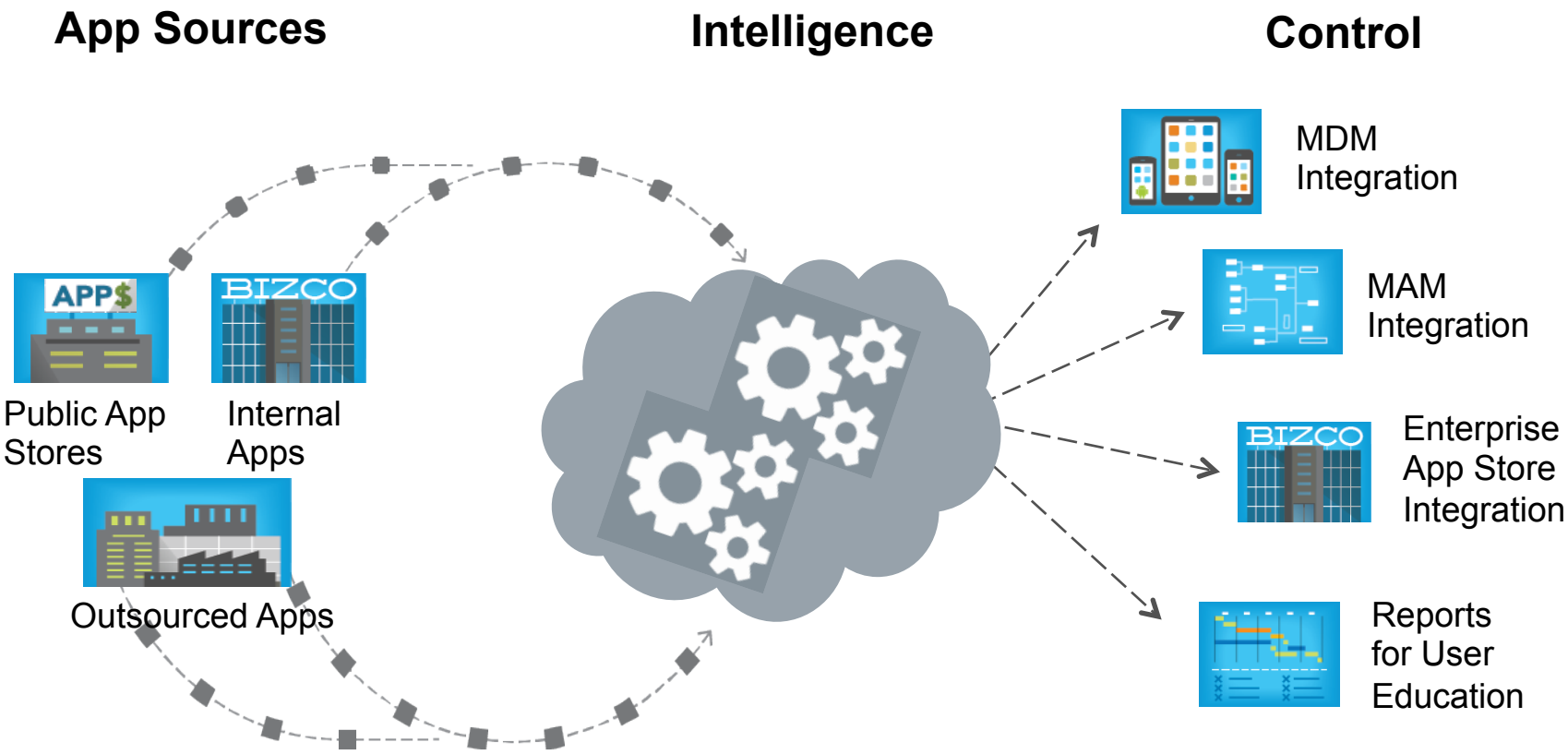
App Wrapping

Enterprise Developers

Outsourced Developers

BUT INTELLIGENCE IS REQUIRED!

ACT THROUGH MOBILITY MANAGEMENT



INTELLIGENCE INTEGRITY THROUGH INNOVATION

Basic Heuristics

Signatures

Signatures

Signatures

Manual Testing

Advanced Machine Learning

Static Analysis

Dynamic/Behavioral Analysis

QUESTIONS


ISACA®
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA
2013 Fall Conference – "Sail to Success"