Security in knowledge

THOUSANDS OF APPS CAN'T BE WRONG: MOBILE APPLICATION ANALYSIS AT SCALE

Chris Eng

Vice President, Research

VERACODE

RSA CONFERENCE EUROPE 2013

Session ID: MBS-T08

Session Classification: Intermediate

Agenda

- State of Mobility in the Enterprise
- Understanding Attacks on the Mobile Security Stack
- Strategies for Securing in a Mobile World
- Q&A

State of Mobility in the Enterprise

Security in knowledge

#RSAC

RSA CONFERENCE
EUROPE 2013

What mobile apps did you use to plan for this conference?

Weather

Air Travel

Traffic

Maps

Top Weather Apps

80% have location permissions or monitor the device's location

96% interact with other types of Sensitive Data

- 32% access system log files

7% have access to the contact list

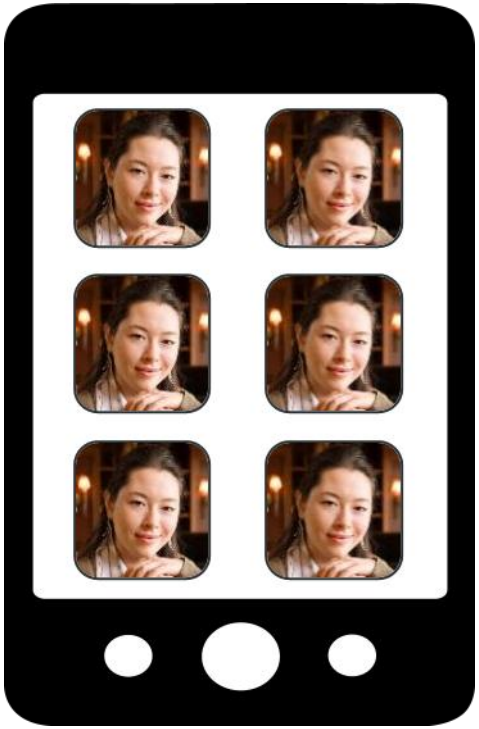
Top Traffic Apps

60% have location permissions or monitor the device's location

46% interact with other types of Sensitive Data

26% have access to the contact list

My Phone is My Digital Life



BYOD now BYOA

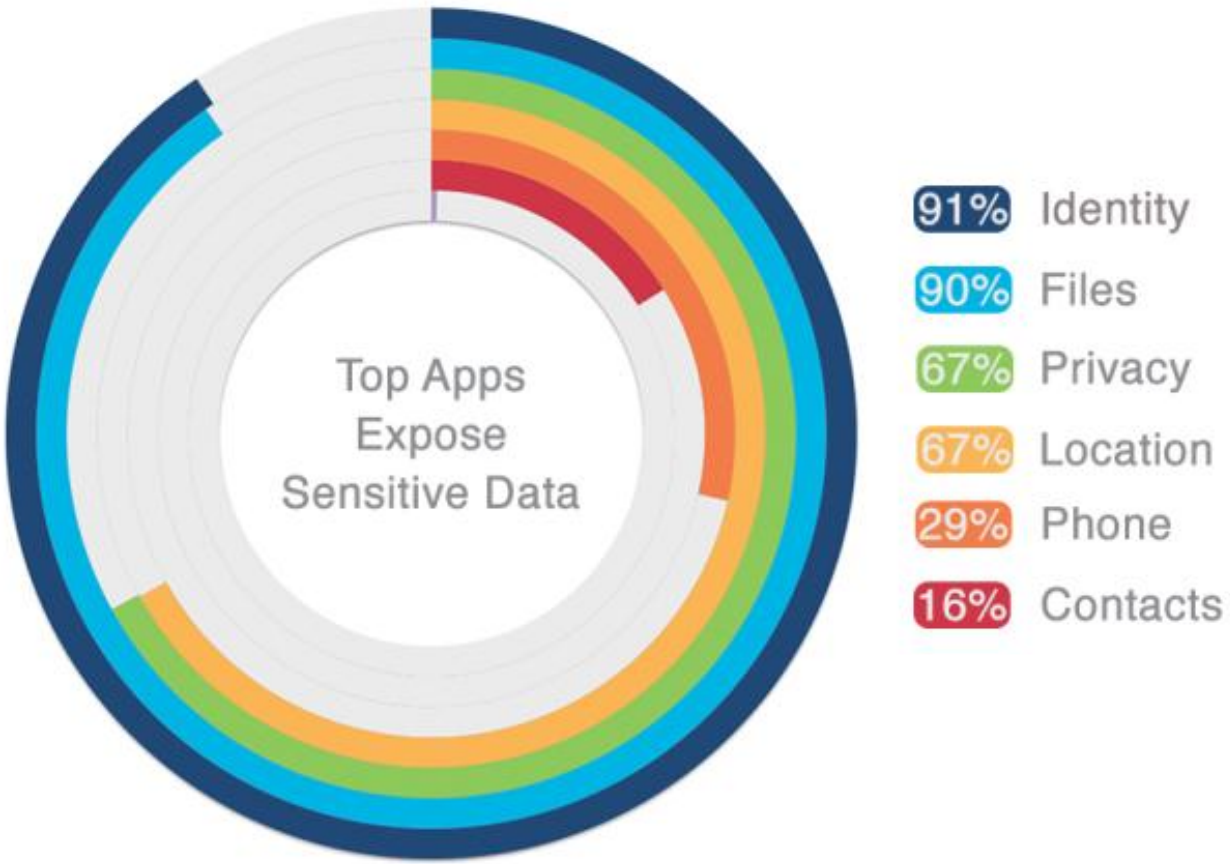
The next phase of mobile security is protecting sensitive data from risky apps

46B
mobile apps downloaded in 2012 – Gartner[1]

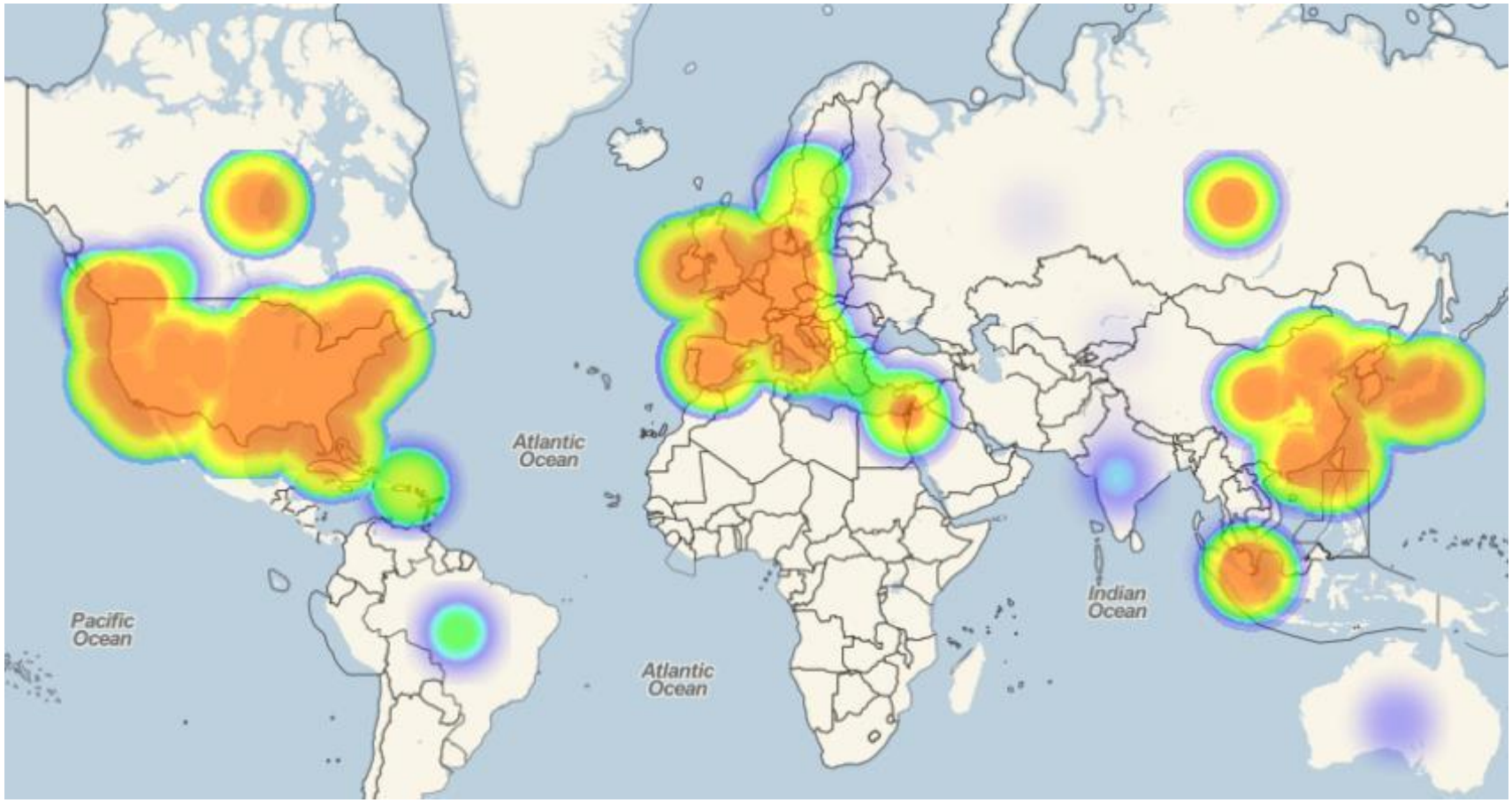
400 Billion
stars in our galaxy

2017
more app downloads than stars

Top Apps Expose Sensitive Data



Where Does App Data Go?



How many of you used these apps on devices you also use for business?

You Are Not Alone

821 Million
smart devices purchased worldwide in 2012[1]

36%
of companies have a BYOD policy [4]

50%
employers will require BYOD by 2017[2]

11%
agencies have a BYOD policy today[3]

[1] http://www.gartner.com/newsroom/id/2227215
[2] http://www.gartner.com/newsroom/id/2466615
[3] MobileWorkExchange "Federal Mobile Workforce Trends"
[4] http://www.zdnet.com/cisco-bt-survey-only-36-percent-of-companies-have-a-byod-policy-7000016432/

VERACODE
Securing the Software That Runs the World

2013 Enterprise Challenge: A Balancing Act

Employee

- Ease of use
- Unfettered access to any application, any device
- Productivity & freedom above anything else

Development

- Create new code faster
- Use existing third-party code and libraries to gain speed advantage
- Use cool new languages and frameworks

- Insight
- Control
- Data Security
- Employee Privacy

IT

Security

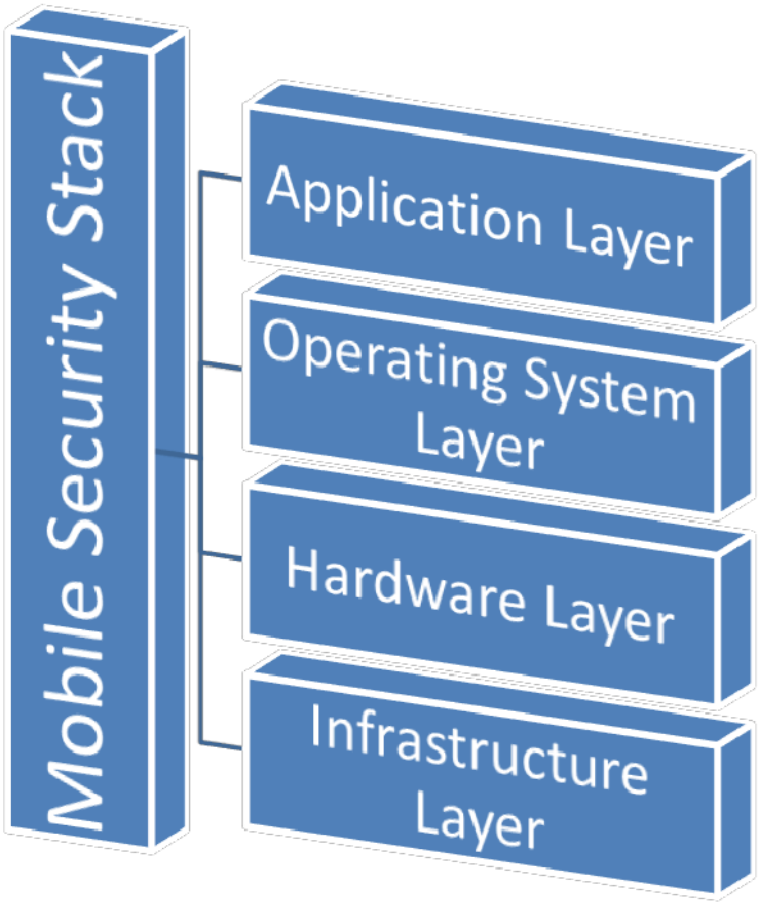
Understanding Attacks on the Mobile Security Stack

Security in knowledge

#RSAC

RSA CONFERENCE
EUROPE 2013

Every Mobile Layer is Attackable



Infrastructure Example

Attackers can slip malicious code into many Android apps via open Wi-Fi

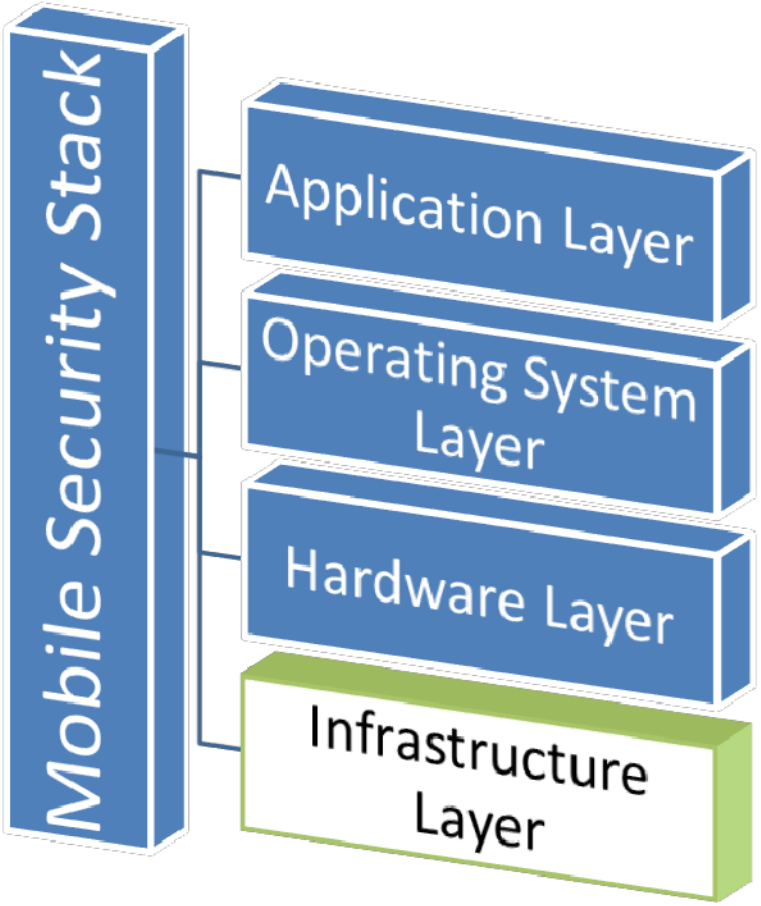
Connection hijacking could put users at risk of data theft, SMS abuse, and more.

by **Dan Goodin** - Sept 27 2013, 7:25am PDT

ANDROID HACKING 40

greyweed

A vulnerability mostly affecting older versions of Google's Android operating system may make it possible for attackers to execute malicious code on end-user smartphones that use a wide variety of apps, researchers said.



Hardware Example

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 iPhor*

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.*

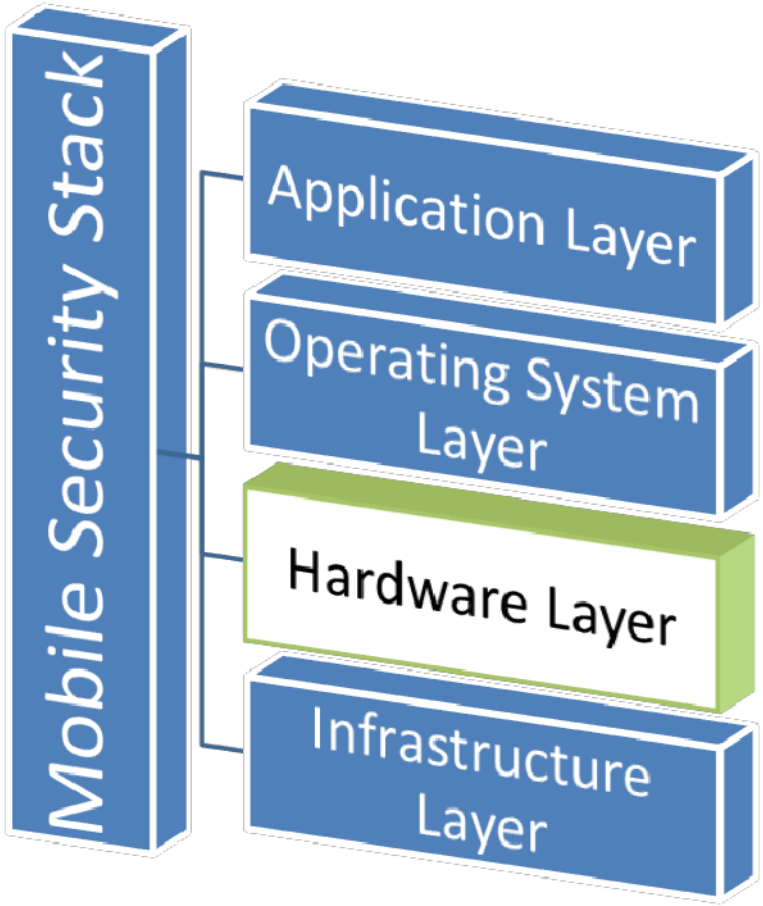
By Violet Blue for Zero Day | July 31, 2013 -- 22:05 GMT (15:05 PDT)
Follow @violetblue

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 Example

PC MAG.COM 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

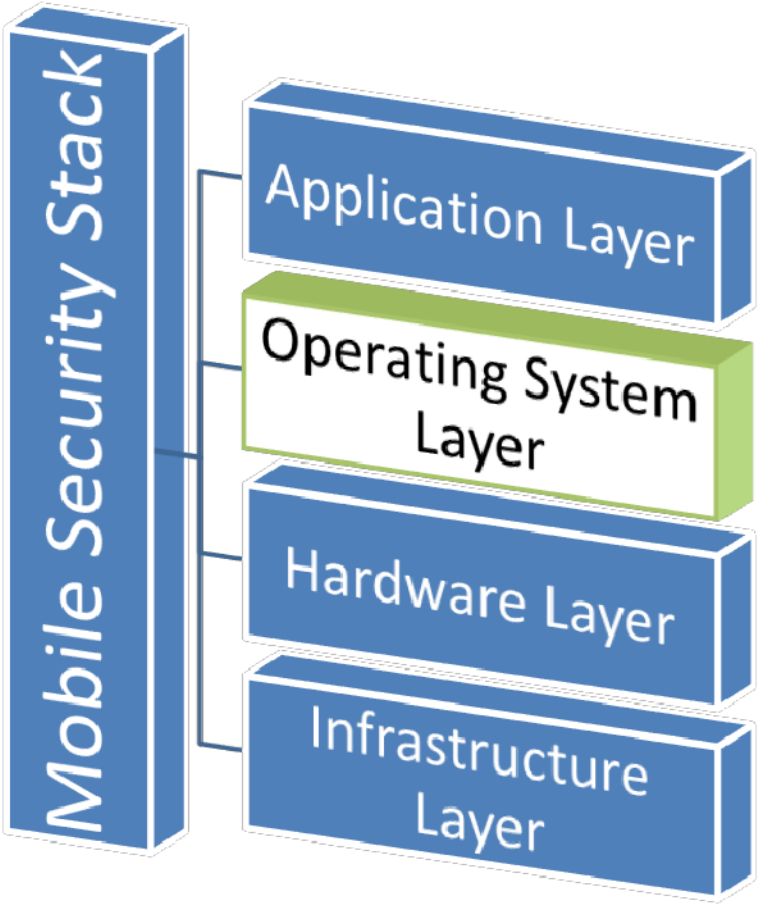
Forward Thinking

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."



Application Example

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.

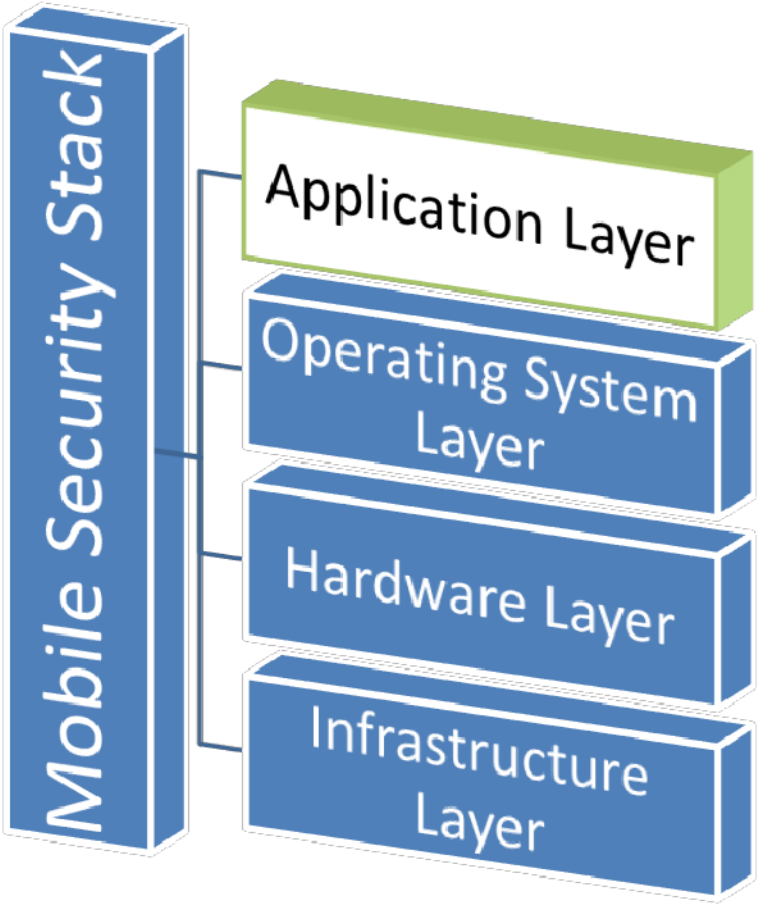
By David Talbot on August 15, 2013

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.



Without Application Security…

- …Adversary tactics
  - Utilize unprotected app credentials for on-device & traditional network attack
  - Exfiltrate sensitive application & OS level information from mobile device
    - Contact list, text messages, unprotected app data
  - Any apps data is vulnerable to these attacks, without additional security controls
  - User and applications not aware of malicious behavior

Strategies for Securing in a Mobile World

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

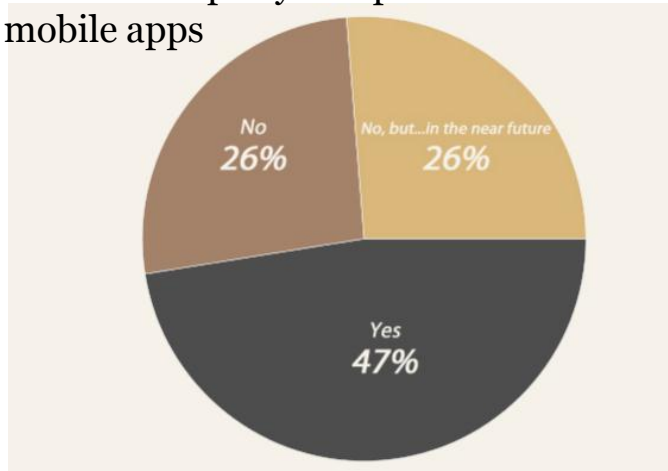
Enterprise Mobile Development

APP PRODUCER

Mobile SDLC:

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

Use of third party components in mobile apps

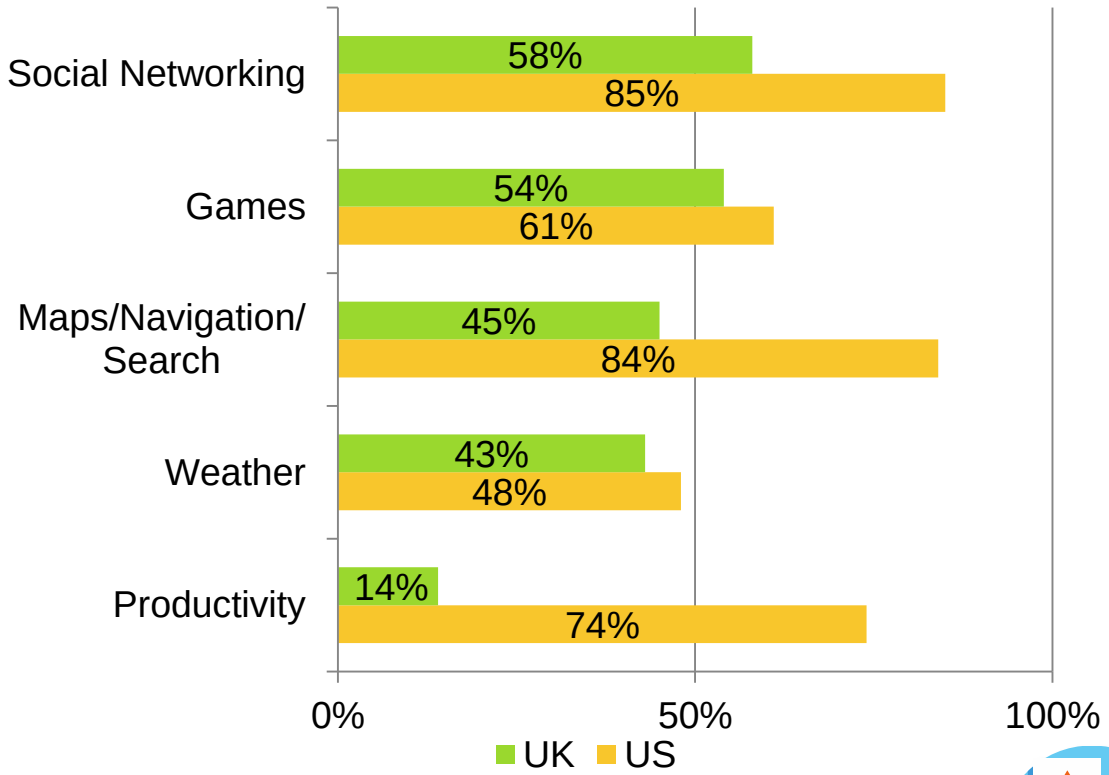


http://www.appcelerator.com.s3.amazonaws.com/pdf/developer-survey-Q2-2013.pdf
http://www.chupamobile.com/blog/2012/06/18/chupamobile-survey-shows-that-50-of-mobile-developers-use-3rd-parties-components-to-build-their-apps/

VERACODE
Securing the Software That Runs the World

Employee Mobile Apps

Which apps do people use?



http://www.nielsen.com/us/en/reports/2013/mobile-consumer-report-february-2013.html

APP CONSUMER

BYOD (or BYOA):

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

Dual Focus Required to Manage Risks

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

Spectrum of Enterprise Risks

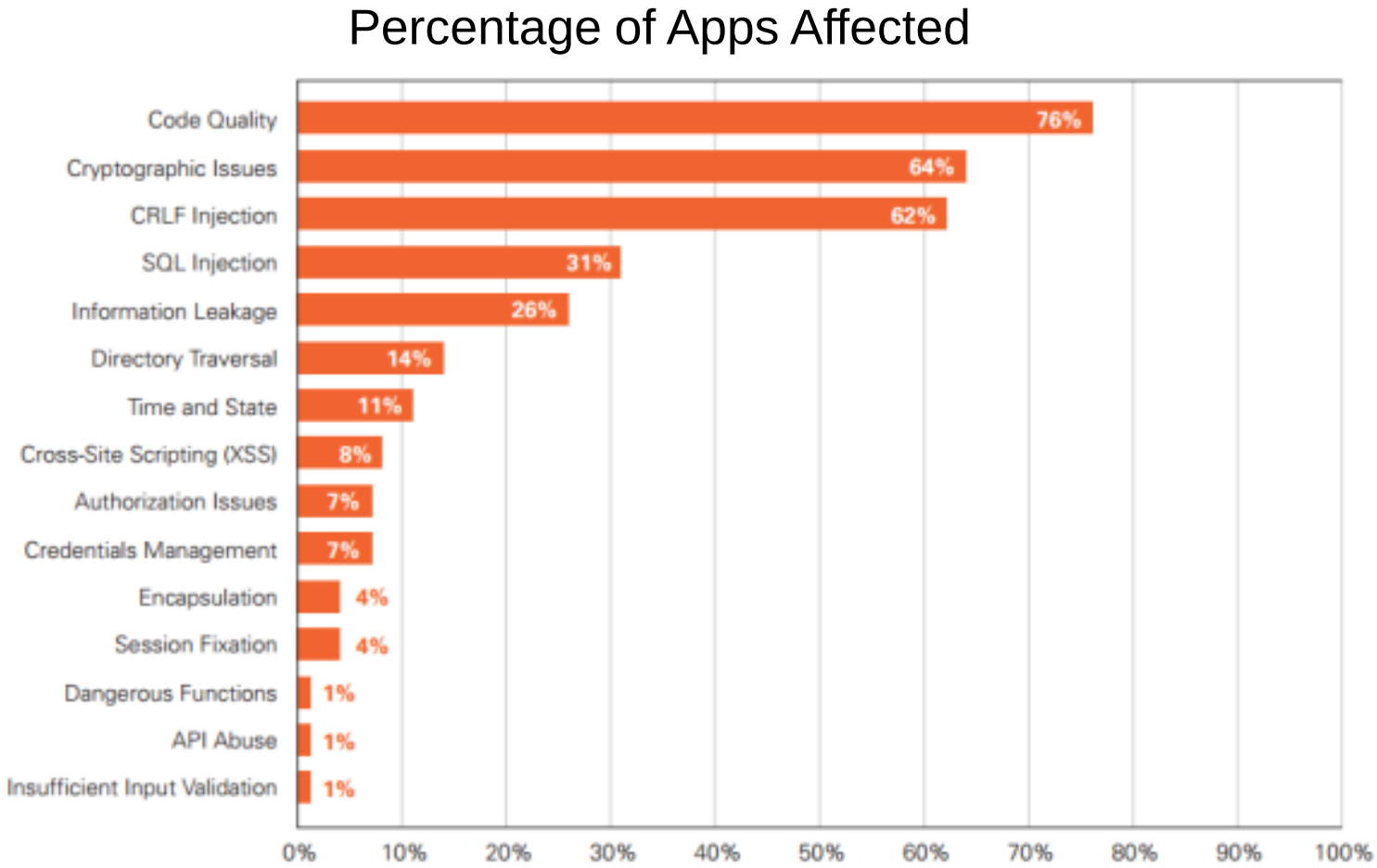
Concerns for App Consumer

Concerns for App Producer

What Can We Do About Mobile Application Risks?

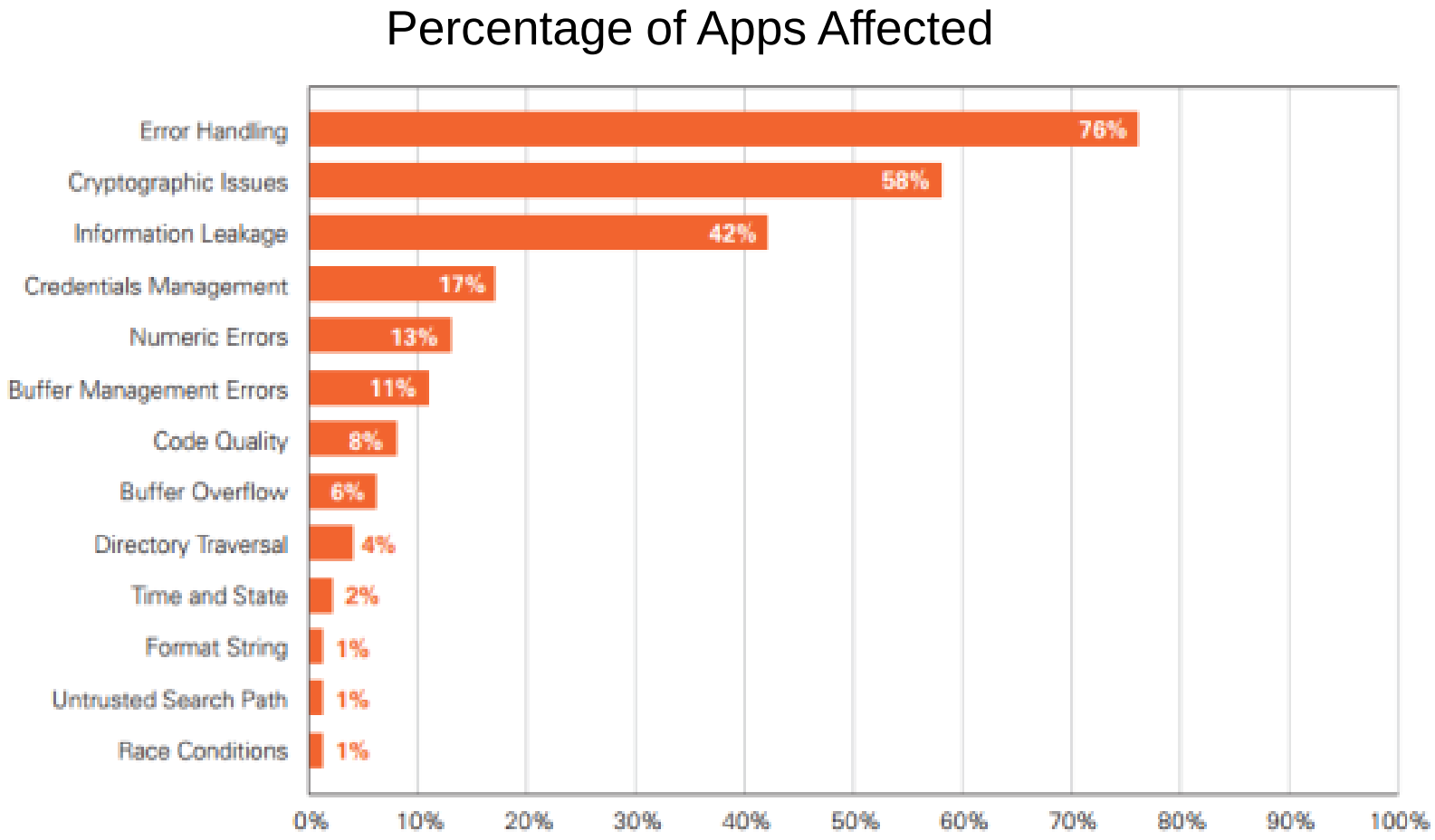
Understand the vulnerabilities, risky behavior and malicious code present in mobile apps.

Android Vulnerability Prevalence



Veracode State of Software Security Report Volume 5

iOS Vulnerability Prevalence



Veracode State of Software Security Report Volume 5

Flashlight Apps

Rank	Platform	App
2	iOS	Flashlight ?
5	iOS	Flashlight ?
7	iOS	Flashlight ?
8	iOS	Flashlight for iPhone
14	iOS	iTorch Flashlight
23	iOS	Flashlight !
32	iOS	Magnifying Glass W
34	iOS	Light - LED Flashligh
59	iOS	Flashlight ?

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

6

Suspicious App Behavior

MARS Analysis Feb 2013

It's Not Malware!

AVG	0
Agnitum	0
Identity	0
AntiVir	0
Antiy-AVL	0
Avast	0
BitDefender	0
ByteHero	0
CAT-QuickHeal	0
ClamAV	0
Commtouch	0
Comodo	0
DrWeb	0
ESET-NOD32	0
Emsisoft	0
F-Prot	0
F-Secure	0
Fortinet	0
GData	0
Ikarus	0
Jiangmin	0
K7AntiVirus	0
Kaspersky	0
Kingsoft	0
Malwarebytes	0
McAfee	0
McAfee-GW-Edition	0

However, it asked for many permissions:

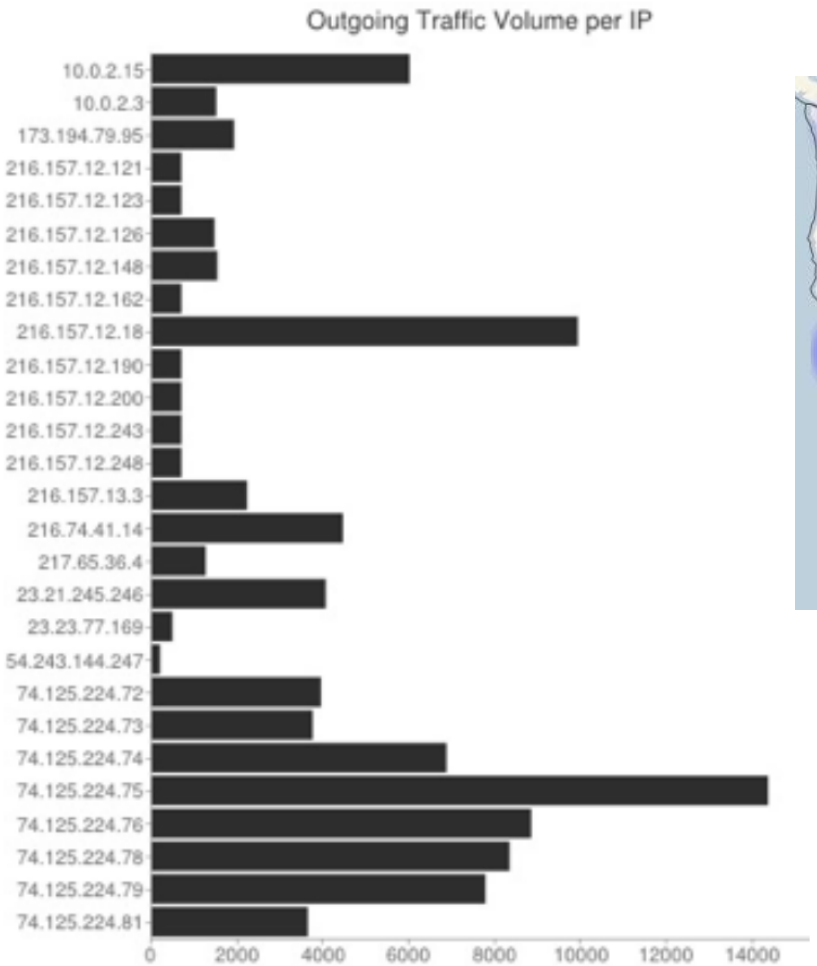
Category	Permission	Category	Permission
LOCATION	android.permission.ACCESS_COARSE_LOCATION	PRIVACY	com.android.launcher.permission.READ_SETTINGS
LOCATION	android.permission.ACCESS_FINE_LOCATION		com.android.launcher.permission.UNINSTALL_SHORTCUT
NETWORK	android.permission.ACCESS_NETWORK_STATE	PRIVACY	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		

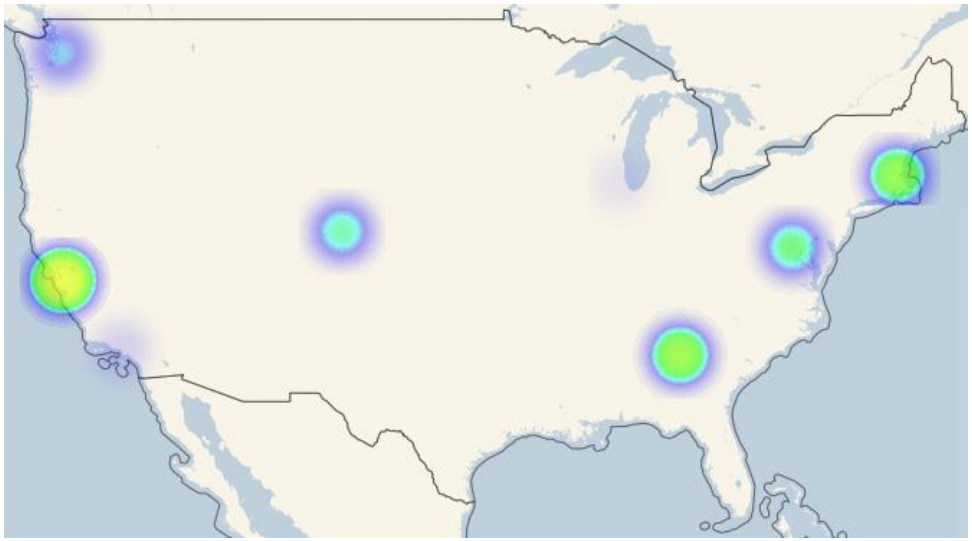
Its code did some odd things:

- Check if device is an emulator
- Seeks to become super user
- Launch Java processes via command line
- Enabling or loading Javascript on Webviews
- Reads Android system logs
- Monitors contact list
- Time delay code structures
- Send SMS messages

MARS Analysis Feb 2013

… and it sends data to many places

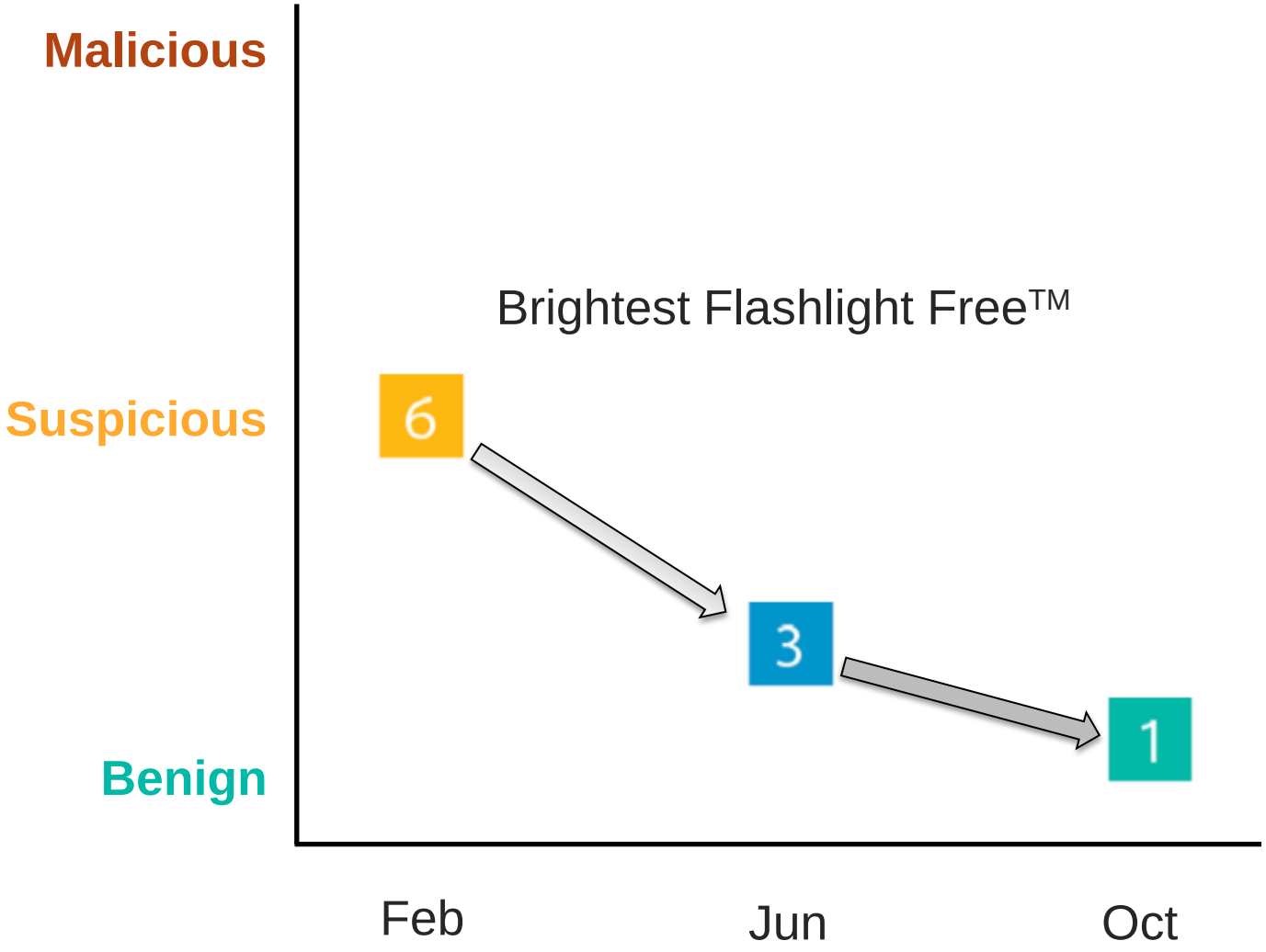




Should this app be on your phone?

MARS Analysis Feb 2013

Good News: It Improved Over Time



Testing once isn't enough

What Can We Do About Mobile Application Risks?

Understand the vulnerabilities, risky behavior and malicious code present in mobile apps.

Detect which mobile apps violate enterprise policy quickly and efficiently.

Detecting Vulnerabilities, Risky Behaviors & Malicious Code

Learn from the Past

Basic Heuristics

Signatures

Signatures

Signatures

Manual Testing

Advanced Machine Learning

Static Analysis

Behavioral Dynamic Analysis

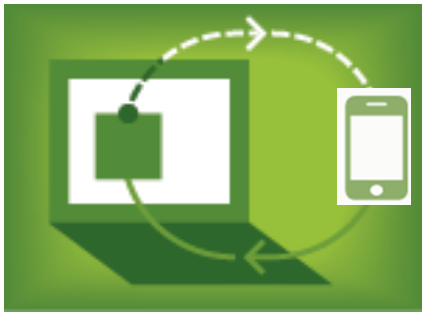
What Can We Do About Mobile Application Risks?

Understand the vulnerabilities, risky behavior and malicious code present in mobile apps.

Detect which mobile apps violate enterprise policy quickly and efficiently.

Act intelligently to mitigate risk and protect data.

Enterprises Act Through Control Points



Mobile Device Management (MDM)

Mobile Application Management (MAM)

Enterprise App Stores

App Wrapping

Mobile App Policies:

- Customize employee risk profiles
- Conduct app risk analysis
- Encourage use of lower risk apps
- Keep testing! (once is not enough)

BUT INTELLIGENCE IS REQUIRED!

Enterprises Act Through Control Points

Enterprise Developers

Outsourced Developers

Code Defensively:

- Assume device storage is insecure
- Don't ask for more permissions or data than you need
- Don't trust the other mobile layers to always do the right thing
- Test early and often

BUT INTELLIGENCE IS REQUIRED!

The Path Forward

Behavioral Analysis + Malware Detection + Vulnerability Analysis + Enterprise Control Points = **A Safer Mobile Path**

Security in knowledge

Thank you!

Chris Eng
Veracode

ceng@veracode.com

@chriseng