

# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.  
Learn.  
Secure.

Capitalizing on  
Collective Intelligence

## Why Mobile Should **STOP WORRYING** -AND LEARN TO- **LOVE THE ROOT**

SESSION ID: MBS-R03

Andrew Hoog

Co-Founder/CEO  
viaForensics  
@ahoog42






# The Storyline

- ◆ Chapter One: History, or How We Came to Fear the Root
- ◆ Chapter Two: Present Day – The Cold War
- ◆ Chapter Three: Conclusion (An Armistice Proposal)
- ◆ The End



# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



***“It is the fate of  
operating systems to  
become free.”***

**Neal Stephenson**





**RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

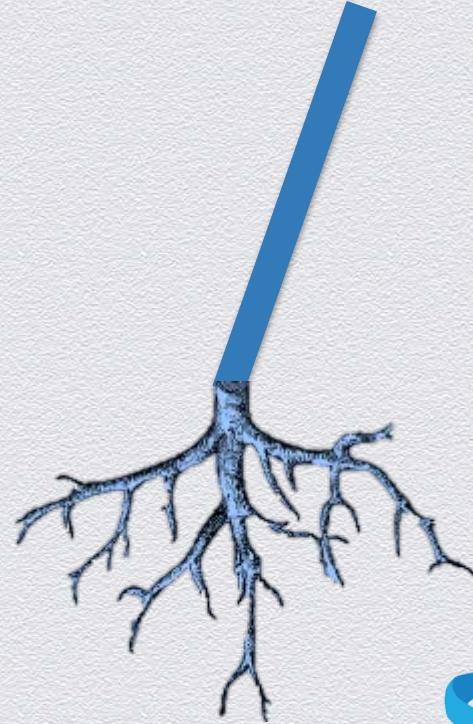
## **Chapter One: History, or How We Came to Fear the Root**



# Root's Roots

**or, origin of the superuser**

- ◆ “UNIX security” oxymoron
- ◆ Open systems
- ◆ There can be only one!





# The Root... Of All Evil?

## Root Can:

- ◆ Modify the Operating System
- ◆ Ignore file permissions
- ◆ Break out of sandbox
- ◆ Install software
- ◆ Steal souls





# 1990's – Computers Mean Business

## Windows reinvents the OS

- ◆ Did someone say security?
  - ◆ 3.0 (90)... 95... 98...
  - ◆ Win2K is secure! (ok maybe XP)
- ◆ Admins could not block user from root until Windows 2000

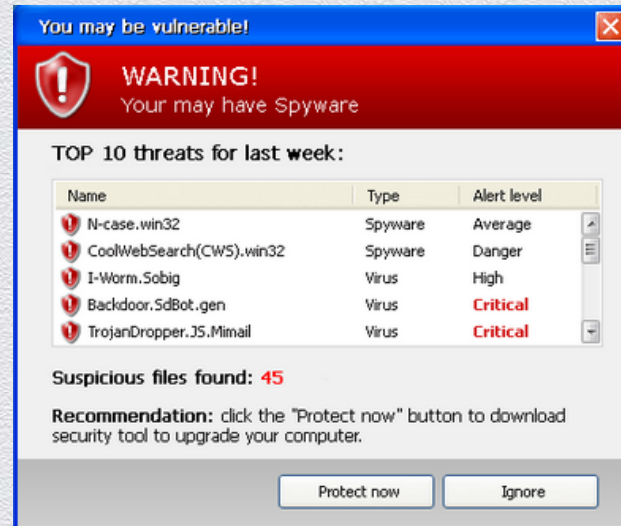




# A New Era In\_Security

## M\$ got serious about security

- ◆ No rights for you, user
- ◆ Antivirus
- ◆ Cyber security solved
- ◆ Businesses rejoice!





# Fast Forward

## The CEO wants what?

He wants an iPhone?

No, we have secure Blackberry phones, tell him he can't have an iPhone.

(1 week later...)





# Consumerization

## New smart phones for all!


- ◆ Ok, just a *few* iPhones
  - ◆ Became Full BYOD
- ◆ Secured by Apple!
- ◆ Android too, no root for you.





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



***“This and no other is  
the root from which a  
tyrant springs; when he  
first appears he is a  
protector.”***

**Plato**





## Chapter Two: Present Day – The Cold War





## Fact: Users Worry About Mobile Security

What are we concerned about?



# Top Mobile Security Concerns

**Source:** [Informationweek Survey State of Mobile Security](#) (April 2013)

- ◆ **78%** - Lost/Stolen Devices
- ◆ **36%** - Users Forwarding Corp. Information to Cloud Storage
- ◆ **34%** - Malware from App Stores
- ◆ **32%** - Penetration of Corp Wi-Fi
- ◆ **25%** - Security at Public Hotspots
- ◆ **22%** - Devices jailbroken/rooted by end users
- ◆ **21%** - Malware exploiting internally developed mobile apps
- ◆ **19%** - Interception of OTA traffic
- ◆ **17%** - Users forwarding email to personal accounts
- ◆ **5%** - Penetration of home Wi-Fi
- ◆ **1%** - Other





## Fact: Carriers and OEMs Lock Users Out of Root

What are they worried about?

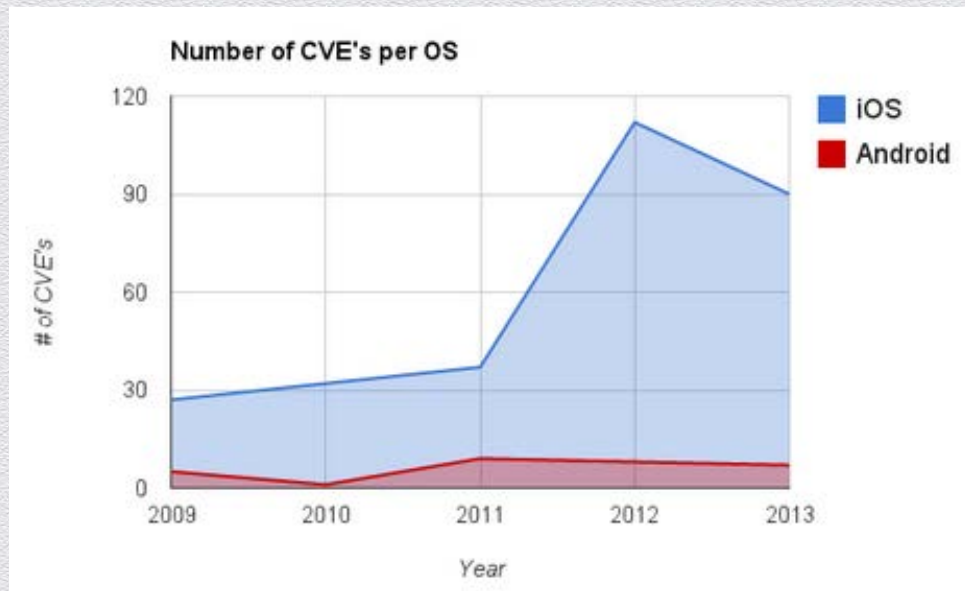


# Carrier/OEM Use of Root Lockout

- ◆ Pre-installed apps (aka “bloatware”)
- ◆ Carrier locking
- ◆ App store restriction
- ◆ DRM
- ◆ Exclusivity on security



# Track Record: iOS and Android



Source: CVEDetails.com (MITRE CVE Reports)

## History of vulnerability

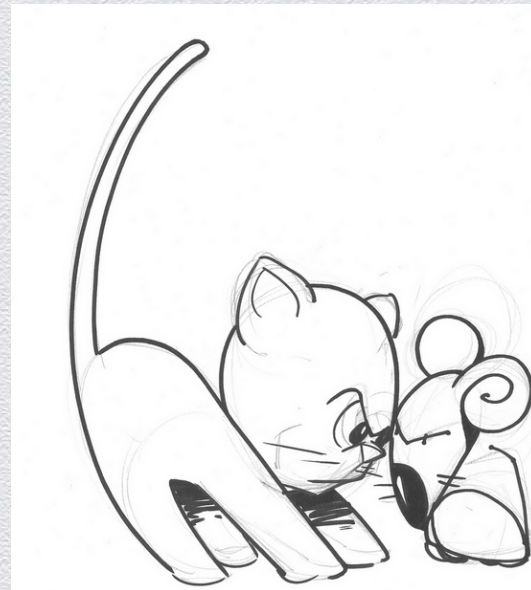
- ◆ Faster patching in hacker space
- ◆ Every major version rooted/jailbroken
- ◆ Some remote / 1-click exploits
- ◆ Many more on iOS (surprised?)



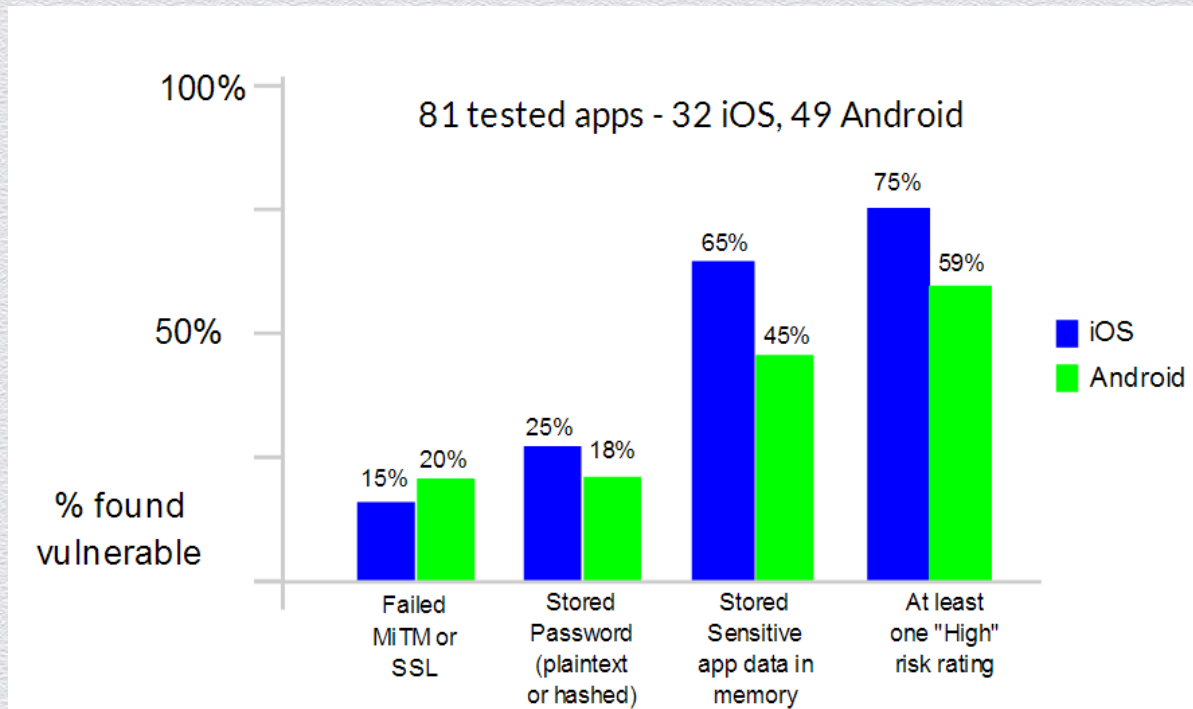
# Root #FTW

## Cat and mouse

- ◆ Jailbreakme
- ◆ Gingerbreak
- ◆ HTC, ZTE backdoors
- ◆ Master Key
- ◆ Malicious charger
- ◆ Fort KNOX?







## Fighting the Wrong Enemy

Malware may not be reaching many devices – but many vulnerable apps are.



# Results of Root Exclusivity

## Intended Purpose

- ◆ Pre-installed apps
- ◆ Carrier Locking
- ◆ App Store Limit, DRM
- ◆ Security Exclusivity

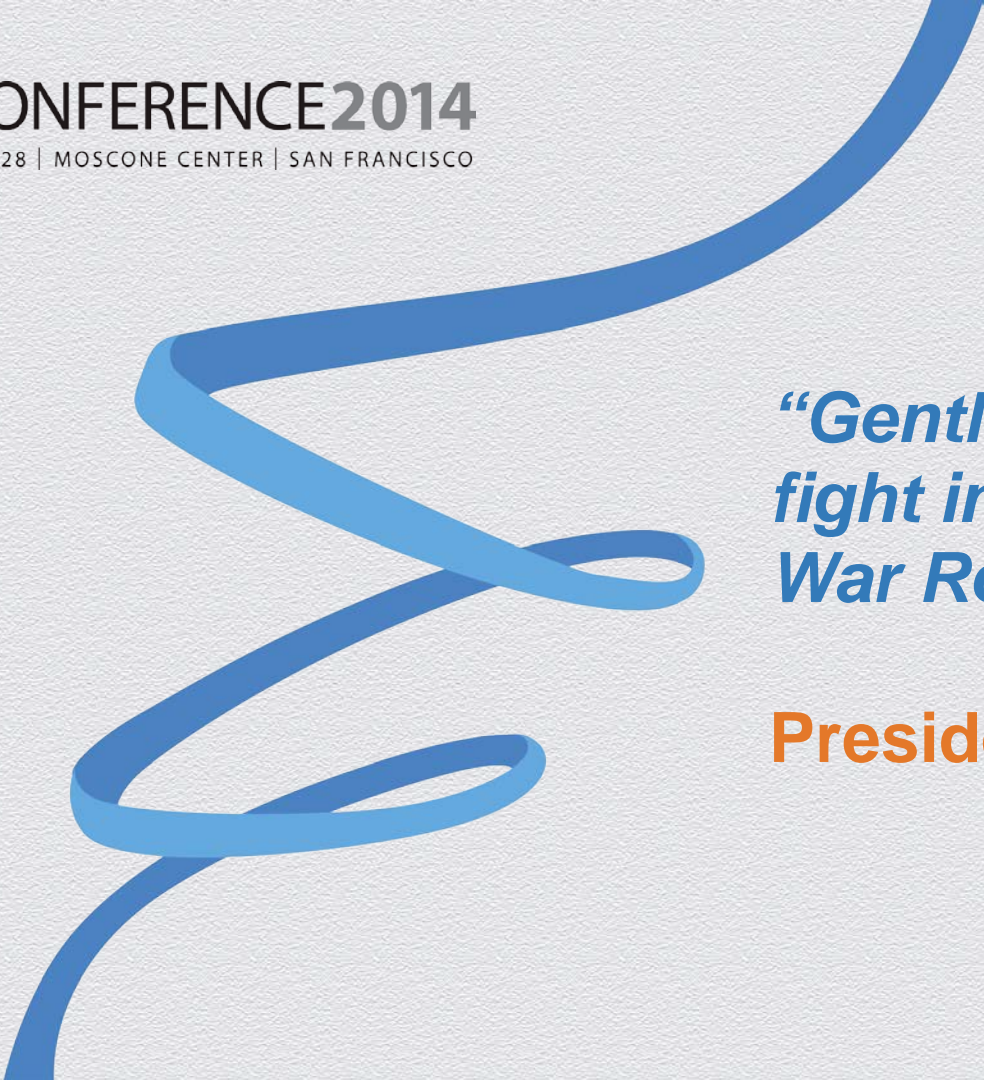
## Result

- ◆ Users root to install CyanogenMod
- ◆ Users jailbreak to switch carriers
- ◆ Users jailbreak to use Cydia
- ◆ Security tools inside sandbox



# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



***“Gentlemen, you can't  
fight in here! This is the  
War Room!”***

**President Merkin Muffley**





**RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

## **Chapter Three: Conclusion (An Armistice Proposal)**





## Securing Mobile – Whose Interests Are We Protecting?

Consumers and business bear the risk, shouldn't they have control?



# Real Mobile Security Risks

- ◆ App vulnerability/misbehavior
- ◆ Lack of visibility
- ◆ Insider threat
- ◆ Advanced adversaries
- ◆ Malware





VIA

PROTECT

Search

DASHBOARD

REPORTS

Apps Installed

Battery Charge

Geo Location

Network

Countries

Netstat

Protocols

Organizations

Traffic

Aggregate

SETUP

Netstat (country:China)

samsung GT-N7100 (note-ii-jan-2014)

CUSTOM

Show 100 entries

Search:

APP	DESTINATION	PROTOCOL	COUNTRY	ORGANIZATION	WHEN
Maxthon Browser	223.202.36.53	http	China	China Unicom Beijing	11 Jan 2014, 10:44 AM
Maxthon Browser	223.202.36.53	http	China	China Unicom Beijing	11 Jan 2014, 10:44 AM
Maxthon Browser	223.202.36.52	http	China	China Unicom Beijing	11 Jan 2014, 10:14 AM
Maxthon Browser	223.202.36.52	http	China	China Unicom Beijing	11 Jan 2014, 08:44 AM
Maxthon Browser	223.202.36.52	http	China	China Unicom Beijing	11 Jan 2014, 07:44 AM
Maxthon Browser	223.202.36.52	http	China	China Unicom Beijing	11 Jan 2014, 06:44 AM
Maxthon Browser	223.202.36.52	http	China	China Unicom Beijing	11 Jan 2014, 05:44 AM

## Drive Visibility

Do we really know what's happening on our devices?



# A Different Approach

## Root for the Good Guys

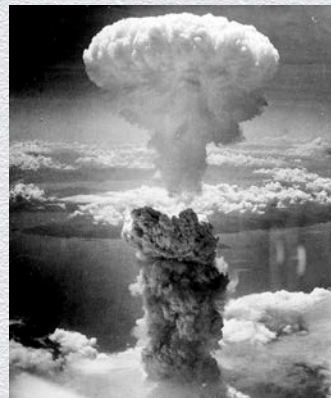
- ◆ Enterprise cert embedded by OEM
- ◆ More unlocked options
- ◆ Apple developer phone
- ◆ Security vendor programs
- ◆ Less paranoia





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



## The End

Andrew Hoog

Co-Founder/CEO  
viaForensics  
@ahoog42