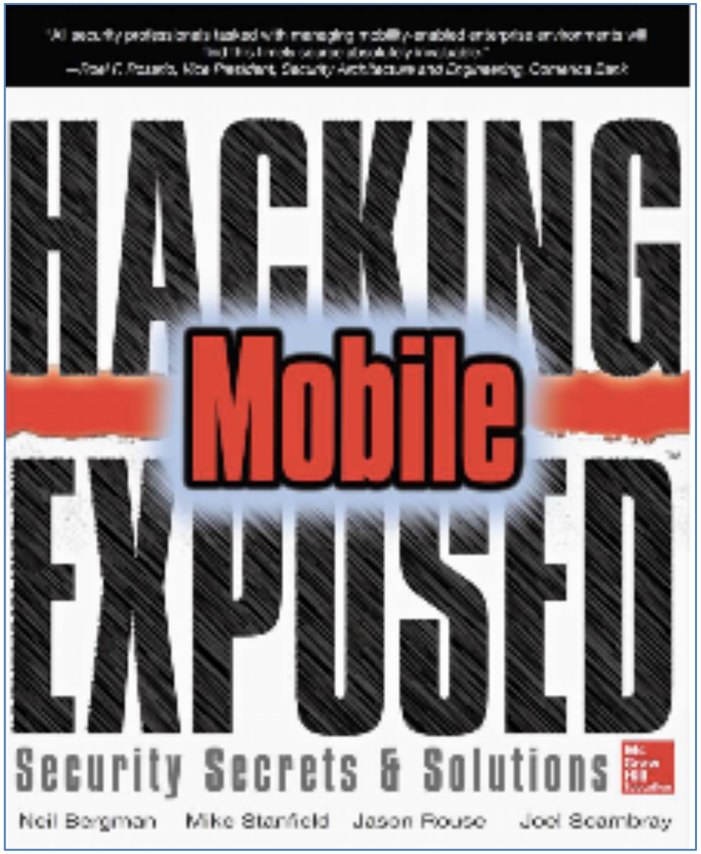
Ch 3: iOS



CNIT 128: Hacking Mobile Devices

Part 1

Loc. 1204-1471

rev. 2-6-17

Part 1

- Start of chapter 3 to the section titled
- "The JailbreakMe3.0 Vulnerabilities"

History of iOS

- Very popular, 500 million sold as of 2013
- Modern versions are very secure
- Closed system: by default,
  - Third parties are not allowed to modify the OS in any way
  - Users cannot access their iThings remotely
  - Can only install apps from Apple's App Store, no third parties
- Hackers work to overcome these restrictions

History of the iPhone

- In the 1980s, Steve Jobs founder NeXT
    - The NeXTSTEP OS was based on the Mach kernel and BSD Unix
    - Used Objective-C for programming apps
- 1996: Apple purchased NeXT
    - NeXTSTEP used as the basis for OS X
- 2001: Mac OS X released

History of the iPhone

- 2007: iPhone introduced
  - Running iOS, a pared-down version of OS X
- Over the next few years came the iPod, Apple TV, and iPad in various versions, all running iOS
- All run on ARM processor
  - 64-bit starting with iPhone 5s (link Ch 3b)
  - 32-bit for earlier versions

How Secure is iOS?

- First iPhone did not allow any third-party apps
  - Only a Web browser to allow Web apps
  - This lowered security requirements
- 2008: App Store introduced
  - Over 800,000 apps now
  - New security measures introduced

Early Versions of iOS

- Very little security
- All processes ran as root
- No sandboxing or restriction on use of system resources
- No code signing
- No Address Space Layout Randomization (ASLR)
  - No Position Independent Executable (PIE) support

Security Measures Added

- Third-party apps ran under a less-privileged user account named *mobile*
- Sandboxing restricted apps to a limited set of system resources
- Code signature verification supported
  - Apps must be signed by Apple to execute
  - Code signatures verified both at load time and runtime, to prevent injection of new code into memory

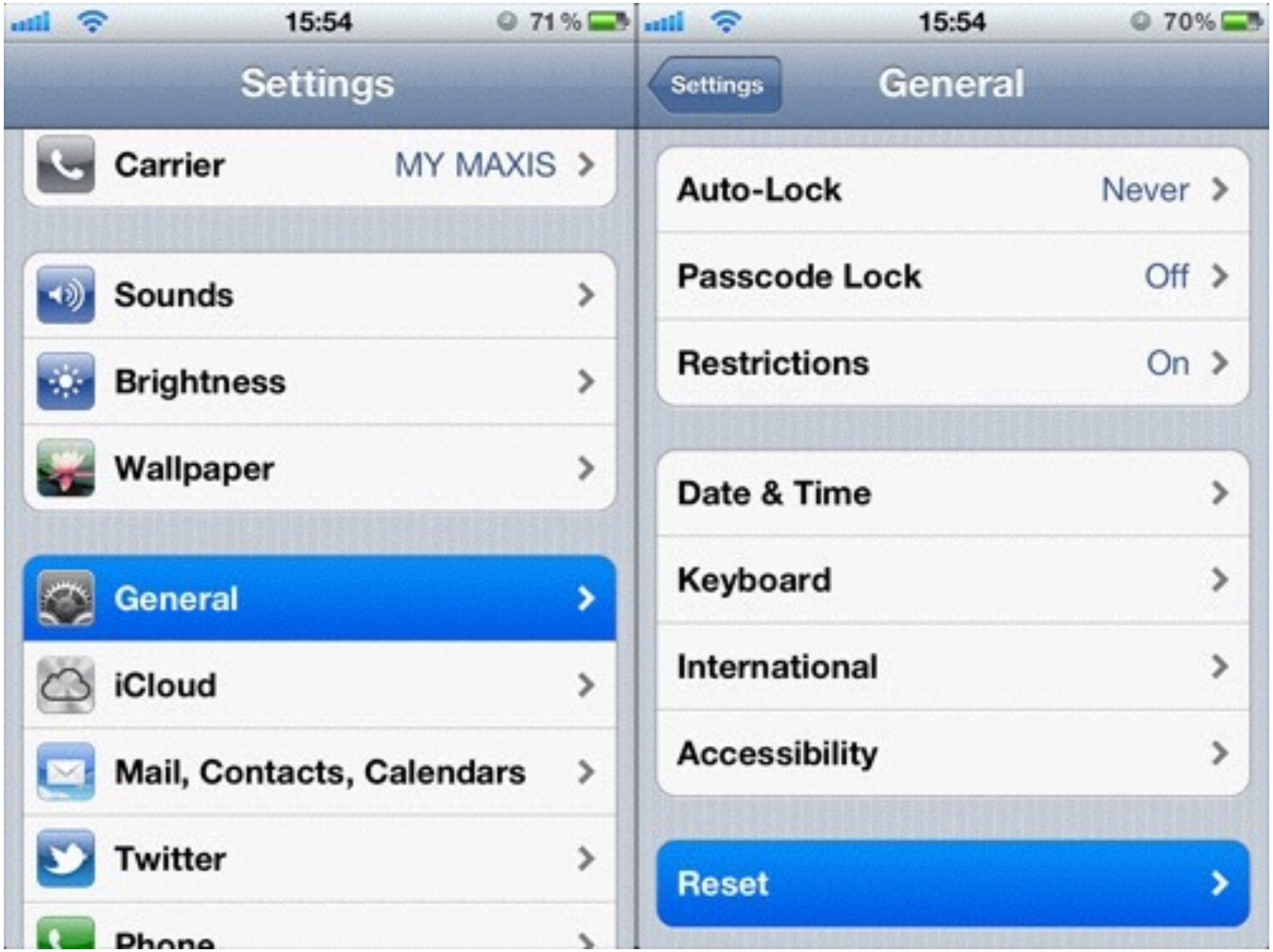
Security Measures Added

- ASLR added for kernel, OS components, and libraries
- PIE supported as a compile-time option in Xcode
    - PIE apps load at a different base address every time they execute
    - Makes exploitation of buffer overflows more difficult

Encryption

- iPhone 3GS and later devices encrypt the file system with AES
  - Using a hardware AES cryptographic accelerator
  - The key is not available to the CPU
- This makes wiping all data instantaneous
  - Simply delete the File System Key
- In earlier devices, wiping the SSD took hours
  - Link Ch 3d

Wiping your iPhone



Carrier MY MAXIS

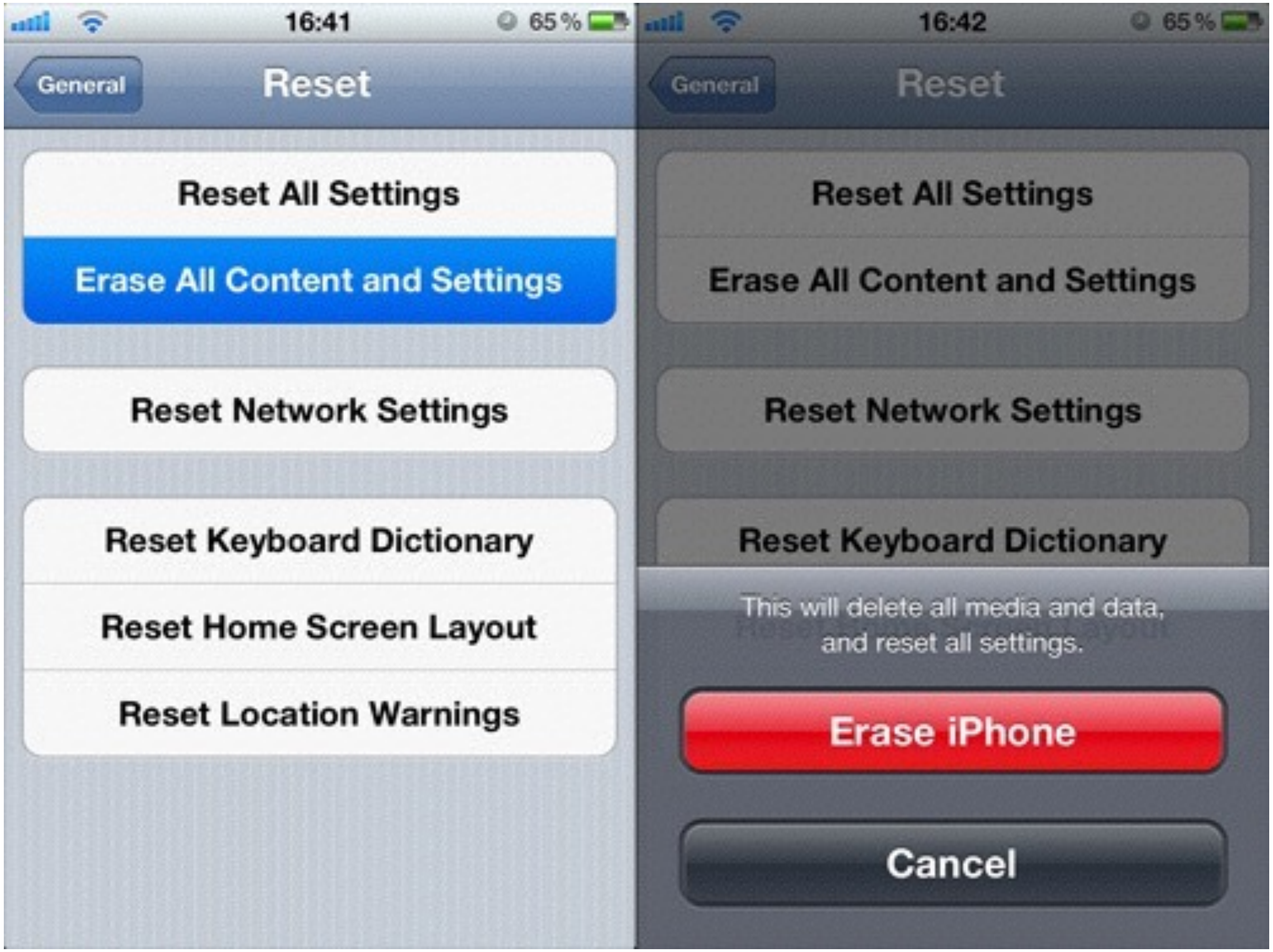
Auto-Lock Never

Passcode Lock Off

Restrictions On

- Image from hongkiat.com

Wiping your iPhone



This will delete all media and data, and reset all settings.

- Image from hongkiat.com

Security of Modern iPhone (& other iThings)

- The most secure consumer-grade operating system available
  - Unless you jailbreak it
- No antivirus or firewall is available, because you don't need them
- No spreading viruses
- Limited, targeted attacks are still possible

Jailbreaking:
Unleash the Fury!

Users Defeating Security

- The owner of an iPhone does not have root access to their own device by default
- You need to defeat Apple and hack your own phone to get it
- This offends a lot of freedom-lovers, but it makes you a lot safer

Liberty or Death!

- *"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." – Ben Franklin*
  - A widely misunderstood quote (link Ch 3)

Jailbreaking

- Taking full control of an iThing
- May require downloading software, or, occasionally, just a visit to jailbreakme.com
- You get access to Cydia, a large store of unauthorized apps
  - Also stolen commercial apps
  - Code signing is disabled, so you can run any app, good or bad

Risks of Jailbreaking

- Jailbreaking is an exploit against a vulnerability
- Trojaned Jailbreak apps could do anything to your device
- Jailbroken phones may lose some functionality
  - Such as iBooks
- You may "brick" your device
- Voids your warranty

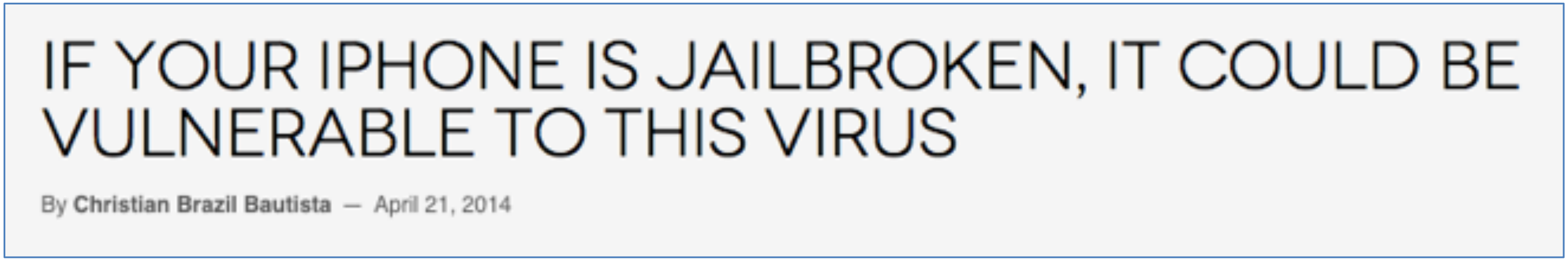
Point of No Return

- Even if you back up your device first with iTunes
- There is no easy way back to a completely clean system after jailbreaking
  - Except, possibly, reset to factory defaults

Security Becomes Your Responsibility

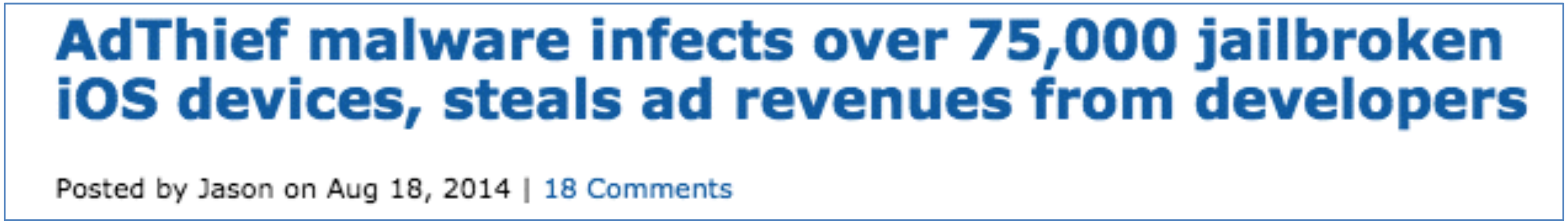
- Your device is no longer protected by Apple
- The jailbreak community is a very powerful security research force

Viruses on Jailbroken iPhones



IF YOUR IPHONE IS JAILBROKEN, IT COULD BE VULNERABLE TO THIS VIRUS

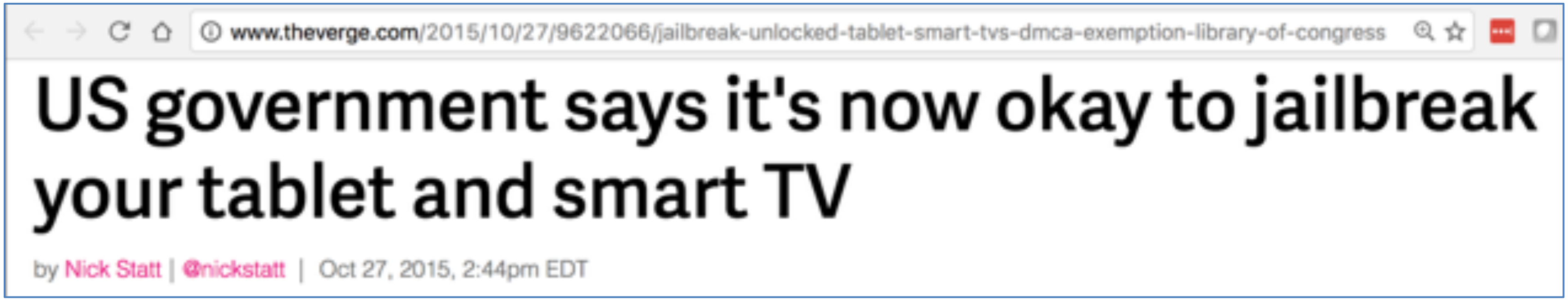
By **Christian Brazil Bautista** — April 21, 2014



AdThief malware infects over 75,000 jailbroken iOS devices, steals ad revenues from developers

Posted by Jason on Aug 18, 2014 | 18 Comments

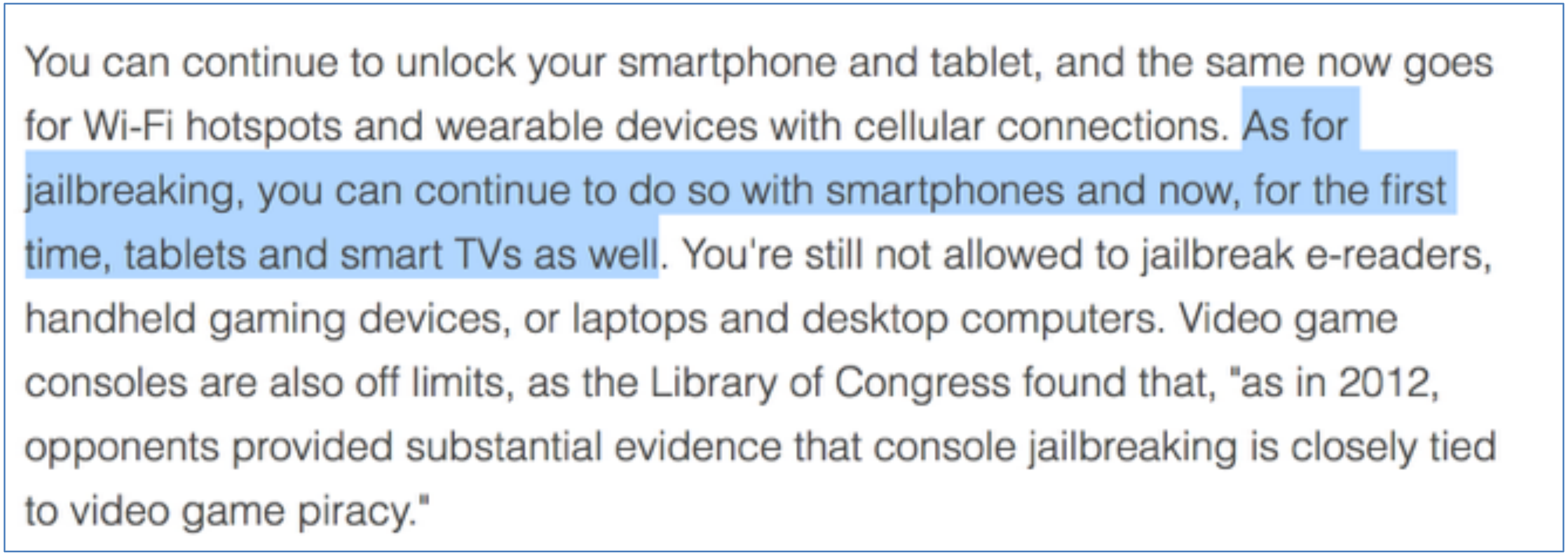
- Links Ch 3h, 3i, 3j



www.theverge.com/2015/10/27/9622066/jailbreak-unlocked-tablet-smart-tvs-dmca-exemption-library-of-congress

US government says it's now okay to jailbreak your tablet and smart TV

by Nick Statt | @nickstatt | Oct 27, 2015, 2:44pm EDT



You can continue to unlock your smartphone and tablet, and the same now goes for Wi-Fi hotspots and wearable devices with cellular connections. As for jailbreaking, you can continue to do so with smartphones and now, for the first time, tablets and smart TVs as well. You're still not allowed to jailbreak e-readers, handheld gaming devices, or laptops and desktop computers. Video game consoles are also off limits, as the Library of Congress found that, "as in 2012, opponents provided substantial evidence that console jailbreaking is closely tied to video game piracy."

Jailbreaking and Unlocking iPhones are Legal Now

- Jailbreaking
  - Gaining root access
  - Legal through 2018 for phones and tablets through a time-limited exception to the DMCA
- Unlocking
  - Enabling you to switch carriers
  - Also legal

Methods of Jailbreaking

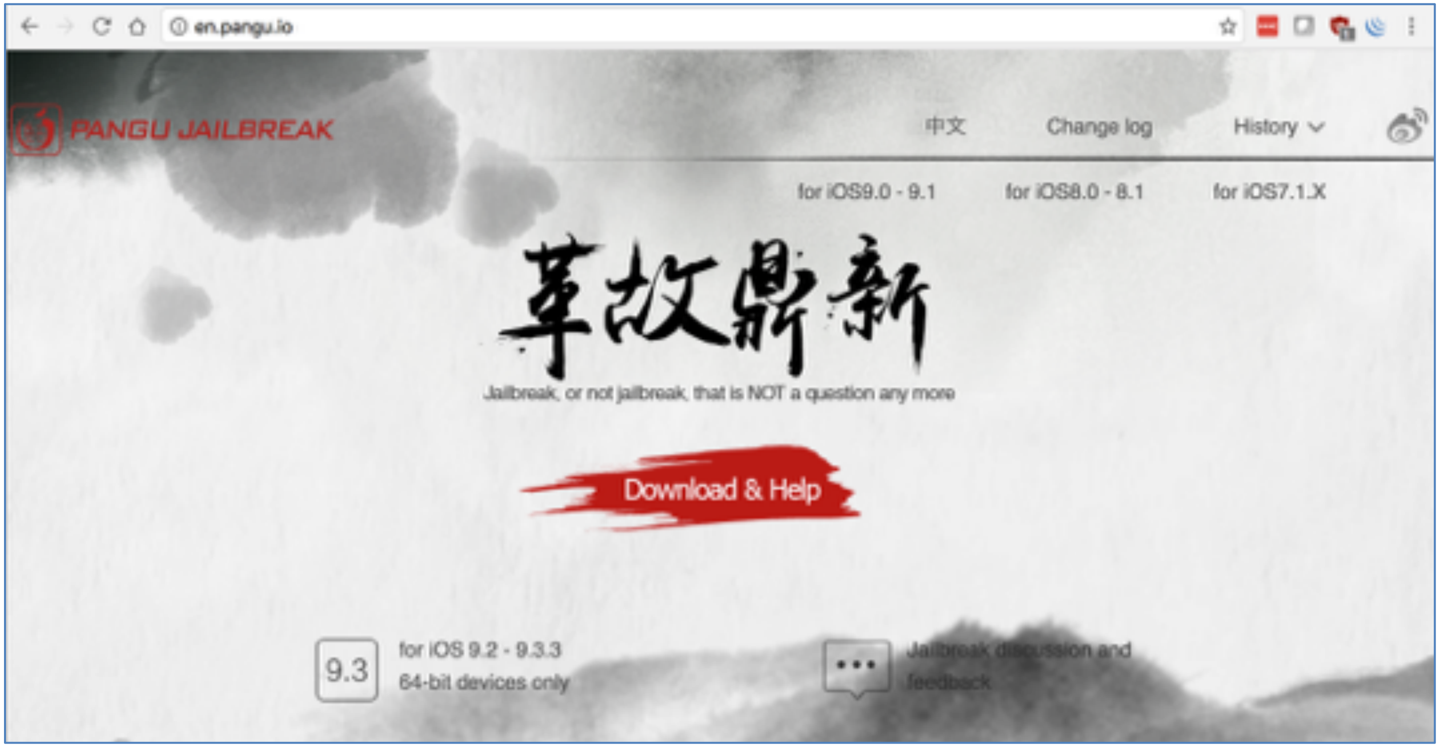
- Take control of the boot process
  - Push a custom firmware image to the device
  - Works on older devices: iPhone 3G/3GS/4G, iPod 4G, iPad 1
- Remote jailbreaking
  - Load a file that
  - Exploits and takes control of a user land process
  - Then exploits and takes control of the kernel
  - jailbreakme.com

More Recent Methods

- Corona or Absinthe jailbreak
  - Works on iPhone 4S and iPad 2/3 running iOS v. 5
- Evasion
  - Works on iPhone 5, iPod 5G, iPad 4, and iPad mini running iOS v. 6.x
  - Newest version works on iOS v. 7 (link Ch 3n)

Pangu Jailbreak

- Works on iOS 7, 8, and some versions of 9



革故鼎新

Jailbreak, or not jailbreak, that is NOT a question any more

for iOS 9.2 - 9.3.3
64-bit devices only

Jailbreak discussion and feedback

Tethered v. Untethered

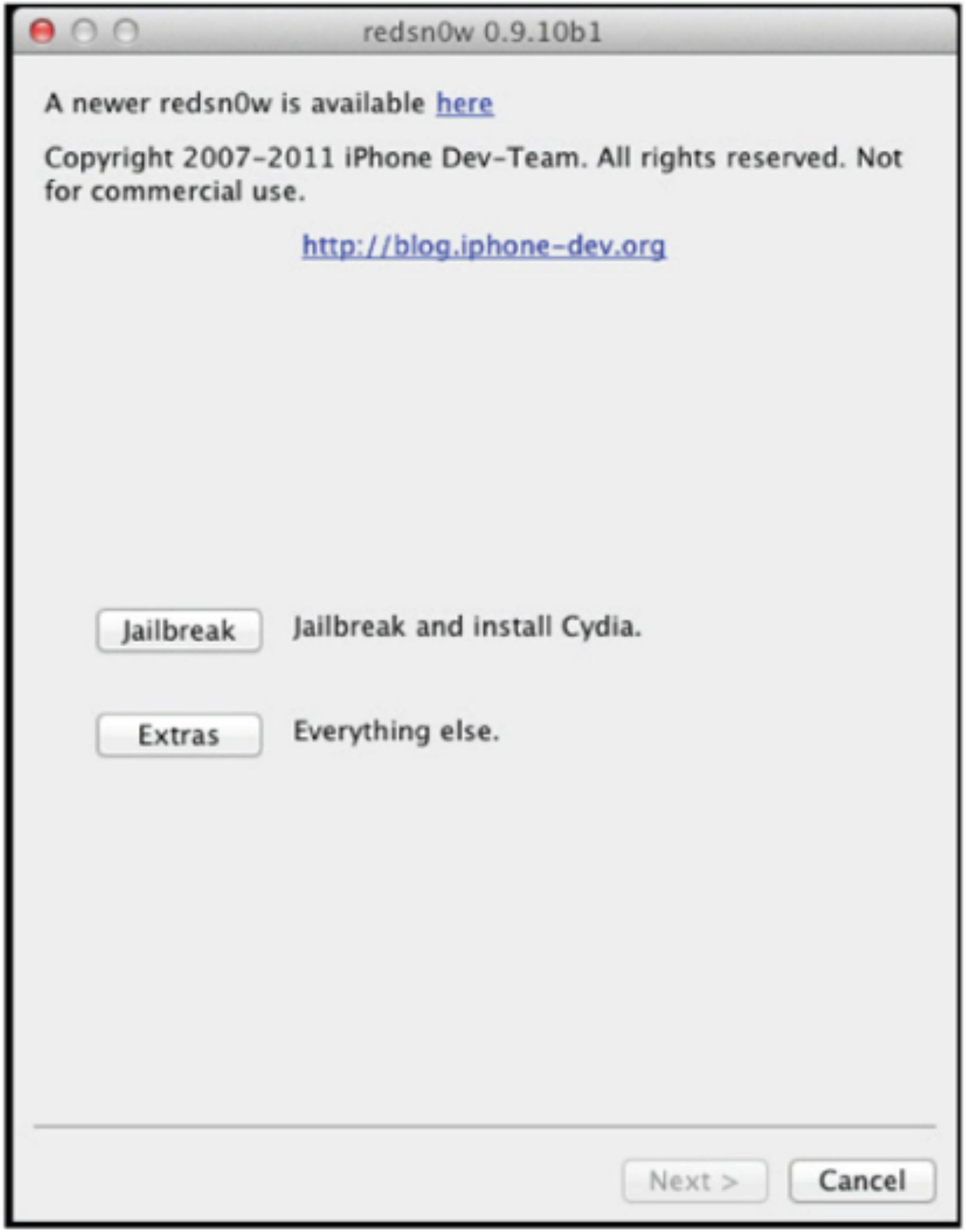
- A tethered jailbreak needs to be connected to a computer via USB on every reboot
  - Used only by people who demand the very latest versions, or jailbreak developers
- An untethered jailbreak is far more convenient
  - iDevice can reboot on its own
- Link Ch 3o

Boot-based Jailbreak

Steps for Boot-based Jailbreak

1. Download appropriate iOS firmware image from Apple (called IPSW)
   - Get the version for your device version and iOS version, such as "iPhone 4 firmware 4.3.3"
2. Download jailbreak software
   - Such as Redsn0w, GreenPoison, or limera1n
3. Connect iDevice to computer via USB

4. Launch the jailbreak app on the computer



A newer redsn0w is available here

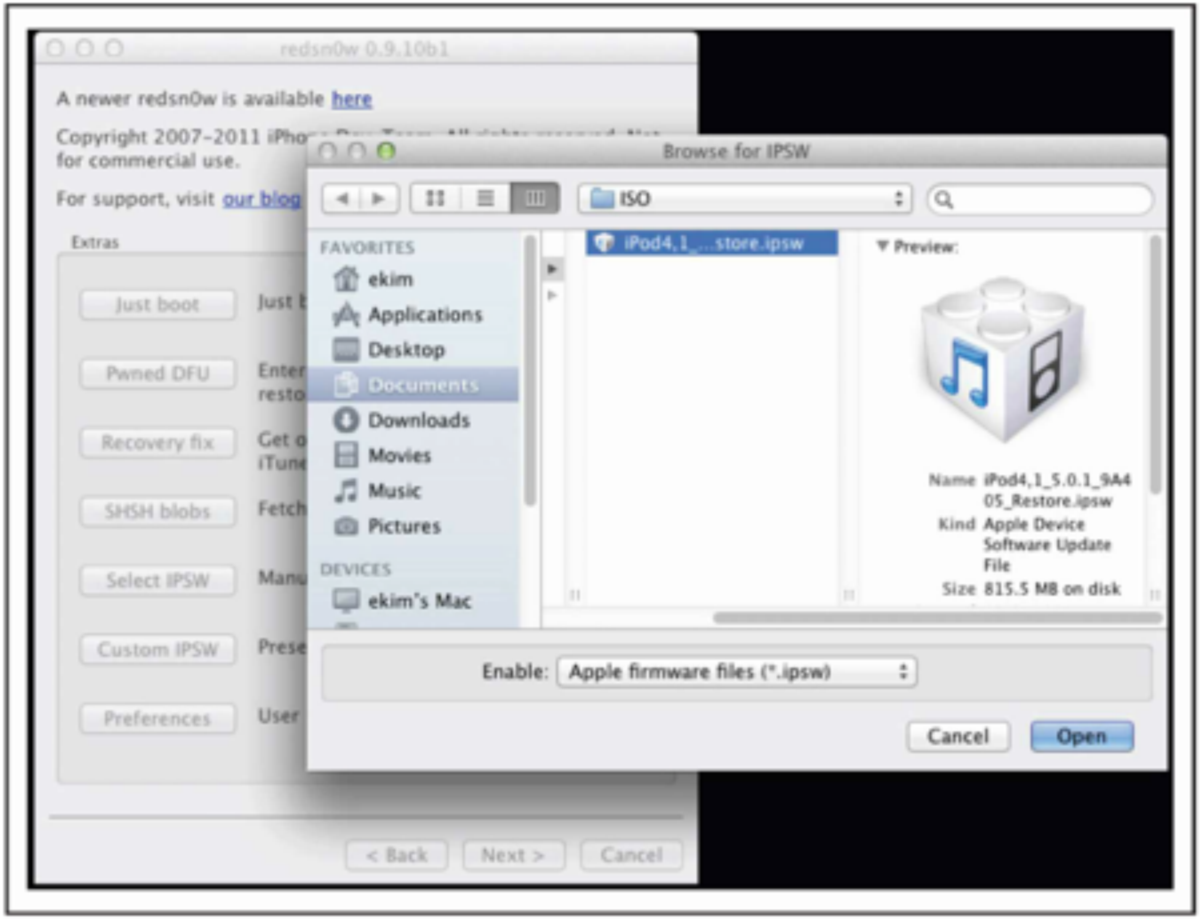
Copyright 2007-2011 iPhone Dev-Team. All rights reserved. Not for commercial use.

http://blog.iphone-dev.org

Jailbreak and install Cydia.

Everything else.

5. On the computer, select the IPSW file



A newer redsn0w is available here

Copyright 2007-2011 iPho
for commercial use.

For support, visit our blog

Name iPod4,1_5.0.1_9A405_Restore.ipsw

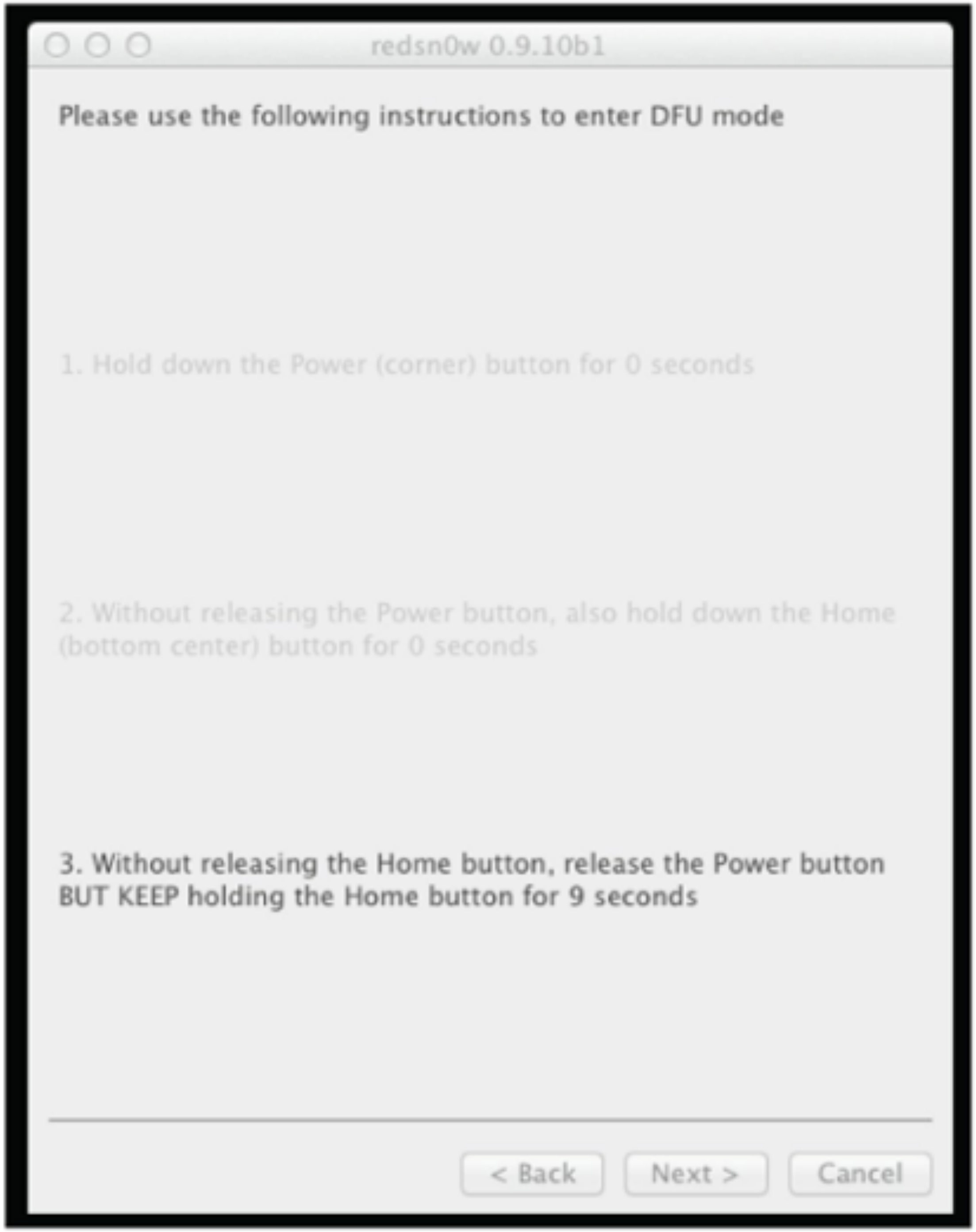
Kind Apple Device Software Update File

Size 815.5 MB on disk

Enable: Apple firmware files (*.ipsw)

6. Put iDevice into Device Firmware Update (DFU) Mode

- Hold power and home buttons down for 10 seconds
- Release power and hold home down another 5 sec.



Please use the following instructions to enter DFU mode

1. Hold down the Power (corner) button for 0 seconds

2. Without releasing the Power button, also hold down the Home (bottom center) button for 0 seconds

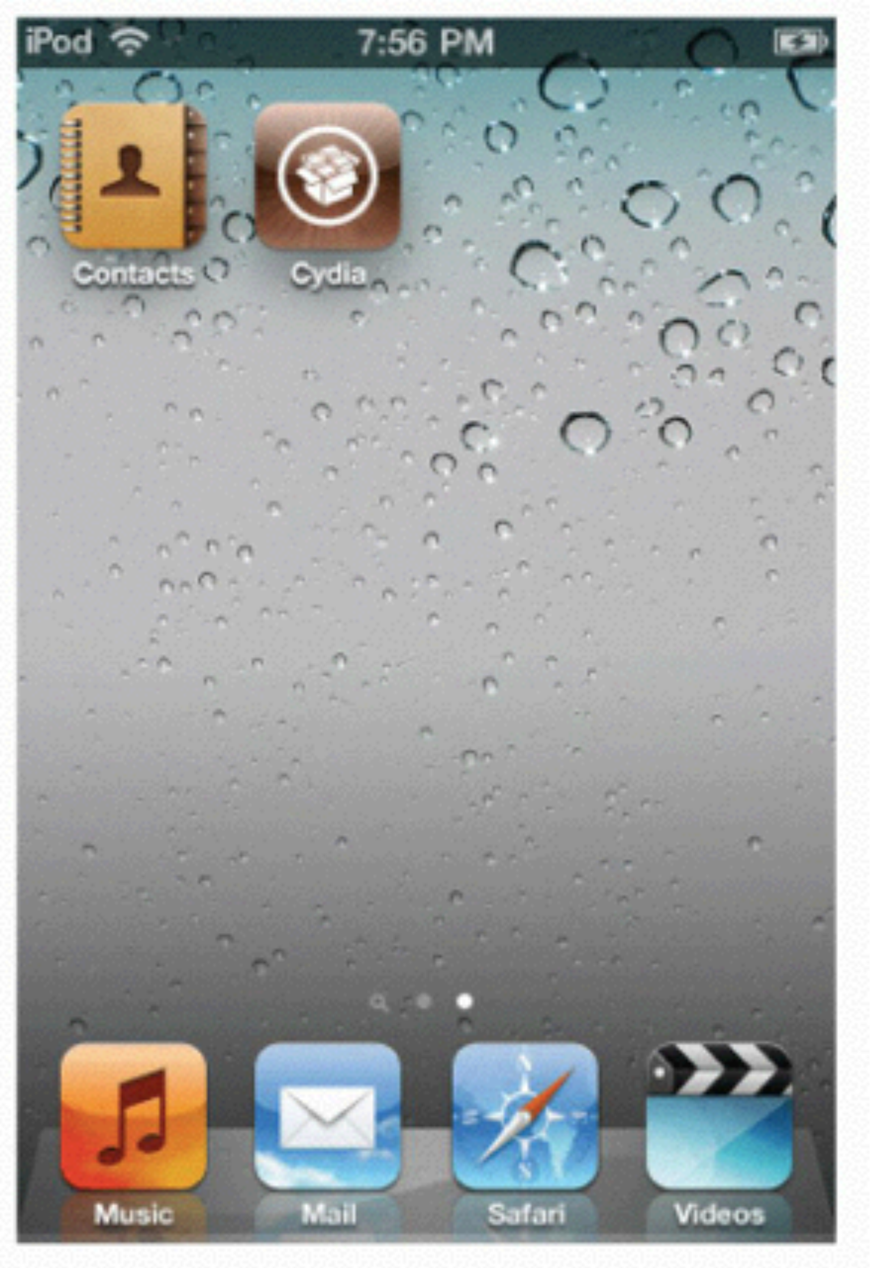
3. Without releasing the Home button, release the Power button BUT KEEP holding the Home button for 9 seconds

7. Wait

- It takes a several minutes
- Scary text scrolls by
  - I saw upside-down red error messages, then a totally black screen, then right-side-up green error messages, then another long black screen
- Device reboots

Cydia

- Jailbroken iThings now have Cydia
- The unrestricted App store



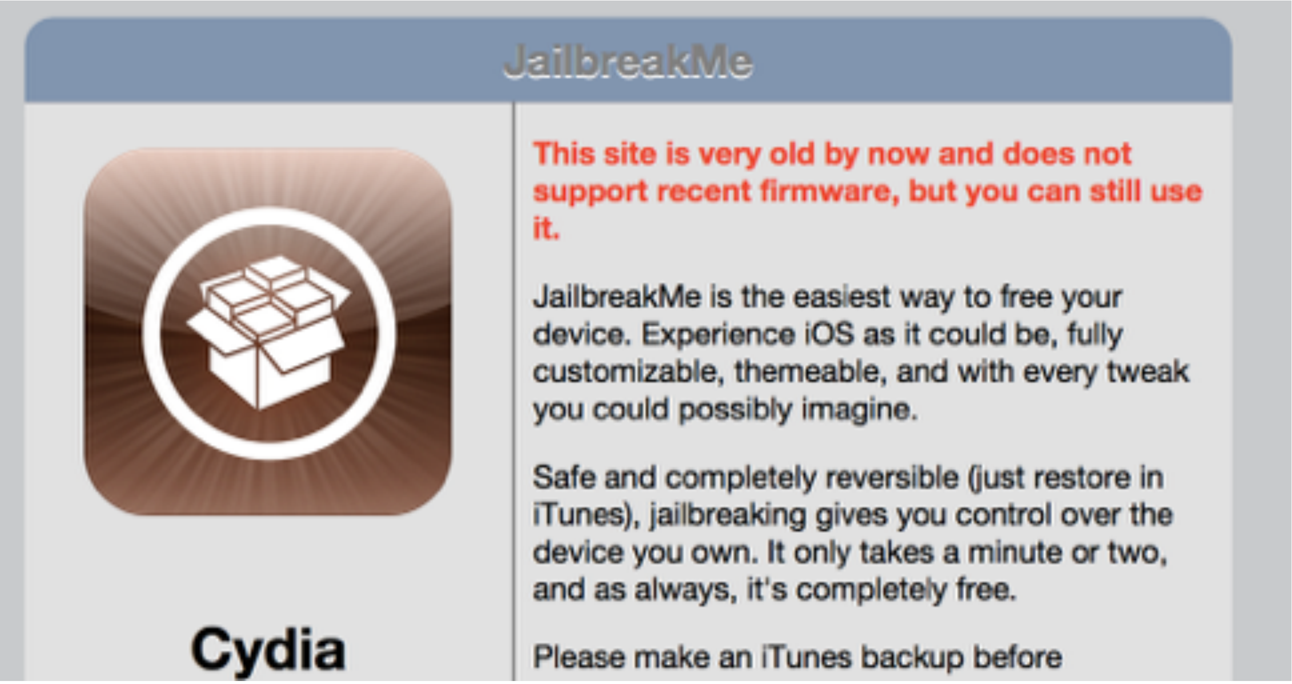
Remote Jailbreak

Much Easier

- Boot-based jailbreaks require moderate technical expertise and a lot of time
- Remote jailbreaks merely require loading a specially crafted PDF file into the iPhone's Mobile Safari web browser
- Often hosted at jailbreakme.com

Jailbreakme.com

- Only visible from an iDevice, or Google cache
- Only works for older iOS (v4 and below)



This site is very old by now and does not support recent firmware, but you can still use it.

JailbreakMe is the easiest way to free your device. Experience iOS as it could be, fully customizable, themeable, and with every tweak you could possibly imagine.

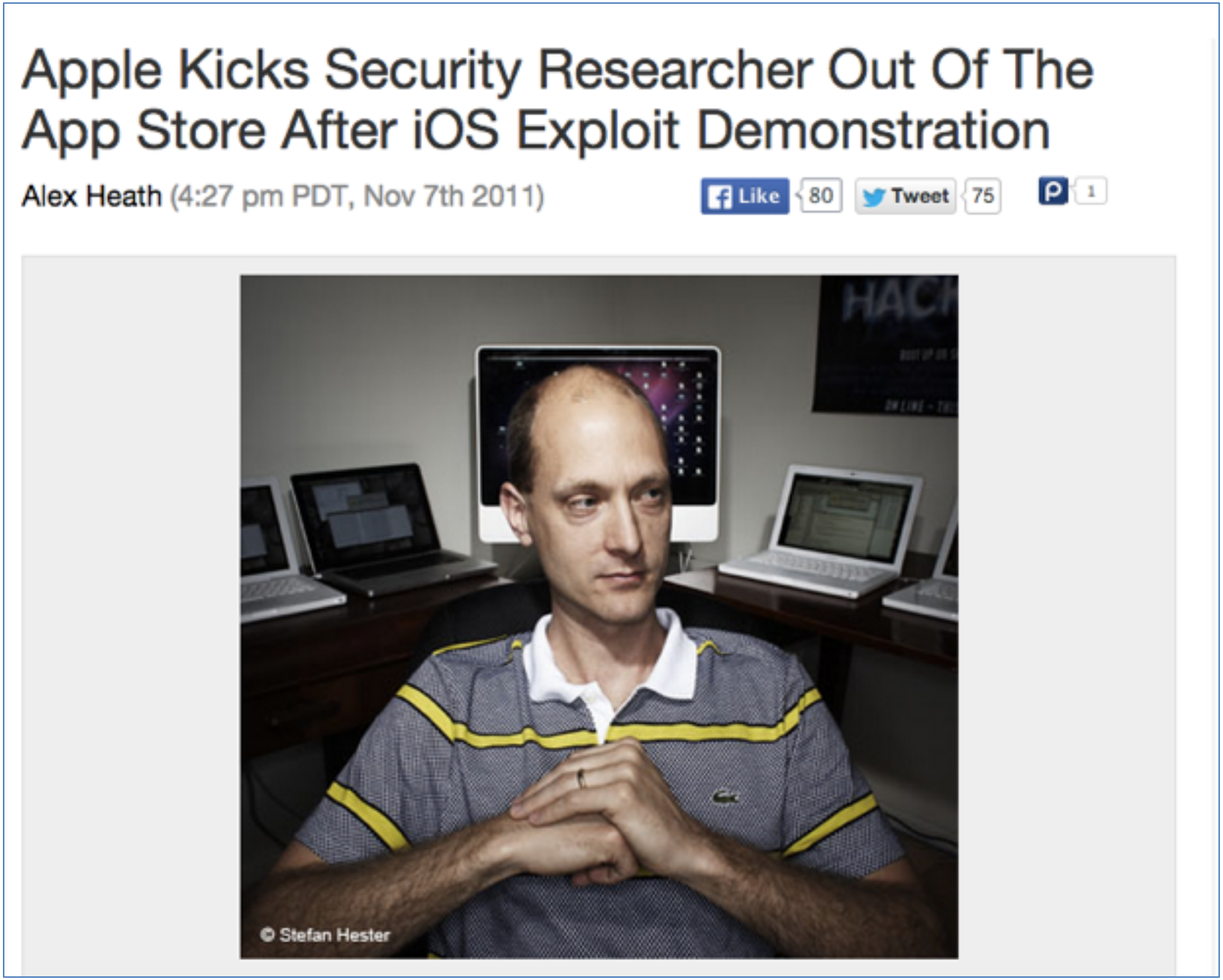
Safe and completely reversible (just restore in iTunes), jailbreaking gives you control over the device you own. It only takes a minute or two, and as always, it's completely free.

Please make an iTunes backup before

Hacking into Someone Else's iPhone

Limited Attack Surface

- Most network-based attacks are impossible
  - No browser plug-ins like Flash
  - No ability to download and execute a file, except from the App Store
- Sneaking a malicious app into the App Store is not impossible, but very impractical
  - And you can only do it once, and then be banned



Apple Kicks Security Researcher Out Of The App Store After iOS Exploit Demonstration

Alex Heath (4:27 pm PDT, Nov 7th 2011)

© Stefan Hester

Network-Based Attacks

- iOS has a minimal network profile
- All or most access to network services is disabled by default
- Some jailbroken devices have SSH running with the default password 'alpine'
  - A small but easily-exploited minority

Attack Vectors Available

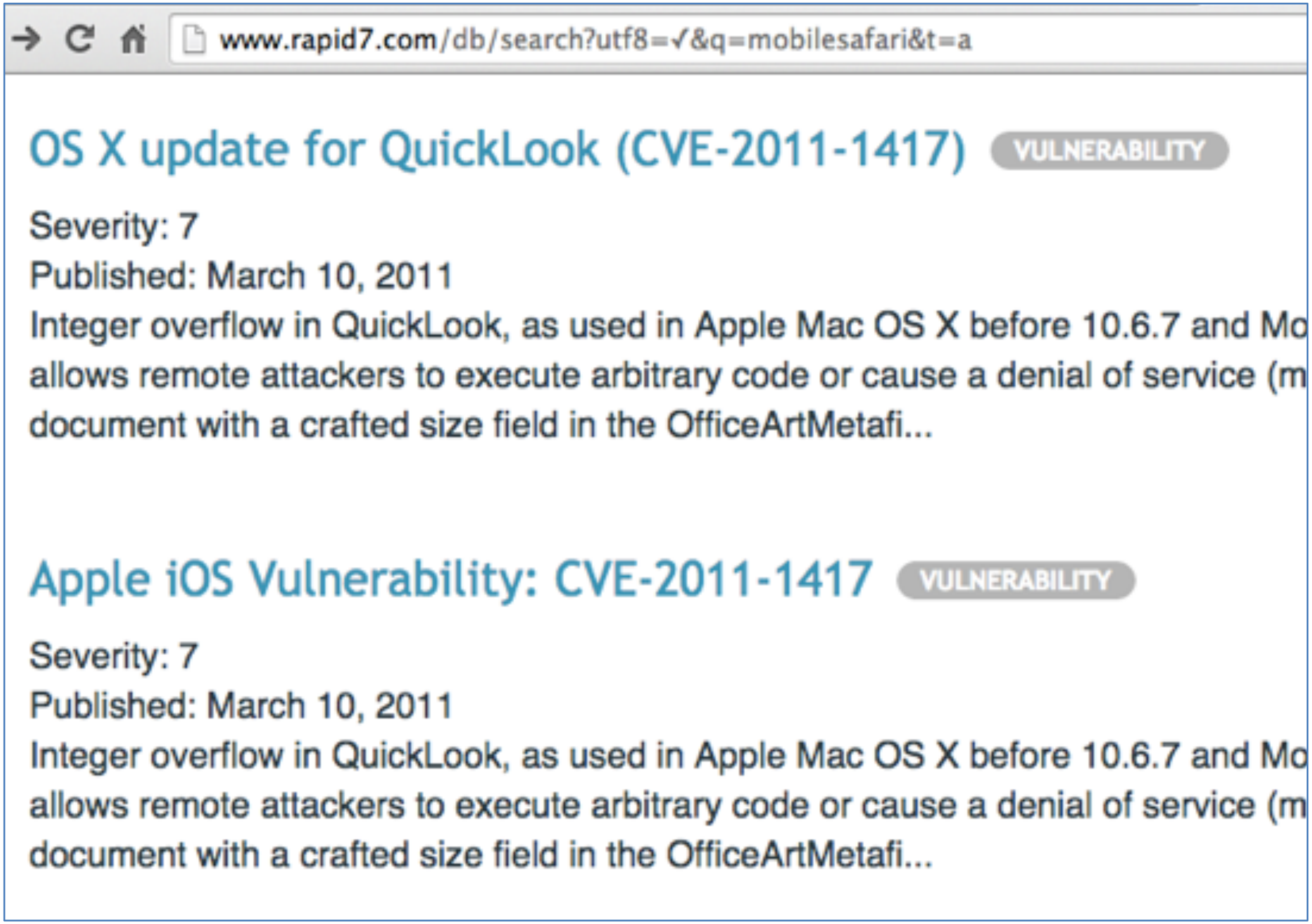
- Client-side vulnerabilities
- Local network access
  - Typically by luring the device to connect to a malicious Wireless Access Point (WAP)
- Physical access to a device
  - Can perform boot-based jailbreak
  - Requires a physical theft or seizure

Client-Side Attacks

- Exploits have been found, mainly in Mobile Safari
- Methods:
  - Host malicious files on Web servers
  - Deliver them via email

RCE Vulns in MobileSafari

- Link Ch 3q



www.rapid7.com/db/search?utf8=✓&q=mobilesafari&t=a

OS X update for QuickLook (CVE-2011-1417) VULNERABILITY

Severity: 7
Published: March 10, 2011
Integer overflow in QuickLook, as used in Apple Mac OS X before 10.6.7 and Mo
allows remote attackers to execute arbitrary code or cause a denial of service (m
document with a crafted size field in the OfficeArtMetafi...

Apple iOS Vulnerability: CVE-2011-1417 VULNERABILITY

Severity: 7
Published: March 10, 2011
Integer overflow in QuickLook, as used in Apple Mac OS X before 10.6.7 and Mo
allows remote attackers to execute arbitrary code or cause a denial of service (m
document with a crafted size field in the OfficeArtMetafi...

Sandbox

- Third-party apps also have vulnerabilities
  - But exploit will be trapped in the app's sandbox
  - Enabling attacker to steal that app's data, but no more
  - Unless there is a kernel-level vuln to break out of sandbox
- Kernel-level vulnerabilities are rare
  - Especially for modern iOS versions

Target Old Versions

- Most practical measure
  - Use exploits when they are new, before users update their devices
  - Target users with old versions of iOS
- iOS hacking tools are rare
  - Most effort goes into jailbreaking, which is usually done with the permission of the device's owner

END OF PART 1

Part 2

- The section titled "The JailbreakMe3.0 Vulnerabilities" to the end of chapter 3

Specific Attack Examples

The JailbreakMe3.0 Vulnerabilities

- Jailbreaking generally uses exploits locally
  - User downloads a file intentionally
- But they can be used remotely
  - Trick user into downloading a malicious file
  - Deliver it via website, chat, email, etc.
- JailbreakMe 3.0 exploited two vulns
  - A PDF bug
  - A kernel bug

Details

- CVE-2011-0226
  - FreeType Type 1 Font-handling bug
  - Remote code execution
  - Specially crafted Type font in a PDF file
- CVE-2011-0227
  - Invalid type conversion bug
  - Affecting IOMobileFrameBuffer
  - Leads to arbitrary code execution with system-level privileges (links Ch 3r, 3s)

Exploiting JailbreakMe 3.0

- View a malicious PDF in MobileSafari
- Exploit logic takes over the app
- Exploits the kernel to take full control of the device
- Patched in iOS 4.3.4 (July, 2011)

JailBreakMe 3.0 Vuln Countermeasures

- Updating iOS with latest patches is a security best practice
  - Jailbreaking requires you to stay behind, using a vulnerable version, and prevents you from putting on patches

Updates and Jailbreaking

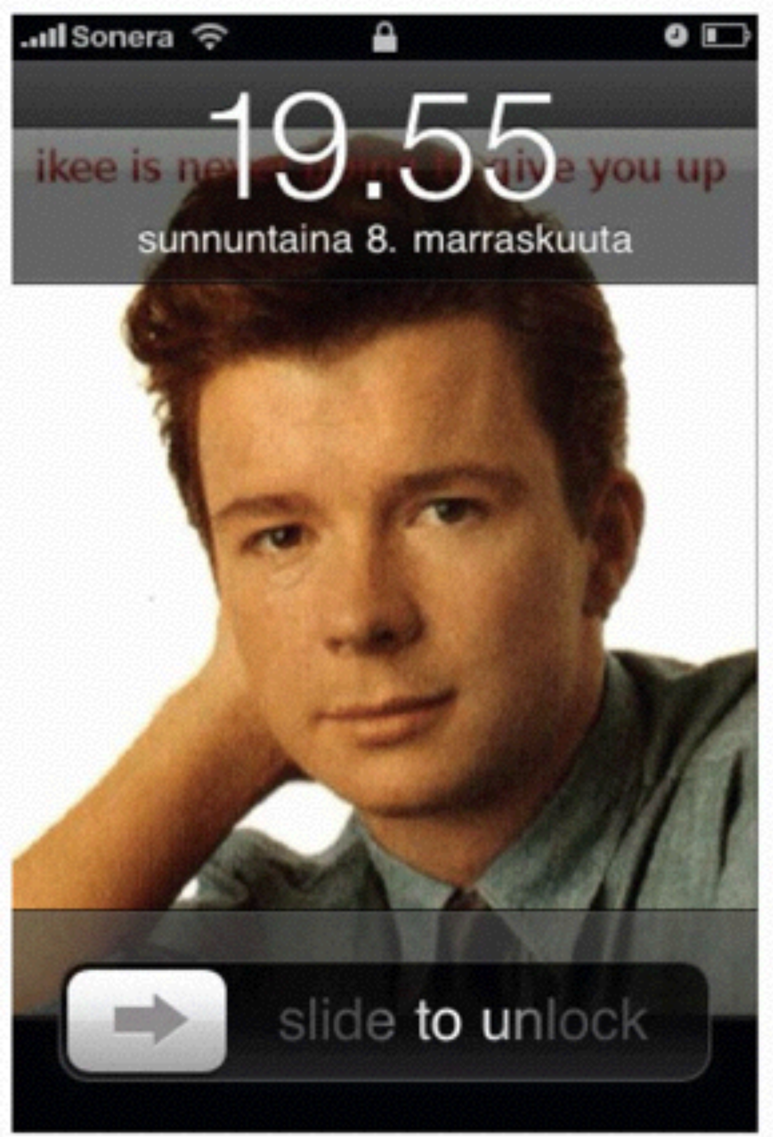
- Jailbreaking requires you to have an old, vulnerable iOS version
  - And you can't install patches from official sources
- You either have to continue using an old, unpatched OS, or
- Put patches on from unofficial sources, or
- Update, and then re-jailbreak your device

Over-the-air Updates

- iOS 5.0.1 and later introduces over-the-air patching for the OS and apps
- You can install them on jailbroken devices

iKee Worm

- Rickrolled people
- Changed wallpaper to Rick Astley
- Only affected iPhones that downloaded and ran SSH, and left the default password "alpine" unchanged



iKee

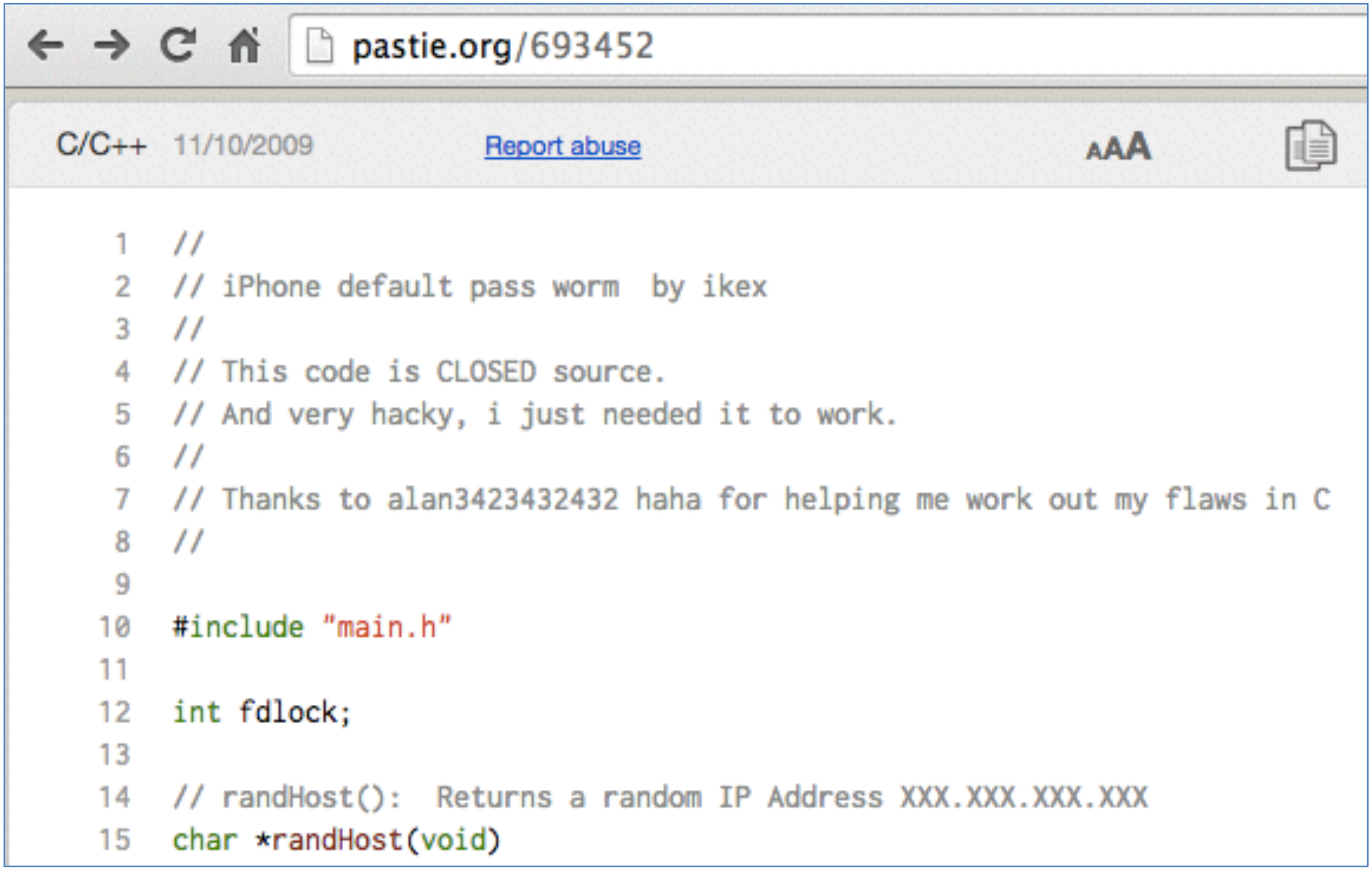
- iKee was the first spreading worm on iOS
- It scanned network blocks (in Netherlands and Australia) for open port 22
- Attempted to log in with "root" and "alpine"
- Once it got in:
  - Disabled SSH server
  - Change wallpaper
  - Make a local copy of the worm binary
  - Scan for and infect more devices

iKee Variants

- Introduced botnet-like functionality
  - Remote control of infected devices via a command-and-control channel
- A milestone
  - First and only publicly released , clear-cut, non-proof-of-concept example of malware successfully targeting iOS

iKee Source Code

- Link Ch 3t



```
//
// iPhone default pass worm  by ikex
//
// This code is CLOSED source.
// And very hacky, i just needed it to work.
//
// Thanks to alan3423432432 haha for helping me work out my flaws in C
//

#include "main.h"

int fdlock;

// randHost():  Returns a random IP Address XXX.XXX.XXX.XXX
char *randHost(void)
```

iKee Countermeasures

- Don't jailbreak your device
- If you do, and install SSH, change the default password
- Enable network services like SSH only when they are needed
  - Use SBSettings app
- Upgrade to the latest jailbreakable version of iOS when possible
- Install patches as soon as practicable

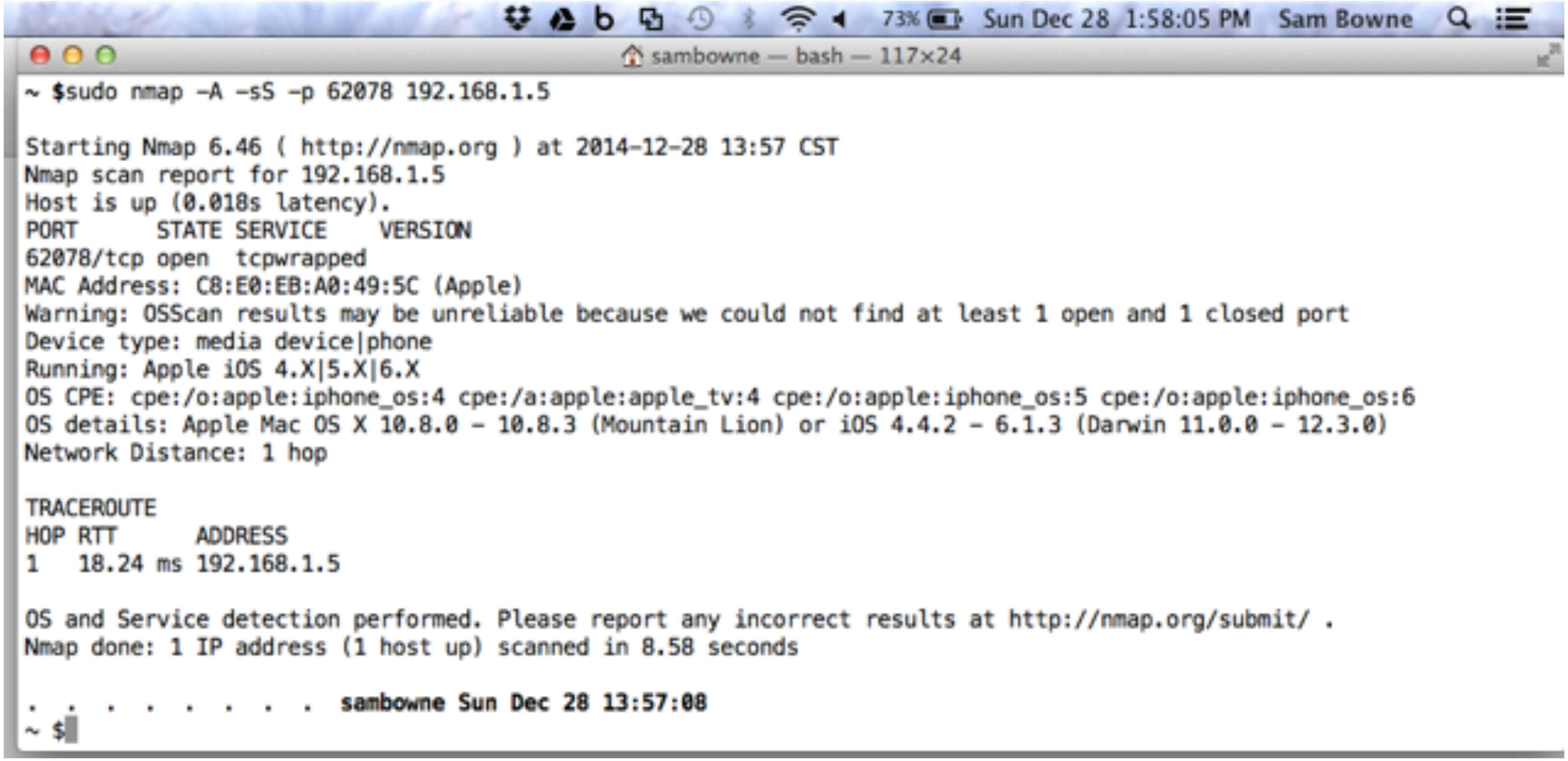
Attack Options for iOS

- Remote network attacks exploiting vulnerable network services
- Client-side attacks, including exploitation of app vulns
- Local network attacks, such as MITM
- Physical attacks that require access to the device

iOS Defenses

- A fresh, new, iPhone has only one TCP port open
  - Port 62078
    - Port # incorrect in text (62087)
  - No known attacks for this service
  - Links Ch 3u, 3v

Port Scanning 62078



```
~ $sudo nmap -A -sS -p 62078 192.168.1.5

Starting Nmap 6.46 ( http://nmap.org ) at 2014-12-28 13:57 CST
Nmap scan report for 192.168.1.5
Host is up (0.018s latency).
PORT      STATE SERVICE    VERSION
62078/tcp open  tcpwrapped
MAC Address: C8:E0:EB:A0:49:5C (Apple)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: media device|phone
Running: Apple iOS 4.X|5.X|6.X
OS CPE: cpe:/o:apple:iphone_os:4 cpe:/a:apple:apple_tv:4 cpe:/o:apple:iphone_os:5 cpe:/o:apple:iphone_os:6
OS details: Apple Mac OS X 10.8.0 - 10.8.3 (Mountain Lion) or iOS 4.4.2 - 6.1.3 (Darwin 11.0.0 - 12.3.0)
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   18.24 ms 192.168.1.5

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.58 seconds

. . . . . . . . .  sambowne Sun Dec 28 13:57:08
~ $
```

- iPhone3 (Model A1429) with iOS 7.0.2

Remote Vulnerabilities

- Reset device with ICMP request (ping of death)
  - CVE-2009-1683
  - Affected iOS 1.0 through 2.2.1
  - Link Ch 3w
- Remote Code Execution via SMS
  - CVE-2009-2204
  - Affected iOS before 3.0.1
  - Links Ch 3x, 3y

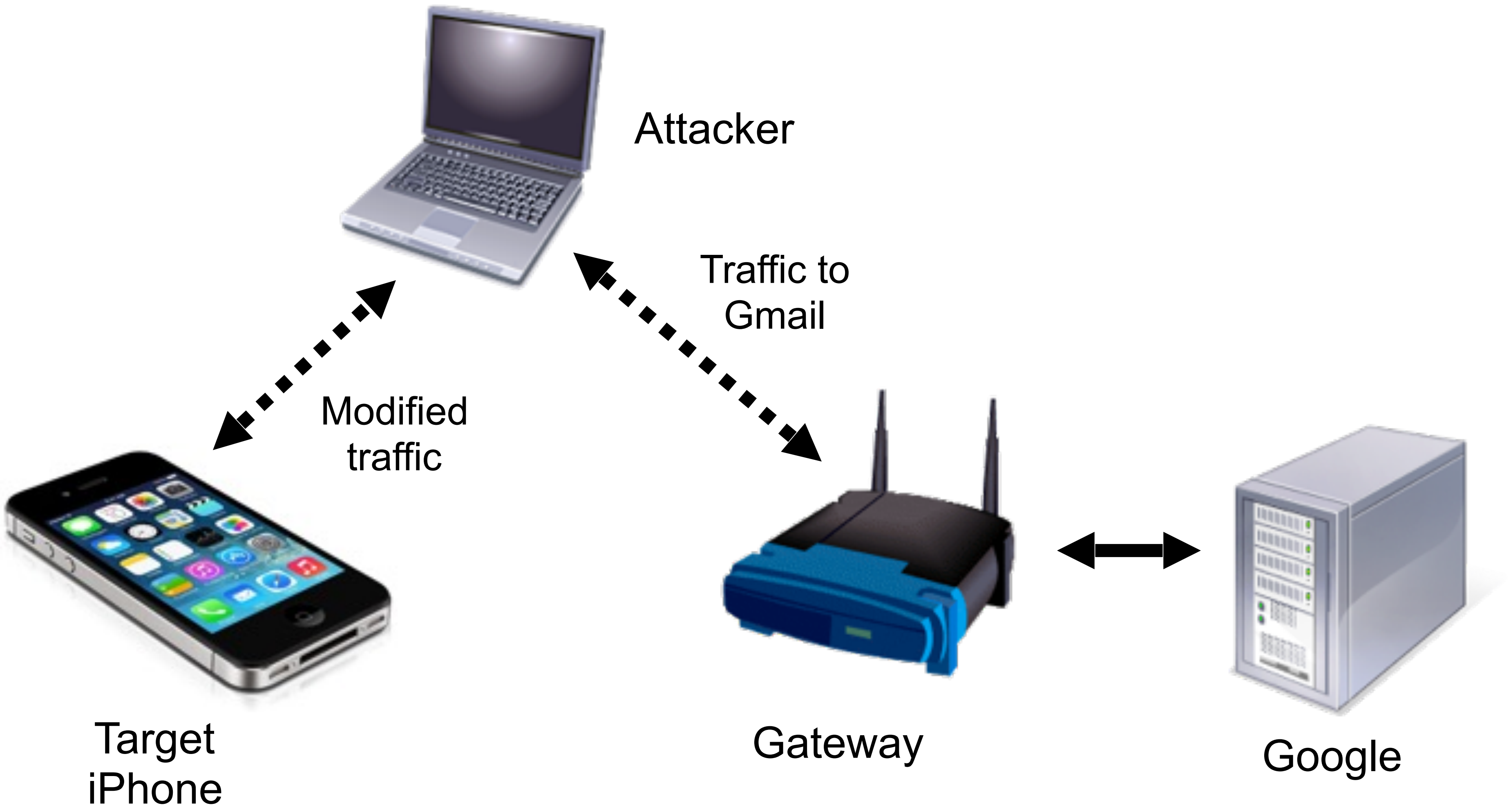
Other Potentially Vulnerable Services

- Bonjour (UDP 5353)
- Other radio interfaces
  - Baseband
    - Cellular modem firmware (Link Ch 3z)
  - Wi-Fi driver
  - Bluetooth
  - etc.

Focus 11 MITM Attack

- Attack laptop acts a rogue Wi-Fi access point
- Target is tricked into connecting to it
- Attacker is now in the middle
- Attacker can intercept HTTPS traffic by exploiting the CVE-2011-0228 X.509 certificate chain validation vulnerability

Focus11 MITM Attack



Silent Exploitation

- Attacker injected a JailbreakMe 3.0 PDF file into the Gmail page, modified to make no visible changes
  - No Cydia icon added
- The PDF then loaded SSH and VNC servers on the device
- The iPhone ends up owned, converted to a bot

Focus 2011 MITM Countermeasures

- Update device
  - That stops the JailbreakMe 3.0 attack
  - And the HTTPS MITM attack
- Don't join new, unknown Wi-Fi networks
  - Very impractical
- Don't store sensitive data on your device
  - Also very impractical

App Store Security

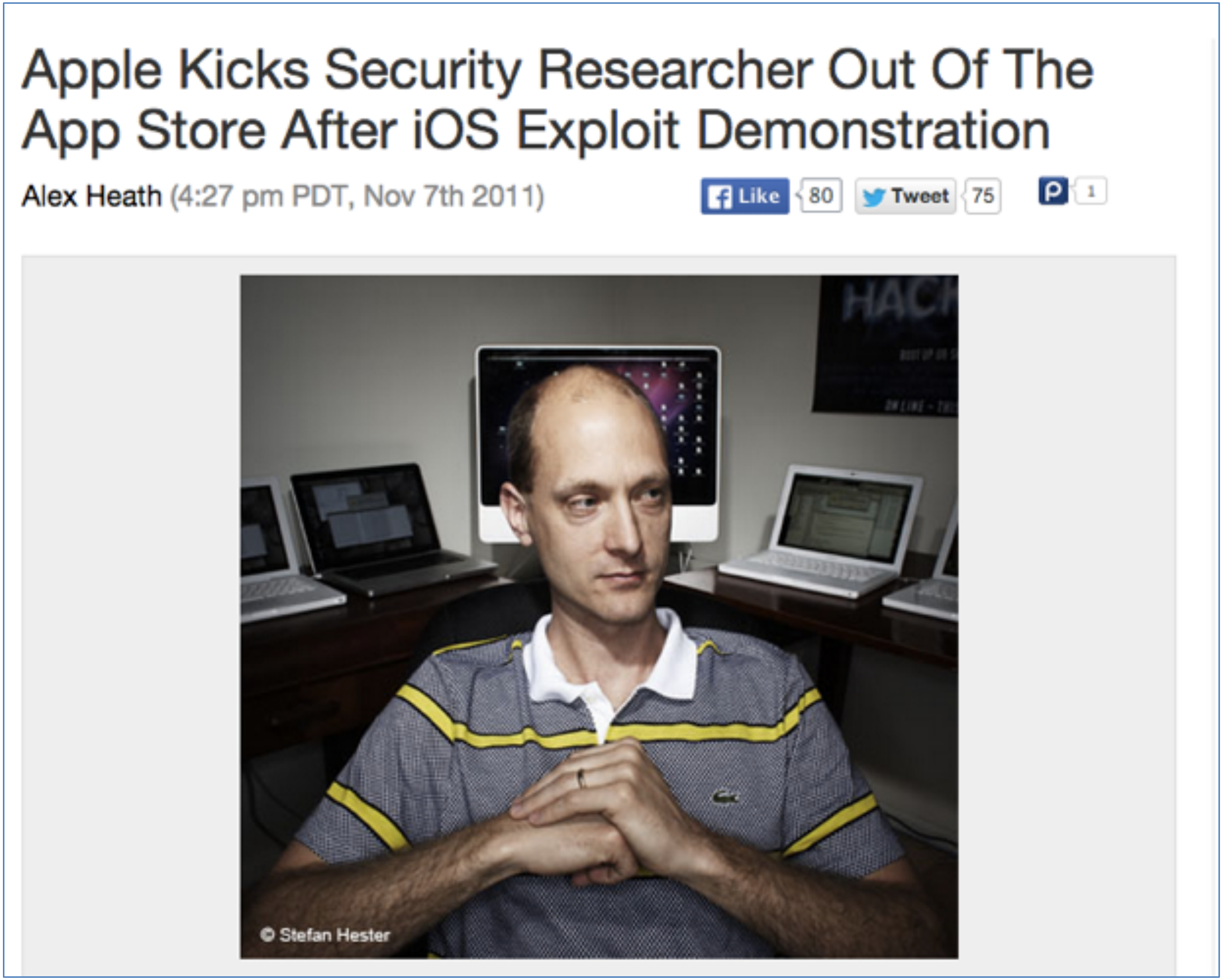
- To attack unjailbroken iDevices,
- A malicious app must deceive the end-user, and also deceive Apple (to get into the App Store)
- All apps must be signed by Apple
- Apps can only be installed from the App Store
- Review process is not detailed publicly
  - But it has been defeated a few times

Handy Light

- Approved and placed in the store in 2010
- Contained a hidden tethering feature
  - Use an iPhone as a wireless access point, for free
- Violated an Apple policy against tethering apps
- How did Apple miss that during the review process?

InstaStock

- Approved in 2011
- Charlie Miller wrote it
- Exploited a zero-day vulnerability to place iPhones under remote control
  - Which allowed execution of unsigned apps



Apple Kicks Security Researcher Out Of The App Store After iOS Exploit Demonstration

Alex Heath (4:27 pm PDT, Nov 7th 2011)

© Stefan Hester

App Store Malware Countermeasures: Trust Apple

- Risk is low, because of Apple policing the App Store
- If there were antivirus or firewall products in the App Store, they might reduce this risk
  - But Apple won't approve them

Vulnerable Apps: Bundled and Third-Party

- Bundled Apps
  - Included with iOS
  - Many vulns found, especially in Mobile Safari
- Third-Party Apps
  - Not included, added later from the App Store
  - Very few important vulns found
  - But very few apps are universally installed
    - Like Flash on PC's

Third-Party App Vulns

- CVE-2010-2913
  - Citi Mobile App v. 2.0.2 and below
  - Stored sensitive banking information on the device
  - A lost or stolen device could expose it
- CVE-2010-4211
  - Paypal App X.509 certificate validation issue
  - Failure to validate server hostname values
  - Allows SSL MITM attacks

Third-Party App Vulns

- Sept. 2011
  - XSS vuln in Skype app v. 3.0.1 and below
  - Script embedded in the "Full Name" field of messages could access the file system of Skype app users
  - Enabled an attacker to steal the contacts database

Third-Party App Vulns

- April 2012
  - Multiple apps store authentication credentials insecurely
  - Including Facebook and Dropbox apps
  - Attacker could copy the credentials off the phone with an app such as iExplorer
  - And re-use the credentials to log in to others' accounts

Third-Party App Vulns

- Jan. 2013
  - ESPN ScoreCenter app v. 3.0.0 had two issues
  - XSS vuln and cleartext authentication vuln
  - It did not sanitize user input, and transmitted it unencrypted over the network

Difficulty Exploiting Third-Party App Vulns

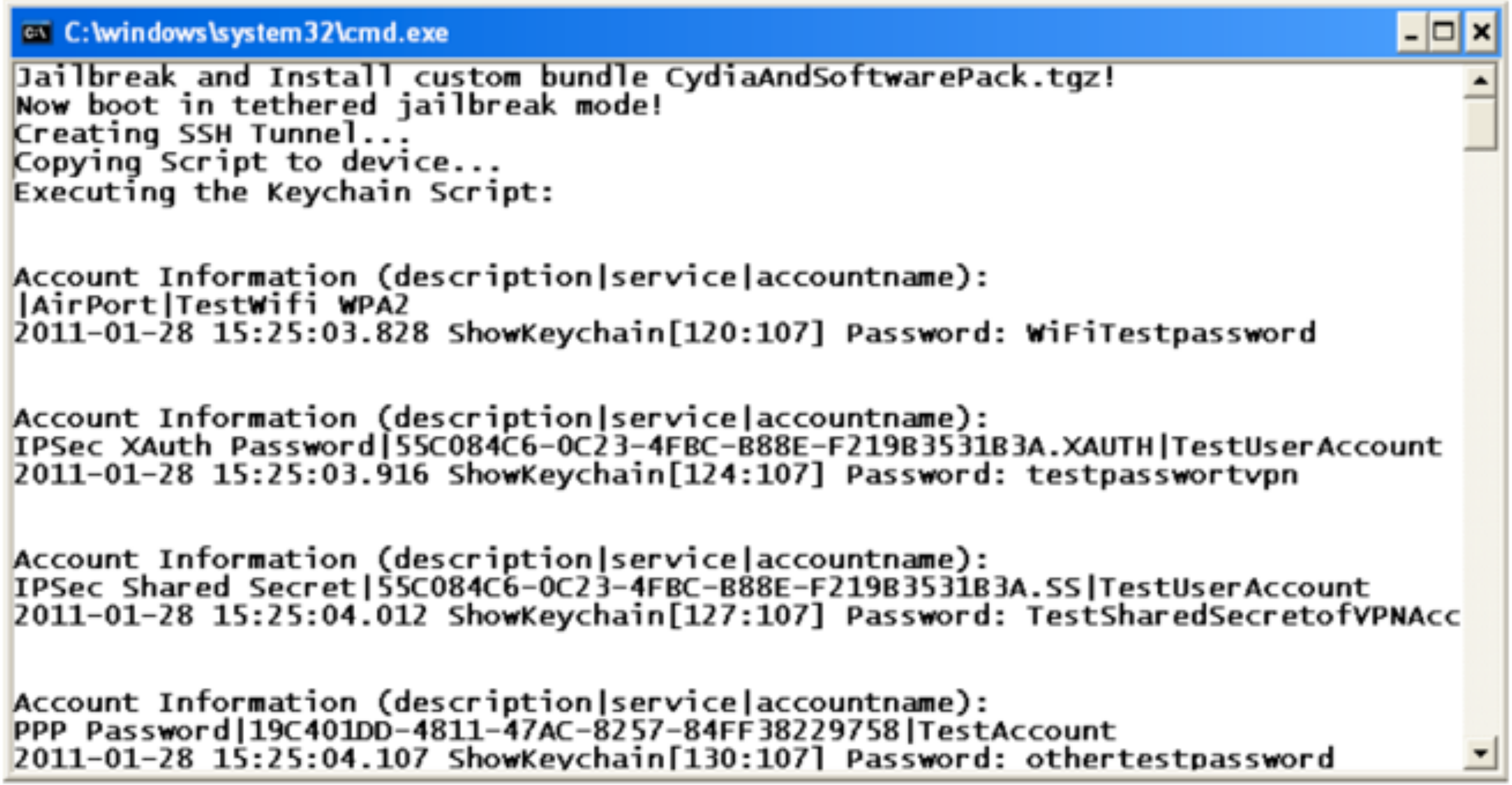
- Gaining control over an app is only half the battle
- Obtaining information from the target device, and persisting across app executions, are difficult, because of
  - App sandboxing
  - Code signature verification
- True owning requires app-level vulns and kernel vulns

App Vulnerability Countermeasures

- Update iOS and apps

Physical Access

- Lots of important personal and business data is on iDevices these days
- Devices are lost and stolen often
- The encryption key did not depend on the passcode up through iOS 6.0.1
  - Enabling retrieval of stored passwords in just six minutes, by using a special boot script
  - Link Ch 3z2



```
Jailbreak and Install custom bundle CydiaAndSoftwarePack.tgz!
Now boot in tethered jailbreak mode!
Creating SSH Tunnel...
Copying Script to device...
Executing the Keychain Script:


Account Information (description|service|accountname):
|AirPort|TestWifi WPA2
2011-01-28 15:25:03.828 ShowKeychain[120:107] Password: WiFiTestpassword


Account Information (description|service|accountname):
IPSec XAuth Password|55C084C6-0C23-4FBC-B88E-F219B3531B3A.XAUTH|TestUserAccount
2011-01-28 15:25:03.916 ShowKeychain[124:107] Password: testpasswortvpn


Account Information (description|service|accountname):
IPSec Shared Secret|55C084C6-0C23-4FBC-B88E-F219B3531B3A.SS|TestUserAccount
2011-01-28 15:25:04.012 ShowKeychain[127:107] Password: TestSharedSecretofVPNAcc


Account Information (description|service|accountname):
PPP Password|19C401DD-4811-47AC-8257-84FF38229758|TestAccount
2011-01-28 15:25:04.107 ShowKeychain[130:107] Password: othertestpassword
```

iExplorer

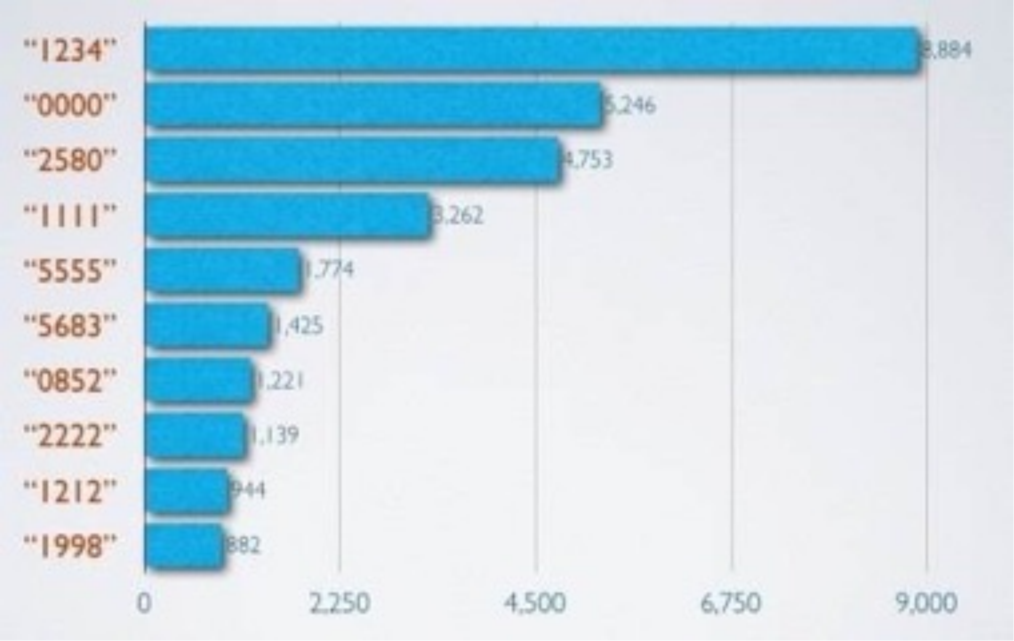
- Installs on your computer
- Connect iDevice with USB cable
- Browse file system on iDevice and copy any files you like
    - But some are encrypted

Bypass Screen Lock

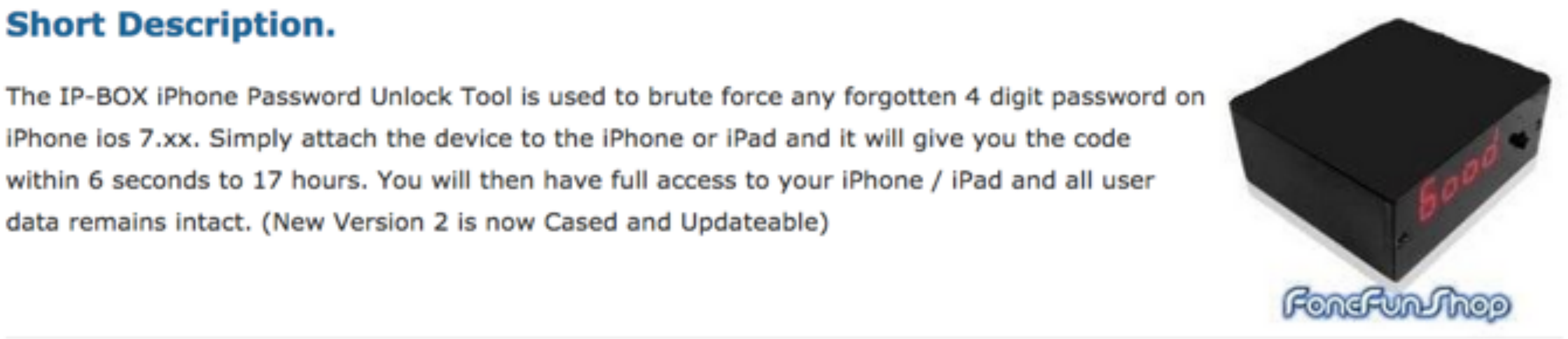
- iOS versions through 8.0.2 allow a user to exploit them without knowing the passcode, by exploiting
  - Emergency call feature
  - Siri
  - Links Ch 3z3 – 3z5

Brute-Forcing Passcodes

- Four-digit passcodes are intrinsically weak, and can be brute-forced
  - – Link Ch 3z6
- People often choose weak ones
  - – Link Ch 3z7



IP-BOX iPhone Password Unlock Tool



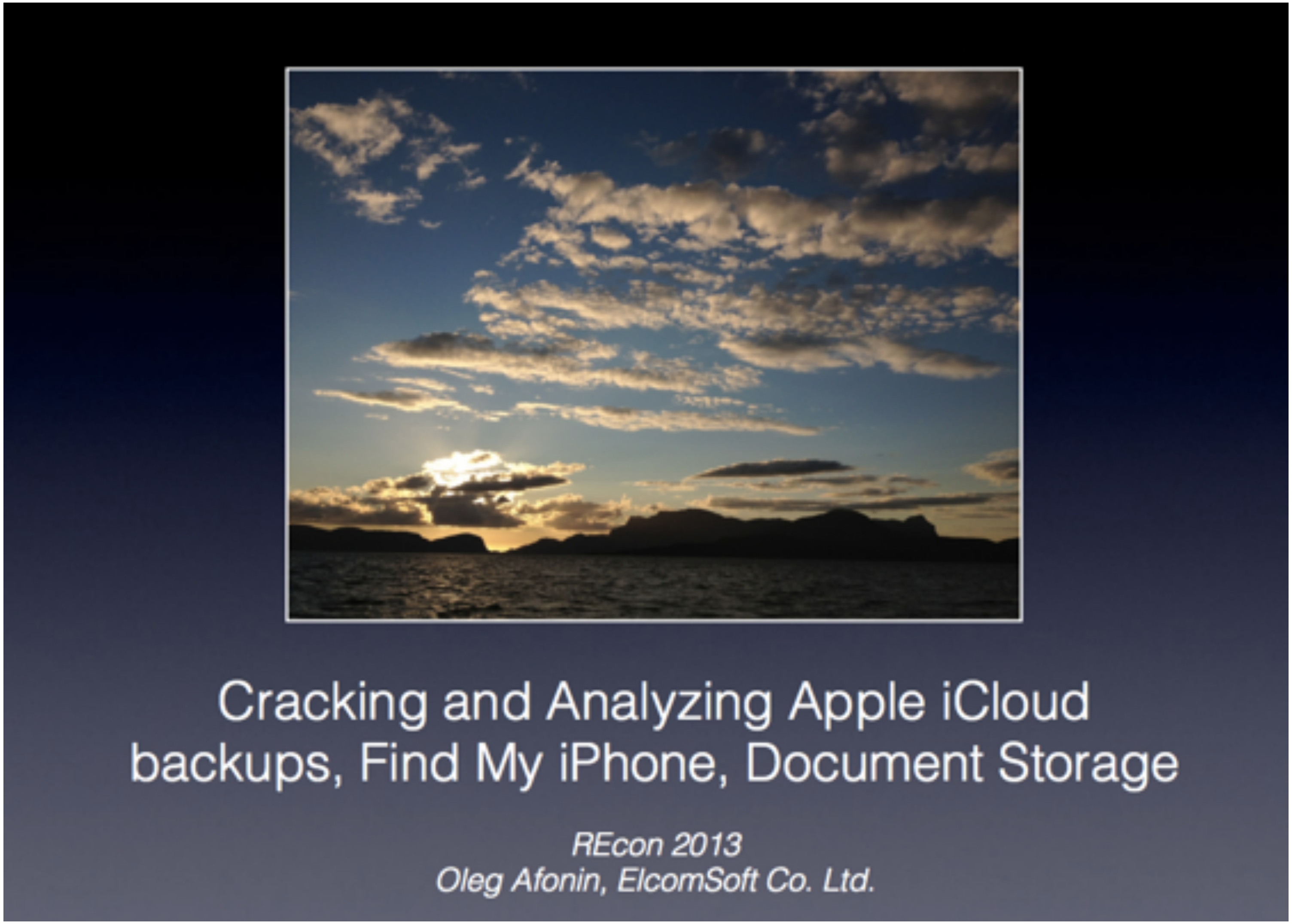
Short Description.

The IP-BOX iPhone Password Unlock Tool is used to brute force any forgotten 4 digit password on iPhone ios 7.xx. Simply attach the device to the iPhone or iPad and it will give you the code within 6 seconds to 17 hours. You will then have full access to your iPhone / iPad and all user data remains intact. (New Version 2 is now Cased and Updateable)

- Link Ch 3z8

Hacking iCloud

Not in textbook



Cracking and Analyzing Apple iCloud backups, Find My iPhone, Document Storage

REcon 2013
Oleg Afonin, ElcomSoft Co. Ltd.

- Link Ch 3z9

iCloud

- Introduced in Oct 2011
- Introduced with iOS 5
- 5 GB free storage
- Up to 50 GB paid storage
- Over 300 million users in June 2013
- Backups, documents, notes, calendar, Find My Phone

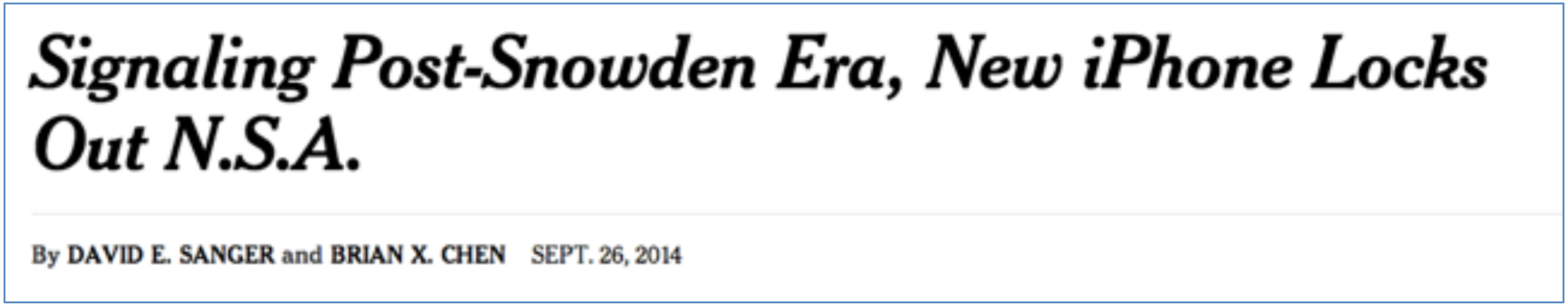
iCloud backups: why?

iCloud backup - when

- Backup runs daily when the device is:
    - Connected to the Internet over Wi-Fi
    - Connected to a power source
    - Locked
- Can force backup
    - [Settings] | [iCloud] | [Storage & Backup] | [Back Up Now]

iCloud backups - summary

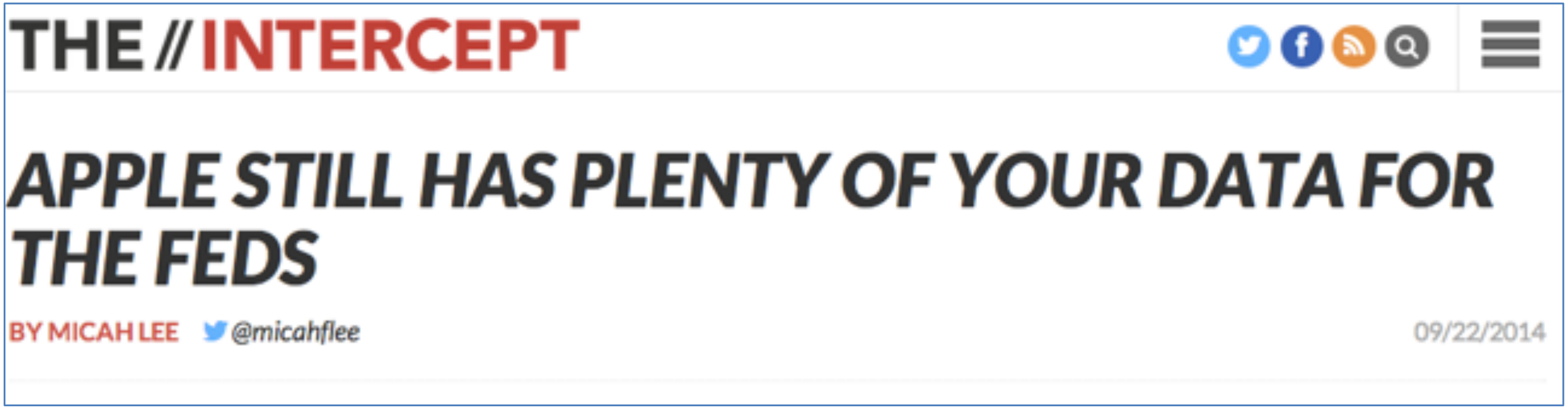
- There is no user-configurable encryption for iCloud backups
- iCloud backups are stored in Microsoft and Amazon clouds in encrypted form
- Apple holds encryption keys and thus have access to data in iCloud backups
- If Apple stores 0x835 keys then it can also have access to Keychain data (i.e. passwords)
- Apple may have legal obligations to do this (e.g. legal enforcement)



Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.

By DAVID E. SANGER and BRIAN X. CHEN SEPT. 26, 2014

- iPhone 6 data is encrypted with a key based on the user's PIN
- So Apple can't decrypt it, even in response to a court order
  - – Link Ch 3z10



THE // INTERCEPT

APPLE STILL HAS PLENTY OF YOUR DATA FOR THE FEDS

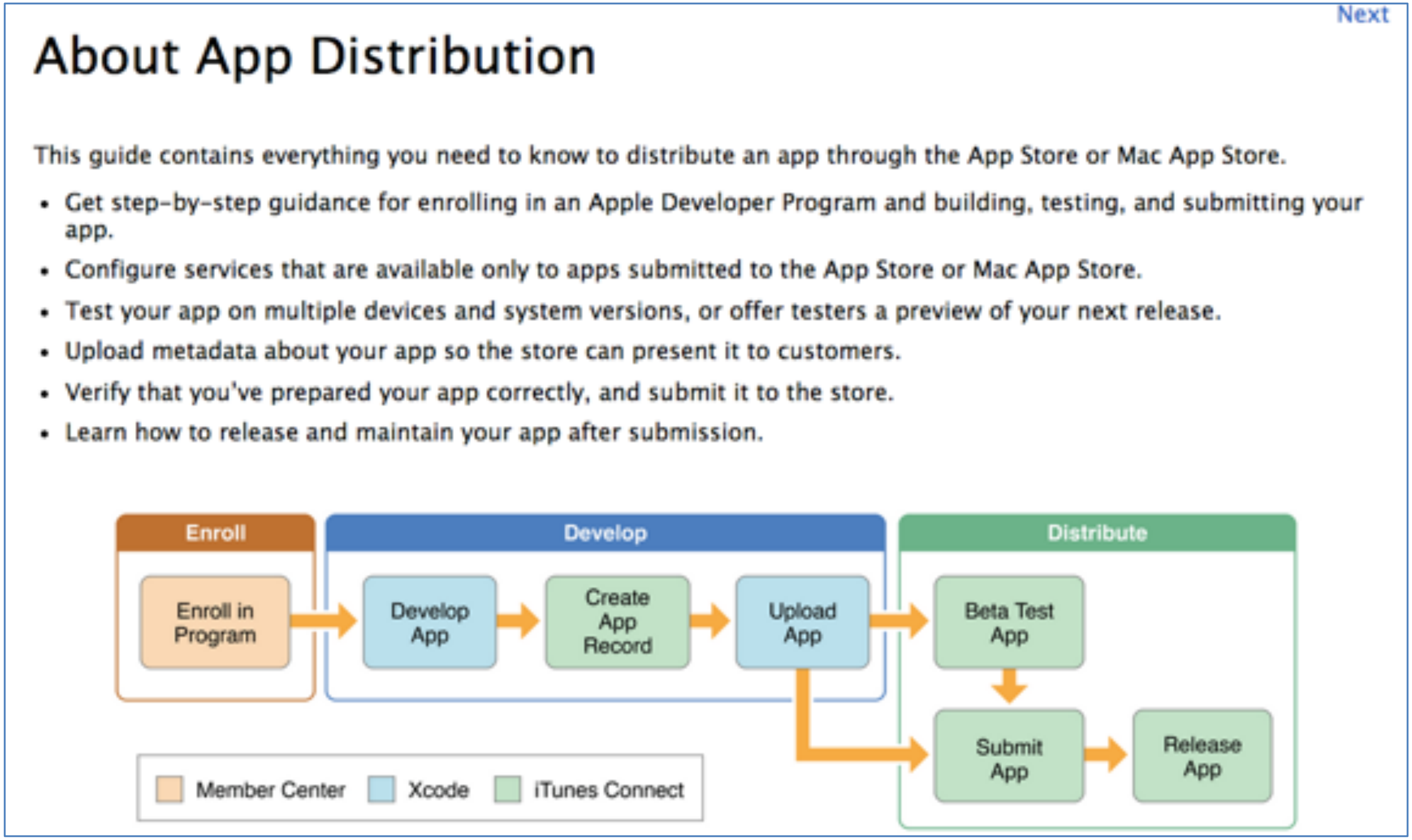
BY MICAH LEE @micahflee 09/22/2014

- BUT Apple still has the keys to iCloud
  - Link Ch 3z11

Apple Pay

- Introduced with iPhone 6 in 2014
- Uses NFC (Near Field Communication)
- Better than Google Wallet (link Ch 3z13)

Making iPhone Apps



Next

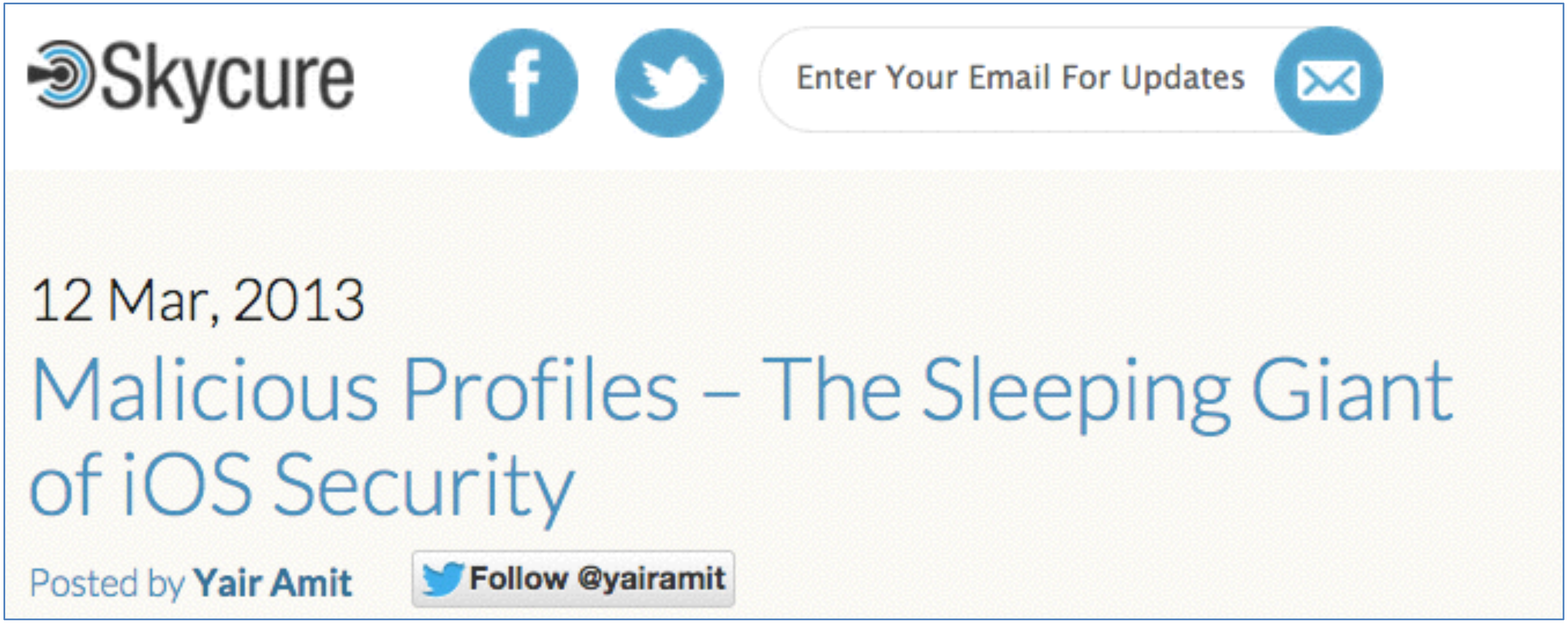
About App Distribution

This guide contains everything you need to know to distribute an app through the App Store or Mac App Store.

- Get step-by-step guidance for enrolling in an Apple Developer Program and building, testing, and submitting your app.
- Configure services that are available only to apps submitted to the App Store or Mac App Store.
- Test your app on multiple devices and system versions, or offer testers a preview of your next release.
- Upload metadata about your app so the store can present it to customers.
- Verify that you've prepared your app correctly, and submit it to the store.
- Learn how to release and maintain your app after submission.

- Links Ch 3z14, 15, 16

Malicious Configuration Files



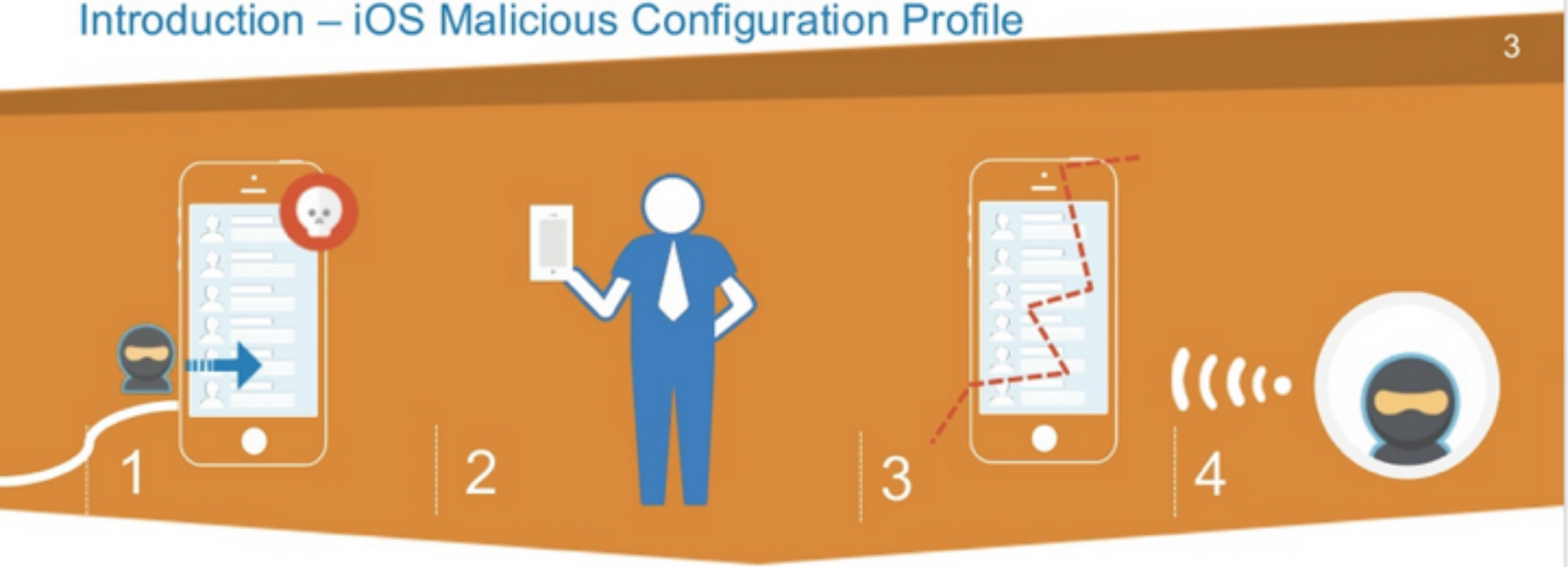
12 Mar, 2013

Malicious Profiles – The Sleeping Giant of iOS Security

Posted by Yair Amit

- Links Ch 3z17, 3z18, 3z19

Introduction – iOS Malicious Configuration Profile



iOS Configuration Profiles can be loaded on any iOS device with relative ease. Each configuration profile can include settings for managing the devices proxy, VPN, and certificates 1

Through social engineering like email phishing or web link an attacker can convince the user to install a malicious profile and compromise the device settings 2

The attack can silently route network traffic from a device using the profile to a remote proxy over SSL using a self-signed certificate authority that appears valid to the end user 3

Once the attacker re-routed all traffic from the mobile device to an attacker-controlled server, he can further install rogue apps, and decrypt SSL communications 4

How iOS Attacks 'Get in"

Three Main Infection Vectors for iOS Attacks

Physical Access | 1

Social Engineering | 2

Rogue WiFi HotSpots | 3

- Malicious Profiles
- Fake Certificates
- Zero-Day Vulnerabilities

✉ Get in touch

LACOON MOBILE SECURITY

Malicious Profiles example
LinkedIn Intro

5
LinkedIn
NOTIFICATIONS
PENDING MESSAGES
1
2
in

Example:

LinkedIn Intro

User downloads app or accepts new functionality from one of their apps that requires an update to their device's Profile.

Example: LinkedIn Intro's new Profile reroutes all email to the LinkedIn Servers.

1

LinkedIn is now intercepting all emails and modifying their content (adding user info).

This is known as a man-in-the-middle (MitM) attack!

More Info

2

LACOON MOBILE SECURITY

✉ Get in touch

Lacoon MobileFortress - iOS Threat Coverage

Certificate Validation

Ability to check validity of certificates and accurately identify the source of the application

Advanced Jailbreak Detection

Ability to identify when a device has been jailbroken using continuous background service

Configuration Profile Analysis

Ability to identify changes to configuration profiles and understand when those changes make the device vulnerable (e.g. compromise secure containers)

Malicious App Detection

Ability to understand communications from the app, regardless of how it was installed on the device, to see what it's doing (e.g. recognize traffic to and from unknown servers)

Man-in-the-Middle Attack Mitigation

Ability to trigger a VPN to isolate user when on a WiFi or other unsecured network

LACOON MOBILE SECURITY

✉ Get in touch