iPhone Security

Large threats come in small packages.

Kaan Kivilcim

24 March 2011

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 8, 350 Collins Street
Melbourne VIC 3000
Australia

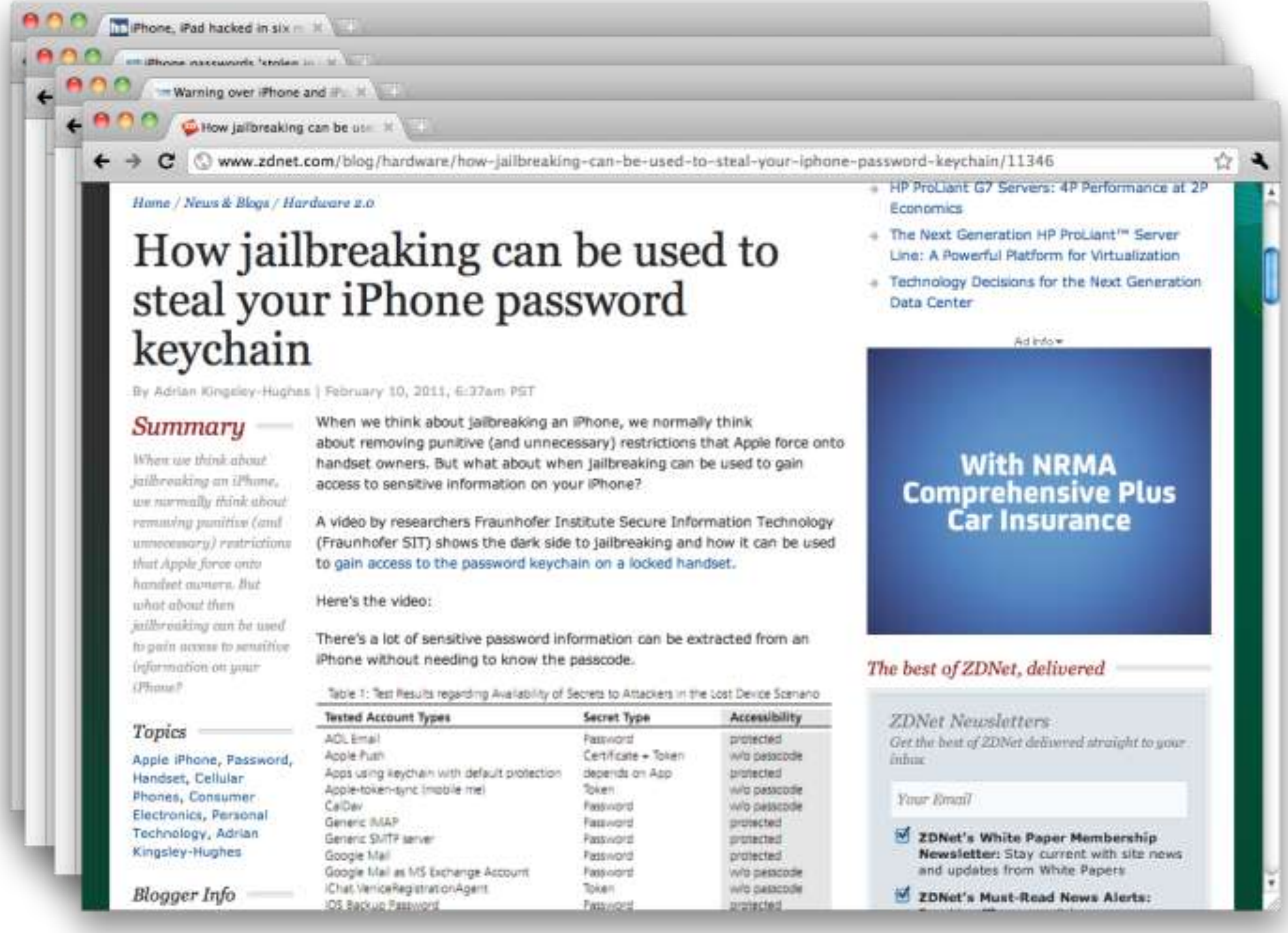
T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Introduction

- Apple iPhone has reached ‘critical mass’
- Cultural changes in the workplace
- BYOD (Bring Your Own Device)
- Introduction of iPad 2
- Resistance is futile

Recent Media Coverage


iPhone, iPad hacked in six m
iPhone passwords 'stolen in
Warning over iPhone and iP
How jailbreaking can be use
www.zdnet.com/blog/hardware/how-jailbreaking-can-be-used-to-steal-your-iphone-password-keychain/11346

Home / News & Blogs / Hardware 2.0

How jailbreaking can be used to steal your iPhone password keychain

By Adrian Kingsley-Hughes | February 10, 2011, 6:37am PST

Summary

When we think about jailbreaking an iPhone, we normally think about removing punitive (and unnecessary) restrictions that Apple force onto handset owners. But what about when jailbreaking can be used to gain access to sensitive information on your iPhone?

Topics

Apple iPhone, Password, Handset, Cellular Phones, Consumer Electronics, Personal Technology, Adrian Kingsley-Hughes

Blogger Info

When we think about jailbreaking an iPhone, we normally think about removing punitive (and unnecessary) restrictions that Apple force onto handset owners. But what about when jailbreaking can be used to gain access to sensitive information on your iPhone?

A video by researchers Fraunhofer Institute Secure Information Technology (Fraunhofer SIT) shows the dark side to jailbreaking and how it can be used to gain access to the password keychain on a locked handset.

Here's the video:

There's a lot of sensitive password information can be extracted from an iPhone without needing to know the passcode.

Table 1: Test Results regarding Availability of Secrets to Attackers in the Lost Device Scenario

Tested Account Types	Secret Type	Accessibility
AOL Email	Password	protected
Apple Push	Certificate + Token	w/o passcode
Apps using keychain with default protection	depends on App	protected
Apple-token-sync (mobile me)	Token	w/o passcode
CalDav	Password	w/o passcode
Generic IMAP	Password	protected
Generic SMTP server	Password	protected
Google Mail	Password	protected
Google Mail as MS Exchange Account	Password	w/o passcode
iChat VeniceRegistrationAgent	Token	w/o passcode
iOS Backup Password	Password	protected

The best of ZDNet, delivered

ZDNet Newsletters

Get the best of ZDNet delivered straight to your inbox

Your Email

☑ **ZDNet's White Paper Membership Newsletter:** Stay current with site news and updates from White Papers

☑ **ZDNet's Must-Read News Alerts:**

Agenda

1. iPhone Fundamentals
2. Security Mechanisms & Protection Measures
3. Security Weaknesses & Threats
4. Risk Management & Conclusions

Agenda

1. <u>iPhone Fundamentals</u>
2. Security Mechanisms & Protection Measures
3. Security Weaknesses & Threats
4. Risk Management & Conclusions

Introduction to iOS

- Previously called iPhone OS
  - Used on iPhone, iPod Touch, iPad, Apple TV
- Derived from Mac OS X
  - Based on Darwin UNIX operating system
- Shares common technologies with Mac OS X
- Well documented and easily accessible
- Behind the UI there's a UNIX command line

Keychain

- Apple’s password management system
- Holds passwords, private keys, certificates, wireless network keys, secure notes, etc.
- Introduced in Mac OS 8.6 in 1997
- Key component of Mac OS X and iOS
- Encrypted with 3DES
- By default, unlocked with login password

Agenda

1. iPhone Fundamentals
2. <u>Security Mechanisms & Protection Measures</u>
3. Security Weaknesses & Threats
4. Risk Management & Conclusions

Overview of iPhone Security

- Designed with an emphasis on security
- Hardware-based data encryption
- Application sandboxing and code signing
- Device policies and restrictions
- Remote wipe
- Encrypted backups
- Data protection when the device is locked

iOS Data Protection

- Goal of data protection is to keep data safe even if the device itself is compromised
- Encryption is tied to the device passcode
- Both file system and keychain are protected
- Protected data is only available when the device is unlocked
- Apple’s goal is for adoption by all applications
- Requires secure application development

Data Protection Classes

Availability	File System	Keychain
When unlocked	ProtectionComplete	WhenUnlocked
After first unlock		AfterFirstUnlock
Always	ProtectionNone	Always

Email Client Example:

Component	Location	Data Protection
Credentials	Keychain	AfterFirstUnlock
Email Contents	File System	ProtectionComplete
Email Headers	File System	ProtectionNone

Agenda

1. iPhone Fundamentals
2. Security Mechanisms & Protection Measures
3. Security Weaknesses & Threats
4. Risk Management & Conclusions

Jailbreaking the iPhone

- What is jailbreaking?
- Why do people jailbreak?
- How is it done?

- What’s the problem with that?

Threats from Jailbroken Devices

1. The device becomes a powerful UNIX-based attack platform connected to the corporate network and the Internet via GSM network
2. The operating system, applications and data are no longer protected by the multiple layers of security that Apple has implemented within iOS – only data protection remains!

Threats from Jailbroken Devices

- Consider an authorised yet jailbroken device that is connected to your corporate network environment
- You can use the iPhone connected to the corporate wireless network to bridge the internal network to the Internet
- You can also conduct attacks from the device itself to other systems on the network

Data Protection

- Data protection is tied to passcode
  - Data protection is useless without a passcode
- Developers are responsible for data protection
  - They must also implement it correctly!
- Apple does not and cannot validate the use of data protection within applications
- Temporary or cached data often overlooked
- Are credentials being stored in the keychain?

Cookies & Cached Data

- Cookies stored from application UIWebView
  - Junos Pulse SSL VPN Client
  - Facebook, Twitter, LinkedIn
- Cached data is common within all applications
  - Facebook
- What about your corporate applications?

Traditional Vulnerabilities

- Applications are written in Objective C
- Vulnerable to buffer overflows and memory corruption

- Are applications developed securely?
  - Probably not!
- Success of applications based on speed of release and new features – not security!

Syncing with ‘The Cloud’

- Information for most applications syncs with a remote server for various reasons

- What information is being sent?
- Is data sent over a secure channel using SSL?
- What’s the security of the third-party like?
- How are users using their iPhone?

Agenda

1. iPhone Fundamentals
2. Security Mechanisms & Protection Measures
3. Security Weaknesses & Threats
4. <u>Risk Management & Conclusions</u>

Policies, Procedures and Standards

- Update policies, procedures and standards
- Ensure that smart phone devices are not treated like mobile phones
  - Treat them more like laptop computers!
- Ensure that iPhone applications follow an SDLC
- iPhone Applications should be security reviewed in a similar fashion to web applications
- Mandate the use of secure coding guidelines

Mobile Device Management Solutions

- Profiles, configurations and security related settings can be enforced over-the-air
- Application white-listing is available
- Jailbroken devices and unpatched devices can be detected
  - Block or trigger precautionary actions
- All vendors provide a similar level of functionality through an MDM solution
  - All use the MDM APIs provided by Apple

Fundamental Security Principles

- Consider placing iPhones on a separate wireless network that is appropriately secured
- Implement IPS, IDS, NAC and leverage existing security mechanisms
- Consider implementing a private 3G VPN

User Education & Training

- Be transparent with your policies, procedures and standards
  - Recent graduates and younger employees understand security concerns
- Provide training before providing access or use of iPhone devices within the corporate network
- Education and training should be targeted
- Education and training should be continuous

Conclusions

- iPhones can be integrated securely by:
  - Updating policies, procedures and standards
  - Performing relevant security reviews
  - Implementing a mobile device management solution
  - Enforcing fundamental network security principles
  - Providing user education and training

Thank You!

Questions?