SCORE Security Checklist

iOS Platform Security

Version: Release Candidate 2

Date: 30h August 2011

Authors:

Lee Neely

Dave Mold

Neal Hindocha

Tom Neaves

Table of Contents

iOS Platform Security ... 1

1. Executive Summary ... 3

2. Introduction ... 3

3. Purpose ... 4

4. Threats ... 4

5. Platform Security ... 4

5.1. Vulnerabilities ... 4

5.1.1. Recovery of data ... 4

5.1.2. Insertion of unauthorized application / functionality ... 5

5.1.3. Change of security policy ... 6

5.1.4. Jailbreaking ... 6

5.1.5. Malware ... 6

5.1.6. Unsupported firmware and patching ... 7

5.2. Controls ... 7

5.2.1. Authentication Controls ... 7

5.2.2. Authorisation Controls ... 8

5.2.3. Data Security Controls ... 8

5.2.4. Auditing and Logging Controls ... 10

5.2.5. Assurance Controls ... 10

5.2.6. Security Monitoring Controls ... 12

5.2.7. Incident Response Controls ... 12

5.2.8. Security Profiles ... 13

5.2.9. Built-In Encryption ... 13

5.2.10. Control of connections ... 13

5.2.11. Backups ... 14

5.2.12. Additional Encryption ... 14

6. Checklist ... 14

6.1. Avoid Data Leakage ... 14

6.2. Vulnerabilities ... 14

6.3. Controls ... 14

6.4. General ... 15

1. Executive Summary

Apple has introduced three highly successful mobility platforms (iPod, iPhone and iPad, collectively known as iDevices). It is possible to store large amounts of data on the iDevices. The data can be anything from documents to emails to sensitive information such as passwords.

This document aims to provide practical step-by-step guidance to securing data on the iDevice. This guide is structured for users configuring a stand-alone device or corporations without central mobile device management solution, wishing to protect the valuable information stored on their device.

Apple iOS Security is a developing technology. Optimal security requires a combination of technical and administrative controls. Not only must the device be securely configured, and the applications use the security API's to protect their data, but also the user must not extract data from a secure application and insert it into a less secure application. Security settings for Jailbroken (aka hacked) devices are out of scope for this guide as the security features are no longer at a known state.

Following the guidelines in this document, it is possible to secure the iDevice(s). However, with the existence of vulnerabilities, the difficulty in full file system encryption and the rules imposed on app-developers by Apple, it is not possible to secure them to the extent a hardened computer system can be secured.

2. Introduction

Securing iDevices is a combination of security settings (technical controls) and smart user action (administrative controls.) This guide is intended for individual users or corporate users without a central mobile management solution.

As iOS and the iDevice hardware has matured, the corresponding security options have also matured. For this guide, we assume you are using iOS 4 or higher, with current hardware, at a minimum an iPhone 3GS, iPad and iPod touch 3rd or 4th generation.

This guide will lead you through security settings and practices which can be configured natively on the device and the computer you synchronize the device with.

The security measures start with the basics: Enable remote wipe, select a good passcode and configure the device to wipe after a set number of passcode failures. Consider where you connect to the network. Wi-Fi hotspots are being spoofed or otherwise exploited to capture credentials of unsuspecting users. Then consider the applications installed on the device as not all applications implement the same data protection model.

The information provided in this guide is intended to be the foundation for a risk based decision on the type of information you want to store on the device and how you would operate the device in that risk envelope.

A word on Jailbreaking (or hacking iOS); changing the device theme, installing applications or functionality disallowed by Apple, or simply enabling a third party app store are common reasons people hack iOS. As this introduces an unknown element in the device security settings and behavior, we cannot guarantee our suggestions on a Jailbroken device. Corporate users are encouraged to make policy regarding these devices and install appropriate technical and/or administrative controls in support of that policy.

3. Purpose

This is intended to be a quick reference on securing iDevices. Information presented here is gathered from multiple sources and consolidated to describe the threats, risks and mitigations to make informed decisions for appropriate iDevice security.

4. Threats

Threats can be intentional or accidental, and include but are not limited to:

- Theft/Loss: Whether this is a mobile device being stolen or a misplaced in a public place, the ability for petty criminals to convert devices into cash makes physical theft one of the highest threats to portable devices. A recent study found 1 in 20 devices was lost or stolen.

- Interception and Spoofing: Interception of traffic to a Mobile Device in the simplest of form can come from eavesdropping on a conversation by listening to the Wi-Fi, 3G or Bluetooth connection using hacking tools. Having intercepted traffic, it can be modified or new traffic can then be added to attack endpoints. The tools are increasingly easier to use, with some being freely downloadable from the internet. The accompanying YouTube videos make the use of these techniques increasingly more frequent.

- Unauthorised access, hacking and malware: Stealing information is becoming increasing easy in its most simplistic form this can come from accessing messages in a voice mailbox with no PIN, or copying SMS messages and contacts from a SIM card using a reader . Stealing information can occur from malware on infected websites, in email attachments, in SMS messages, from Bluetooth pushed files or rouge applications. Hacked Mobile Devices are even capable of having microphones and cameras remotely activated so they become eavesdropping devices.

- Insecure Disposal/Asset Transfer: Mobile Devices store information on SIMs, internal memory and media which is hard to clear, and can be retrieved. Even after a standard file delete with the right know-how data can be simplistically recovered. The results from a study on the information found on disposed phones is shown below.

5. Platform Security

5.1. Vulnerabilities

5.1.1. Recovery of data

http://blog.crackpassword.com/2011/05/elcomsoft-breaks-iphone-encryption-offers-forensic-access-to-file-system-dumps/

http://mocana.com/blog/2011/02/18/iphone-hackers-can-gain-access-to-your-passwords-in-6-minutes-or-less/

http://www.cellebrite.com/ufed-iphone-physical-extraction-extraction-and-encryption-faq.html

If data encryption is disabled, it is possible to retrieve all information stored on the iDevice. PIN codes and passwords can be bypassed on any iDevice that is vulnerable to a bootrom vulnerability, or by using physical extraction. Currently, all iDevices on the market, except the iPad 2, are vulnerable to at least one bootrom vulnerability. It should be noted that bootrom vulnerabilities cannot be distributed through iOS updates.

iDevices contain two partitions; The OS partition, which is the first 1GB of storage, and the user partition, which is the remaining space. Even if data encryption is enabled, the OS partition is not encrypted. Decrypting a bit-image of the User partition is possible when you have physical access to the device. If a simple passcode is enabled, brute force attempt to recover the passcode is a quick task, taking under 20 minutes on an iPhone 4. Brute force is not necessary if you have the escrow keys. These are created by iTunes on the computer backing up the device.

There are however files on the user partition that will still be encrypted after the partition is decrypted, for example the email storage and the keychain.

Mechanisms are being devised to recover/decrypt the contents of fully encrypted iDevices. In general, these mechanisms rely on having not only the device but also the device that is backing it up. Some of these techniques involve brute force password attacks on the raw device at a level below the configurable iOS setting that wipes the device on repeated password failures.

To mitigate this issue, make sure that access is not provided to both the iDevice and the system that performs its backup. Furthermore, brute force attempts can be made on PIN codes and passwords. Therefore, make sure to follow current best practices when choosing the password and do not use short PIN codes such as four digits.

Protections could include not only disk encryption of the device, but also taking a layered approach for sensitive data where the COTS solution provided protection to data stored on the device in addition to storing application specific data in their own container.

Finally, it should be noted that although information such as pictures have been deleted, it may still be recoverable. To permanently remove such information, use an app that cleans the free space at regular intervals.

http://www.zdziarski.com/blog/?page_id=407

5.1.2.Insertion of unauthorized application / functionality

http://www.reghardware.com/2011/06/15/pin_spy_app_pulled/

By default, iDevices can only load applications through either the Apple App Store or a corporate App Store connected with the Apple Developer Program. Applications in these stores must pass a minimal certification, and in the event Apple determines they are “inappropriate” they may be deleted from devices. Some applications in this avenue have additional functionality which may not be desirable, such as uploading your location data when the application is used to record all the users of a given application. Aside from location data, applications may attempt to leverage the microphone, camera, screen captures and keystroke logging.

Hacked iDevices can install applications from multiple application stores which don't have Apple's oversight. These are the most likely sources of unauthorized application functionality. Hacked device owners are dependent on the third-party application providers for security and/or appropriate use of the available technology and don't have Apple's QA or oversight to protect them. Using a Hacked device is a risk based decision, and the alternatives, risks and impacts should be considered.

5.1.3.Change of security policy

Apple iPCU (iPhone Configuration Utility) allows for the creation for security policies (aka profiles) for iDevices. The policies can be signed, encrypted, and may require a password for removal. In the extreme case, they can be made permanent and only removed via device wipe. When creating security profiles, at a minimum require a unique strong password to remove it.

Profiles can be delivered to the device via the web, email attachment or pushed via MDM (Mobile Device Management) solution. Depending on the source of the security profile, the device user/owner may or may not be involved in accepting those policies. Some products expire the certificates necessary to communicate with corporate resources when a new policy is published to incentivize user adoption of the updated profile.

Multiple security profiles can be active on a single iDevice. Security profiles are layered, with the most restrictive setting for any option being enforced.

5.1.4.Jailbreaking

http://en.wikipedia.org/wiki/IOS_jailbreaking

Jailbreaking an iDevice allows applications to be installed from sources other than the approved application store, as well as providing remote access, such as SSH access, to the device. iOS has preloaded password tables which include well known username/password combinations. The root password for example, has been "alpine" since the release of the first iPhone. Users and corporations will have to make a risk based decision on their acceptance of hacked devices. Application Developers have to assume deployments include hacked devices and implement necessary security protections, if any.

If you elect to hack your device, be sure to change all the built-in passwords.

5.1.5.Malware

http://krebsonsecurity.com/2011/05/weyland-yutani-crime-kit-targets-macs-for-bots/

iOS Malware falls into three categories. Code designed to hack (or jailbreak) the device, code designed to take advantage of the changed security settings on a hacked iDevice or code designed to exploit vulnerabilities. Workarounds and/or software updates are published to counteract the first and third category. The owner of a hacked device must investigate and find fixes for any malware that exploits the changes in security settings resulting from jailbreaking the iDevice.

5.1.6.Unsupported firmware and patching

http://www.theregister.co.uk/2011/03/10/apple_update_omits_iphone3g/

Apple limits the long-term support, aka backwards compatibility of new iOS releases with older iDevices. In general, Smartphones have an effective support lifecycle of 18-24 months due to the rate of technology and device evolution. This is not a vendor specific phenomenon. Lifecycle replacement cost and timing needs to be planned into any Smartphone purchase to ensure continuing support and security.

5.2. Controls

The level of platform security which is required and can be engineered into a platform’s configuration is very much dependent on the role of the device and whether the security policy and controls are managed on or off the device. This document describes the controls from the perspective of an unmanaged device i.e. that which is typically a personal.

5.2.1.Authentication Controls

The user authentication to the iDevice is controlled by the configuration or a single user account and password. It is important that this is enabled and configured to ensure a strong password is always required to access the device. To determine the best password policy to set it is recommended to ensure length, use of character space, session and frequency settings are optiminsed. Online resources like the following are useful for this purpose.

http://askthegeek.us/pwd_meter/index.htm

https://www.grc.com/haystack.htm

As a minimum the following settings are recommended

- Set a password to access the iDevice. Use: Settings->General->Passcode Lock->Turn Passcode On (with simple Passcode Off). The longer and more complex password the better at least 8 characters. Holding a key (e.g. A, E, Y, W, U, . , etc.) on the keypad reveals extended charters and is a go way of using complexity. Change this password if someone else knows it or after 30 days.

- Enable inactivity time out. Set the auto-lock to 5 minutes or less. Use: Settings->General->Auto-Lock

- Enable maximum session before a Passcode needs to be entered to protect from the theft of an unlocked device. Use: Settings->General->Passcode Lock->Require a Passcode-> after 1 hour or less.

- Enable Erase Data to automatically erase the device after ten failed passcode attempts. Settings->General->Passcode Lock-> Erase Data->On.

- Make your account for iDevice different for other passwords or websites which are likely to be stored in a less secure manner

5.2.2. Authorisation Controls

As the iDevice is a single user device authorisation controls are in the main related to the connections to the device. It is recommended the unused connections are disabled and configured for best security where needed. The following controls are configured

To disable connections

- Turn off Bluetooth to prevent unauthorised access by this vulnerable communication channel. Use: Settings->General->Bluetooth->Off. Guidance on the security aspects are available from NIST (see http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf)
- To disable VPN use: Settings->General->Network->VPN->VPN-> Off.
- To disable Wi-Fi use: Settings->General->Network->Wi-Fi->Wi-Fi->Off.

To use connections

- When turning on Wi-Fi it is recommended ensuring connections are authorised by the User. Use: Settings->General->Network->Wi-Fi->Wi-Fi->Ask to join Networks->On. When using a Wi-Fi connection the following steps are recommended:
    - Do not use untrustworthy hotspots
    - Only use encryption on open Wi-Fi networks to avoid eavesdropping
    - Check site certificates on any web authentication pages before entering any credentials
- When turning on Bluetooth there are three principle areas to consider which are: Discoverability, Passcode strength and use of Encryption. To ensure correct implementation of the protocol use Devices which display the appropriate "experience icon" (http://www.bluetooth.com/Pages/Experience-Icons.aspx). Limit the time the iDevice is discoverable to avoid detection i.e. only for initial pairing. Protect the communications by using encryption and a long pass phrase or PIN because the key is susceptible to brute force attacks default and short pass phrase or PINs must be avoided. An 8 digit passphrase or PIN should protect a against the time window likely for an opportunistic attack i.e. the length of time to drink a cup of coffee in a public location.

  http://www.f-secure.com/weblog/archives/00002003.html

5.2.3. Data Security Controls

The iPhone 3GS+, 3rd and 4th generation iPod and iPad feature built-In AES 256 hardware encryption. This encryption must be properly enabled for it to work. Devices delivered with iOS 4+ are properly configured out-of –the box. Devices that have been upgraded to iOS 4 must be restored to properly enable the full hardware encryption.
http://support.apple.com/kb/HT4175

Once configured, a passphrase must be set on the device to create an encryption key that then prevents unauthorized access to data on the device as well as configuring an automatic wipe after a specified number of password attempts. It is possible to brute-force attack the encrypted data to recover the password; therefore it is important to choose a strong password.

Another weakness in this scenario is that if the computer used to backup/configure the device is captured with the corresponding device, the device backups on that computer can be examined/exploited to gain access to data otherwise stored on the iDevice. iTunes is used to backup an iDevice and stores the data (on Windows Vista or Windows 7) in the location C:\Users\<login name>AppData\Roaming\Apple Computer\MobileSync\Backup. It is possible to modify this location to, for example, an encrypted location e.g. hardware encrypted flash drive for extra security. Alternatively set a strong Passcode.
NOTE: As this can't be changed it is recommended the password is at least 20 characters long.
To set a Passcode In the iTunes Summary screen, select "Encrypt <iDevice> backup" if you want to encrypt the information stored on your computer when iTunes makes a backup. Encrypted backups are indicated by a padlock icon (See the Deleting a Backup section here: http://support.apple.com/kb/HT4079), and a password is required to restore the information to iDevice (See http://support.apple.com/kb/HT4079 for the information iTunes backs up).

If you must travel with both the iDevice and a computer that has been configured to sync to the device, be sure to properly secure that computer as well. E.g. only synchronise with iTunes on devices which have appropriate controlled access (e.g. Disk Encryption and strong user passwords) and good hygiene (e.g. automatic updates, up to date anti-virus software). In iTunes under preferences->devices, you should see your most recent back-up date/time.

Cloud based backup solutions are also available through various providers e.g.

Apple: iDisk and iCloud

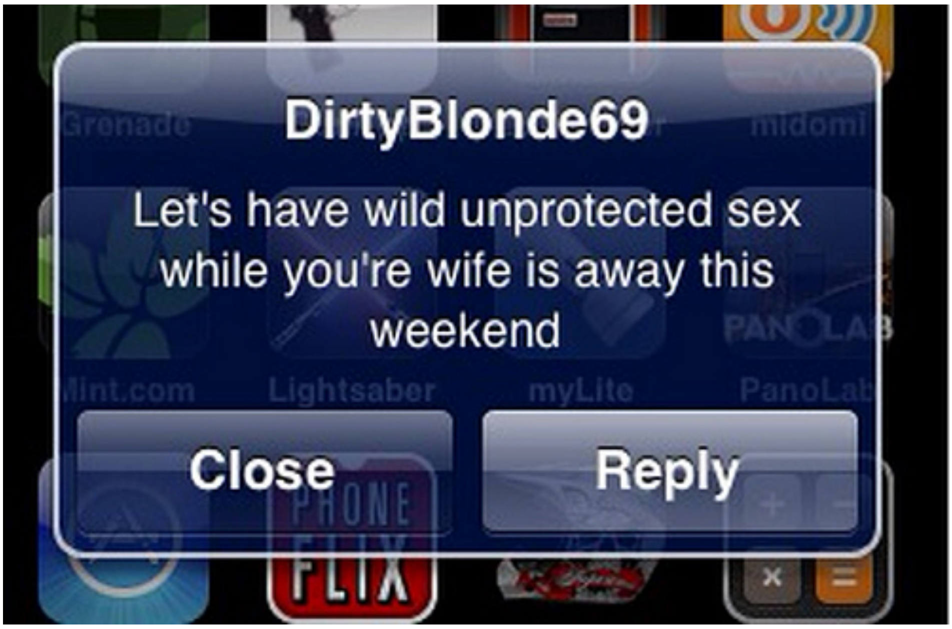
Cydia: DataDeposit & Dropbox

However, even with the device encryption and passcode and encrypted backups there is the risk of the attacker accessing the device and data and most good practice require application controls to protect the data. Unfortunately there are issues with data leakage form application protection and the following steps are recommended

- Exit the application using application options and not the home button to avoid capturing screen shots of sensitive data by the Apple system.
- If there is no exit option in the application, click the home-button once to exit the application, then double-click the home button and terminate the application from the bar showing running applications.
- Do not cut and paste sensitive data.

- Set device to erase on incorrect password guesses. Use: Settings->General->Passcode Lock->Erase Data->On.

The device should be configured to prevent SMS preview to prevent the revelation of sensitive information without appropriate authentication. Use: Settings->General->Passcode Lock->Show SMS Preview->Off



DirtyBlonde69

Let's have wild unprotected sex while you're wife is away this weekend

To prevent data leakage through the browser configuration settings, it is recommended the Autofill option is restricted. Use: Settings->Safari ->Auto fill ->Off.

5.2.4.Auditing and Logging Controls

Most logs are not normally viewable on the device, and the easiest way to see them is through syncing with iTunes and then viewing log files. Application crash logs, which maybe symptomatic of malicious activity, can be found in the following locations:

Mac OS X
~/Library/Logs/CrashReporter/MobileDevice/<your iDevice’s name>/

Windows XP
C:\Documents and Settings\<login name>\Application Data\Apple computer\Logs\CrashReporter\<your iDevice’s name>\

Windows Vista
C:\Users\<login name>\AppData\Roaming\Apple computer\Logs\CrashReporter\MobileDevice\<your iDevice’s name>\

5.2.5.Assurance Controls

While no vulnerability scanners, anti-virus, firewall and IDS products exist in the normal security sense for iDevices; certain controls can be engineered.

The first control is to ensure the firmware is patched to the most current level using iTunes. On the device, use: Settings->About to display the version installed version, which can be compared to the latest version, either via iTunes and an internet connected PC, or online via the Apple support pages.

http://support.apple.com/kb/ht1222

In a similar way to patching iOS, it is important to maintain the installed applications and these should be checked regularly for updates. iTunes can help with this, under the Applications tab on iTunes (usually below the Podcast tab), there is an option to manually check for App updates. Just click on it and you will see the list of out-dated apps that you have. Either update everything or one-by-one.

Rogue apps are a concern and steps should be taken before and after installation an app including:

1. Checking reviews and security blogs
2. Understanding the vendor, is the company location and contact details available
3. Is the source trustworthy, app store distributed products undergo more assurance
4. Take a full back up before installation
5. Check permissions needed
6. Updates and side channel communications should be checked.

Some legitimate apps are susceptible to malicious use; one example of such an app is Flexispy. After all, why do you need to worry about Trojans when there is an app for that?

Malware protection is an emerging market as well as infecting the iDevice itself. A lot of malware is being engineered to use mobile and removable media to cross infect networks bypassing perimeter malware filters. To this end, it is vital to ensure any device used for synchronisation has up-to-date antivirus protection and similarly all traffic is screened for malicious code.

A few vendors are starting to address this including intego's virusbarrier and K9's Web Protection Browser. It is also possible to use other filtering services like OpenDNS.

In a similar way, email traffic should be scanned for malicious content.

Phishing is a particular concern on mobile devices. URL shortening is common in user interfaces, and users are therefore more likely to be tricked on a mobile device.

Check online tools

http://security.symantec.com/sscv6/home.asp?langid=ie&venid=sym&plfid=23&pkj=LVXFYHGBYNCJEIMXQKC

http://security.symantec.com/sscv6/WelcomePage.asp

http://www.f-secure.com/en_UK/security/security-lab/tools-and-services/online-scanner/

5.2.6.Security Monitoring Controls

There are limited controls that can be applied for security monitoring considerations are limited and mainly for corporate gateway scanning e.g. SEIM on a proxy log. However some controls and should be considered.

While Apple has dropped its short lived Jailbreak API, some tools do attempt to detect jailbreak behaviour such as Good Technologies.

Some detection rules are now appearing in IDS solutions. E.g. snort signatures exist for jailbreak exploits and routing iDevice non-3G network traffic through an inline IPS is recommended.

5.2.7.Incident Response Controls

Businesses need to develop and publish incident response policy which includes iDevices. Reporting, tracking and response resources need to be available to assist with forensic, response and reporting requirements.

Self-managed devices must rely on services such as find my iPhone to remotely wipe, lock, locate and/or put a message on the device screen, as well as regularly watch for security alerts both from Apple and leading security sources such as SANS.

Location tracking

It is possible to establish the location of a device remotely through GPS tracking.
http://www.apple.com/uk/ipad/built-in-apps/find-my-ipad.html

Notification of appropriate service providers, authorities and insurance contact may be required. Check your local requirements.

Forensics

Forensic tools are available to capture and analyse content on iDevices. Some forensic tools are capable of decrypting the encrypted content, including the keychain and file systems.
http://iphone-forensics.com/ http://ixam-forensics.com/ http://katanaforensics.com/
http://www.iosresearch.org/

Most forensic tools are dependent on exploiting bootrom vulnerabilities to extract data from encrypted iDevices. As of this writing, the iPad 2 is the only device with no identified bootrom vulnerabilities.

Remote Device Wiping

Without an MDM solution, Apple's Find My iPad or Find My iPhone is the best mechanism for remote wipe. Note that this depends on a Mobile Me account on the device, and only one Mobile Me account can be configured for Find My iPhone. Adding an additional Mobile Me account to the device will disable the existing Find My iPhone account.

Manual Device Wiping

You can remove all settings and information from an iDevice using "Erase All Content and Settings." Use: Settings->General->Reset.

http://support.apple.com/kb/ht2110

Restore Process

iDevices can be restored from backup using iTunes.

http://ioscentral.co.uk/?p=189

5.2.8.Security Profiles

Apple iPCU and MDM solutions for iDevices can install security policies (or profiles) on the devices. The profiles can be signed, encrypted, and may require a password for removal. In the extreme case, they can be made permanent and only removed via device wipe. When creating security profiles, at a minimum require a unique strong password to remove it.

Profiles can be delivered to the device via the web, email attachment or pushed via MDM solution. Depending on the source of the security profile, the device user/owner may or may not be involved in accepting those profiles. Some products expire the certificates necessary to communicate with corporate resources when a new profile is published to incentivize user adoption of the updated profile.

Multiple security profiles can be active on a single iDevice. Security profiles are layered, with the most restrictive setting for any option being enforced.

5.2.9.Built-In Encryption

iDevices use AES 256 bit hardware encryption. Enabling a passcode turns on the encryption.

5.2.10. Control of connections

It is recommended the unused connections are disabled and configured for best security where needed. The following controls are configured

To disable connections

- Turn off Bluetooth to prevent unauthorised access by this vulnerable communication channel. Use: Settings->General->Bluetooth->Off . Guidance on the security aspects are available from NIST (see http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf)
- To disable VPN use: Settings->General->Network->VPN->VPN->Off.
- To disable Wi-Fi use: Settings->General->Network->Wi-Fi>Wi-Fi>Off.

To use connections

- When turning on Wi-Fi it recommended ensuring connections are authorised by the User. Use: Settings->General->Network->Wi-Fi->Wi-Fi->Ask to join Networks->On. When using a Wi-Fi connection the following steps are recommended:
    - Do not use untrustworthy hotspots
    - Only use encryption on open Wi-Fi networks to avoid eavesdropping
    - Check site certificates on any web authentication pages before entering any credentials

5.2.11. Backups

iDevices are backed up using iTunes. Encrypt the backups using a non-trivial password to make it harder to access.

5.2.12. Additional Encryption

Third-party encryption apps are available to protect the confidentiality of data for advanced applications and should be considered where advanced protections are required.

6. Checklist

6.1. Avoid Data Leakage

- Use strong passwords for all services and accounts accessed from the device.
- Protect your personal email by encrypting traffic. Use: Settings->Mail, Contacts, Calendars -><Select an Account>->Advanced, then scroll down to the Use SSL option. This will prevent others being able to read your email over public Wi-Fi networks.
- Do not backup company data to cloud services like Mobile Me iDisk or Dropbox.
- Do not use your iDevice for information or communications which is regulated.
- Do not send work related email to personal email accounts.
- Erase or wipe iDevices when reassigning, replacing, returning, or other disposition.

6.2. Vulnerabilities

- Store the iTunes backup securely
- Store valuable data in applications that secure it in its own container
- Use an app that clears free space at regular intervals
- Consider the risk and gain trade-off when deciding whether or not to jailbreak the device
- Always update both iOS and installed apps when updates are made available, check at least once a month for updates
- When the device has reached end-of-life and is no longer supported with new updates, consider upgrading the device
- When replacing, retiring or reassigning a device, wipe the device to prevent data leakage.

6.3. Controls

Enable the following controls

- Password Protection
    - Use a Complex Password
    - Use a Unique Password
- Device Encryption

- Auto-Lock set to 5 minutes
- Maximum Session
    - Set to require passcode immediately.
- Automatically Erase Data after 10 failed Authentication Attempts
- Ask to Join Wi-Fi networks
    - Do not use untrustworthy hotspots
    - Ensure that data is transferred encrypted when sent over open Hotspots
    - Always check certificates on webpages

Disable the following when not in use

- Bluetooth
- Wi-Fi
- VPN
- Location Services

6.4. General

- Do not leave the device unattended when travelling and try to avoid displaying it in public areas. One in twenty mobile devices is lost or stolen.
- Fit a privacy screen to avoid someone looking over the shoulder at the screen.
- When browsing using the iDevice, try to avoid unknown sites, and pay special attention to certificates to ensure they are valid.
- Only download apps from reputable developers in the Apple or Corporate App store.

Last Updated: February 7th, 2026

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Secure Caribbean 2026	**Kingston, JM**	**Feb 16, 2026 - Feb 21, 2026**	**Live Event**
SANS Surge 2026	**La Jolla, CAUS**	**Feb 23, 2026 - Feb 28, 2026**	**Live Event**
SANS Dublin February 2026	**Dublin, IE**	**Feb 23, 2026 - Feb 28, 2026**	**Live Event**
SANS Secure Japan 2026	**Tokyo, JP**	**Mar 02, 2026 - Mar 14, 2026**	**Live Event**
SANS London March 2026	**London, GB**	**Mar 02, 2026 - Mar 07, 2026**	**Live Event**
SANS DC Metro March 2026	**Arlington, VAUS**	**Mar 02, 2026 - Mar 07, 2026**	**Live Event**
SANS Secure Singapore 2026	**Singapore, SG**	**Mar 02, 2026 - Mar 14, 2026**	**Live Event**
SANS Paris March 2026	**Paris, FR**	**Mar 09, 2026 - Mar 14, 2026**	**Live Event**
SANS Open-Source Intelligence Summit 2026	**Arlington, VAUS**	**Mar 16, 2026 - Mar 22, 2026**	**Live Event**
SANS Thailand March 2026	**Bangkok, TH**	**Mar 16, 2026 - Mar 21, 2026**	**Live Event**
SANS Amsterdam March 2026	**Amsterdam, NL**	**Mar 16, 2026 - Mar 21, 2026**	**Live Event**
SANS Melbourne March 2026	**Melbourne, VIC, AU**	**Mar 16, 2026 - Mar 21, 2026**	**Live Event**
SANS Cybersecurity Leadership Summit & Training 2026	**Arlington, VAUS**	**Mar 17, 2026 - Mar 22, 2026**	**Live Event**
SANS 2026	**Orlando, FLUS**	**Mar 29, 2026 - Apr 03, 2026**	**Live Event**
SANS London April 2026	**London, GB**	**Apr 13, 2026 - Apr 18, 2026**	**Live Event**
SANS Rome April 2026	**Rome, IT**	**Apr 13, 2026 - Apr 18, 2026**	**Live Event**
SANS Secure Australia 2026	**Canberra, ACT, AU**	**Apr 13, 2026 - Apr 18, 2026**	**Live Event**
SANS Rocky Mountain 2026	**Denver, COUS**	**Apr 20, 2026 - Apr 25, 2026**	**Live Event**
SANS SEC535 at AI Cybersecurity Summit & Training 2026	**Arlington, VAUS**	**Apr 20, 2026 - Apr 27, 2026**	**Live Event**
SANS AI Cybersecurity Summit & Training 2026	**Arlington, VAUS**	**Apr 20, 2026 - Apr 27, 2026**	**Live Event**
SANS Amsterdam April 2026	**Amsterdam, NL**	**Apr 20, 2026 - Apr 25, 2026**	**Live Event**
SANS ICS Munich 2026	**Munich, DE**	**Apr 20, 2026 - Apr 25, 2026**	**Live Event**
SANS Doha April 2026	**Doha, QA**	**Apr 26, 2026 - Apr 30, 2026**	**Live Event**
SANS Cyber Incident Management 2026	**OnlineAU**	**Feb 09, 2026 - Feb 13, 2026**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**