Global Information Assurance Certification Paper

iPad Security Settings

And Risk Review For iOS 4.X

GIAC (GSEC) Gold Certification

Author: Jim Horwath, jim.horwath@rcn.com
Advisor: Johannes Ullrich

Accepted: February XX, 2011

Abstract

Many corporations are starting to investigate the use of mobile computing devices by staff and field agents. The introduction of consumer devices such as the iPad into the business world, brings a new set of risks and concerns to a corporation. The settings defined in this document try to balance a corporation's regulatory and customer obligations to reduce risk while still allowing the user population an enjoyable user experience. The paper will investigate this problem from a deployment in an effort to give sales and marketing a business edge. The CIS benchmark for Apple iPhone OS 3.1.2 was the starting point for this effort. The settings in this document have undergone a trial period with users of differing abilities, and their feedback helped formulate this document.

1. Introduction

The introduction of mobile computing introduces new risks and concerns to the firm. There are many questions concerning the operation, compliance, cost and risk with mobile computing devices. The iPad runs the iPhone Operating System commonly called iOS. The current version of iOS during the writing of this paper is 4.2. The iPad is a mobile computing device that is a hybrid, not a full-fledged computing device such as a laptop, but more user friendly than current phones and Blackberries. The iPad is available in two different models with or without 3G capability. The ability to use a 3G cellular network will cost you about $130 U.S. Dollars.

The iPad is a small device that delivers graphics and performance in a small package.

The hardware specifications are as follows:

- Wi-Fi
- Digital compass
- Assisted GPS (Wi-Fi + 3G model)
- Cellular (Wi-Fi + 3G model)
- Wi-Fi model
- Wi-Fi (802.11a/b/g/n)
- Bluetooth 2.1 + EDR technology
- Wi-Fi + 3G model
- UMTS/HSDPA (850, 1900, 2100 MHz)
- GSM/EDGE (850, 900, 1800, 1900 MHz)
- Data only
- Wi-Fi (802.11a/b/g/n)
- Bluetooth 2.1 + EDR technology (Apple, 2010)

The iPad has great eye appeal, and the design of the component hardware and software has a goal of maximizing the user experience. Apple produces products that have consumer appeal. Power consumption on mobile devices is an issue and poor battery life can result in a bad user experience. The iOS will shutdown components not actively used to conserve battery power and allow the user longer periods of device usage. The iOS Application Programming Guide has a section that covers reducing power consumption in applications. The design of the device seems more consumer-based than business based. Controls that will help business meet regulatory obligations and corporate policies are either missing or require additional tools to enable them. **(Apple, 2010)**

2. Mobile Device Management

Managing more than a few iPads can quickly become a laborious task and a resource drain. Mobile Device Management (MDM) software allows corporations a single interface for managing a fleet of mobile devices. These MDM products allow users to create profiles that advantage Apple API's to extend the security settings of the device. Apple provides a free utility, *iPhone Configuration Utility* (ICU) for creating device profiles. The ICU does not enforce policies and manage the devices. With the mobile device market starting to explode, many vendors recognize the new business opportunity. Apple's ICU is a great utility to start learning what features and security controls are available on the iPad. Because this paper talks about extended security settings available through Apple's APIs, there is frequent mentioning of ICU throughout this paper. Apple has made API's available that allow developers to interface with the iPad. These API's allow developers to configure and extend certain setting on the iPad. For example, without any external tools, passwords consist of exactly four digits, you cannot create alphanumeric passwords. The API's allow for stronger passcode policies that allow alphanumeric and special characters. The most secure API's that deal with VPN support are only available to Cisco and Juniper under an NDA. Apple has a programming guide available describing what API's are available, and the expected behavior of the device when using these calls. This guide contains great resources that will help people gain a deeper understanding of how the iPod/iPhone/iPad technology works.

3. Profile Removal

Third party management tools create device profiles that extend the security capabilities of the iPads. Deployment of these profiles to end-user occurs by pushing them either by e-mail, or by using third party management software. Depending on the software used to create the profile, the user may or may not be able to remove or modify settings defined in the profile. The ICU by default allows users to have the ability to remove profiles. There are API's for the iPad allowing profile removal, allow profile removal via password protection, or disallow removal. Users should not have the authority to alter the corporate iPad configurations. Many third party MDM products will allow user the ability to remove profiles from the device; this removes all corporate data and leaves personal data unscathed. The author tested this with several different MDM products during a proof of concept for MDM products.

4. Apple Technology

The i-technology (iPod/iPhone/iPad) requires the installation and use of iTunes. There is no way to use these devices without the use of iTunes. Apple does not allow any other option for backing up, restoring and synchronizing data other than iTunes. Some corporations may have policies that require packaging of corporate approved applications to company assets. iTunes would become another application for corporate distribution and installation on company assets. Corporate storage environment may not be ready to handle the additional burden of iPad backups. In addition, many storage environments do not exclude any files during daily backups, so business related sound files along with valid and pirated songs, movies, and pictures will be under the control of your corporate storage and backup environment. Apple is also selective as to get access to the most secure API's. Apple keeps tight control over the iPad software environment allowing the installation of applications available and approved by the Apple Store. However, if the user jailbreaks the device, a completely new world of software becomes available. A *jailbroken* device is the user loading software unapproved by Apple onto the device to

allow greater access to the device. Jailbroken devices can run SSH and FTP servers and even penetration testing software such as Metasploit. There is a procedure available at The Mayhemic Lab WEB site describing a Metasploit installation. (Mayhemic Labs, 2010) The Dev-Team Blog is a great resource for researching more about *jailbroken* devices and customization of iPads. (Dev-Team Blog, 2011)

5. Default Configuration

The default configuration of the iPad out-of-the-box has very little security controls. This is a consumer device that favors convenience over security. The lack of security controls that would make a teenager happy will send chills up the spine of the corporate security and risk staff. Out of the box, the iPad does not come with any password protections. Without applying any additional configuration tools, the iPad only supports a four-digit password. Apple could ship the device with a default password, but this would give a false sense of security to most non-technical users. One issue with shipping devices with default passwords is many users would never change the default password. This would instill a false sense of security to this portion of the user population. A better feature would be shipping the device with a default password that the user would need to update when they activated the device. The iPad does feature built-in hardware encryption using AES 256-bit encoding. By default, the device does not enforce any locking that would require a password/passcode for access. It is possible to implement device locking after so many minutes of inactivity, but this is not the default behavior. (Apple, 2010)

6. Device Authentication

The default configuration of the iPad does not require a passcode for access. The device will allow access to anyone who slides the unlock bar on the screen. The user does not have the ability to implement alphanumeric passwords. This allows a user to choose a passcode from one of 9,999 different combinations. There are password "recovery" programs available from companies like Elcomsoft that can crack passwords on an iPad. (Elcomsoft, 2011) Due to the small number of choices, cracking the password on an iPad is quick and trivial with the right software. The company *Elcomsoft* sells an iPad

password cracker. (Elcomsoft, 2011) Not allowing a complex passcode/password to the device lessens the security posture of the device. Out of the box, the password complexity would fail any sane corporate password policy.

There are additional options missing from the default options that users can enable via third party tools such as Apple's ICU. The default configuration does not allow controls around passwords that would allow the device to meet most corporate policies. Here are features Apple makes available via API's, but are not available in the default product. There is a setting to allow or prevent the use of simple passwords, the use of descending, ascending and repeating character sequences. This allows lazy ways to simplify passcode phrases thereby rendering some of the security controls less effective. In the default configuration, there is no setting for defining the minimum number of characters for a valid passcode. The device should allow users the ability to define a minimum password length. Most corporate policies specify minimum password lengths. Most corporate policies define a minimum number of complex characters that users must include in passwords. Apple provides an API for defining the minimum number of complex characters (*, !, etc) in a valid password. Finally, the device should address the issue of password aging. The default does not allow any password aging ability, but this is available in the API. The absence of these features above hinders the adoption of the iPad into the business world. Corporations need to invest time and resources into third party tools to help increase the security posture of the iPad.

Luckily, the Apple ICU and other third party tools can solve this problem and allow users to implement strong alphanumeric passwords providing better protection to data on the iPad. Additionally, Apple provides an API that implements an autodestruct feature for wiping data from a device after X number of failed attempts. This feature is not available without applying additional tools such as Apple's ICU, or a third party MDM vendor. This feature assists users and corporations protecting data stored on the device. This feature should be available by default, and if the user wants to disable it, they should have the option. The most devious thing that can happen from an auto-wipe is somebody purposely trying X number of bad passwords to force a wipe. If the user is away from on

business, they cannot fully restore their iPad until they get access to the computer containing their backup. With an active Internet connection and iTunes, a user can get the iPad running, but the restoration of personal data is not possible until the user has access to the computer containing the iPad backup.

Implementing alphanumeric passwords brought out a "feature" of touch screens that undoes all the security the complex passwords tries to build in. Implementing alphanumeric passwords enabled the echoing of characters as users input their passwords. The screen echoes each character for a few seconds before it turns into a '*." Shoulder surfing was trivial! This condition is a "feature" of touch screens to help poor typists. When deploying iPad devices to users, administrators should socialize this behavior to users so they can make adjustments when accessing the device in the company of other people. Additionally, the device will echo alphanumeric passwords required by WEB pages.

One feature for the device that Apple did a horrendous job of naming is "Auto-Lock" and "Grace Period." These options deal with activating a screen saver and locking the device requiring a password for access. The auto-lock feature is really screen saver activation, and is separate from locking the device and requiring a password for access. The grace period value defines the locking of the device requiring a password for device access. A better naming scheme would be screen saver for auto-lock, and device lock for grace period. The Auto-Lock value activates the screen saver, or picture frame as Apple refers to it. It appears to happen to save battery and screen life. When the timer is up the screen saver activates.

The system has the ability to wipe its configuration and data after a certain amount of authentication failures. Normally excessive authentication failures are a sign the device is in possession of somebody other than the owner, and the device is under a password guessing attack. Configuring the device for 10 authentication failures should protect the device from password guessing attacks, while protecting users from trying wrong passwords repeatedly. This does have the downside of allowing somebody to DOS a

user's iPad by trying a bunch of failed authentication attempts. The user most likely will not have immediate access to backups, so this will disable the user until a restoration can take place. Starting with iOS 4.x, there are API's available to reset passwords from a remote location for users who forgot their passwords. This tool can help corporate support staffs with authentication issues with users.

During testing with colleagues, family members and others, typing complex passwords was cumbersome and brought nothing but complaints from the test cases. After several days of using the device, navigating around on the iPad keyboard became second nature and was no longer a big deal. However, implementing alphanumeric passwords enabled echoing of characters as users input their passwords. This condition happens when a user must input hidden data (such as credentials) into the Safari browser. The echoing of characters to the screen is something Apple should address to help enhance the security posture of the iPad. (Apple, 2010)

7. Keeping iOS Current

Keeping the device iOS level current is an important best practice to increase the firm's security posture. Any iPad device connecting to the corporate network should be at the most recent iOS level. Staying up-to-date with iOS releases is important for increasing security postures. As Apple increases their market presence, they will become a bigger target for nefarious people. The most recent release addresses known security and performance issues related to the iPad. The only way to update iOS is via iTunes. Apple does not provide a way for corporations to download and distribute iOS to mobile devices similar to Microsoft's SCCM or SMS. Corporations implementing a third party product to manage devices will still find this missing from their product of choice. The MDM product should be able to enforce a minimum iOS version before letting device access corporate resources. The MDM software will prevent users from accessing resources until the device meets the minimum defined standard. However, the end user is still responsible for keeping the mobile device current. The reason for not pushing code

directly to the iPad might be bandwidth conservation and cost savings. Pushing a seventy-five Megabyte update to an iPad over a cellular connection could become very expensive. A nice enhancement for Apple would be a service similar to Microsoft SMS where a corporation can distribute iOS to corporate mobile devices.

8. Backups

Backups are a business critical process that most users do not think about until the need one for restoring important data. Apple tries to simply the process by using iTunes as the central point for all backup, restore and synchronization operations. Each iPad can hold 16, 32, or 64GB of information depending on the model you purchase. Apple empowers the users to help control their own backup destiny. This power also allows users the ability to skip backups if they are too busy to dock to their primary computer. During the setup of an iPad, each device has a notion of a primary computer that it associates with. It is possible to backup and restore an iPad to or from a different computer, an iPad device knows which computer is the primary backup computer. By default, iTunes stores backups in the following locations (based on platform):

Mac: ~/Library/Application Support/MobileSync/Backup/ **Windows XP**: \Documents and Settings\(username)\Application Data\Apple Computer\MobileSync\Backup\ **Windows Vista** and **Windows 7**: \Users\(username)\AppData\Roaming\Apple Computer\MobileSync\Backup\

Corporations must decide if users can leverage corporate assets for backing up iPad devices. If employees backup the iPad to their corporate asset such as a laptop, this is going to increase the burden on the storage area at the corporation. If users leverage corporate assets for backups, the company should have policies and procedures for backing up laptops. Many corporations do not backup laptops and may implement network storage for keeping important data save. If a user uses a personal asset for backups, the chance of a home user backing up their computer system is not a sure thing. Although a user may use a home computer to backup their iPad, there is the real

possibility of not being able to recover the home computer backups in the event of a system crash. Although the iPad can function again, if there is a failure on the iTunes computer and an iPad failure, data may be lost.

The iTunes backup contains all your personal information with the exception of the iTunes library. Not including the iTunes library can prevent companies from piracy stemming from employees swapping music and movie files. By default, iTunes does not encrypt iPad backups; the user must force encryption on backups. When users create backups without encryption they expose all personal and confidential information stored on the device. Enabling backup encryption is an option on the iTunes interface. When the user enables backups, a password governs access to the backup. If the user forgets the password, they are out of luck. A better design would be Apple only allowing encrypted backups, or creating encrypted backups by default. (Apple, 2010)

If you backup you iPad device, it will contain any sensitive information you store on the device. An article in the Apple Knowledge Base lists the following data as information stored in an iPad backup. The information below came directly from the Apple Knowledge Base HT1776. (Apple, 2009)

Address Book and Address Book favorites.

- App Store Application data (except the Application itself, its tmp and Caches folder).
- Application settings, preferences, and data.
- Autofill for webpages.
- CalDAV and subscribed calendar accounts.
- Calendar accounts.
- Calendar events.
- Call history.
- Camera Roll (Photos, screenshots, images saved, and videos taken. Videos greater than 2 GB are backed up with iOS 4.0 and later.)
- Note: For devices without a camera, Camera Roll is called Saved Photos.
- In-app purchases.
- Keychain (this includes email account passwords, Wi-Fi passwords, and passwords you enter into websites and some other applications. If you encrypt the backup with iOS 4 and later, the keychain information is transferred to the new device. With an unencrypted backup, the keychain can only be restored to the same iPhone or iPod touch. If you are restoring to a new device with an unencrypted backup, you will need to enter these passwords again.)
- List of External Sync Sources (Mobile Me, Exchange ActiveSync).
- Location service preferences for apps and websites you have allowed to use your location.
- Mail accounts.
- Managed Configurations/Profiles. When restoring a backup to a different device, all settings related to the configuration profiles will not be restored (accounts, restrictions, or anything else that can be specified through a configuration profile). Note that accounts and settings that are not associated with a configuration profile will still be restored.
- Map bookmarks, recent searches, and the current location displayed in Maps.
- Microsoft Exchange account configurations.
- Network settings (saved WiFi spots, VPN settings, network preferences).
- Nike + iPod saved workouts and settings.
- Notes.
- Offline web application cache/database.
- Paired Bluetooth devices (which can only be used if restored to the same phone that did the backup).
- Safari bookmarks, cookies, history, offline data, and currently open pages.

- Saved suggestion corrections (these are saved automatically as you reject suggested corrections).
- SMS and MMS (pictures and video) messages.
- Trusted hosts that have certificates that cannot be verified.
- Voice memos.
- Voicemail token (This is not the Voicemail password, but is used for validation when connecting. This is only restored to a phone with the same phone number on the SIM card).
- Wallpapers.
- Web Clips
- YouTube bookmarks and history. (Apple, 2010)

The files that contain the iPad backups are ordinary binaries in a SQLite database format. The files have very long alphanumeric names that are viewable in editors such as "*vi.*" The file names appear to be some sort of long hash value. In a text editor or using the UNIX "*strings"* command, there is not a lot of valuable information you can gather from the files. However, an attacker can easily load the data into a SQLite database and have access to your private information. Jonathan Zdziarski's book, "iPhone Forensics: Recovering Evidence, Personal Data and Corporate Assets" describes this process very well. The important point is the information is available on the computer in an unprotected format. Because of the sensitive nature of the information stored in the backup files, and the ease of access to the information, it is important to have these files encrypted. **(Zdziarski, 2008)**

9. iPad Remote Wipe and Restoration

There are API's that allow a remote wipe of data, and API's to initiate a wipe based on authentication failures. The ability to wipe remotely a device you need a vendor supplied MDM, there are no free tools available from Apple to wipe remotely a device. Testing authentication failures to trigger a device took a few minutes to complete. A quick mount of a "wiped" iPad did not reveal any data available. There were not any extensive tests to see if there was data available. When the system completed the wipe, there was message saying the user needs to connect the system to *iTunes.* An active internet connection is a requirement for a device restores, trying without an active internet connection results in failure. A backup on a computer without an active *iTunes*

connection will not work. The iPad connects to the *iTunes* and then restores the files.

When the iPad completes the restoration, the device is unlocked and not protected by the password of the device. If you wait a few minutes and let the iPad lock, your previous password still works and all the settings are in tact. During testing of the device, the restoration process did not restore any iPad applications; the applications required synchronization from iTunes.

10. Data Loss

The issue of data loss is perhaps the largest security issue with the iPad. The tight coupling of the iPad with iTunes allows the storing of corporate data nearly anywhere. It is likely a user will end up downloading company data onto their iPad. If the user backups their iPad, and thus the company data to a home system, the corporation no longer has control over that information. The information at rest will be at risk on the home computer. When the user leaves the company, there is no easy way for a company to remove their data from an employee's personal assets. There is no logging or audit trail available for data owners to track where their data resides. Loading productivity tools onto the device allows documents to reside locally on the iPad and end up on a backup once when the user backs up the device. Productivity applications such as *Pages* integrate with *MobileMe iDisk* allowing the storing of data on a remote site.

Google and other third party sources are starting to make document access available to iPad users. This opens a DLP issue if mobile users start storing confidential documents on third party servers such as Google Docs. If there is a compromise with the third party hosting vendor, corporations have little control over data. On a home computer, the iPad resembles a large external storage device. There are iTunes applications that allow users to mount drives and move data around. During the writing of this paper, none of these applications underwent any extensive testing. Starting with iOS 4.X, there is a native application called *AirPrint* that is available in iOS for printing data from an iPad. Users can easily use an iPad to transport confidential data outside of a company and simply

print the data on a home printer. There is no audit trail for documents printed from the device.

Consider the case where an employee leaves a company either voluntarily or through a dismissal. The employee leaves the company and surrenders their iPad prior to separation. The employee was diligent about keeping current iPad backups on their personal computers. The employee obtains another iPad and they can restore all the data from the surrendered iPad onto the new device. The previous employer will have no idea or tracking method to stop this action. This is an easy business decision for Apple, if they make restoration of backups to other iPad is difficult; there is no incentive for consumers to buy the latest device offerings from Apple. Consumer bought products and should be able to move those purchases to other devices if they upgrade their devices. Maybe in the future companies can work with Apple to produce data encryption on company owned data requiring a key from the company to decrypt it. Employees who no longer have ties with a company would not be able to decrypt the data.

11. Email

E-mail communication is part of business, society, and personal lives, a mobile device would not be very mobile if it did not offer e-mail services. The iPad allows user access to corporate and personal e-mail. The iPad has native support for the following e-mail services:

- Microsoft Exchange
- Mobileme
- Gmail
- Yahoo!.mail
- AOL

There is the likelihood of corporate data co-existing with personal data and potentially data from other companies. Most users will have multiple e-mail accounts setup on the iPad device for both personal and business use. It is common practice for one user to have several different e-mail addresses, each with a unique purpose. Once the user does a backup of their iPad, e-mail is part of the backup. With employee separation there is no

way for a corporation to verify company data no longer resides on non-company assets such as an employees' personally owned computer.

With iOS 4.X Apple provides API's that provide the ability to remove only corporate e-mail data and leave personal e-mail alone. This functionality and API's was not available for iOS 3.X. Most thirty products used to manage mobile devices will incorporate the ability to remove corporate data and leave personal data untouched. One thing that users may initially find confusing is how e-mail works on the device. For POP3 e-mail services, the iPad downloads e-mail but does not do any synchronization with the POP3 server. IMAP e-mail services do synchronize the iPad with the service. Lotus Traveler and Microsoft ActiveSync do synchronize e-mail that users access and manipulate via the iPad. There exists no option to setup an automatic mail forward from any of the e-mail clients. However, this does not stop anyone from doing a manual forward of company Intellectual Property to an e-mail account that is not under the control of your corporation. There is an exposure of certain settings because they are visible to users, such as information on ports, servers, and e-mail type.

If a corporation makes there e-mail available to mobile devices, any device can connect as long as the user has valid credentials. This is an exposure and a risk to all corporate data. A malicious employee can connect to the e-mail server download their e-mail, contact information, and calendars on any mobile device and there is nothing a corporation can do, unless they are using MDM software to govern device and user access. This case really drives the business case for purchasing Mobile Device Management software. Without having the software to protect who and what devices are accessing sensitive e-mail data, there is a serious risk of losing sensitive data. MDM software normally has the ability to send a remote wipe command and remove data in the event the device is lost or the employee separates from the company. The MDM software can wipe all data or only the company owned data.

If a company outsources e-mail services, the use of mobile devices and the use management software becomes more complicated. Companies will need to investigate

what controls are available to protect sensitive data, and reduce risk to company Intellectual information. There may be cases where the use MDM software does not fit into the architecture of e-mail. This important consideration requires diligence.

12. Cellular Data

If you are lucky enough to have a 3G model iPad, you have the ability to use an AT&T cellular network connection. As of this writing, AT&T is the only cellular carrier available for iPad devices. There is no way to disable this option; if you have the 3G, you can use the cellular option. Users can disable the 3G service, but there are no API's available to remove the functionality. Having cellular service is convenient and is likely to be a business requirement for most mobile workers. Cellular connections provide a competitive edge by allowing mobile workers to stay connected to customers. Cellular connections from the iPad to the cellular carrier are somewhat safe. Sniffing cellular data is illegal, expensive, and requires technical depth. The chances of traffic attacks from the iPad to the provider are slim, but not impossible. Once the data reaches the provider (AT&T) network, the data is no longer safe since it is on the Internet backbone. When the iPad has both a Cellular and a WiFi connection, it will use the WiFi connection by default. Third party tools do not provide a way to force one connection over the other.

The exposure to sniffing traffic over a cellular connection is there, but there is little risk due to the complexity and expense needed to sniff cellular traffic. Setting up the equipment to sniff cellular networks will cost over $1000 U.S. dollars, and congress passed a law in the late 1990's making cellular traffic sniffing illegal even for security researchers. Attackers with the ability to sniff Cellular data would likely be highly skilled and difficult to stop if they really wanted to steal data from your iPad.

13. Location Services

Location services allow geo-specific applications such as Maps to use information from cellular, GPS, and networks to determine an approximate location of an iPad.

Location services uses information collected anonymously in a form that does not personally identify you. Apple reports this information is anonymous and does not personally identify anyone. There are no API's to configure this feature; it is directly under the control of the user and is active by default. Some applications use location services to gather information based on your location. Maps are an example of an application that uses Location Services to gather data based on the iPad's location. A 3G model iPad uses cellular data, a GPS and local Wi-Fi network information to determine your location. If the iPad is not a 3G model, local Wi-Fi information is the basis for calculating the approximate location of the device. This service does lessen battery life, so disabling this feature if you are starting to run low on the battery may slightly increase the battery life. If the user is in a high security area, the user may need to disable this feature. Maybe a nation-state would have the funding to use location services to locate individuals or devices, but the work force should not be targets of hostile nation-states. For a mobile workforce this feature seems like a nice business addition. The ability to leverage location services while traveling to a client can help a mobile worker. (Kane-Parry, 2010)

14. Wi-Fi

The iPad is a mobile device that at a minimum includes Wi-Fi connectivity. There are API's that allow corporations the ability to configure known Wi-Fi hot spots for users. However, there is no way to prevent a user from configuring a Wi-Fi connection to the device; there is no API available to remove configuration ability. This allows users to connect to available Wi-Fi connections when they are available. Sniffing and cracking Wi-Fi traffic is trivial. This opens users to MITM (Man in the Middle) attacks and possible data theft. The iPad alerts users to active Wi-Fi connection by displaying three curved bars on the screen. The Wi-Fi configuration does allow the configuration of more secure protocols such as WPA2. As a note, when using Wi-Fi on an iPad, the device remains associated with the Wi-Fi access point while the iPad is asleep.

15. Forget this Network

The iPad has the ability to forget about networks that it had previous associations. The default action of the iPad is to remember and automatically join networks with which it had a previous association. An attacker may spoof a trusted network causing an iPad to join without asking a network if the device does not forget about the network after use. For networks with default SSIDs such as Linksys, the probability of joining a hostile network increases. This is another reason employees should configure home networks with unique SSIDs. The user must manually forget networks; there is no setting to forget automatically networks after each use. This setting offers nothing but laziness to for the user. Most users do not check carefully when connecting to networks, their attitude is, "if it is free, it is for me." This puts data at risk. Apple should have left this option out of the product. (Kane-Parry, 2010)

16. Ask to Join Networks

This setting displays a list of all available Wi-Fi networks available to a user if the user is no longer in range of a Wi-Fi network previously used. The iPad will list all available Wi-Fi networks and let the user choose which network they would like to join. If this setting is OFF, the iPad will join known networks automatically, if there are no known networks available the user needs to select a network. Forcing the user to configure a Wi-Fi network reduces the risk of having a device joining a hostile network with the same or similar name. This is a setting Apple should have active by default, and remove the ability for a user to override the setting.

17. VPN

A VPN (virtual private network) provides secure network access over the Internet between two points. The iPad can connect to a VPN using L2TP, PPTP, or Cisco IPSec protocols. The API's necessary for creating secure tunnels are the most guarded Apple has; with only the companies Juniper and Cisco having access to these API's under an NDA. Allowing mobile devices into a corporate network does not make sense and introduces risk to an organization. Mobile devices are young and immature at this point,

their very nature allows users to connect from almost anywhere. This gives users the freedom to connect from beaches, parks, and airports into the corporate network. An exploit that allows a nefarious user to gain control of an iPad or bypass security controls will have easy access into the network. Allowing internal access with an iPad that has little security controls does not make business sense. Not allowing VPN access will help reduce the attacking surface that malicious software or exploited iPads have. If corporate access is a business requirement, the best option for allowing access to internal applications is to use Citrix or a Citrix like product. This can shield the corporate environment and allow users access to applications and resources they need to do their jobs.

18. Bluetooth

The iPad has the ability to enable Bluetooth protocols to allow devices like hands-free headsets and keyboards the ability to interface with the iPad. Natively the iPad does not function as a phone, although there are applications available to enable voice communications. Enabling Bluetooth allows keyboard or headset access to the device. The latest version of iOS does have API's to disable Bluetooth and its associated devices. Disabling Bluetooth would lessen the attack surface, but many users prefer the convenience of wireless headsets when listening to audio from a mobile device. The iPad alerts users to active Bluetooth connections by displaying an interwoven triangle on the screen.

The exposure to sniffing traffic over a Bluetooth connection exists, but there is little risk due to the complexity and expense needed to sniff Bluetooth traffic. Setting up the equipment to sniff Bluetooth networks will cost over $1000 U.S. dollars, and sniffing Bluetooth is difficult because the traffic frequently switches channels. The sniffer would have to sniff all channels (full spectrum sniffer) in order to gather the traffic as it jumps channels. The bigger issue is a MITM (man in the middle attack) attack where an attacker tricks the iPad into pairing with a rogue attacker's device. The attacker can then inspect

al traffic as it flows through the rogue device.

19. Airplane Mode

The iPad has the ability to disable all receivers and transceivers. This is useful for high security areas where all communications must cease, for example on an airplane. There is no API available to disable this function, and even if there were, it would not be a good idea to prevent a user from entering *Airplane Mode*. Users will still be able to use their iPad even in high security areas, albeit without an internet connection, but at least the device is usable. When the system is running in *Airplane Mode* there is an icon of an airplane on the display.

20. Logging

One of the most powerful tools to help diagnose problems is logging. Logging is also critical to any audit, compliance and security regulations that apply to a firm or line of business. The iOS system is missing a native facility for logging application, security, and operational events. The iOS does not have any external applications or agents that enable logging of the device or applications on the device. A few examples of actions logged that would be helpful are records of backups, restores and synchronizations. Because of the wireless nature of this device, using a ubiquitous facility such as syslog is not practical. Apple should make a facility available resident on the device like a Windows Event Log. Then Apple could provide an agent or build in the ability to transfer logs when it connected to well-known environment. Having records of when an iPad backups, restores, and synchronizes data will help corporations know the locations of data off-site. This scheme is not full proof, but it does provide some benefits to a company in the event of employee separation or incident response. Regulated industries that adhere to federal regulations would have an easier time adhering to the regulations and designing policies to help protect firms while embracing this technology. Operationally, logging events would aid development and support efforts in the event

there are device or application issues. This is a serious flaw in the iOS offering that Apple should consider addressing in the future.

21. Set Screen Lock Banner

This is not really a security issue, but rather a potential cost savings. Most users have a personal picture or graphic as the screen lock wallpaper. Instead of creating a banner with personal images, creating a banner with the help desk number on it, for recovery of lost devices may save a few lost devices. This banner is simple but effective. User can implement this banner as a wallpaper under the configuration settings. There is no method to push and implement a corporate screen saver with third party tools. Other than a visual inspection, there is no tool to enforce displaying company approved banners on devices. A major problem with announcing a number or company on an iPad device is the possibility of social engineering attacks. A skilled social attacker can use the contact number to gather important reconnaissance about the target. There is a very pedestrian lost and found banner below. Apple should have a feature similar to Windows where the user can easily customize screen savers. (Baggett M. H., 2010)

22. Application Implementation

iPads that are not in a *jailbroken* state will only install applications Apple approved applications available from the Apple Store. Apple provides an iOS Software Development Kit (SDK) that runs on an Intel-based Macintosh computer. Developers

can create applications that once approved by Apple are available in the Apple Store. Apple implements an *Application Sandbox* for the applications running under iOS. This sandbox operates similar to a chroot'd environment under UNIX where the operating system jails an application into a particular file system. Under normal circumstances, applications from one sandbox cannot access data in another application sandbox. This measure will only protect applications from each other; it does nothing to protect an application against poor programming or design. Poor programming practices that result in buffer overflows receive no protections from a sandbox environment. Applications can use a feature that encrypts all its files when the iPad locks. This encryption leverages the hardware encryption available on the iPad. (Apple, 2010)

The iPad and other Apple products use a keychain to store passwords and other sensitive data. This data structure provides a secure, encrypted container for data. The system stores this data outside of the application sandbox and does not suffer any adverse affects when users upgrade applications. Prior to iOS 4.0, keychain data would only restore to the device that performed the backup. Now there exists a key*: kSecAttrAccessibleAlwaysThisDeviceOnly* that defines whether keychain data is capable of restoring to a device different from the one that created the original backup. If this key is not set, keychain data will only restore to the device that performed the backup. Application upgrades have no affect on keychain data, and maybe why Apple stores keychain data resides outside of the application sandbox. (Apple, 2009)

Applications available in the Apple App Store must go through an approval process with Apple. There are little details about what happens at Apple during the verification process. The application must work as advertised, cannot crash the iPad, and cannot use any private API's. With the amount of software now available, it seems there is a risk of having a smart developer slip malicious code by the review process. There have been a few cases of Apple removing applications, but it seems like a great attack vector.

23. Malware Protection

Early in the deployment of iOS 4.2 there is no facility available for malware protection on the iPad device. There is no Anti-Virus (AV), Host Intrusion Detection Service (HIDS), Host Intrusion Prevention Service (HIPS), firewall, or Web Application Firewall (WAF) available for an iPad. Several security vendors are planning to offer a WAF for the iPad in 2011. The application sandbox design does not lend itself well to malware protection on the device. Each application has its own sandbox, limiting it to the directory it resides. A malware application would need to have access to all the application sandboxes on the iPad so it could scan files and directories for malware. If the malware protection extends beyond scanning files, it would need access into the kernel. It would seem against the design model to allow such actions by an application. Maybe at some point Apple will collaborate with a vendor and bundle security services right into the iOS product. This would be a great marketing item, and would help adoption by corporations and help business oriented uses.

24. Adobe Flash Player

Many Web sites use Adobe Flash player to enhance the experience for the user. The iPad does not support Adobe Flash Player, making some WEB sites unusable. This was a business decision made early during the design of the iPad. There is no alternative, so the result is that sites using Adobe Flash player do not work as designed on an iPad. Although Adobe is frequently in the news for vulnerabilities, the reason for the lack of Flash Player support is to increase battery life. It seems this business decision ties back to improving the user experience and increasing sales because of the long battery life.

25. Safari Settings

Safari is the native browser on the iPad. The browser is an important component because it is the gateway to the Internet and helps drive many user experiences. Apple does have an API that will not allow the use of Safari by the user. The browser is available by

default, and the user needs to use third party tools to disable Safari. Although Safari does pose a business risk by allowing user to access nefarious and questionable content, not allowing Safari will reduce the business usefulness of the device. Internet access is a business requirement for a mobile workforce. Several options for Safari have a bearing on the security posture of the iPad.

AutoFill is an option that remembers data entered into common forms with the intention of automating form completion by the Safari browser. This feature is on by default. The iPad can set Safari to fill automatically any web forms using contact information, names and passwords previously entered, or both. The option "Use Contact Info" will use information from Contacts to complete fields on web forms. The option "Names and Passwords" remembers names and passwords from web sites visited, and will use this information to complete web forms when you revisit web sites. The option "On" specifies to use both "Use Contact Info", and "Names and Passwords." Disabling AutoFill can help avoid storing credentials increase the security risk of data loss in the event of losing a device, or having unauthorized access to the device. There is an API for controlling this feature, and most MDM vendors are including this in their product. It would be an improvement to have this setting disabled by default, and force the user to enable it.

Force fraud warning is an option to add a small level of protection against a possible fraudulent or compromised Internet site. Google maintains a blacklist of sites that determines whether a site is potentially fraudulent. If the user visits a suspicious site, Safari issues a warning and does not load the page. This setting will help protect the user and company against phishing attacks. This is on by default, and was unreliable during testing of the option. The results with this setting were no consistent, at times finding fraudulent sites and other sites labeled incorrectly. There is an API for controlling this feature, and most MDM vendors are including this in their product.

The ability to allow or deny JavaScript is an option in the settings, Safari allows the execution of JavaScript. JavaScript is a programming language that lets programmers

enhance the user experience on WEB pages. JavaScript often creates pop-ups, real-time dates, etc. Certain WEB sites may not work if with JavaScript disabled. There is an API for controlling this feature, and most MDM vendors are including this in their product. Disabling JavaScript would improve the security posture of the device, but will cause some sites not to function correctly. During testing there were a few smaller companies sites that did not work well, and slide picture display popular with media outlets did not work. Being practical most companies will need to enable JavaScript to have the devices function in the most business effective manner.

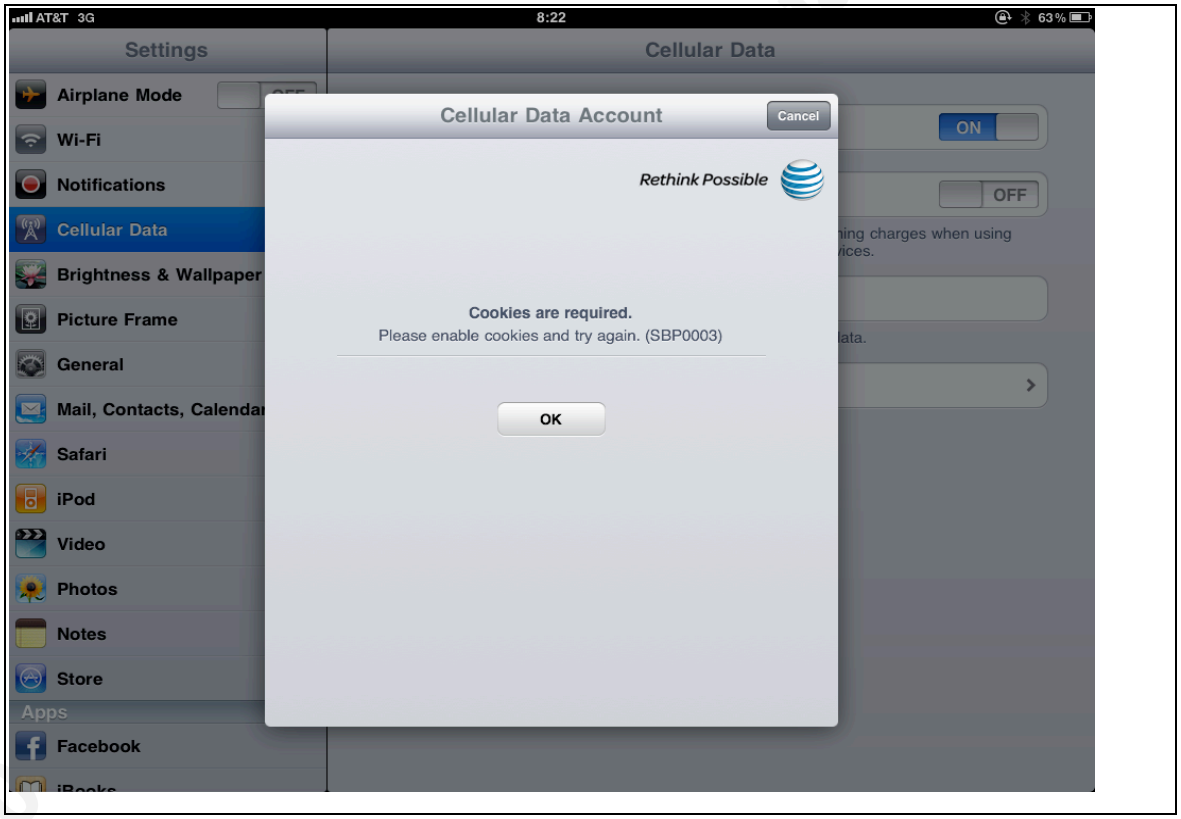
Nothing can ruin a user experience more than pop-ups. Pop up ads on the Internet are advertizing and marketing tools used by site owners to generate revenue. Both legitimate and less-reputable companies leverage pop up ads to promote products and services. Users find this parade of pop-up marketing and advertising highly annoying. By default, the iPad has a setting to block pop-ups enabled. This option, "Block Pop-ups," blocks only pop-ups that appear when you access a page by typing its address, or close a page. There is the possibility that certain features of a WEB site may not work because Safari is blocking pop up ads. Nevertheless, the benefit of stopping pop-up ads from polluting your display is a risk worth taking.

Cookies are files with information that a Website stores on the iPad so the device will remember certain things about you for future visits. Some Websites will not work if the device does not accept cookies. There are API's to configure how cookies work on the device. Here are the values available for configuration.

- Never
- From visited
- Always

The default value is *Always*, which allows a site to dump cookies not only cookies not only from their sites, but also cookies from sites of business partners. Behind the scenes a WEB site may be loading cookies from not only there site but others. A nice compromise would be have the default value be *From visited*, which restricts cookie downloads to only the company's site you are visiting. The browser will not accept

cookies from the WEB site the browser is visiting, third party cookies do not download. During testing, there were issues with having the device set to *Never.* Users manage their AT&T account directly from the device. When cookies are set to *Never,* the user cannot access the site because of the cookie restriction. If an executive needs to modify their credit card information, they cannot access the AT&T site with cookies set to *Never.* Imagine a sales person looking to close a large deal and the deal falls through because of a cookie restriction. The value of "*From visited"* should be the default by Apple since it seems to be the best security compromise. If a device requires higher security, the company can elect to change the cookie value to *Never.*



26. Content Restrictions

There is an interesting option that allows you the ability to restrict media content based on a movie rating system. This interesting option allows you to define what sort of media

content the device can access. During testing with content ratings, almost any rating restricts what content the device can access via Safari and YouTube. Morally it may be nice to have a protected device, but testing did uncover that the filters blocked a large volume of content, and not all of it was adult oriented. An adult user base should use good judgment on what is or is not appropriate content. Additionally there is a setting to block explicit music and podcasts. This will hide explicit music and video when a user is in the iTunes store. (Apple, 2010)

27. Push Notifications

Notifications address the issue of only allowing one application can run in the foreground at a time and having to alert the user about something. If an application is running in the foreground or background a notification lets users know there is something for them. Notifications differ depending on the application, but may include text or sound alerts, and a numbered badge on the application's icon on the home screen. This could be messages or data from a remote server. Applications use push notifications to alert you about new information, even when the application is not running. Notifications can be *local* or *push* depending on the need. *Push notifications*, commonly called remote notifications arrive from outside the device. *Local notifications* are local to the device and the target an application. Users can turn notifications off if they do not want a notification, or want to conserve battery life. There are API's for programmers to use notifications within programs. Remote notifications are a one-way data flow that contains two pieces of data, a device token and the payload. Remote notifications use Apple Push Notification Service (APNs) to route messages. The device token enables the APNs the ability to locate a device. Each device establishes an accredited and encrypted IP connection that remains persistent. Notifications travel over this channel; the token in the message locates the correct device and delivers the payload. Alerting of the application occurs by the payload which is a JSON-defined property file specifying the alert details. Remote notifications use Wi-Fi only if a cellular connection is not available. APNs require two different levels of trust known as trust and token trust for providers, devices, and their communications. A connection trust is a certificate that provides

assurance the APNs connection is with an authorized provider that Apple has agreement with to deliver messages. The token trust provides assurance of accurate message routing. The device token is an identifier the APNs gives to the device when they first connect. This token is part of the notification from the provider allowing the APNs to deliver the message to the correct target device. If an attacker can exploit this model and deliver malicious payloads, the attacker can dictate behavior of some applications. (Apple, 2010)

28. Support Issues

Most corporations treat and define security as minimizing risk to the firm. There is no doubt that introducing mobile devices will introduce additional risk to the firm. Along with the obvious dangers, there are additional support costs that firms should be ready to handle. Asset management will become an issue unless a third party tool is managing devices. The Apple ICU is not a tool to help with management of assets; it can build profile but not manage much beyond profiles. Firms should have a tool that forces devices to connect to a management server and enforce policy settings. ICU only creates profiles for users, once the user install the profile, there is nothing forcing the device to check in or enforce policies. Concerning asset management, the device will take the name of the profile created in ICU or a third party tool. If the profile has the name "*SANS Gold Build,"* then the iPad device will assume the name *SANS Gold Build* when the user docks it to a computer. Devices sharing the same profile will have the same name creating an asset management and ownership problem. There is no ability to name individual devices with names useful for asset management. The Apple serial number is the only unique identifier companies can use for asset management.

When setting up and registering an iPad, the user must have an active iTunes account to complete the setup. The final stage of the setup requires either a credit card or iTunes gift card to keep on file. This forces users to surrender sensitive information just to start using the device. Maybe as an added incentive, corporations will give users an iTunes gift card for a small amount of money. This is an additional and possible hidden cost to corporations deploying mobile devices.

There will be non-technical users who will have trouble using the newer mobile technology. Their ignorance is going to result in mistakes and calls to support desks for help. These added calls add cost to running a help desk.

Finally, there is the issue when there is the issue of breaches and exploits. Incident response is more difficult because of the mobile nature of the device, and the myriad of places Intellectual data may reside. If there is a large-scale exploit of iOS, making sure devices and user are safe will require resources. For example, in 2010 AT&T had a breach that revealed e-mail addresses and credentials for authentication onto the AT&T network.

29. Conclusions

The mention of adding mobile devices into a corporate infrastructure is reason for concern from the security and risk departments. Instead of becoming a hindrance to accepting a new way to do business, corporations at all levels should embrace the mobile technology and work together to limit exposure from the devices. It is clear that mobile computing is here to stay and will continue to become part of normal business operations. The security controls built into the iPad iOS 4.X are poor and are easy to override. Of all the major device vendors, Apple spends the least amount of money on security, and it shows. This is a flashy consumer device that is becoming a business necessity; the security of the device needs to catch up with the business demand. Integrating the iPad into business operations without a MDM (Mobile Device Management) tool is irresponsible. The user has the ability to modify nearly any setting they desire, and jail breaking an iPad with an ICU profile is trivial. The MDM software helps enforce policy and reduce the labor required for deployment of mobile devices.

The most disturbing item found was the inability of the device to mask characters while entering a password. This appears to be a "feature" of all touch screen keyboards. Android devices also suffer from this malady. It seems the echoing of characters as users

touch them allows poor touch screen users, or users with fingers like sausages to see what key they hit. Shoulder surfing is trivial with the device, and will be made worse with the alphanumeric password requirement. This character echo also appears on Safari pages that require authentication.

The device fails to meet several best practice requirements with version iOS 3.X running on the device, be sure to have the latest version of iOS running. Users who work for multiple companies may end up with conflicting security policies. If there is multiple security policies (policies) applied, the strictest policy wins. This also means there maybe data from competitors existing on the same device.

Having a breach on the device will create a headache when it comes to determining what happened because this is a mobile device.

Access to corporate resources should only occur through a gateway such as Citrix. This would allow corporations to "publish" business critical applications and lessen the chances of malware entering the environment via a mobile device. Having an Intrusion Detection System or Deep Packet Inspection firewall inline on the inbound mobile device network would provide additional protection to corporate assets.

Finally, there is no way getting around iTunes and the whole Apple suite of applications. Apple is consumer oriented and should start to make a business friendly device. Beside Blackberry, there is not a vendor that is very business focused in the mobile device market. As security professionals, we need to understand and embrace mobile technology to help business gain an edge of competitors.

30.

References

Apple. (2010). *Apple - iPad - View the technical specifications for iPad.* Retrieved 12 03, 2010, from Apple Computers: http://www.apple.com/ipad/specs/

Apple. (2010, 04). *Enterprise_Deployment_Guide.pdf.* Retrieved 09 03, 2010, from Apple: http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf

Apple. (2010, 11 15). *iOS Application Programming Guide.* Retrieved 12 14, 2010, from Apple: http://developer.apple.com/library/ios/documentation/iphone/conceptual/iphoneosprogrammingguide/iPhoneAppProgrammingGuide.pdf

Apple. (2010, 04 19). *iPad_User_Guide.pdf.* Retrieved 07 29, 2010, from Apple: http://manuals.info.apple.com/en_US/iPad_User_Guide.pdf

Apple. (2009, 09 09). *iPhone and iPod touch: About backups*. Retrieved 11 01, 2010, from Apple: http://support.apple.com/kb/HT1766

Apple. (2010, 12 26). *iPhone Configuration Utility.* Retrieved 12 28, 2010, from Apple: http://developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility/Introduction/Introduction.html

Apple. (2009, 10 19). *Keychain Services Programming Guide.* Retrieved 01 03, 2011, from Apple: http://developer.apple.com/library/mac/documentation/Security/Conceptual/keychainServConcepts/keychainServConcepts.pdf

Apple. (2010, 08 03). *Local and Push Notification Programming Guide.* Retrieved 01 15, 0211, from iOS Reference Library: http://developer.apple.com/library/ios/#documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/ApplePushService/ApplePushService.html

Baggett, M. H. (2010, 06 05). *Master Degree in Information Security - SANS Technology Institute.* Retrieved 08 12, 2010, from SANS STI: http://www.sans.edu/resources/student_projects/201007_2.ppt

Baggett, M. H. (2010, 06 05). *SANS STI.* Retrieved 08 12, 2010, from Design Phase

One of an iPhone Rollout: http://www.sans.edu/student-files/projects/201007_02.pdf

Bejtlich, R. (2004). *The Tao of Network Security Monitoring: Beyond Intrusion Detection.* Boston: Addison-Wesley Professional.

Dev-Team Blog. (2011) *Dev-Team Blog.* http://blog.iphone-dev.org/

Elcomsoft. (2011) *Password recovery, forensics, system and security software from Elcomsoft: recover or reset lost or forgotten password, remove protection, unlock system*, http://www.elcomsoft.com/

Kane-Parry, D. (2010, 10 10). *CIS_Apple_iPhone_Benchmark_v1.2.0.pdf.* Retrieved 12 01, 2010, from CIS: https://www.cisecurity.org/tools2/iphone/CIS_Apple_iPhone_Benchmark_v1.2.0.pdf

Mayhemic Labs. (2010, 05 04). *Installing the metasploit Framework on the iPad.* http://www.mayhemiclabs.com/node/15

Oliver, M. (2010). *Mobility Management for Dummies.* West Sussex: John Wiley & Sons, Ltd.

Whalen, S. (2008, 10 13). *iPhone Forensics - SANs.pdf.* Retrieved 08 12, 2010, from SANS: http://files.sans.org/summit/forensics08/PDFs/iPhone%20Forensics%20-%20SANs.pdf

Wikipedia. (2010, 09 30). *IOS - Jailbreaking - Wikipedia, the free encyclopedia*. Retrieved 01 10, 2010, from Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/IOS_jailbreaking

Zdziarski, J. (2008). *iPhone Forensics Recovering Evidence, Personal Data, and Corporate Assets.* Sebastopol: O'Reilly Media.

Helpful Reference Sites

iPad Forums.net the Ultimate Apple iPad Site
http://www.ipadforums.net

M@D Mobile Active Defense
http://mobileactivedefense.com/

DEV-TEAM BLOG
http://blog.iphone-dev.org/

Jonathan Zdziarski's Domain
http://www.zdziarski.com/blog

Glossary

ICU – iPhone Configuration Utility is a free utility developed by Apple that can create user profiles for Apple iPods, iPhones, and iPad devices. These templates can improve the device security.

Jailbreaking is a process that allows iPad, iPhone and iPod Touch users to install homebrew applications on their devices by unlocking the operating system and allowing the user root access. Once jailbroken, iPhone users are able to download many extensions and themes previously unavailable through the App Store via unofficial installers such as Cydia. A jailbroken iPad, iPhone or iPod Touch is still able to use the App Store and iTunes. (Wikipedia, 2010)

MDM – Mobile Device Management is a solution using hardware and/or software to management on an enterprise level mobile devices such as iPhone, iPad, Android, etc.