



10 ENTERPRISE iPhone OS SECURITY BEST PRACTICES

Advantage Technologies Inc.

Website: <http://www.ATechnologies.com>

Phone: (866) 730-1700

With over 75 million iPhone OS devices in use, the odds are that someone is connected to your corporate network with an unauthorized iPhone or iPod Touch right now. There's nothing wrong with allowing your end users to access your network with an iPhone, provided that the device has the appropriate IT security settings. Left unsecured, the iPhone OS however can present security risks to both corporate and customer data. Stolen personally identifiable information or trade secrets is the last crisis any IT manager or executive wants to manage. The compliance risk alone is staggering. As a recent Aberdeen Group report detailed, a single compliance lapse (e.g., SOX, Privacy, PCI, HIPAA) can cost a company up to \$2 million USD. A single lost or stolen iPhone incident may encompass multiple compliance lapses. Authorizing, securing, and updating the iPhone OS should be a top priority.

The risk is real. Apple is diligent at fixing and patching security risks. But, is your mobile workforce or IT administrator as diligent at applying Apple's updates? An unpatched iPhone - not the iPhone itself - is the real security risk. In the last two iPhone OS updates alone, Apple identified and fixed 15 security risks.¹ Numerous iPhone Safari security patches were made that fixed the device's vulnerability to exploits from basic web surfing. More worrisome still is the recently repaired recovery mode vulnerability that allowed for someone with physical access to a device to bypass passcode and access user data. Additional remote attacks and security vulnerabilities are identified every month.² A secured and updated iPhone can empower mobile workers to be more productive than ever before.

There is good news: Apple has taken significant steps to improve iPhone security for the enterprise. You can implement a number of iPhone training, process, and IT best practices that greatly mitigate the security and financial risk to your company. In this white paper, we identify ten best practices that you should consider implementing immediately to best support iPhone OS devices.

Overall, we suggest that corporations that support the iPhone OS use Microsoft Exchange 2007 or 2010 with Active Sync and use Apple's iPhone Configuration Utility. Combining these two applications with other well-known certificate, directory, and authentication security services make implementing these best practices possible.

¹ <http://support.apple.com/kb/HT3860>,
<http://support.apple.com/kb/HT4013>

² Fisher, Dennis. "iPhone Vulnerable to New Remote Attack." Accessed on Feb. 2, 2010 at: <http://threatpost.com/>.

1. MONITOR FOR AND BAN JAILBROKEN IPHONES

Jailbroken iPhones and iPod Touches can represent the largest security threat to an IT department. A jailbroken phone is one that has been modified in order to use the device on non-issuing carriers. Last year, a worm (i.e., ikee-b) was launched that exploited an SSH service activated during the jailbreaking process.³ This was just the first of many likely attacks against vulnerable iPhones.

As an enterprise, it is best to monitor and disable jailbroken iPhone OS devices. There are several methods that can be employed. First, ensure that all iPhones are running the latest iPhone OS. Typically, it takes the hacking groups responsible for jailbreaking applications a couple weeks to exploit the latest iPhone OS. Disable or force that older OS versions are upgraded before being allowed back on the network. Next, perform periodic network scans for port 22 (SSH's port) on Wi-Fi networks where iPhones can be connected. Finally, certain jailbroken phones will register using old or manipulated HTTP user agents, such as: "Cydia/1.0.3044-65." Constantly monitoring for and disabling jailbroken devices will help mitigate many known and easily created exploits.

³ Skipper. "Protect iPhone 3GS Against ikee attack." Accessed on Feb. 2, 2010 at: <http://www.redmondpie.com/protect-iphone-3gs-against-ikee-virus-attack-9140090/>

2. REQUIRE EXPLICIT IPHONE ACCESS PERMISSION AND CORPORATE DATA ENCRYPTION

Require each mobile user to explicitly enroll and configure both employee- and company-owned iPhones. Managing over-the-air enrollment and configuration for the iPhone is possible via the tools provided by Apple. IT departments must create their own iPhone Profile Distribution Service that accepts HTTPS connections, authenticates users, and creates iPhone mobileconfig profiles. Users with new, recently activated iPhones can access a simple URL (e.g., <https://iphone.company.com>) via Safari to make the enrollment process seamless.

We recommend that you disable those default Microsoft Exchange mobile access protocols that allow for normal authentication. Authorization and authentication should be handled via a Public Key Infrastructure (PKI), corporate authentication services (e.g., ActiveDirectory), and a Simple Certificate Enrollment Protocol server. This allows for secure profiles to be installed on the iPhone, ensuring that only those authorized are able to access the corporate network. As is true with other remotely accessed corporate applications, mobile applications should only be accessible through a secure and encrypted connection (e.g., Mobile VPN). The iPhone supports the following VPN protocols: Cisco IPSec, L2TP / IPSec, and PPTP.

3. TRAIN EMPLOYEES ON IPHONE DATA SECURITY

Every employee who has an iPhone should undergo training on not only how to configure and use the device, but also what to do if the device is lost, stolen or compromised. Trainings can be delivered online or in person, and need to stress the importance of immediately contacting the IT department as the moment a device is lost or stolen. Training employees how and when to react to security issues could save your corporation millions of dollars in security and compliance breaches.

4. MANAGE IPHONE EMPLOYEE DEPARTURE DEACTIVATION QUICKLY

Many times a corporation's IT department fails to immediately disable mobile access to a terminated employee's corporate applications or email. Ensuring that deactivation happens simultaneously with an

employee's departure or termination is critical to protecting a company's intellectual property and essential to meeting regulatory compliance requirements. Remotely wiping the employee's mobile profile and disabling Exchange Active Sync (EAS) are critical steps to minimizing exposure on employee-owned devices.

5. CONFIGURE AND ENFORCE IPHONE SECURITY POLICIES

Always secure and restrict iPhones. Like any other network-connected system, an iPhone must have well-defined security policies that are monitored and enforced. By using the iPhone Configuration Utility, you can create profiles for different organizations (e.g., sales, marketing, engineering) that have different payload settings. Payload settings define a collection of individual settings for certain purpose, such as VPN settings. Policies can be created for the iPhone that comply with other mobile phone security policies, including: passcode requirements; Wi-Fi settings; application and hardware restrictions; email, calendar, and directory settings; and, credential settings.

Profile compliance is checked whenever a user connects to the corporate network. Profiles can be configured to periodically expire to ensure that new profiles are requested when dormant devices access the network again.

6. TRACK WHICH IPHONE OSS ARE CONNECTING TO THE NETWORK

It's hard to manage and secure devices if you have no visibility around what devices are connecting into your network. Tracking and ensuring that security policies are created for both older and newer iPhone OS devices will help your network remain secure and uncompromised. Old iPhone hardware (i.e., < 3GS) and OSes are more open to security exploits and encryption problems. Rapidly managing corporate device and OS upgrades helps minimize the risk of well-documented exploits. Apple recently announced the iPad, which will start connecting to corporate networks in March. Proactively establishing profiles and security settings for the iPad before it shows up will help manage risks new devices typically present.

7. TRACK WHO HAS ACCESS AND WHAT TYPE OF ACCESS THEY HAVE

Always track who has access to your corporate network. Changes in 2006 to the United States Federal Rules of Civil Procedure now require maintaining a full record of electronic data used for any business correspondence. Failing to comply is costly in the US. That said, European Union Directives (i.e., 95/46/EC) strongly protects personal data and such data cannot be collected. Managing regional security and privacy policies is critical to managing legal risk.

Beyond legal requirements, knowing what type of access each user or iPhone has can help isolate and disable suspicious devices before a single security incident becomes a security crisis. To help with isolation, Wi-Fi networks should be segmented. Some organizations have even created special Wi-Fi networks for mobile devices to further minimize this threat.

8. CAREFULLY MANAGE PROVISIONING & UPDATES TO CORPORATE APPLICATIONS

Apple's iTunes can be configured to only install what software your company requires. For example, omitting Bonjour from users' desktop or laptop could eliminate other network security threats. iTunes's features can also be restricted. Using Microsoft's Group Policy Object Editor, you may adjust iTunes's registry settings to restrict users from: updating iTunes or iPhone OSes automatically, syncing devices, accessing the iTunes store (including the AppStore), and accessing explicit content. This level of control can eliminate potentially problematic third-party applications from being installed.

iTunes is also used to back-up iPhones. All encrypted profiles automatically use AES256 when being backed up. Applications your company develops itself can also be distributed and updated based on Enterprise Distribution Profiles. While the actual application will not be backed-up using iTunes, any application data created is backed up. Users must manually download and drag enterprise applications into iTunes for them to be synchronized with the device. Only AppStore applications may be installed without additional user interaction. Strictly managing enterprise and third-party applications often eliminates security risks and support hassles.

9. CONFIGURE AND ENFORCE AUTO-LOCK, PASSCODES AND REMOTE WIPE POLICIES

Requiring strong passcodes and auto-lock policies is strongly recommended, especially for companies that do not require a password or an authentication token to access corporate services. Exchange 2007 is your friend when it comes to managing and updating iPhone device policies. The iPhone's integration with EAS allows you to: enforce device passcode and auto-lock, specify passcode complexity, auto-wipe after four or more failed attempts, and enforce policy updates and device encryption. Auto-lock after a certain number of minutes of inactivity can also be remotely set using an EAS policy. Policies set by EAS are easy to maintain and are automatically updated.

10. PROACTIVELY MONITOR FOR SECURITY BREACHES, MALICIOUS ATTACKS AND COMPLIANCE VIOLATIONS

Deploy a proactive mobile infrastructure monitoring and reporting system to warn of recent attacks or suspicious behavior. According to the Aberdeen Group, best-of-breed IT departments support an average for 3.3 different device types. Deploying a solution to uniformly manage iPhones as well as other platforms (e.g., BlackBerry, Windows Phone, and Android) will help you minimize security and financial risks that these devices cause in your enterprise.

ABOUT ZENPRISE

Zenprise®, a provider of enterprise mobile device management software, provides real-time visibility into the most critical iPhone security threats. Zenprise MobileManager™ allows IT departments to identify who is using an iPhone, how the iPhone is accessing the network, and what version of the iPhone OS is installed. Security policy and compliance reporting capabilities ensure that unauthorized, non-updated, or non-compliant iPhones can be isolated and blocked from the network. Enterprises will also be able to centrally authorize, provision and apply uniform security policies from MobileManager for any iPhone device.

MobileManager also provides end-to-end proactive monitoring and troubleshooting capabilities that guarantee iPhone users are always productive. Zenprise already helps hundreds of the largest global companies and the most clandestine government agencies deliver secure and 100% compliant iPhones to their mobile workforce. Join them. Learn more about Zenprise's Enterprise iPhone Security.