

DEEPER INSIGHT

**PRESENTED BY ROOK**

**SECURING**

**iDEVICES IN THE**

**ENTERPRISE**



Michael Ivy

# IOS Devices

by Michael Ivy

12-April-11

If you haven't been listening, there's a quiet wind blowing in the operations of many enterprises. Sure, there have been loud demands and often shouts of "just make it work", but the small wind is change. The change we are seeing is that iPhones, iPads, iPods, iYou-Name\_It...are being incorporated into the enterprise. Not simply because they are a status symbol, but because they can also increase productivity and often supplant the need for a laptop for those that only need to be effective while they are mobile without requiring a full desktop replacement. However, most security professionals have resisted this change since the beginning..

Today we are seeing large banking, healthcare and other similarly regulated and or security conscious companies embrace these IOS devices and roll them out within their enterprise environments. Some even developing customized mobile apps to tie directly into their enterprise systems. Why, because Apple has been working to become an enterprise company outside of the traditionally more open educational/creative space. They have developed deployment guides and tools to enable administrators to configure these devices with security in mind. Items such as requiring passwords, automatic locking of the device, a full erasure of data upon excessive failed login attempts and even remote wiping capabilities once only available on the ubiquitous BlackBerry are now available for current IOS devices.

Expanding on these basic security features - further enterprise functionality includes Exchange support, VPN connectivity and enterprise WiFi configuration through profiles with certificate-based authentication. These are beginning to add up to a potent package that may allow for the average user to be more efficient and remain securely connected to the enterprise while looking cool doing it.

Securing an IOS device for the enterprise is not much different than securing the device for personal use. The scale of work however is much greater as implementing security controls must be consistent and efficient. To help with IOS configuration Apple has updated the iPhone Configuration Utility to support the iPad. The configuration utility is offered in Windows and OSX flavors and creates .mobileconfig profiles to be loaded onto the IOS devices. These XML profiles contain security policies, VPN configurations, WiFi

settings, APN, Mail, Exchange configurations and certificates that will allow for your current IOS device to connect to the enterprise.

So what are the quick steps to securing an i\* for the enterprise:

1. Update the Firmware
2. Require a strong password (require passcode and require alphanumeric)
3. Set the auto-lock timeout
4. Disable the grace period for lock
5. Enable data erasure upon excessive login failures
6. Enable the fraud warning for Safari
7. Enable data protection

But, there is a catch - as there always is. With any device you must maintain proper physical security controls. A recent demo has shown that an iPhone in the hands of an attacker can have its password harvested in around six minutes. The same can be said for just about any device - if an attacker has physical access to your device, it's not your device any longer. I did mention remote wipe - and this \*may\* be an option, but reports are that it is tenuous at best as it requires several configuration options and an active connection to the Internet. Remote wipe may be made more difficult in the enterprise as end users have to notify someone that they lost the device. Will the devices be reported missing and will your processes allow for the initiation and completion of a remote wipe in less time than it takes to jailbreak an i\* and reveal it's password, ergo it's contents? I once had a systems administrator take more than three months to report his BlackBerry as missing...

Going back to item 7 in the security configuration list - Data Protection - should not be taken as a panacea. Data Protection only offers encryption (with a key derived from the user's passcode) for applications that are aware of the Data Protection functionality - so be careful what data you keep on the device. [More about Data Protection](#). Other challenges exist as well:

1. Securely connecting to enterprise wireless - certificates versus passphrases
2. Application provisioning
3. Authentication schema integration
4. Auditing and accountability

## Delivering What Matters: IOS Devices

5. Secure development practices
6. Enhanced investigative and response abilities (local or outsourced)
7. OSI Layer 8 (remember that's politics) - can the device be used for personal use?

Tackling these other obstacles will take time and investment to get them right, and you may find that these devices can be made to work securely in most environments. However, if your appetite for risk is very low and you have a high security environment you may have to lock down the device so much that it's extensibility outside of the primary use case is removed altogether. As with any new technology or technological shift, proceed cautiously and modify the system (people, processes and technology) to find an acceptable amount of risk. The answer may just be that these devices don't fit the corporate appetite for risk - even if they are cool. In the end, you'll need to revisit policy and procedure, configure the technology and train the people responsible for administering, securing and using the new technology.

## How We Help Companies Succeed

Rook provides IT Risk Advisory services that support log management initiatives for organizations at various phases of maturity in their overall monitoring program. Whether your organization is dealing with an emerging regulatory compliance effort, or if you are looking to improve upon your existing program, Rook can provide the methodology and team members with the technical, audit, and management strategy expertise required for success.

**Readiness Review** - We assess the current state of controls to the desired state of controls to support management strategy, sales enablement, or general compliance efforts. Whether for HIPAA, HITECH, ISO 27002, SOX, PCI, GLBA, FISMA, NIST, or a myriad of other regulations and standards, we provide the knowledge and experience necessary to identify the approach best fit to your organization and prioritized to guide compliance efforts.

**Requirement Definition** - Working closely with your management and technical teams, we provide experienced professionals who identify the business and technical requirements necessary to a successful log management initiative.

**Data Mapping** - Whether the scope is known or unknown, we work closely with process owners, system owners, and data owners to determine the data flows for critical and sensitive data, then identify the infrastructure that is in scope

based on the data location when at rest, in use, or as it traverses the network.

**Control Identification** - When the data mapping is complete and in-scope infrastructure has been identified, controls are identified throughout the process. Identified controls are compared to the desired future state in a gap analysis, and then gaps are documented, and prioritized based on the requirements, budgetary constraints, existing technology, and human factors such as knowledge and internal politics.

**Vendor Selection** - Requirements are utilized to create Engineering Requirements and a resultant vendor selection matrix. Vendors are reviewed to determine adequacy based on analyst guidance, past experience, internal contacts, and marketing materials. Vendor capabilities are documented, analyzed, the proposal process managed through vendor selection, contract evaluation, and project plan creation.

**Health Check** - The existing implementation is reviewed to determine if the end-to-end process, team members, and technology (comprising of the Monitoring Program) is operating at optimal efficiency. Areas for improvement are identified, technical configurations are updated, process improvements are managed, documentation updated, and training conducted.