



iPhone Security
Risks with iPhone Integration
in an Enterprise Environment



Introduction

Apple introduced the iPhone in 2007 and appealed to a large number of consumers. IT departments in many corporations were asked by its employees if the iPhone could be rolled out within the organization. With the integration of the Microsoft Exchange extension and ActiveSync feature Apple gave a clear signal to the enterprise market that the iPhone is a viable device. Steve Jobs made several announcements in the beginning of 2010 indicating Apple's roadmap to extend support of the iPhone for business use and enterprise application development.

The iPhone is already on the radar of the business world but the integration of the device into enterprise IT has not been as easy as it has been with other mobile handhelds. Furthermore, security questions have not yet been the first priority in the enterprise discussion. Therefore, IT departments are facing the challenge of integrating iPhones into the corporate mobile communication platform supporting e-mail, calendar and business applications.

Two basic scenarios can be considered as operating models when integrating iPhones into enterprise communication:

- a) Corporate IT distributes the device to its employees. The IT department is fully responsible for the implementation and system management.
- b) Employees own their iPhones and are allowed to connect to specific collaboration services, like e-mail, address books and calendar functions.

The selection of the scenario depends solely on the business needs of the enterprise; however, scenario b) appears to raise more organizational security issues in the management of the devices.

This whitepaper gives an overview of the current security architecture provided by Apple and potential solutions and risks when integrating Apple iPhones in an enterprise environment.

The Integration of iPhones

Scope

For enterprise environments the iPhone-architecture currently only supports push mail and a centralized password policy if operated in a Microsoft Exchange environment. Therefore, this paper focuses only on this type of architecture.

The security of iPhone Apps as well as the iPhone App Development process are not part of this document but should be part of a competitive enterprise specific risk assessment.

General Considerations

Information Security

Mobile devices can host business as well as private information in form of e-mails, contacts, calendars and documents. They are used outside the secured company perimeter and have the tendency to get lost, as lost and found statistics prove on a frequent basis. Therefore, the adequate protection of local data stored on the device as well as communication channels is essential to information security. Un-authorized access to the mobile device or its data might be abused to obtain business critical information or to get access to the company's IT infrastructure.

Secure Device Management

Another very important issue is the remote deployment and control of settings and restrictions on the iPhone. Without centralized management of the iPhones' security features and settings as well as automated update processes there is a risk that iPhones could run on outdated or insecure software versions or might not be configured according to enterprise policies.

General System Requirements

iPhone Configuration Utility

Apple provides a configuration generator for the iPhone which is called the iPhone Configuration Utility. It supports the IT department in generating configuration profiles and deploying them onto the iPhones. The deployment can either be done directly via USB, by mail, per download or via SCEP (Simple Certificate Enrollment). However, as Apple does not provide any kind of enterprise integration services, there is a strong need for additional systems to enable the central IT to distribute configuration profiles and certificates.

Microsoft Exchange Server 2007 ActiveSync

Microsoft Exchange Server 2007 with the ActiveSync extension is required as a collaboration platform to enable

the latest security features of OS version 3.1.X which is installed on the iPhone 3GS hardware. The platform enforces most of the password policy settings.

Infrastructure Requirements

The following additional technical requirements or software must be implemented to ensure secure iPhone integration as recommended by Apple:

- Cisco ASA Security Appliance as VPN Concentrator/ Cisco stand-alone VPN Concentrator (recommended by Apple to secure the communication channel via VPN)
- iPhone 3GS with hardware encryption
- iPhone OS 3.1 or later
- Certificate Enrollment and Revocation List Server (SCEP, OCSP, SCVP)
- Root CA
- Apple iTunes Software
 - The software as such is not a security component but is necessary to roll-out and update software on the device
 - Depending on the integration requirements iTunes has to be installed on each client computer of the iPhone user. Alternatively iTunes may be installed only on administration computers, although this would require that administrators receive physical access to all iPhones to perform the updates.

Operational Requirements

Since Apple does not provide additional management tools besides the iPhone Configuration Utility and the ActiveSync integration, a secure integration and operational architecture requires additional procedural elements. The key elements are, but are not limited to:

- secure methods for configuration profile deployment which are not covered by iPhone Configuration Utility
- mechanisms which help to identify if a user has accepted and installed a configuration profile
- mechanisms which enable the IT department to monitor the relevant settings on the managed iPhones

Secure Architecture and Integration Samples

To support the security requirements of most standard business environments Apple recommends a combination of platforms that are based on the above mentioned software tools and implementations. The following three architecture samples highlighted below serve the described use cases:

- Microsoft Exchange 2007 ActiveSync – for access to e-mail, calendar and contacts in an Microsoft Exchange Environment (Lotus Notes extensions are currently not available)
- VPN Remote Access – for access to the company network and resources
- WiFi Access – wireless access to e.g. the company network, internet or as a VPN entry point

These implementation samples serve as basic blue prints. It is recommended to implement additional security measures as listed in the section Additional Security Measures.

Please note, that the recommended platforms do not address application security and the protection of data residing on the iPhone.

Exchange 2007 ActiveSync

The iPhone Exchange communication secured by 128Bit SSLv3 and signed certificates, is a secure way to access E-Mail, Calendar and Contact data (see figure 1).

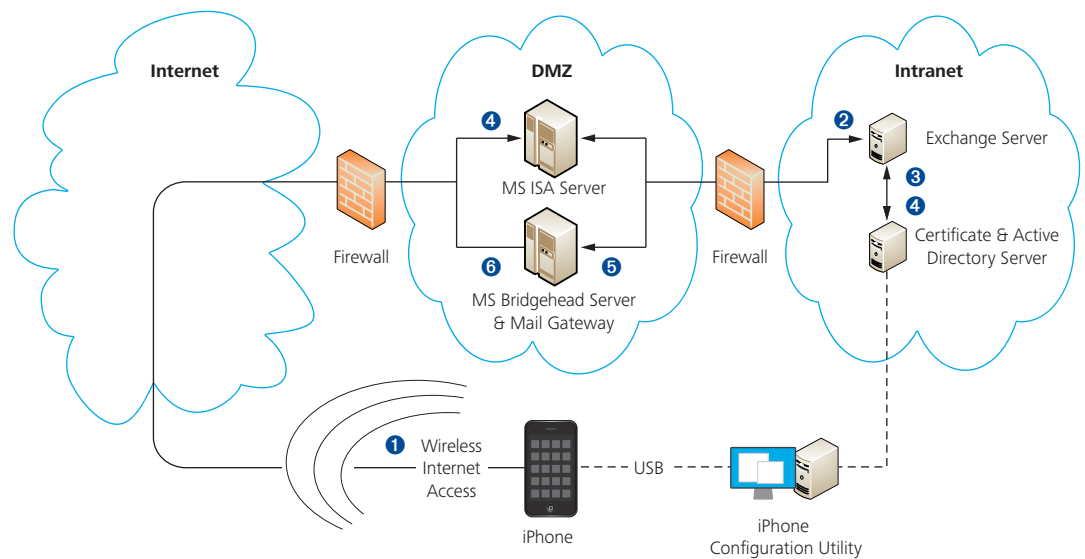
VPN Remote Access

Accessing the company network by VPN is a straight forward process following standard mechanisms also used by regular IPSec VPN Client Computers (see figure 2).

WiFi Integration

Integrating the iPhone with the companies WiFi networks is done in the same way as integrating any other Wireless Client Computer (see figure 3).

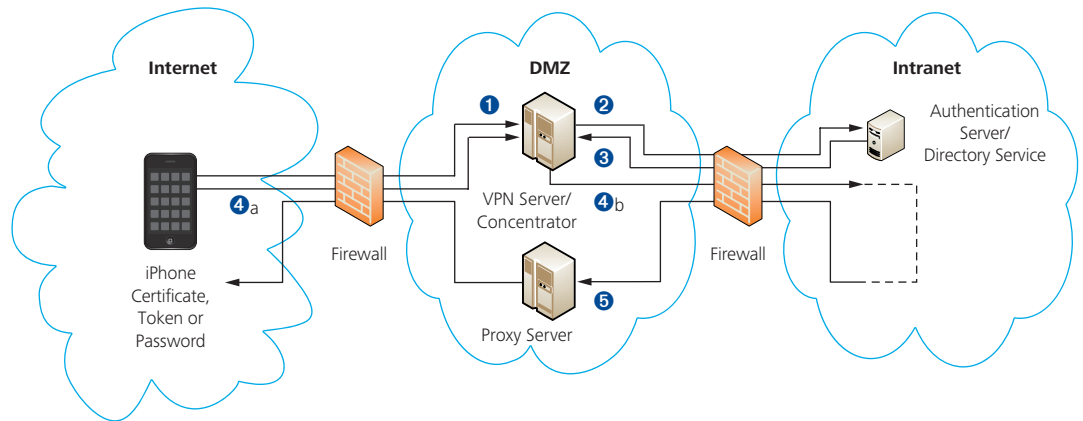
Fig. 1 – Exchange 2007 ActiveSync



The iPhone Exchange communication is secured by 128Bit SSLv3 and signed certificates, this is a secure way to access E-Mail, Calendar and Contact data (see figure 1).

- 1 The iPhone uses HTTPS (TCP Port 443) to access the Exchange Services from the internet through the firewall.
- 2 The Microsoft ISA Server forwards the connection to the Exchange Server.
- 3 The Microsoft Exchange Server authenticates the incoming user via the certificate and Active Directory server.
- 4 If the user is authenticated successfully, the server establishes a connection to the appropriate mailbox.
- 5 ActiveSync establishes a connection that is used for the Push Mail Service. Changes and updates in mailbox or the client are replicated in both directions.
- 6 Outbound mail is typically sent through a bridgehead server or equivalent or directly through an external mail gateway.

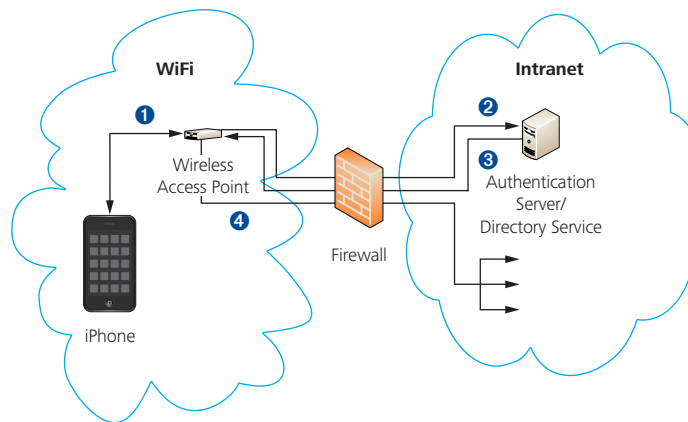
Fig. 2 – VPN Remote Access



Accessing the company network by VPN is a straight forward process following standard mechanisms also used by regular IPSec VPN Client Computers (see figure 2).

- ❶ The iPhone connects to the VPN Server/Concentrator and requests access to the intranet.
- ❷ The incoming request is passed to the Authentication Server/Directory Service for validation.
- ❸ Depending on the applied authentication mechanism, the authentication server verifies the certificate, token or password and, if successful, grants access to the intranet.
- ❹ If the authentication server responds with a positive answer (4a), the VPN Server/Concentrator grants the secured and encrypted network access to the intranet (4b).
- ❺ If a proxy server is implemented the internet access of the iPhone can be established and secured via this proxy.

Fig. 3 – WiFi Integration



Integrating the iPhone with the companies WiFi networks is done in the same way as integrating any other Wireless Client Computer (see figure 3).

- ❶ The iPhone connects to the Wireless Access Point and requests access to the Wireless network.
- ❷ The Access Point passes the request to the authentication server which makes the decision if the access will be granted based on the information of the directory service.
- ❸ The authentication server responds to the access point providing it with the information needed to allow or disallow access to the wireless network.
- ❹ The Access Point is going to provide the appropriate access rights once the user is authenticated based on the information provided by the authentication server.

Process Requirements

Based on the assumption that the devices are owned by the end users there is a set of processes which should be considered in order to respect the security needs of an enterprises organization.

These contain, but are not limited to:

- Accepted Use Policies and Device Management Procedures
- Incident Handling Policies and Procedures
- Access Restrictions for Apps and Systems
- Policy Violation Monitoring
- First Level User Support
- Regular Control and Review Processes

To ensure a minimally secure administration of mobile services, typical security and operations processes in an appropriate infrastructure must be in place. The following list contains an overview of relevant topics to be addressed:

- Key and Certificate Management
- Security Management
- Change Management
- Patch Management
- Incident Management
- Business Continuity Management
- Log Management
- Backup Management

The specific implementation of the processes is strongly determined by the results of a detailed analysis of the existing IT environment and the security requirements.

Additional Security Measures

In addition to the security measures recommended in the chapters above, the IT department should consider implementing the following technical and procedural elements to reduce risks and threat scenarios as much as possible.

Secure methods for configuration profile deployment

- By default there are only three “remote” ways available for deploying the configuration profiles:
 - Via e-mail (user interaction needed). The IT department sends out the configuration profiles via e-mail and users have to install them on their own.
 - Via download to the iPhone (user interaction needed). The IT department pushes the configuration profiles to a web server from which users must download and install the new configuration.
 - Via SCEP (user interaction needed – most secure and recommended method). The IT department bundles the configuration profiles with the certificates and pushes those on a SCEP web server from which users must download and install the new configuration.

Mechanisms which can help to identify if a user accepted and installed a configuration profile

- By default it is not possible to determine if a user has accepted and installed a configuration profile. This issue could be solved in combination with a SCEP deployment (validating the SCEP Server logs).

Mechanisms for restricting the Internet/www access of iPhones and to secure the communication channels used

- The iPhone does not provide the option to restrict the use of the web browser besides disabling it completely. But there are a few ways to get around this limitation:
 - By configuring the HTTP proxy server settings with a secured configuration profile and use the proxy for restricting the access to the Internet.
 - By forcing the iPhones to only connect to the Internet over the secured and restricted VPN solution and the Proxy Server.

System Weaknesses and Known Vulnerabilities

Configuration and Policy Design Issues

Central configuration of the iPhone is done with configuration profiles which are generated with the iPhone Configuration Utility. Table 1 lists the settings and parameters that are currently supported:

Table 1

Area of Settings	Values
Passcode	Passcode required Allow simple value Require alphanumeric value Minimum length Minimum number of complex characters Maximum age Auto-Lock Passcode history Grace period for device lock Maximum number of failed attempts
Restrictions (YES/NO decisions)	Allow explicit content Allow use of Safari Allow use of YouTube Allow use of iTunes Music Store Allow installing apps Allow use of camera Allow screen capture
Wi-Fi	Which network to connect automatically to
VPN	Connection and encryption settings
E-Mail	E-Mail account settings
Exchange ActiveSync	Exchange communication settings
LDAP	LDAP communication settings
CalDAV	CalDAV communication settings
Subscribed Calendars	Calendars which should be subscribed
Web Clips	Web link on the Homescreen
Credentials	Certificates to be placed on the iPhone
SCEP	SCEP communication settings
Advanced	APN connection settings

Microsoft Exchange Server 2007 with Active-Sync allows to manage the following settings remotely:

Table 2

Area of Settings	Values
ActiveSync	Enforce password on device Minimum password length Maximum failed password attempts Require both numbers and letters Inactivity time in minutes Allow or prohibit simple password Password expiration Password history Policy refresh interval Minimum number of complex characters in password Require manual syncing while roaming Allow camera Require device encryption

Nevertheless there are a lot of security relevant settings missing which are necessary in order to build a secured mobile environment.

Application Restrictions

The possibilities provided by the configuration profiles and exchange policy features are limited to a set of basic settings. Right now it is not possible to restrict the usage of features and functions within applications. The IT department can either allow use of an application with all features or disallow it completely; e.g.:

- Safari Web browser – On or off. No granular restrictions possible;
- Install applications (AppStore) – No granular restrictions possible like white or Blacklisting;
- No Mail Account limitation – Users can always add any mail account they want besides the implemented corporate account;
- No Wireless LAN limitation – User can join any Wireless Networks they want;

User Interaction Required

One of the most important design limitations with the remote configuration and profiles approach of the iPhone is that there is no option to deploy settings without users' interaction. The user must always be active and accept changes before the changes can be deployed. Furthermore, there is no option to check iPhones for policy violations and security incidents.

These limitations and the lack of granular remote configurations create challenges to the broad enterprise integration of iPhones, as opposed to the BlackBerry, which has primarily been designed to serve in corporate environments.

Software, Communication, Encryption and Device Design Issues

Software Management

iPhones come with several restrictions that one would not expect from a mobile device that can be integrated in the corporate world. These contain, but are not limited to:

- No over-the-air software updates – Users need to have access to a PC with iTunes installed;
- No over-the-air custom application installation – Users need to have access to a PC with iTunes installed;
- No auditing, monitoring and reporting;
- No central management

E-Mail Encryption

The iPhone currently does not support the use of S/MIME certificates or PGP encryption. Therefore the mails sent cannot be encrypted and mails received which are encrypted cannot be read.

Hardware Encryption

Beginning with the iPhone 3GS the device has a hardware based encryption. This encryption has been proven to be insecure and hackable in several ways.

(http://www.wired.com/gadgetlab/2009/07/iphone_encryption/

of July 23, 2009).

Jailbreaking Software

Another serious argument against the iPhones security is that users will always be able to jailbreak their iPhone without notifying or alarming the IT department. Jailbreaking is a process that allows iPhone and iPod Touch users to run any code on their devices, as opposed to only the code authorized by Apple. Jailbroken iPhones are known to be less secure because they allow running any unsigned software and are not using the iPhone's application sandboxes which help to prevent applications from accessing sensitive data or opening communication channels to unauthorized sources.

<http://blog.iphone-dev.org/>

From Jan. 2008 until now, Apple has released eight security updates for the iPhone OS. Most of them contained critical security fixes.

<http://support.apple.com/kb/HT1222>

Threat Scenarios and Persistent Risks

Currently persistent security risks caused by the lack of security features and known vulnerabilities render iPhones prone to a wide range of attacks. The following scenarios summarize a set of potential risks to the information security of iPhones and indicate where compensating measures and controls need to be implemented.

Compromise Local Data with Physical Access

All mobile devices have a high risk of getting lost and falling into the hands of criminals: this is not an iPhone specific issue. However, iPhones' data encryption have been proven to be ineffective: several free tools are available on the internet to de-encrypt all data on an iPhone.

Risk: Unprotected Information on the iPhone

When the device gets stolen a semi-advanced attacker can apply the decryption tools and read all data on the device.

Measures and Controls

Currently the most common hard disk encryption tools do not support iPhones. Therefore, sensitive data or critical information should not be stored on the device. End users must be made aware of the risk of data exposure. Sensitive mails should be encrypted even though they cannot be read on the iPhone.

Compromise Local Data with Remote Access

There are several tools available on the internet to inject hostile program code into the operating system of the iPhone remotely, allowing the attacker to steal the disk image of the device over the online connection and with it all data stored on the device. This method is also called jailbreaking and is explained in section Software, Communication, Encryption and Device Design Issues of this document.

Hostile software can be installed on the iPhone through so called scams where the user is invited to access a website. Once the user is on the website the malware is uploaded to the iPhone, allowing the possibility to remotely connect to the device. There are also other methods, such as misusing e-mail, for uploading malicious software.

One reason that this relatively simple method can compromise an iPhone is that software management is not controlled and monitored centrally and that for all security updates user interaction is necessary.

Risk: Stolen Data and Access to Local E-Mails

An attacker with the ability to remotely access the device can download all data from the device.

It is also possible for the attacker to read all e-mails that have been pushed from the central servers onto the device.

Measures and Controls

Users must be trained not to access suspicious websites and report all phishing mails that try to pull users to such sites.

Users must immediately perform security updates when central IT makes them available. The awareness program must make clear that the common protection mechanisms that people know from laptops do not work with iPhones.

Unauthorized Access to Corporate Network via Compromised iPhone

The iPhone connects via a legitimate VPN connection to the Microsoft Exchange environment. Once the attacker has obtained remote control over the iPhone it is likely that he will be able to connect to the corporate network and access central systems.

Risk: Reading Sensitive E-Mails and Corrupt Central Systems

Attacker with access to the central systems will be able to retrieve e-mails also from other user accounts.

An attacker will assess the underlying infrastructure and use system weaknesses to move on to other internal systems and access corporate information.

Measures and Controls

A two-factor authentication as described above should be implemented to limit access to the corporate network via VPN as there is the real risk that the iPhone can be hacked.

iPhone connections with the central infrastructure must be monitored for suspicious activities and communication requests.

Compromised iPhone Apps

Although we have not seen compromised iPhone Apps yet, it is very likely that malware and trojans will be published that are embedded in apparently legitimate Apps. Malware could be of any type and have any function that has been developed for other platforms before. Hackers will always try to either access data on the device, control the device for further access to central systems or abuse it for other purposes e.g. denial of service attacks etc.

Risk: Accessing Sensitive Corporate Information and Abuse Central Systems

Risks include the loss or compromise of corporate information and the IT infrastructure: a detailed risk assessment should be performed.

Measures and Controls

Only Apps that have been tested and approved by the central IT department should be installed on the device.

Conclusion

The iPhone is a high tech mobile device with many useful and easy to use features. Together with the connectivity services, the iPhone becomes a connected device supporting people's day-to-day activities, e.g. reading and sending e-mails, arranging meetings or just browsing the internet.

With iPhone version 2 Apple started implementing the features most requested by enterprises all around the globe. However, it appears that all efforts focused on usability and style. The lack of granular security settings and remote management possibilities as well as the missing remote monitoring mechanisms for security incidents can cause serious security concerns.

A reasonably secure iPhone enterprise landscape requires at a minimum well defined processes, policies and procedures, and building security awareness at end users. Nevertheless, fundamental security risks will remain and they have to be evaluated, accepted or remediated prior to the implementation by the organization.

Appendix – List of Resources and References

Table 3

Reference	Date
iPhone OS – Enterprise Deployment Guide – Second Edition, for Version 3.1 or later (Apple)	2009
iPhone in Business – Security Overview (Apple)	Jun. 2009
iPhone in Business – Deployment Scenarios and Device Configuration Overview (Apple)	Jun. 2009
http://www.wired.com/gadgetlab/2009/07/iphone-encryption/	Jul. 2009
http://blog.iphone-dev.org	No date
http://support.apple.com/kb/HT1222	11 Mar. 2010

Contacts

Peter J. Wirnsperger

Tel: +49 (0)40 32080 4675

pwirnsperger@deloitte.de

Richard Sammet

Tel: +49 (0)69 75695 6354

rsammet@deloitte.de

For more information please visit our website at www.deloitte.com/de

Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft as the responsible entity with respect to the German Data Protection Act and, to the extent legally permitted, its affiliated companies use your data for individual contractual relationships as well as for own marketing purposes. You may object to the use of your data for marketing purposes at any time by sending a notice to Deloitte, Business Development, Kurfürstendamm 23, 10719 Berlin or kontakt@deloitte.de. This will incur no additional costs beyond the usual tariffs.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

This client information exclusively contains general information not suitable for addressing the particular circumstances of any individual case. Its purpose is not to be used as a basis for commercial decisions or decisions of any other kind. This client information does neither constitute any advice nor any legally binding information or offer and shall not be deemed suitable for substituting personal advice under any circumstances. Should you base decisions of any kind on the contents of this client information or extracts therefrom, you act solely at your own risk. Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft will not assume any guarantee nor warranty and will not be liable in any other form for the content of this client information. Therefore, we always recommend to obtain personal advice.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.