

Smartphones in the Enterprise

Security Implications of Smartphones

Graham Murphy, Simon Clow
whitepapers@contextis.co.uk

13th December 2010



Contents

Contents	2
Executive summary	3
Smartphones in the enterprise	4
General considerations	5
Governance of smartphones in the enterprise	5
User awareness	6
Configuration (and implementation)	8
Maintenance	11
Detailed review	14
Sampled devices - indicative of major operating systems	14
Summary of security features by OS	15
Symbian Series 60 3rd Edition	19
iOS (iPhone)	22
Android (multiple devices)	24
Windows Mobile 6.5 (HTC Rhodium)	26
Smartphone Exchange ActiveSync clients	28
Introduction	28
Android 2.1+ mail client	28
iPhone mail application	28
Moxier Mail	29
RoadSync	31
Appendix A: Windows Mobile 6.5 policy items	33
Appendix B: Smartphone anti-malware software	37
Appendix C: Configuring IPSec VPNs on Smartphones	39
Nokia Symbian Series 60 3rd Edition	39
iOS iPhone	39
Android	39
Windows Mobile	39
About Context	40



Executive summary

In the past few years smartphone sales have grown exponentially. In the second quarter of 2010, over 62 million devices were shipped worldwide¹ and smartphones now account for 17% of all global mobile handset sales, according to figures from Gartner.

The widespread availability and popularity of affordable smartphones has encouraged many organisations to consider their use as a means of providing employees with mobile access to corporate resources, a move that can create significant cost and efficiency gains for employees and employers.

However, businesses that deploy smartphones in anticipation of these productivity gains must give due consideration to the security risks involved, which are ever increasing. For example, there has been a recent significant rise in the numbers of incidents in which smartphones specifically have been targeted by malware as part of an orchestrated attack.

This white paper is intended to raise awareness of those risks, and to provide both technical and strategic guidance for enterprises seeking to secure smartphone deployments within the enterprise. The first section of the white paper highlights the common security implications of deployment and offers high-level guidance that is applicable to any smartphone deployment. It outlines a range of issues that may be encountered during deployment, and provides a technology-independent baseline for good practice.

This high-level advice is followed by in-depth analysis of the market's most popular smartphones and the best available means of securing them. Platforms reviewed include Windows Mobile, Symbian Series 60, Android and iPhone. Although the Research in Motion (RIM) BlackBerry series has not been reviewed specifically, it is included in a comparison of features between each of the platforms reviewed.

Our analysis reveals that the majority of smartphones available today offer only limited security features and are subject to inherent security flaws. The security features offered with many handsets add up to little more than superficial additions to consumer products, rather than having been incorporated as a fundamental part of the device design.

By contrast, Context's previous experience testing the BlackBerry platform has shown that, because it was designed from the start for business users, it is based on secure design principles. Even so, the security of BlackBerry devices still depends on effective deployment of a robust set of security policies. The means to secure smartphones designed with a consumer, rather than a business user in mind, do exist in the form of third party add-ons. The effectiveness of these solutions is not specifically discussed in this report.

Clearly, while the theoretical benefits offered by use of smartphones within the enterprise are many, their use also creates a series of security risks and issues that can only be mitigated at the cost of some time and effort. Businesses intending to proceed with smartphone deployments must exercise caution and should arm themselves with knowledge about the relevant risks and the measures that can be taken to counter them. Managers will need to take an informed view as to whether at this stage, considering the security measures currently available, the rewards still outweigh the risks.

¹ British Broadcasting Corporation. BBC News - Google Android phone shipments increase by 886%. <http://www.bbc.co.uk/news/technology-10839034>.



Over the course of the next few years, as smartphones continue to proliferate, both the methods used to attack and to defend them will evolve rapidly. Context will continue to work at the cutting edge of research in this area and endeavour to share our knowledge in future publications.

Smartphones in the enterprise

The BlackBerry, which might be considered the 'original' smartphone, has been popular as a tool for providing business executives with email on the move for some years. More recently new smartphone brands have entered the market, with handsets offering users impressive storage capability, web browsers and custom applications as standard.

As a result, smartphones are no longer limited in function to checking email. Users can now use them to work on and store documents and for other purposes including participating in business workflows and to access contact details and other corporate information.

These activities may be performed via the device's web browser, customised applications or proprietary systems such as Lotus Notes or Microsoft Exchange. Whatever the technology used, clearly the smartphone has become the custodian of a large amount of corporate data, sometimes including highly sensitive information.

But as the complexity of smartphones increases, so too does their susceptibility to configuration weaknesses and security vulnerabilities. As smartphones are not equipped with security measures of equivalent strength to those usually found in other mobile IT equipment like laptops, it is hardly surprising that they are now often targeted by criminal organisations.

So it is absolutely crucial that any business user planning to deploy such devices considers carefully whether or not the use of smartphones for such purposes is appropriate and can be achieved securely.

The next section offers high-level advice for enterprises planning to implement and manage a secure smartphone deployment.



General considerations

Regardless of the manufacturer or type of smartphone chosen, many different factors act to determine the security impact of deployment in the enterprise.

We have broken these down into four areas: governance, user awareness, configuration and maintenance.

Governance of smartphones in the enterprise

As with any enterprise assets, smartphones must be included in a governance structure if they are to be managed effectively by the business. Effective governance provides management with oversight and control of the deployment and can act as a frame within which to direct efforts to secure the deployment.

Risk assessment

The first step in securing any enterprise smartphone deployment is a risk assessment. Comprehensive risk assessments identify and define threats, outlining both the probability that they will affect the organisation and the damage they could cause. Without this information, it is much more difficult for enterprises to mitigate these risks to an acceptable or practical degree.

Smartphones continue to evolve rapidly, so risk assessments should be repeated whenever either a technological or enterprise change alters the nature of the deployment.

In addition, a new risk assessment should be conducted whenever a new exploit is released, i.e. changing the threat profile of the deployed devices.

Enforcement of a corporate acceptable usage policy

Most organisations already have a corporate usage policy for IT equipment, many of which incorporate specific requirements for both laptops and for the use of other mobile devices. Both these sets of requirements will apply to smartphones.

Any smartphone security policies should be aligned with existing policies addressing the threat posed by loss or compromise of mobile devices. They should cover every relevant process, from the issuing of a smartphone to its recovery when no longer required by the user, including the procedure to be followed in the event of a device being lost.

Some of the smartphones reviewed in the Detailed review section of this whitepaper permit the technical enforcement of corporate usage policies. These may prohibit the installation of applications by end users, and can confirm that a minimum level of protection is in place before the device is connected to an internal network. They can also extend to disabling functions such as the device's camera, voice calls, Bluetooth or WiFi. While such features can be useful, the decision to implement them must be taken by the relevant authority within the enterprise.

Personal smartphones

With the rapid proliferation of smartphones, it has become increasingly common for employees to use a personal smartphone. Naturally, for their own convenience, employees may want to synchronise this with their office desktop or laptop computer. This could include placing their VPN credentials on the personal smartphone to enable direct communication with an organisation's Exchange servers, allowing them to retrieve their email – but using a device that is not controlled under company policy.



To counter the problems this may create, organisations should explicitly and appropriately address the use of personal smartphones within policies, either incorporating new measures within existing acceptable usage policies or issuing a standalone smartphone policy.

Security awareness programme

The best policy in the world is useless if not adequately publicised and enforced, so the next most important step is to inform employees of its existence. This should form part of a wider security awareness programme, including the provision of information outlining the security risks associated with smartphones.

The following section on user awareness describes the relevant key issues which should be addressed within the security awareness programme.

User awareness

Even if the smartphones used do contain security features, problems can still arise if users are not well-informed about the risks posed by their devices.

Encourage healthy scepticism in users

In many ways, today's smartphones are more like personal computers than traditional mobile phones. While the advantages of these enhanced capabilities are obvious, with greater complexity comes an increased likelihood that users will unwittingly expose their devices to security risk.

The trouble is that users soon come to 'trust' their mobile phones. Several years ago there was a fashion among teenagers to use Bluetooth to send notes or calendar entries to strangers in acts of mischief termed 'Bluejacking'. The unfortunate victims who accepted these calendar entries could then find themselves woken by alarms at highly antisocial hours. Although being woken up at 4am could be dismissed as a minor irritation, it does also demonstrate how easily a trusting user can be duped.

A more worrying example is seen in the malware strain "Cabir", which spread on Symbian devices via Bluetooth.

In order to contract this virus, the victim user had to:

1. Accept a connection from an unknown device;
2. Save the received data to the phone;
3. Execute the code; and finally
4. Accept the warning that the code was not signed.

In all, this amounted to four warnings being displayed before the user managed to successfully infect their phone. Yet the Cabir malware still managed to spread to 16 countries².

² Millard, Elizabeth. Technology News: Wireless: Cabir: World's First Wireless Worm. 16 June 2004. <http://www.technewsworld.com/story/34542.html?wlc=1275018693&wlc=1285067289>.



Keep physical control

As with any laptop or mobile device, keeping a smartphone under physical control goes a long way to keeping it secure. Even if no other safeguards are in place, preventing other people from physically accessing the device does prevent many forms of attack.

For example, allowing someone else to use a smartphone for just five minutes gives them enough time to install malware or change security settings. Likewise, leaving the device unobserved in a public place for as little as 30 seconds is long enough for the device to be tampered with or stolen.

The best defence for organisations is to educate users about the dangers of leaving devices unattended or allowing other people to use them.

Only install trusted applications

The number of applications developed for smartphones has increased dramatically in the last few years. Smartphone manufacturers, operating system developers and mobile network operators have all sought to maximise their share of the associated commercial benefits by providing an easy route to market for application developers.

These fast and easy routes to market offer very little validation of an application's functionality beyond statements made by the developer. Despite this, the applications are published by what many smartphone users perceive to be trusted sources, either through their presence in an official marketplace, or the existence of a certificate which merely confirms that the application was developed by the person who claims to have developed it. Individuals buying these applications are effectively placing their trust in an application that has been developed by an unknown party. There have already been numerous examples of this trust being abused.

For example, in the Android market two applications, once downloaded, executed code outside the 'sandboxing' protection that Android provides. Although these applications were not malicious, the same technique could be used to install malware on the device. The Apple Store has published applications that passed personal data relating to the device user back to the application developer; and Windows Mobile applications have been modified to include auto-dialler malware. Even BlackBerry smartphones are not exempt from these sorts of problems, having been targeted by spyware³.

Given these risks, it is recommended that applications are not installed unless the publisher and developer are both known and trusted. Ideally, before enterprise deployment, a full test of each application's functionality should be performed, to assess the likelihood of security settings being compromised or of the unsuspecting user gaining 'extra' functionality.

³ Higgins, Kelly Jackson. Smartphone Malware Multiplies. 07 June 2007.
<http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=225402185>.



Configuration (and implementation)

A strong security policy and user education can reduce the security threat posed by the use of smartphones, but cannot protect the enterprise from sophisticated or targeted technical attacks, or from the security threat posed by the loss of mobile devices. This section discusses the variety of approaches that can be taken to secure most smartphones.

Ensure authentication is required

Although maintaining physical control of a smartphone is very important, organisations must also put technical safeguards in place to deal with theft or loss of the devices. In this scenario, the simplest defence is to enable user-authentication on the device.

Smartphones allow the configuration of an authentication mechanism to unlock the device, such as a Personal Identification Number (PIN) or password. Devices should be configured to 'lock' and require re-authentication after a reasonable period of inactivity, for example three to five minutes.

Most SIM cards also support PIN-based authentication, although some smartphones do not. Unfortunately not all smartphone manufacturers have taken the necessary steps to clarify the difference between the device PIN and SIM card PIN to the average user.

This can lead the user to believe that both phone and SIM card are protected when actually only the SIM card is. Those managing enterprise smartphone deployments must make this distinction clear to those employees using the smartphones to access corporate data.

Enforce a robust password policy

With authentication in place, one of the simplest ways for criminals to defeat it is to guess the users' passwords. This can sometimes be as simple as running through a list of simple or commonly found passwords.

So a robust password policy is important. It should specify the type and number of characters required in a password, how often the password needs to be changed and how many times it can be entered incorrectly before the device is wiped or disabled.

The Detailed Review in the second half of this whitepaper compares the capabilities of this kind offered by the smartphones under consideration.



Encrypt sensitive data

While locking a phone with a PIN or password can prevent someone from using the device as the manufacturer intended, it does not prevent a skilled attacker from gaining access to the data stored on the device. For this reason, it is strongly recommended that any sensitive information stored on the smartphone is encrypted.

Some smartphones ship with built-in encryption, but this does not necessarily mean that any encrypted data is fully protected. Context has assessed smartphone implementations where it was discovered that the encryption methods used did not provide any effective additional protection.

There are also security concerns relating to the operation of the smartphones. For example, two different smartphone operating systems are known to permit applications to access encrypted data on the device. So although the encryption may protect the device against physical examination of the memory chips, it offers no protection against the threat posed by malware.

As a rule, the encryption methods used on a smartphone should be subjected to detailed examination before deployment. The Sampled Devices section of this white paper details the effectiveness of each manufacturer's encryption methods.

Limit the sensitive data stored

When no encryption is in use, the time required for a skilled attacker to gain unauthorised access to data stored on the device can be as little as minutes, depending on the make and model of the device. Even when a device supports encryption, this may not provide adequate protection.

Either way, it should still be assumed that it is only a matter of time before the information stored on a device that falls into the wrong hands is compromised. For this reason, limiting the amount of sensitive data on the smartphone will help to minimise the impact of any disclosure if the device is lost.

Consider installing anti-malware software

Smartphones used within an enterprise environment have the ability to access, create and modify corporate data – and so have the potential to contaminate that data with malware.

Also, while mobile devices may be regarded primarily as a means for the transmission of malware, some malware is designed to target the mobile devices themselves. This may compromise the privacy of communications from the handset, could allow the proxying of attacks on the internal network of a user's organisation and can also be used to perform toll fraud.

Fortunately, there are a number of software options available that can help protect smartphones against malware. For details of anti-malware software available at the time of writing refer to Appendix B: Smartphone anti-malware software.

Install firewall software

If smartphones are to be integrated into an enterprise environment, then they should be regarded as requiring the same security protection as would any other portable device offering Internet connectivity.

Most organisations would not dream of deploying laptop builds without using some form of firewall technology, yet may allow smartphones direct access to the internal network when the smartphone is also permitted unprotected access to the Internet. In such cases, compromised smartphones can be used as a form of proxy between an Internet-based attacker and the internal networks, bypassing normal firewall protection.



Ingress filtering

Context's security review of the current generation of smartphones has identified that, for the most part, the default configuration is to be deployed without listening services on the devices' IP stack (either on the 3G interface or WiFi where supported). This reduces the attack surface available against a handset in default configuration, but third party software may expose listening network sockets.

Where Bluetooth is available on a handset, the current tendency is for it to be disabled or deployed in "hidden" mode and has to be explicitly configured as "visible" to support pairing. Android-based devices expand on this principle by limiting the visible window to 120 seconds, and visually counting down before automatically hiding the Bluetooth interface.

Egress filtering

Effectively configured IT equipment benefits from egress protection, which ensures that malware cannot communicate with command and control channels. There is a desire for smartphones to be controlled in a similar fashion, but, unlike traditional IT equipment, smartphones also have the ability to place phone calls and send text/picture messages. Malware can, and has, taken advantage of these abilities to monetise the infection of the smartphone⁴.

Limit remote access

One of the capabilities smartphones offer that distinguishes them from other mobile phones is tight integration to data network bearers. These can include the mobile phone network (3G interface), local wireless (such as WiFi and Bluetooth PAN) or even infra red (IrDA) connections.

Generically, software that binds network sockets on a smartphone makes no distinction as to the interface to which it binds. For example if the smartphone is configured to share its media via a user's local WiFi network, then it may also be sharing the same media over the 3G or Bluetooth PAN.

Leaving these unused interfaces active increases the attack surface of the device. One example has been seen in relation to the "jailbreaking" performed on iPhones. A default username and password had been defined by Apple, but was not accessible until the phone underwent jailbreaking, at which point, anyone who could reach the phone through 3G or WiFi could access the smartphone and modify/read data stored remotely⁵.

⁴ Higgins, Kelly Jackson. Smartphone Malware Multiplies. 07 June 2007.
<http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=225402185>.

⁵ Carr, Josh. Worm rickrolls unsecured jailbroken iPhones via SSH. 7 November 2009.
<http://www.tuaw.com/2009/11/07/jailbreak-worm-rickrolls-the-unsecured/>.



Maintenance

Once a smartphone deployment is complete, a maintenance structure is required to manage day to day security requirements.

Ensure firmware updates are applied

All smartphone manufacturers produce firmware updates to improve functionality and plug security holes in their devices. These updates generally cover the operating system and any applications shipped by the manufacturer.

The High Tech Computer Corporation (HTC) originally shipped its Hero Android smartphone with a boot loader that was openly accessible, allowing access to any files on the device even if the handset was locked. A user only needed to download the freely available Android software development kit (SDK) to make changes to the phone. HTC subsequently addressed this by changing the boot loader in a firmware update⁶.

Network operators sometimes customise the firmware on devices they sell, either to include applications or to restrict functionality. Where an operator has customised firmware, it is important to ensure that it has not also introduced applications that contain known problems.

Most operators test that a new firmware image operates correctly on their network; and updates released by a manufacturer must be approved by an operator before being released to users. But there is not usually any centralised way of checking the current version of firmware, or of reviewing what has been changed in the firmware version. That means users and IT departments are forced to check manufacturer and operator websites to find out what the current firmware version is and so determine whether or not it addresses security issues.

Device provisioning 'over the air'

The ability to provision (configure) a smartphone over the air allows administrators to set up smartphones with all the settings they need to operate correctly within the environment in which they are deployed. It also permits changes in policy or configuration to be communicated to the devices without requiring them to be returned for reconfiguration.

Configuration control

Any smartphone deployed by an enterprise should be subject to some form of device management. There are a number of different methods for doing this, each with its own merits.

Exchange ActiveSync policy

Exchange natively provides a method for performing a certain level of management for ActiveSync compatible smartphones. These settings generally only permit the password policy and lockout policy to be set, but do also permit a remote wipe, if this is supported. But an Exchange ActiveSync policy does not generally require any additional services beyond the Outlook Web Access portal, meaning deployment is straightforward.

⁶ modo. NOOB guide HTC HERO root and adb. 13 December 2009.
<http://htcpedia.com/forum/showthread.php?p=31496>.



Open Mobile Alliance (OMA) Device Management (DM)

The Open Mobile Alliance (OMA) was conceived to provide a more holistic method for management and provision of handsets. Prior to the launch of the OMA's Device Management (DM), each vendor had its own mechanism for provisioning handsets. OMA DM offers a method enabling centralised control over a number of different handsets, which could be from different vendors.

However, operation of OMA DM does require the use of additional services. Typically these would include a certificate server, a web server, and some method of generating WAP push messages that notify the smartphones of forthcoming configuration changes.

While OMA DM provides a framework for device management, different vendors still have different ways of implementing the provision and management of devices. If different types of smartphones are to be managed, this can make it more difficult to ensure that smartphone policies are deployed in consistently.

Vendor-specific mechanisms

Some vendors may provide a proprietary mechanism for managing their smartphones. In many ways, Research in Motion's BlackBerry platform serves as an example of how effectively this kind of proprietary mechanism can work.

In this case Context did not encounter any other vendor specific management mechanisms during the testing process. But proprietary vendor neutral products do exist, including the Good for Enterprise suite from Good Technology, which can be used to provide management functionality across a wide range of smartphone types.

Perform data backups

Like laptops, smartphones are capable of storing significant amounts of data. Also like laptops, smartphones can be stolen, lost or suffer hardware failure, rendering this data irretrievable. It is therefore advisable to provide some form of external backup facility.

A number of options are available for backing up data held on smartphones, depending on the make and model of the device in question.

The easiest way to backup a smartphone is via memory card. The main drawback of this approach is that the memory card is often left in the smartphone. Although this solution enables data to be retained in the event of hardware failure, it offers no protection if the device is stolen or lost while the memory card is still inside.

Personal smartphone owners are typically provided with desktop software bundled with the product that enables the user to back up data to another computer. It is important to ensure that this data remains accessible, so that it can be used if the smartphone is lost.

Some backup solutions use 3G or WiFi to copy data to a remote location. Enterprise deployments should carefully evaluate these solutions with respect to the availability and the security of the offsite storage provided.

For enterprise use, no data should be stored on the device that is not also mirrored at another location.



Perform secure wipe before disposal

It is not uncommon for smartphone handsets to be sold on when the original owner has decided to upgrade to a new device. Whilst this should not occur with enterprise devices, Context is aware that sometimes such devices do still end up being sold. One might hope that erasing a device before reselling would be a matter of plain common sense; there have been incidents where this has not happened in the case of some devices purchased through avenues such as eBay⁷. If this does happen, any information stored on the device may be recovered easily by the new owner, depending on the device.

Erasing a device typically means removing any user files, contacts, text messages, photos, videos and web history. A number of devices have an option to wipe all user data from the smartphone. This option should be used, and the smartphone subsequently checked to ensure that no data remains. Any data previously stored on the devices should be unrecoverable.

Deactivate compromised devices

If there is a suspicion that a device has been compromised it should be treated as un-trusted and not used until it can be returned to a trusted state. This will generally require the erasure of all storage media followed by re-deployment of a firmware image from a trusted location such as the manufacturer or carrier's website. Unless an appropriate backup strategy is in place, this will result in the loss of data from the handset.

It is important to identify and then close the vector used to compromise the handset – there's not much point returning a handset to a trusted state only for it to be compromised again!

Remote device wiping

Although the ability to remotely invoke erasure of a device looks at first glance like the ideal solution to use in the event of a smartphone is being lost, this will only actually happen if the device receives the message that will trigger erasure. In the case of a targeted attack, the device may be prevented from receiving this message, thus leaving the data on the device intact. So relying on a remote wipe command to prevent information disclosure cannot ensure that data on the device will be irretrievably erased.

Some smartphones can also perform a device wipe after a set number of failed password entry attempts. Although this provides a degree of protection in the event that a device is lost or stolen, it will not prevent a skilled, determined attacker from gaining access to data stored on the device.

Remote wiping and device wiping features in general are therefore useful, but should be used in the context of a more comprehensive security solution.

⁷ Zetter, Kim. BlackBerry Reveals Bank's Secrets. 25 August 2003.
<http://www.wired.com/techbiz/media/news/2003/08/60052>.



Detailed review

This section contains the results of a detailed review of seven smartphones, performed by Context. It begins with a recommendation of the minimum security settings which should be applied to any smartphone. This is followed by a comparison of common security features supported by the devices reviewed. Finally we present a detailed analysis of the security capabilities of each device.

Sampled devices - indicative of major operating systems

Context selected seven smartphones for review that are considered to be representative of the major underlying operating systems used in the smartphone market. However, as some platforms are tailored by the manufacturer, there may be features or issues that are specific to a manufacturer or model.

Smartphone Models	Underlying Operating Systems
Nokia E71/E72	Symbian Series 60 3rd Edition
iPhone 3G	iOS 3.1.2, iOS 3.1.3
iPhone 4	iOS 4.0.1, iOS 4.1.0
HTC Hero Sony Ericsson X10 Dell Streak	Android 1.6 and Android 2.1
HTC Rhodium	Windows Mobile 6.5



Summary of security features by OS

The table below summarises at a high level the security features that can be configured and controlled via the centralised management of the different platforms reviewed. For more detailed information on a specific platform, please see the section pertaining to that platform.

Value	Meaning	Value	Meaning	Value	Meaning
✔ Green	Positive security impact	⊖ Amber	Neutral security impact	⊗ Red	Negative security impact

	Symbian Series 60	Windows Mobile 6.5	Android 1.6	Android 2.1	iPhone	BlackBerry
Server Internet Exposure						
Inbound Connection needed from Internet to Email Server	⊗ Yes	⊗ Yes	⊗ Yes	⊗ Yes	⊗ Yes	✔ No
Email Support						
Microsoft Exchange	Native and 3rd party	Native	3rd party software	Native and 3rd party	Native	Native (through BlackBerry Enterprise Server)
Lotus Notes	Notes Traveller	Notes Traveller	N/A (Available 2010)	N/A (Available 2010)	Notes Traveller	Native (through BlackBerry Enterprise Server)
Management						
Exchange ActiveSync Policy	✔ Yes	✔ Yes	⊗ None	✔ Yes	✔ Yes (iOS 2.0 and above)	⊗ None
OMA DM Support	⊖ Fair	✔ Comprehensive	⊗ None	⊗ None	⊗ None	⊖ 3rd Party Software
Vendor Specific Management	⊗ No	⊗ No	⊗ No	⊗ No	✔ Yes	✔ Comprehensive



	Symbian Series 60	Windows Mobile 6.5	Android 1.6	Android 2.1	iPhone	BlackBerry
Password Policy						
Requires Password	✔ Yes	✔ Yes	✘ No	✔ Yes	✔ Yes	✔ Yes
Password Length Enforced	✔ Yes	✔ Yes	✘ No	✔ Yes	✔ Yes	✔ Yes
Lock Time	✔ Yes	✔ Yes	✘ No	✔ Yes	✔ Yes	✔ Yes
Wipe After Failed Password Attempts	✔ Yes	✔ Yes	✘ No	✔ Yes	✔ Yes	✔ Yes
VPN Support						
PPTP VPN Supported	✘ No	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✘ No
L2TP VPN Supported	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes (Only over WiFi)
Supports IPSEC VPN with Pre Shared Key	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes (Only over WiFi)
Supports IPSEC VPN with Certificates	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✘ Unknown
Supports Triple DES for IPSEC VPN	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes (Only over WiFi)
Supports AES for IPSEC VPN	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes (Only over WiFi)
Vendor Specific VPN	✘ No	✘ No	✘ No	✘ No	✘ No	✔ Yes (BES)



	Symbian Series 60	Windows Mobile 6.5	Android 1.6	Android 2.1	iPhone	BlackBerry
Centralised Functionality Control						
Prevent Voice Calls	⊗ No	⊗ No	⊗ No	⊗ No	⊗ No	☑ Yes
Prevent SMS/MMS	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No	☑ Yes
Disable Browser	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No	☑ Yes
Disable Memory Card slot	⊗ No	☑ Yes	⊗ No	⊗ No	☑ N/A	☑ Yes
Disable WiFi	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No	☑ Yes
Disable Bluetooth	⊗ No	☑ Yes (Off or Handsfree)	⊗ No	⊗ No	⊗ No	☑ Yes
Disable IrDA	⊗ No	☑ Yes	⊗ No	⊗ No	☑ N/A	☑ Yes
Disable Camera	⊗ No	☑ Yes	⊗ No	⊗ No	☑ Yes (iOS 3 and above)	☑ Yes
Disable POP/IMAP Email	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No	☑ Yes
Prevent Application Installs	☑ Yes, but through certificate management.	☑ Yes, but through certificate management.	⊗ No	⊗ No	⊗ No	☑ Yes
Whitelisting of Acceptable Applications	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No	⊗ No
Prevent Unsigned Applications Executing	☑ Yes	☑ Yes	⊗ No	⊗ No	☑ Yes	☑ Yes



	Symbian Series 60	Windows Mobile 6.5	Android 1.6	Android 2.1	iPhone	BlackBerry
Encryption						
Internal Memory	✔ Yes	⊖ Partial (User Data)	⊗ No	⊗ No	⊖ Some Models	✔ Yes
Memory Card	✔ Yes	✔ Yes	⊗ No	⊗ No	✔ No memory card supported	✔ Yes
Memory Card Key	✔ Yes	⊗ No	⊗ No	⊗ No	✔ No memory card supported	✔ Yes
Remote Wipe	✔ Yes	✔ Yes	⊗ No	✔ Yes	✔ Yes	✔ Yes
Off Network Wipe	⊗ No	⊗ No	⊗ No	⊗ No	⊗ No	✔ Yes



Symbian Series 60 3rd Edition

Introduction

Context used the popular Nokia E72 as a representative example of the Symbian Series 60 3rd edition devices. The device examined was running version 023.003 of this software.

Nokia provides the Mail for Exchange (MfE) mail client, available from the OVI store. This application for Nokia handsets provides limited EAS client functionality.

During testing of this software (1st Quarter 2010) it was not possible to connect the MfE client to an Exchange environment unless the default policy explicitly allowed non-provisionable device support. Due to this requirement it was not possible to enforce any IT policy on handsets running the MfE client.

Symbian Series 60 3rd Edition/Nokia E72

Security Features

The Nokia E72 supports features such as:

- Remote wipe
- SIM lock (PIN code & PIN code request)
- Phone Locking (Lock code)
- Remote Phone Locking
- Encryption of main memory
- Encryption of memory card
- Memory card encryption key management

VPN Support

The Nokia E72 supports the use of IPSEC VPNs. The following IPsec encryption methods are supported in CBC:

- AES128/192/256
- 3DES
- DES
- NULL
- Authentication methods supported:
 - RSA signatures
 - DSA signatures
 - Pre-shared key
 - EAP_AKA
 - EAP_SIM

Device Management

The Nokia E72 uses the standard OMA DM protocol to manage the device. Currently the following items can be managed:

- VPN settings
- User certificates
- Device certificates
- Email (including Mail for Exchange)



Symbian Series 60 3rd Edition/Nokia E72

Suggested Settings

The E72, like all consumer-oriented smartphones, ships with minimal security settings enabled. Thus, the minimum settings that should be enabled on an E72 to protect data stored should be:

- Set a pass-code
- Ensure that the phone locks after a reasonable period (eg. three to five minutes)
- Encrypt the memory card

If these settings are not in place, a user with Nokia's freely available PCSync software can simply extract the data from the phone.



Symbian Series 60 3rd Edition/Nokia E72

Potential Security Issues**Disable Platform Security**

The security policy on Series 60 devices relies on a trusted root on the phone. However, it is possible for a user to modify the trusted root on the device, and then modify the firmware on the device. This includes the ability to override the settings pushed down by the Exchange Server or through OMA DM messages. One freely downloadable tool to perform this task is HelloOX2⁸.

Policy Interactions

The interaction between the Exchange ActiveSync policy and the Nokia E72 password implementation is noted to cause some unexpected behaviour. If the Exchange ActiveSync policy is configured to require a password, but does not have a password timeout set, then the Nokia E72 handset will force the user to set the password, but will not require the password for any operations (with the exception of changing the password!).

So it is recommended that the Exchange ActiveSync Policy is configured to both require a password, and to have a device lock time in order to enforce a password on the Nokia E72 handsets.

FBus / MBus access to Handset Memory

Most Nokia handsets provide at least one of two diagnostic interfaces. These appear to be used for debugging and for fault finding. Both interfaces are asynchronous serial. The MBUS interface is an older half-duplex connection, and the FBUS interface is a newer full-duplex connection. These interfaces are typically exposed as a set of pads within the battery compartment of the smartphone.

Using a suitable controller (typically a form of USB to serial interface) together with a suitable harness to connect to the pins of the smartphone, the memory on the phone can be directly inspected and, in some cases, modified.

This has previously been used to extract numeric PIN pass codes from the running firmware within Nokia handsets.

Recognizer Autorun

As the Symbian platform does not use file extensions to identify the type of files that are opened, an alternative mechanism is used instead. Instead, a process of using "Recognizers" is used. A Recognizer is a small section of code that examines the data file, and returns the MIME type if it is recognised. This process can be abused to automatically start an application that performs malicious functions, such as recording conversations or sending emails to a malicious third party.

⁸ HelloOX2 Team. HelloOX2 Official Website. 2010. <http://helloox2.com/>.



iOS (iPhone)

Introduction

Context reviewed several versions of the iPhone handset (3G, 3GS, and 4) running iPhone Operating System (iOS) versions 3.1.2, 3.1.3 and 4.

While the iPhone is possibly the most iconic and user acclaimed smartphone released, it was initially designed as a consumer device, with enterprise functions only added during updates to iOS.

The iPhone has the ability to integrate into an enterprise environment and using the tools provided by Apple an effective security policy can be both designed and then deployed. However these tools are not interoperable with other handsets.

iOS 3.1.2/iOS 3.1.3/iOS 4/iPhone 3G/iPhone 3GS/iPhone 4

Security Features

The iPhones tested support the following enterprise security functions with the stock software image:

- Remote wipe
- SIM lock (PIN code & PIN code request)
- Phone locking (lock code)
- Remote phone locking
- Encryption of main memory

VPN Support

The iPhones tested support the following transport protocols to establish secure communications within enterprise environments:

- Cisco IPsec
- L2TP/IPsec
- PPTP
- SSL VPN
- The following methods can be used to perform authentication of the VPN tunnel:
 - Password (MSCHAPv2)
 - RSA SecurID
 - CRYPTOCARD
 - x.509 Digital Certificates
 - Shared secret (PSK)
 - 802.1x authentication protocols
 - EAP-TLS
 - EAP-TTLS
 - EAP-FAST
 - EAP-SIM
 - PEAP v0, v1
 - LEAP Device Management



iOS 3.1.2/iOS 3.1.3/iOS 4/iPhone 3G/iPhone 3GS/iPhone 4

Device Management

Versions of the iPhone operating system (iOS) prior to version 4 have more limited management abilities. Device management can be performed using Exchange ActiveSync and through the deployment of Apple-specific device management configuration files. These can be deployed through the iPhone Configuration Utility (ICU), via the Safari web browser or using the Over-the-air Enrolment and Configuration service.

Version 4 provides an API that allows third party programs to manage the configuration of the device. However, such applications can also override configuration settings set via EAS or ICU.

Suggested Settings

The iPhone, like all consumer oriented smartphone handsets, is provisioned by default with minimal security settings enabled. In order to make the opportunistic theft of data stored on the device more difficult, the following settings should be enabled:

- Set a pass-code
- Ensure that the phone locks after a reasonable period (eg. three to five minutes)

Without these basic settings in place, a user with any computer can mount the iPhone as a disk and extract data from the public media partition.

Potential Security Issues**Jailbreaking**

The iPhone security model relies heavily on the integrity of the iOS operating system and the chroot jail in which all user-installed applications run. However, the "jailbreaking" community provides tools that can be used to gain access to the root partition and allow the execution of arbitrary code, regardless of any password or pass-code protection.

Context was able to leverage the techniques used by the Jailbreak community to trivially negate iPhone security policies and extract the data from both the Media partition and the hidden root partition.

A number of similar techniques have been documented at:

<http://www.iphoneinsecurity.com/>

This issue remains through all iOS and iPhone versions reviewed.

Bootloader

iPhones with hardware encryption provide full disk encryption to protect against the removal of the FLASH memory from the device. But the device is configured to automatically supply the key for decryption upon boot. By supplying the device with a custom kernel Context forced the iPhone to boot under an alternative operating system. This approach was used to remove lock codes and other security features built into the user interface on the device. This technique is commonly known as the Zdziarski method⁹.

⁹ Zdziarski, Jonathan. iPhone Insecurity. 28 April 2010.
<http://www.iphoneinsecurity.com/>.



Android (multiple devices)

Introduction

As the Android operating system has matured, manufacturers have learned how to harden firmware images prior to deployment. This enhanced platform allows for greater resilience and provides a robust base on which to implement a security lockdown.

However, like the iPhone, the security depends on the integrity of the firmware image. The techniques used to "root" a specific Android device (akin to jailbreaking on an iPhone) can often be used to gain enhanced control of a handset, negating the security lockdown implemented within an IT policy.

Android 1.6/ Android 2.1/Sony Ericsson X10/HTC Hero/Dell Streak

Security Features

The current generations of Android devices support the following enterprise security functions with the stock software image:

- SIM lock (PIN code & PIN code request)
- Phone locking (lock code)
- Gesture based unlock
- Remote wipe (only available with Android 2.1 and above)

VPN Support

The Android platform supports the following transport protocols to establish secure communications within enterprise environments:

- PPTP
- L2TP
- SSL VPN
- The following methods can be used to perform authentication of the VPN tunnel:
 - Shared secret (PSK)
 - X.509 Digital Certificates
 - OpenVPN (With a non-standard module)

There is currently no support for XAUTH Group ID and password, making it harder to interoperate with some IPSec implementations (e.g. Cisco VPN).

Device Management

Currently Android does not support the use of OMA DM messages to manage smartphones. For Android 1.6 platforms, there are no native management features. For Android 2.1+ platforms, Exchange ActiveSync provides basic password and remote wipe functionality. Third party software can be used to extend the management ability.



Android 1.6/ Android 2.1/Sony Ericsson X10/HTC Hero/Dell Streak

Suggested Settings

Android smartphones, like other consumer-oriented smartphones, ship with a set of fairly minimal security settings enabled. Thus, the minimum settings that should be enabled on an Android smartphone to protect data stored should be:

- Set a passcode
- Ensure that the phone locks after a reasonable period (eg. three to five minutes)
- Encrypt the memory card
- Disable Unknown Sources
- Disable USB Debugging

Disable "Unknown Sources"

The Unknown Sources setting permits the user of the handset to install applications that have not come through the Android Marketplace. This setting can be found under Settings -> Applications -> Unknown Sources.

Disable USB debugging

USB debugging permits a user who can connect to the USB port to gain access to the state of the phone, as well as various files. On some firmware images this is enabled by default. This setting can be found under Settings -> Applications -> Development -> USB Debugging.

Potential Security Issues**USB Access**

Depending on the source of the device, USB debugging may be found to be enabled. Context examined devices that were shipped with the "generic" variant of Android as well as devices shipped with mobile operator-specific versions of the firmware. USB debugging is designed to permit a developer access to a command shell on the smartphone – but it could also be used to access other elements of the smartphone. This could allow an attacker to access data held on the device, install malicious applications and disable security measures.

Root Access

In a similar fashion to the iPhone's jailbreaking, Android can be manipulated into permitting the user to run software as the "superuser". This effectively removes all restrictions the user has on the device, including removal of the sandboxing between applications. The application "Universal Androot" is designed to provide a simple touch and click method to provide root level access on Android versions 1.6, 2.1 and 2.2.

Password Policy Override

At least one application has been released that is designed to override the password policy pushed down by the Exchange ActiveSync. The application, called "Lockpick" is designed to prevent the phone from locking, even if the Exchange policy mandates it.



Windows Mobile 6.5 (HTC Rhodium)

Introduction

Various incarnations of Windows Mobile have been available for many years, making Windows Mobile a mature platform. When deployed with suitable infrastructure, including an Open Mobile Alliance Device Management server, it is possible to create and manage a comprehensive security policy.

Like Android and the iPhone OS, the security depends on the integrity of the firmware image. Many customised versions of firmware have been produced and could be loaded onto a smartphone easily. This could permit the disabling of any centralised security policy.

Windows Mobile 6.5/HTC Rhodium

Security Features

The HTC Rhodium supports such features as:

- Remote wipe
- SIM lock (PIN code & PIN code request)
- Phone locking (lock code)
- Encryption of some user files
- Encryption of memory card
- Full support for EAS IT policies

VPN Support

The HTC Rhodium supports the following transport protocols to establish secure communications within enterprise environments:

- L2TP IPSEC
- PPTP
- The following methods can be used to perform authentication of the VPN tunnel:
 - RSA signatures
 - DSA signatures
 - Shared secret (PSK)

Device Management

The HTC Rhodium uses the standard OMA DM protocol to manage the smartphone. A large number of parameters can be configured. See Appendix A: Windows Mobile 6.5 policy items ([page no?]) for the full list. The below list is a high level overview:

- Email configuration
- Password policy
- Application
- Wireless Interfaces (WiFi/Bluetooth/IrDA)
- Applications permitted
- Device encryption
- Firmware updates
- Device certificates
- Application installation
- VPN settings



Windows Mobile 6.5/HTC Rhodium

Suggested Settings

The manufacturer of a Windows Mobile device can configure the device to operate in either a single-tier or two-tier mode. Single-tier operation elevates the user to the same privileges as the operating system, making it impossible to secure the device.

Two-tiered mode provides trusted and un-trusted modes of execution, depending on the certificate used to sign the binary being executed. Only trusted applications are permitted to access privileged API calls or access certain files or registry entries. This helps to maintain the security model. Some manufacturers provide both single-tier and two-tier mode firmware images. Context recommends the use of the two-tier mode.

Application installation restrictions can be put in place through the use of digital signatures and certificates. This requires a significant amount of work to configure a description of which is beyond the scope of this white paper.

Potential Security Issues

Autorun

By default Windows Mobile supports the use of "autorun", which permits memory media to be inserted in the device, and an application started when the device is next unlocked (if currently locked). This can provide an attacker with a mechanism for executing malicious code on the device without the knowledge of the owner. Such an application could be used to obtain the data on the device, install malicious applications and disable security. Context was able to produce a proof of concept code that copied all emails and attachments from the device to a different system.

Password Policy Override

A number of applications have been produced that are designed to override the password policy pushed down by the Exchange ActiveSync. Examples include ExchangePolicyPatch and StayUnlock. These prevent the phone from locking, even if the Exchange policy mandates it. Additionally, the ExchangePolicyPatch allows override of the password complexity and failed login wipe settings.



Smartphone Exchange ActiveSync clients

Introduction

The following section reviews the Exchange ActiveSync (EAS) clients used by many handsets to interact with enterprise messaging environments.

Exchange ActiveSync is an extension to the Microsoft Exchange server that allows mobile devices, including smartphones, to access the contents of a user's mailbox. Exchange ActiveSync is also intended to allow enterprises to deploy an IT policy that constrains how the handset should be used. Please see Appendix A: Windows Mobile 6.5 policy items for details on the policy items that can be set.

Android 2.1+ mail client

Inside Android-based handsets enterprise management functions are currently only supported within the Exchange ActiveSync (EAS) policies. Support for these policies is dependent on the version of Android, with Android 2.1 introducing native EAS client support within the mail application.

Support is limited to the basic (EAS 2.5) feature set:

- password (PIN/alpha)
- minimum characters in a password / PIN
- maximum number of failed attempts before a forced wipe
- inactivity timeout
- remote wipe

On older Android devices, the mail application does not support being used as an EAS client. This functionality is provided by third party applications such as Moxier Mail.

IT policy persistence

Context's testing of the IT Policy functions within Android 2.1+ indicated that the policy is only enforced during phone provisioning. This means that users and attackers can override the enterprise lockdown by disabling the requirement for a strong password.

iPhone mail application

The iPhone Mail application can be configured as an EAS client. This can either be performed directly on the handset or, if deploying against multiple handsets, within an enterprise environment via a provisioning profile generated by the iPhone Utility (IPU).

IPU generates XML formatted payloads that can be deployed to a handset via USB, Bluetooth or web download. As the provisioning profiles can contain sensitive information (including VPN configuration or Exchange Server settings and credentials) they should be protected. Consideration must be given as to how to deploy these profiles so that they are not exposed to malicious third parties.

Further details about using the iPhone mail application as an EAS client can be found at: http://images.apple.com/iphone/business/docs/iPhone_EAS.pdf. However like a number of non-Microsoft EAS clients, the iPhone does not currently support the entire suite of EAS policy settings. At the time of writing only the following settings were supported:



iPhone Supported Exchange ActiveSync security policies

- Remote wipe
- Enforce password on device
- Minimum password length
- Maximum failed password attempts (before local wipe)
- Require both numbers and letters
- Inactivity time in minutes (1 to 60 minutes)

Additional Exchange ActiveSync policies (for Exchange 2007 and 2010 only)

- 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
- Allow web browsing

Mail Storage

The iPhone mail application stores all items in clear text within the root partition of the iPhone. If the handset has been "jailbroken" then these items can be retrieved trivially using a modified version of the Zdziarski techniques (<http://www.iphoneinsecurity.com/>).

Moxier Mail

Moxier Mail is an EAS client for Android handsets that supports versions 1.5, 1.6, 2.0 and 2.1. It is provided as the default mail client for handsets such as the Sony Ericson Experia X10.

Moxier mail currently supports Exchange Server 2003 SP2/SP3 or Exchange Server 2007; however, it should be noted that:

- RSA SecurID Protected Servers are not supported
- VPN Protected Servers are not supported

This limitation may discount this EAS client for many enterprise environments.



IT Security Policy

Currently, Moxier Mail only supports the following policy items:

- 2003 certificate-based authentication
- 2003 allowing non-provisionable devices
- 2003 policy refresh intervals
- 2007 allowing html email
- 2007 attachments enabled
- 2007 maximum attachment size
- 2007 maximum calendar age filter
- 2007 maximum email age filter
- 2007 maximum email body truncation size
- 2007 maximum html email body truncation size
- 2007 requiring manual synchronization while roaming

Although this indicates that Moxier mail will honour IT policy (As "2003 Allowing non-provisionable devices" is present), testing by Context has established that in practice this meant that the client advises the Exchange server that the policy has been enforced without actually mandating the settings.



RoadSync

RoadSync is an Exchange Active Sync (EAS) client by Datavis and is provided as pre-installed package on selected handsets by LG, Nokia, Samsung and Sony Ericsson.

Like many third party EAS clients the ability for RoadSync to effectively implement an IT Security policy as defined by the MS Exchange environment is dependent on the platform on which it is running. For example on Android-based handsets the IT policy is honoured, but on Symbian Series 60 handsets it is not.

The following table of features within RoadSync was provided by Datavis at:

<http://www.dataviz.com/products/roadsync/series60/features.html>

Key Features	Android OS	Symbian Series 60
Price (as of August 2010)	\$9.99	\$49
Exchange 2003 (SP2 or higher)	☑ Yes	☑ Yes
Secure SSL Data Transmission	☑ Yes	☑ Yes
Direct Push Synchronization	☑ Yes	☑ Yes
E-mail	☑ Yes	☑ Yes
Attachments	☑ Yes	☑ Yes
Subfolders	☑ Yes	☑ Yes
Calendar	☑ Yes	☑ Yes
Meeting Response (Accept/Decline/Tentative)	☑ Yes	☑ Yes
New Meeting Creation (Invite attendees from device)	☑ Yes	⊗ No
Meeting Conflict Notification	⊗ No	☑ Yes
Contacts	☑ Yes	☑ Yes
Contact Photos	☑ Yes	☑ Yes
Global Address List	☑ Yes	☑ Yes
Tasks	☑ Yes	☑ Yes
GZip Data Compression	⊗ No	☑ Yes
Remote Wipe	☑ Yes	☑ Yes
IT Policy Enforcement	☑ Yes	⊗ No
Exchange 2007 (Initial Release & SP1)	☑ Yes	☑ Yes
HTML E- mail	☑ Yes	☑ Yes
E-mail Flags	☑ Yes	☑ Yes
Online Mailbox Search	⊗ No	☑ Yes



Key Features	Android OS	Symbian Series 60
SharePoint & UNC File Access	⊗ No	⊙ Yes
Fast Message Retrieval	⊙ Yes	⊙ Yes
Auto-Discovery of Server Settings	⊙ Yes	⊙ Yes
Out-of-Office Assistant	⊗ No	⊙ Yes
Device Specific Enhancements	⊙ Yes	⊙ Yes
Getting Started Wizard	⊙ Yes	⊙ Yes
Font Zooming Options	⊙ Yes	⊙ Yes
Sync over Cellular or WiFi	⊙ Yes	⊙ Yes
E -mail Pop-up Notifications	⊙ Yes	⊙ Yes
Keypad Shortcuts	⊗ No	⊙ Yes
Manual & Scheduled Sync	⊙ Yes	⊙ Yes
Peak/Off-Peak and Roaming Sync Options	⊙ Yes	⊙ Yes



Appendix A: Windows Mobile 6.5 policy items

The following table identifies items that can be configured on Windows Mobile, and identifies if they can be set through the Exchange ActiveSync protocol or through the OMA DM messages.

Setting	Description	Exchange ActiveSync	WinCE OMA DM
Allow Bluetooth	Specifies whether a device allows Bluetooth connections. The available options are Disable, HandsFree Only, and Allow. This policy setting requires an Enterprise Client Access License.	⊗ No	☑ Yes
Allow Browser	Specifies whether Pocket Internet Explorer is allowed on the device. This setting does not affect third-party browsers installed on the phone.	⊗ No	☑ Yes
Allow Camera	Specifies whether the device's camera can be used.	⊗ No	☑ Yes
Allow Consumer Mail	Specifies whether the user can configure a personal email account (either POP3 or IMAP4) on the device.	⊗ No	☑ Yes
Allow Desktop Sync	Specifies whether the device can synchronize with a computer through a cable, Bluetooth, or IrDA connection.	⊗ No	☑ Yes
Allow HTML E-mail	Specifies whether e-mail synchronized to the device can be in HTML format. If this setting is set to \$false all email is converted to plain text.	⊗ No	☑ Yes
Allow Internet Sharing	Specifies whether the device can be used as a modem for a desktop or a portable computer.	⊗ No	☑ Yes
Allow IrDA	Specifies whether infrared connections are allowed to and from the device.	⊗ No	☑ Yes
Allow non-provisionable devices	Specifies whether older phones that may not support application of all policy settings are allowed to connect to Exchange 2010 by using Exchange ActiveSync.	☑ Yes	⊗ No
Allow POP and IMAP Email	Specifies whether the user can configure a POP3 or an IMAP4 e-mail account on the device.	⊗ No	☑ Yes
Allow Remote Desktop	Specifies whether the device can initiate a remote desktop connection.	⊗ No	☑ Yes



Setting	Description	Exchange ActiveSync	WinCE OMA DM
Allow S/MIME software certificates	Specifies whether S/MIME software certificates are allowed on the device.	⊗ No	☑ Yes
Allow simple password	Enables or disables the ability to use a simple password such as 1234. The default value is \$true.	⊗ No	☑ Yes
Allow storage card	Specifies whether the device can access information held on a storage card.	⊗ No	☑ Yes
Allow text messaging	Specifies whether text messaging is allowed from the device.	⊗ No	☑ Yes
Allow unsigned applications	Specifies whether unsigned applications can be installed on the device.	⊗ No	☑ Yes
Allow unsigned installation packages	Specifies whether an unsigned installation package can be run on the device.	⊗ No	☑ Yes
Alphanumeric password required	Requires that a password contains numeric and non-numeric characters.	☑ Yes	☑ Yes
Application Blocking	Allows the blocking of binary files to prevent their execution on the smartphone	⊗ No	☑ Yes
Application Installation	Allows the OMA DM server to specify cab files to download and then install on the smartphone to permit remote application deployment	⊗ No	☑ Yes
Approved Application List	Stores a list of approved applications that can be run on the device.	⊗ No	☑ Yes
Attachments enabled	Enables attachments to be downloaded to the device.	⊗ No	☑ Yes
Certificate Enrolment	Permits the OMA DM server to install certificates, role masks, private key containers and renewal information on the smartphone	⊗ No	☑ Yes
Device encryption enabled	Enables encryption on the device. Not all devices can enforce encryption. For more information, see the phone and mobile operating system documentation.	⊗ No	☑ Yes
Maximum attachment size	Specifies the maximum size of attachments automatically downloaded to the device.	⊗ No	☑ Yes
Maximum calendar age filter	Specifies the maximum range of calendar days that can be synchronized to the device. The value is specified in days.	⊗ No	☑ Yes



Setting	Description	Exchange ActiveSync	WinCE OMA DM
Maximum e-mail age filter	Specifies the maximum number of days' worth of email items to synchronize to the device. The value is specified in days.	⊗ No	☑ Yes
Maximum e-mail body truncation size	Specifies the size beyond which email messages are truncated when synchronized to the device. The value is specified in kilobytes (KB).	⊗ No	☑ Yes
Maximum failed password attempts	Specifies how many times an incorrect password can be entered before the device performs a wipe of all data.	☑ Yes	☑ Yes
Maximum HTML e-mail body truncation size	Specifies the size beyond which HTML-formatted email messages are truncated when synchronized to the device. The value is specified in kilobytes (KB).	⊗ No	☑ Yes
Maximum inactivity time lock	Specifies the length of time that a device can go without user input before it locks.	☑ Yes	☑ Yes
Minimum device password complex characters	Specifies the minimum number of complex characters required in a device password. (A complex character is any character that is not a letter.)	⊗ No	☑ Yes
Minimum password length	Specifies the minimum password length.	☑ Yes	☑ Yes
NAP Configuration	Permits configuration of GSM/GPRS/CDMA connections as well as RAS, RTT and desktop pass-through.	⊗ No	☑ Yes
Password enabled	Enables the device password.	☑ Yes	☑ Yes
Password expiration	Enables the administrator to configure a length of time after which a device password must be changed.	⊗ No	☑ Yes
Password history	Specifies the number of past passwords that can be stored in a user's mailbox. A user can't reuse a stored password.	⊗ No	☑ Yes
Password recovery	When this setting is enabled, the device generates a recovery password that is then sent to the server. If the user forgets their device password, the recovery password can be used to unlock the device and enable the user to create a new device password.	⊗ No	☑ Yes
Policy refresh interval	Defines how frequently the device updates the Exchange ActiveSync policy from the server.	⊗ No	☑ Yes



Setting	Description	Exchange ActiveSync	WinCE OMA DM
Require Device Encryption	Specifies whether or not device encryption is required. If set to \$true, the device must be able to support and implement encryption to synchronize with the server.	⊗ No	☑ Yes
Require encrypted S/MIME messages	Specifies whether S/MIME messages must be encrypted.	⊗ No	☑ Yes
Require manual synchronization while roaming	Specifies whether the device must synchronize manually while roaming. Allowing automatic synchronization while roaming will frequently lead to larger-than-expected data costs for the device plan.	⊗ No	☑ Yes
Require storage card encryption	Specifies whether the storage card must be encrypted. Not all device operating systems support storage card encryption. For more information, see your device and mobile operating system for more information.	⊗ No	☑ Yes
Synchronization	Permits the OMA DM server to configure the client settings for Exchange ActiveSync deployment.	⊗ No	☑ Yes
Unapproved In ROM application list	Specifies a list of applications that cannot be run in ROM.	⊗ No	☑ Yes
VoIP	Allows an OMA DM server to configure VoIP settings for use with a SIP server.	⊗ No	☑ Yes
VPN	Permits the OMA DM server to configure VPN setting on the smartphone	⊗ No	☑ Yes
WiFi	Permits the OMA DM server to configure WiFi settings, including globally disabling/enabling it.	⊗ No	☑ Yes



Appendix B: Smartphone anti-malware software

At the time of writing, there are a number of vendors supplying products that claim to provide anti-malware protection for smartphones. These vendors include some of the biggest names in desktop anti-malware as well as providers of bespoke security software designed for smartphones.

Context reviewed a number of these products. All of them detected the standard antivirus test file 'EICAR' within a test lab. All of these tools are also heuristic based and most of them leverage the signatures from within the PC desktop space, meaning they search for code that will have only limited impact on a mobile device. In the longer term, as more mobile-aware malware is developed, this type of software will become more important to the security of mobile devices.

BlackBerry

Smobilesystems.com provides a BlackBerry product that detected EICAR / RedProxy. However, RIM's best practice advice is to deploy an enterprise grade antivirus product at the gateway, perhaps on the BES server in an isolated network.

iPhones

Although there are a number of AV manufacturers planning to provide iPhone support, Trend appears to have succeeded in being the first to market with its "Trend Smart Surfing" application.

Smartphone antivirus packages (Aug 2010)

	Symbian Series 60 3rd Edition	Windows Mobile 6.5	Android	iPhone	BlackBerry
AhnLab Mobile Security http://global.ahnlab.com/en/site/main/main.do	☑ Yes	☑ Yes	⊗ No	⊗ No	⊗ No
Avira AntiVir Mobile http://www.avira.com/en/products/avira_antivir_mobile.html	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No
BitDefender Mobile Security http://www.bitdefender.com/PRODUCT-2149-en--BitDefender-Mobile-Security-v2.html	⊗ No	☑ Yes	⊗ No	⊗ No	⊗ No
BullGuard Mobile Antivirus http://www.bullguard.com/why/bullguard-mobile-antivirus.aspx	☑ Yes	☑ Yes	⊗ No	⊗ No	⊗ No
Dr.Web Mobile Security Suite http://products.drweb.com/mobile/wi/?lng=en	☑ Yes	☑ Yes	☑ Yes	⊗ No	⊗ No



	Symbian Series 60 3rd Edition	Windows Mobile 6.5	Android	iPhone	BlackBerry
F-Secure Mobile Security http://www.f-secure.com/en_EMEA/products/mobile/mobile-security/	☑ Yes	☑ Yes	☑ Yes	⊗ No	⊗ No
Kaspersky Mobile Security http://www.kaspersky.co.uk/kaspersky_mobile_security	☑ Yes (Nokia only)	☑ Yes	⊗ No	⊗ No	⊗ No
Lookout Mobile Security https://www.mylookout.com/	⊗ No	☑ Yes	☑ Yes	⊗ No	☑ Yes
Norton Smartphone Security http://www.symantec.com/norton/smartphone-security	☑ Yes	☑ Yes	⊗ No	⊗ No	⊗ No
Smobile Systems Security Shield http://www.smobilesystems.com/	☑ Yes	☑ Yes	☑ Yes	⊗ No	☑ Yes



Appendix C: Configuring IPsec VPNs on Smartphones

Nokia Symbian Series 60 3rd Edition

Nokia's advice on configuring Series 60 handsets to use a VPN can be found at:

http://europe.nokia.com/EUROPE_NOKIA_COM_3/Get_Support/Software/Nokia_Mobile_VPN/Nokia_Mobile_VPN_Administrators_Guide.pdf

iOS iPhone

Apple has produced a number of guides for configuring iPhones to work in the enterprise. The guide for configuring the iPhone for VPN access can be found at:

http://images.apple.com/iphone/business/docs/iPhone_VPN.pdf

Android

A good guide for configuring VPN connections on Android phones (although focused on the Nexus One) can be found at:

<http://www.knowyourmobile.com/google/nexus-one/nexus-one-guides/396121/how-to-configure-a-vpn-connection-on-your-google-nexus-one.html>

Windows Mobile

The MSDN article documenting the VPN functionality of Windows Mobile can be found at:

<http://msdn.microsoft.com/en-us/library/cc440255.aspx>



About Context

Context Information Security is an independent security consultancy specialising in both technical security and information assurance services.

The company was founded in 1998. Its client base has grown steadily over the years, thanks in large part to personal recommendations from existing clients who value us as business partners. We believe our success is based on the value our clients place on our product-agnostic, holistic approach; the way we work closely with them to develop a tailored service; and to the independence, integrity and technical skills of our consultants.

The company's client base now includes some of the most prestigious blue chip companies in the world, as well as government organisations.

The best security experts need to bring a broad portfolio of skills to the job, so Context has always sought to recruit staff with extensive business experience as well as technical expertise. Our aim is to provide effective and practical solutions, advice and support: when we report back to clients we always communicate our findings and recommendations in plain terms at a business level as well as in the form of an in-depth technical report.





Context Information Security Ltd

London (HQ)

4th Floor
30 Marsh Wall
London E14 9TP
United Kingdom

Cheltenham

Corinth House
117 Bath Road
Cheltenham GL53 7LS
United Kingdom

Düsseldorf

Adersstr. 28, 1.OG
D-40215 Düsseldorf
Germany