



Whitepaper

July 2008

Choosing an Enterprise-Class Wireless Operating System

A J.Gold Associates White Paper

“Security considerations remain the single biggest limitation to more aggressive expansion of wireless device usage in many enterprises. Regulated industries (e.g., financial, insurance, investments, retail, legal, health care, public sector) can not afford to deploy anything that could possibly compromise their data/records security or prevent meeting regulatory compliance requirements. Portable devices, easily lost and/or stolen, represent a threat that while real, can be managed with proper planning and foresight..... It is imperative that companies evaluate a potential device selection based on its inherent platform security capabilities, particularly around the security embedded within the device Operating System (OS)”





Choosing an Enterprise-Class Wireless Operating System

Contents

Introduction	2
<i>Mobile Trends</i>	<i>2</i>
<i>Limitations.....</i>	<i>2</i>
<i>Mitigating Risks.....</i>	<i>3</i>
Why Worry About Security?.....	3
Components of a Secure Mobile OS.....	4
<i>Authentication</i>	<i>4</i>
<i>Data Vaulting</i>	<i>4</i>
<i>Application Verification.....</i>	<i>5</i>
<i>Reliability.....</i>	<i>5</i>
<i>Manageability and Policy Enforcement.....</i>	<i>5</i>
<i>Tamper Resistance.....</i>	<i>6</i>
<i>Security vs. Usability.....</i>	<i>6</i>
<i>Meeting Security Validations.....</i>	<i>6</i>
<i>Allowing Security Extensions.....</i>	<i>7</i>
What Should Enterprises Look For in a Secure Mobile OS?.....	7
<i>Some Questions to Ask During Evaluation:</i>	<i>7</i>
Conclusions.....	8



Choosing an Enterprise-Class Wireless Operating System

Introduction

The accelerating deployment of wireless smart phone devices is being driven in large part by a growing requirement to keep an increasingly mobile workforce connected while outside the company's physical confines. The array of mobile workers continues expanding to include dedicated field workers (e.g., sales, services, delivery, maintenance, construction, public safety), support staff (e.g., IT, health professionals, repair personnel), and management and the executive ranks (e.g., CxO, finance, HR, legal, administrative staff). This expansion is taking place across a broad array of industries (e.g., financial, legal, real estate, retail, hospitality, government, technology) and in companies both large and small. Within the next few years, many workers will be mobile 50%-75% of their normal work schedule, which is becoming more flexible and not always confined to the standard nine to five work hours. As a result, a method for staying connected at any time and from any location to mission critical corporate systems, (e.g., email, ERP, CRM, SFA, FFA) is of highest priority. Increasingly capable mobile smart phone devices with the computing power and storage capacity of a typical PC of only a few years ago, coupled with enhanced cellular networks that provide higher bandwidth at affordable cost, are driving adoption of mobile devices in companies of all sizes and across a vast array of industries. We expect this to continue for the foreseeable future, with a number of emerging mobile trends working to accelerate widespread adoption of wireless technology.

Mobile Trends

As a result of the growth in worker mobility, and the enhancements in device and wireless communications technology, a number of key mobility trends are emerging. Within the next 3-4 years, we expect greater than 85% of enterprise users to have a device capable of email, web access, collaboration (IM, Presence) and back office application interactions. Further, we expect that the vast majority of companies (65%-75%) will have made corporate applications accessible from mobile devices. Voice communications will remain an important aspect of mobile worker productivity, and 25% of users will deploy a mobile device as their only means of staying in contact (eliminating their desk phones). This will require the addition of a unified communications capability to fully enable mobile collaboration. We expect 15%-25% of corporate users to virtually eliminate the need for a notebook PC during their normal business hours, only using a PC-class device occasionally for specific tasks like long document preparation. Finally, we expect the number of smart phone devices to exceed the number of PCs in many organizations as virtually every employee is provided with the basic collaboration tools needed to perform his or her job from virtually any location (e.g., voice communications, email, IM/SMS, web access/application services).

Limitations

The growing influence of wireless devices will dramatically alter the way many companies interact with their workers. However, one of the key limitations to many organizations' ability to enable their mobile users with these highly functional devices is the risk of a security breach. Indeed, security considerations remain the single biggest limitation to more aggressive expansion of wireless device usage in many enterprises. Regulated industries



Choosing an Enterprise-Class Wireless Operating System

(e.g., financial, insurance, investments, retail, legal, health care, public sector) can not afford to deploy anything that could possibly compromise their data/records security or prevent meeting regulatory compliance requirements. Portable devices, easily lost and/or stolen, represent a threat that while real, can be managed with proper planning and foresight.

Mitigating Risks

The first step in making the mobile environment safe for both the end user and the corporation, is selecting a device that exhibits high levels of inherent security. To this end, not all devices are created equal. It is imperative that companies evaluate a potential device selection based on its intrinsic platform security capabilities, particularly around the security embedded within the device Operating System (OS). This paper will explore some of the key criteria necessary in a mobile OS so that enterprise use of the device will not compromise the integrity of the company's security and put it at risk for costly legal and/or governmental actions.

Why Worry About Security?

Security in a wireless environment is no longer just an academic argument. The increasingly common loss of data and security breaches at large and small companies alike, and the increasing levels of regulation and oversight (e.g., HIPAA, SOX), are making it an imperative for organizations to secure their data from loss or "data leakage". While most high profile cases in the past have been a result of notebook theft or loss, the tremendous growth in use of wireless devices and their increasing capability to connect with corporate systems and store substantial amounts of on-board data, make the potential for a significant data breach a high probability. Indeed, we expect to see some highly publicized breaches within the next year. Moreover, it is highly likely that some have already occurred, but organizations have not detected such losses due to poor wireless security policies, monitoring and enforcement.

Many mobile devices are incapable of providing the level of inherent security needed to protect against such losses. In many cases, if data is lost, the user and/or company will not even know. It is therefore imperative that companies select wireless devices that can provide high levels of security to protect sensitive data and conform to compliance and audit requirements that are becoming an increasingly common part of the regulatory landscape.

Certainly nothing can be made 100% secure. This is an impossible task and one that remains an ongoing battle between device manufacturers and their unintentional security flaws. Yet although there is no 100% guarantee, companies must make concerted efforts to choose a device with an environment that affords maximum protection to all data on that device. Providing for an adaptable security capability for various users and processes, selectable by the device administrator, is one of the best ways to achieve the highest level of security needed without the negative impacts it may cause. Ultimately, security should remain transparent to the end user, both in usability and performance.



Choosing an Enterprise-Class Wireless Operating System

Early generations of high level on-board security often made devices slow and cumbersome to operate. Many vendors in the past had to downgrade security to manage performance tradeoffs between providing the highest level of data encryption (number of bits and types of algorithms, e.g., DES, 3DES, AES, 56, 112, 128, 256 bits) and available device resources (e.g., processors speed, memory, battery life). With current generation devices, this is no longer an issue, as adequately designed devices with ample processor and memory capability allow the highest level of security (AES 256 bit) with little system performance degradation. Enterprises should not accept any platform that does not support the maximum level of security, and should make this a prime criterion for device selection.

No large scale deployment to business users can be successful if security gets in the way of the end user experience and ability to perform his or her job effectively. Security done right should not have any substantial negative impact on the processing speeds or on lessening the battery life of the device. Further, it should not significantly slow the network throughput and/or delay data transmissions and reception (i.e., scanning of each message). This has been a major issue in previous generation devices, but has largely been addressed in best-in-class current generation devices. Finally, a secure OS must work in tandem with the platform to insure a cooperative HW/SW approach to total security.

Components of a Secure Mobile OS

There are a number of important components that make an OS secure and safe for business use. Below we identify some of the key attributes necessary to enable any secure mobile platform and that need to be evaluated by any organization considering the use of that platform.

Authentication

Users should not be able to work on any device without adequate levels of authentication to prove he/she is the owner of the device. Passwords and two factor authentication (e.g., smart cards), are being deployed currently, with biometrics to be added in the near future, to insure that only the approved user of the device is allowed to access the functions and data on that device. Any device that can't be forced to require user authentication (through the setting of proper policies) should not be considered a security-ready, business-class device. Further, the ability of the end user to bypass and/or defeat authentication requirements should disqualify the device for any user accessing and maintaining corporate sensitive data, either in emails, or in accessing back office applications. Proper authentication is the first barrier of defense in any secure system, and should not be taken for granted.

Data Vaulting

The need to safely store data on the device, and any external storage, (e.g., SD cards), is a key requirement for any mobile worker with access to company information. Indeed, Data Vaulting offers a second level of protection in conjunction with authentication against device "hacking". All levels of security for any data file and for every application on the device



Choosing an Enterprise-Class Wireless Operating System

should be selectable by policies administered by the device and/or corporate security administrator as defined by company security policy. This should be enforceable at all times, and not just on some of the data some of the time. Some platforms require that all data on the device be either encrypted or not encrypted. However, certain forms of data on the device should be able to be selected to “unprotect” mode, for those files obviously not needing protection from prying eyes (e.g., MP3s, camera photos). Therefore, one criteria of any best-of-class device should be the ability to granularly select files and functions that need encryption, and those that do not, and have the platform act accordingly.

Application Verification

To ensure maximum protection to both the platform and the data, devices should contain a mechanism for verifying that an application is indeed “who and what” it claims to be. Enterprise-class mobile platforms include a method for assessing signatures of various applications that, when checked by the device, can determine an authentic, non-tampered with application, from one that has been modified and/or contains suspect code. Clearly, the ability of the OS to distinguish between legitimate, safe applications and potentially destructive ones offers a major enhancement that any best-of-class mobile device should incorporate. This is an important defense against both malware and rogue applications that could cause havoc with the proper and effective use of the device. As a further requirement, IT must be able to control the approval of any applications resident on the device, and the user must be prevented from tampering with these controls.

Reliability

Any enterprise-class mobile OS should exhibit the reliability end users expect from a robust mission-critical device. This means that the device should never simply decide not to work (e.g., “Blue Screen”), or require unexpected re-boots. Further, in a working-class device, any peculiarities with the OS (e.g., crashes, freezing) will likely cause more than just inconvenience – they will cause work to be lost, lowering overall productivity and raising support costs, not to mention increasing end user frustration levels. This may be acceptable in a consumer device, but not in an enterprise-class production device. Companies should make sure that any mobile OS being evaluated for its mobile workforce be examined for its reliability and capability to withstand the rigors of the mobile work model.

Manageability and Policy Enforcement

A device that can't be remotely managed will add significant amounts of TCO and additional support burdens to any organization deploying it. Companies evaluating devices should examine whether the device OS offer hooks to manage all aspects of the platform (e.g., set up, monitoring, uploading, display of device characteristics, asset management, lock down and kill, re-imaging to a new device, OS software upgrades). If such capability is not inherently available within the OS, it is highly unlikely any security and/or management tools will be able to competently manage all of the functions necessary in a complex, current generation smart phone. Further, companies should examine whether policies can be set up for individual users on specific devices, whether policies can be created to take into account



Choosing an Enterprise-Class Wireless Operating System

various user classes and/or device characteristics, and whether different apps and different data can be provisioned for different classes of users on a case by case basis. All of these functions should be available within any platform designated for efficient and productive organizational use.

Tamper Resistance

Companies should always seek to discover whether any device has been “hacked” or attempts have been made to alter the base level OS. While Malware is not yet a major problem for smart phones, it will be in the near future as more “hackers” view the increasing number of smart phones as an attractive target. The more tamper resistant the OS, the less likely that malware can infect and affect the platform, reducing risks for the company in both safekeeping the individual device, but also in stemming any spread of the malware. An OS that only allows applications to run at a higher level than the core of the OS (e.g., in a Virtual Machine) represent a much lower security risk to the organization than one that allows applications to get deeply into the core of the OS. Companies should at the minimum evaluate the platform’s ability to make the administrator aware of any problems, and preferably provide a sanitized area to contain applications to prevent infections.

Security vs. Usability

Nearly any mobile OS can be secured by totally locking down the device and preventing any meaningful interactions with the OS. However, while it certainly is important to maintain the highest level of security possible, this must be done while maintaining the usability of the apps and end user interface. Creating an environment that enables maximum usability while maintaining the integrity of the system requires a delicate balance. Companies looking for highly secure devices should evaluate the level of security in conjunction with the usability of the system, and whether or not the end user finds the OS easy to use, navigate and customize for reasonable personal preference needs. One size does not fit all, and the level of security must be balanced against the needs of the user community. However, the final choice should be weighted more heavily towards security than usability if a tradeoff needs to be made.

Meeting Security Validations

Many industries require that devices be validated and approved by governmental agencies to ensure that they meet stringent security testing and specifications before they can be deployed to mobile workers. While a number of devices claim to be “compatible” with security standards like FIPS-140-2 encryption, it is imperative that they have been tested and approved by a validated testing agency and not just offer claims of compatibility. Further, new security standards are evolving and will be required for certain classes of users. The ability to prove compatibility with these emerging standards is imperative in many industries and government agencies. Although an entire platform is tested, no device can meet the challenge of security validations without having an OS that is capable of meeting the stringent approval process. Therefore, companies looking for a device with maximum security should begin by looking at the OS and whether it is capable of being validated



Choosing an Enterprise-Class Wireless Operating System

against a variety of security standards, and preferably choose one that has already undergone verification testing and has been accredited.

Allowing Security Extensions

No one vendor can provide everything necessary for all circumstances now and in the future. Companies may have a security need not currently available as an integral part of the platform. An ability to extend the security model should be provided by the vendor through an API. This allows extensions as required (e.g., S/MIME, PGP, RSA). Companies that must implement specialized security enhancements should evaluate the platform for its ability to be extended and conform to those needs in a safe and flexible manner.

What Should Enterprises Look For in a Secure Mobile OS?

As we can see from the above discussion, choosing a secure, robust, best-in-class mobile OS is not a trivial matter. Despite the many OS platform issues identified, many companies are rather lackadaisical about choosing an OS/mobile device platform. They often opt to choose a phone/device without regard to many of the broader implications. We believe that while the ergonomics, features and capabilities of a particular device are indeed important, the underlying platform should undergo extensive examination before any choice is finalized. To that end, we believe companies should, at the minimum, evaluate a mobile OS platform using the following criteria.

Some Questions to Ask During Evaluation:

- What level of security is inherent in the OS and HW platform?
- What is the vendor philosophy towards embedded vs. external (add-on) security?
- Is the security model consistent across all devices powered by the OS?
- How easy is it to bypass security features (e.g., Password)?
- Can end users change the security settings easily?
- Can users defeat policy enforcement on the device?
- Can a system administrator “lock-down” the device?
- What types of tools are provided to manage security?
- What level(s) of encryption is (are) available?
- What is encrypted – all data, selected files?
- How does encryption/security affect performance of the device?
- How safe is the OS from malware attack?
- How has the OS and platform been designed to thwart attacks?
- Is there a protected area for apps to run safely?
- Does an app need to be certified and verified to run on the platform?
- Which security certifications have been achieved (i.e., tested and verified)?
- Is the vendor planning new/additional certifications?
- How easy is it to set user/device policies and enforce them?
- How granular is the policy setting capability (i.e., functions and user classes)?
- Does the platform vendor provide adequate tools or is a third party product required?



Choosing an Enterprise-Class Wireless Operating System

- Is the management philosophy scalable over large numbers of devices?
- Can the device be easily wiped/killed in case of loss?
- How extensible is the OS to allow new capabilities?
- Are peripherals (e.g., memory cards) a protected component of the security model?
- Does the OS security stand-alone, or does it require integration with other products?
- Is the TCO substantially raised by the required security management?
- Can security settings be easily transferred to a new/replacement device?
- How quickly can device security be implemented (i.e., degree of difficulty)?
- Does the OS allow Over The Air (OTA) management or must it be hard-wired?
- How transparent is the security model to the end user?

We believe all of these issues, and other issues specific to an organization's circumstances and deployment requirements, must be evaluated if the organization is to select and deploy the most secure mobile device environment. Failure to adequately determine and evaluate the security capabilities of a selected platform will cause an increased risk of security breaches and compliance exposure that should be unacceptable risks to any organization wishing to protect its most valuable assets – its data.

Conclusions

Wireless mobile devices represent a potential security challenge for organizations with a highly mobile workforce. However, the amount of risk can be managed by carefully selecting an enterprise-class platform with an OS that has included the important features needed to secure the device and data contained therein. Companies of all sizes need to make a device choice based on the attributes that enhance security, manageability, robustness and ease of use. They are further required to balance the needs of the organization with the needs of the individual user for features, functions and ergonomics (the "Wow" factor). It is possible to choose a platform with a compelling user experience while also having a best-in-class secure smart phone device. With careful planning, there is no reason why mobile devices can't be effectively integrated into the strong security policy and implementation environments maintained in many organizations. Mobility is a growing trend amongst companies and organizations of all sizes, and providing tools to maintain or increase productivity of mobile workers of all types and functions is a business imperative. Security should not be used as an excuse not to deploy wireless devices to the workforce. But companies failing to make wise choices and secure their mobile devices will face major problems resulting in fines, regulatory non-compliance, potential legal challenges and ultimately loss of revenues.

About the author

Jack E. Gold is Founder and Principal Analyst at J.Gold Associates. Mr. Gold has over 35 years in the computer and electronics industries, including work in imaging, multimedia, technical computing, consumer electronics, software development and manufacturing systems. He is a leading authority on mobile, wireless and pervasive computing, advising clients on business analysis, strategic planning, architecture, product evaluation/selection and enterprise application strategies. Before founding J. Gold Associates, he spent 12 years with META Group as a Vice President in Technology Research Services. He also held positions in technical and marketing management at Digital Equipment Corp. and Xerox. Mr. Gold has a BS in Electrical Engineering from Rochester Institute of Technology and an MBA from Clark University.

About J.Gold Associates

Founded by an internationally recognized expert and industry veteran with over 35 years of experience in engineering, product marketing, market research and analysis, and technology advisory services, J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.



J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com