



Technology Brief...

August 30, 2008

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

What Should Companies Look for in a Secure Mobile OS? *

INSIDE THIS ISSUE

- 1 What Should Companies Look for in a Secure Mobile OS?
- 2 Does Google's Chrome Indicate What to Expect with Android?
- 3 Using iPhones in the Enterprise
- 4 Recent Research Reports- Published for our Clients

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 device without regard to many of the broader implications. We believe that while the ergonomics, features and capabilities of a particular device are 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 asking the following questions 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?
- Is the management philosophy scalable over large numbers of devices?

"...Failure to adequately determine and evaluate the security capabilities of a selected platform should be unacceptable to any organization wishing to protect its most valuable assets – its data....."

- 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.

Bottom Line: 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.

** The above is an excerpt from the J.Gold Associates Whitepaper: "Choosing an Enterprise-Class Wireless Operating System" - which is available upon request.*

Does Google's Chrome Indicate What to Expect with Android?

Google recently released a new browser set to compete directly with Microsoft's Internet Explorer and Firefox Mozilla. Chrome is supposed to provide a more compelling, easier to use and faster browsing experience, with a look and feel that "Googl-ites" should find familiar (and others may not). Google's goal, or course, is to capture as much of the search and homepage market as it can to increase its revenues (it doesn't make any money on the browser, which is free). But is providing a new browser the best way to establish more dominance, or an indication of its hubris?

"... We should expect to see several problems materialize over the first few months of operation of Android The ultimate test will be ... how well and how rapidly (and how openly) Google admits to the problems and fixes them....."

Google has similarly been working on a new mobile phone operating system, with much fanfare, for the past year. It is getting near launch time (we expect the first Android phone from HTC by the end of 2008). However, do the early issues and holes that are appearing in Chrome provide an indication of what the new Android phone OS might be like? After all, Google has been working on both for some time and assumedly with the same corporate software development and test culture in place.

Building a feature-rich, robust OS of any kind is difficult, especially one for a phone which must not only manage the data side, but also operate all the phone functions. It took most phone OS players, including Palm,

RIM, Symbian and Microsoft, several iterations to get it right (some would argue they still haven't). Even Apple's new iPhone OS has some bugs that require fixing. So it is highly likely that the first version of Android will have issues as well.

Using Chrome as an example of a new and complex Google product trying to provide extensive capabilities may be educational. For instance, Chrome has now only been in operations for a few short weeks, but discoveries have already been made that it exhibits some security issues, may be subject to DOD attacks, may not handle memory as cleanly as initially thought, and may not render all pages correctly. This is not to say that Chrome is a bad product. But it does indicate that first versions of complex products tend to be buggy and prone to security and performance challenges.

Android is being awaited with much anticipation. What should users expect? If they are expecting to see a robust, complete, optimized OS running all the features and functions smoothly and in complete security, they are apt to be disappointed. It is highly probable that Google has not tested every single possible scenario for the OS (it's probably impossible to do so), and that particular vendor implementations and hardware designs will cause some strange problems to occur. This is common and part of any new product cycle.

Bottom Line: We should expect to see several problems materialize over the first few months of operation of Android. The ultimate test will not be whether or not there are issues with Android (there are bound to be), but how well and how rapidly (and how openly) Google admits to the problems and fixes them. This may well mean the difference between success and failure of Android. In the mean time, unless you are willing to put up with a few "gotchas" with Android, you should probably wait until generation two of the devices and OS before jumping in.

Using iPhones in the Enterprise

The iPhone continues to sell in large numbers and has become very popular, including with some enterprise users. And although many companies are planning to support the iPhone eventually, most are still concerned about its lack of robust, enterprise level security features. This is especially true in regulated industries (e.g., banking, insurance, health care, retail) where any data loss or breach can have major ramifications. Despite this concern, many executives are pushing their IT departments to allow iPhone use. Should companies support iPhones for business applications?

We continue to believe that any enterprise that allows its users to store corporate information on an iPhone is putting that data at risk of loss or theft. The lack of encryption and the ease at which "hackers" have been able to access the device have demonstrated it is not robustly secure.

"...most companies should limit the use of the devices to either thin client access over a VPN, or through specially constructed, secured thick client applications....."

Further, the ability of the end user to exert near complete control over the device prevents companies from setting and enforcing lock down policies often necessary to enhance the security of the device. Despite the risks, there is a substantial portion of enterprise users who want the iPhone to become a supported device (including in the executive ranks). While we expect the iPhone to gradually (over the next 1-2 years) make steady improvements in security, companies should consider the device "security challenged" at this point.

Enterprises may choose to allow limited use of iPhones, both to assuage executive users and to test the devices within the corporate setting. There are two ways to do that safely. One way is to allow users to access company information via a thin client (browser) over a VPN connection where no data actually resides on the device. Once the browser is closed or the connection broken, the data is inaccessible. However, that requires reliable, high speed connectivity if performance is not to suffer. The other way is to obtain a third party application that builds its own secured client (via the SDK/APIs). In this case, all data resides in an encrypted "container" separate from the rest of the device. Such a client must be downloaded and installed on the device, and can be secured by the IT department, although the iPhone does allow nearly unlimited end user control of the device and therefore the end user could potentially uninstall or otherwise modify the client. While neither of these methods is perfect, it does allow companies to offer business apps to iPhone users while substantially mitigating risk.

It is clear that iPhones will be making their way into the enterprise, even though Apple has not done an adequate job to date of directly providing the tools needed by the enterprise to secure and manage the device. Nevertheless, third party solution providers (e.g., Lotus, Sybase iAnywhere, SAP) will build applications that overcome the lack of security of the device. This will make it more acceptable from a risk perspective, and allow the demand for the iPhone to be met in many companies for some applications.

Bottom line: We expect Apple to improve the security and manageability of the device over the next 1-2 years making it more attractive to enterprise users across a wider range of applications. Until then, most companies should limit the use of the devices to either thin client access over a VPN, or through specially constructed, secured thick client applications.

Recent Research Reports – For Our Clients

- Can AMD Survive? - What Should Users Do? - Sept 4, 2008
- Intel: SOC it to CE - July 30, 2008
- Andr-ian or Sym-droid? - July 24, 2008
- Nokia Shakes Symbian to its Foundation - June 24, 2008
- iPhone 3G: Still coming Up Short for the Enterprise - June 12, 2008
- Securing Laptops Against Government's Prying Eyes - April 28, 2008



J. Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

*Research, Analysis,
Strategic Consulting*