

# Secure Smartphone Apps: The Next Generation

The latest smartphone applications foster more mobility and productivity than ever before—as long as a secure mobile network is in place.



Patrick  
Stacey: Coming to LA this weekend. Let's book some dinner reservations.  
Patrick: Fantastic! Same place as last time?  
Stacey: Sure - I am good with that. See you tomorrow!  
Patrick: What time are you arriving?  
ge you when my flight arrives!



**It's no secret: Smartphones are infiltrating the corporate world and making employees more productive.**

Their use is no longer dictated by IT departments that provision them to executives and salespeople. The rank-and-file are buying them and receiving them as holiday gifts. And thanks to increased processing speeds and the availability of a wide range of corporate and consumer applications, the role of the smartphones is growing—as well as the risk they potentially pose to the corporate network.

## The Challenge of perception: The Smartphone as a Mini-computer

Respondents to the 2008 J. Gold Associates study *Enterprise Mobile Applications: A Study of Strategies and Adoption Trends* indicated that the median number of smartphone devices would grow 100 percent in three years, with access to corporate applications from those devices growing 196 percent in the same amount of time. And application availability is the primary driver for the rise of smartphones.

The average mobile phone is no longer just a voice and e-mail device. Smartphone users have access to hundreds, if not thousands, of applications at their fingertips. Con-

more than 40 percent of smartphone users have clicked on a link in an e-mail received on their phone. In fact, according to the survey, Windows, Palm, and Symbian OS smartphone users are significantly more likely to click on e-mail links from their smartphone than from their computer. These are alarming numbers considering that smartphones have historically been deployed to provide users with mobile e-mail access, and e-mail is a primary vector for phishing schemes.

"Everyone has thought of mobile devices as something that was different than the PC and therefore not subject to the same problems the PC has had," says Maribel Lopez, founder and CEO of Lopez Research. But that's no longer

**"I would not discount the incredible creativity of bad people. There are people who spend their lives trying to break into things, and you can never be 100 percent secure."**

—JACK GOLD, J.GOLD ASSOCIATES

sider this scenario: Jane is flying to Boston for a convention. Before leaving, she checks the status of her flight with a flight tracking application. Upon arrival to Boston, she uses a GPS application to locate the convention center—and some nearby restaurants. Expense management and call tracking applications facilitate the administrative work associated with her trip. At the convention she uses an application to quickly swap contact information with potential customers. Before having a drink with a high-profile client, she checks his accounts using an enterprise CRM application. All these applications helped Jane improve her productivity—and they're all on her smartphone.

Employees at every level of business recognize the convenience and productivity benefits of running applications on their smartphones. But users are often unaware of the valuable data stored on their smartphones and of the potential security risks.

A 2009 Trend Micro survey shows that 44 percent of more than 1,000 smartphone users are lax when it comes to surfing the Web on their mobile phones, and

the case. Today's devices are loaded with more memory and processing power than ever before. The average mobile phone has been transformed from just a simple cell phone into a minicomputer.

Naturally, users want to connect their minicomputers to the corporate network to access e-mail and business data, and IT departments are hard-pressed to grant them this access. The pressure comes in many forms, from the employee who receives a new smartphone for Christmas to the desire to attract a new generation of workers who want the flexibility to work from anywhere, at anytime. But connecting these devices means exposing the network to potentially insecure computing devices and the questionable applications running on them.

## Mobile Application Security Threats

Despite their many benefits, mobile applications introduce a number of threats to the corporate network. Consumer-based smartphone users can download mobile applications from the operating systems' application stores. These

applications have not necessarily been certified, and there's no guarantee that they're free of bugs or malware. For example, applications such as FlexiSPY capture emails, texts, browsing history and telephone calls, and store the information on a server. Though marketed as tools to catch cheating partners and protect children, the applications are, essentially, spyware—and if the smartphone they're downloaded on is also used to access corporate data, that data will be comprised. All that information is sent off to a server for retrieval by an unauthorized individual. Other spyware applications call a number on the user's phone without leaving evidence in the call history, and then turn on the microphone to listen to everything said within the phone's vicinity.

It's challenging for companies to detect these applications because they attack the device, not the network, explains Jack Gold, founder of J. Gold Associates. But that doesn't mean that someone won't write a piece of malware that can infect the network. "I would not discount the incredible creativity of bad people. There are people who spend their lives trying to break into things, and you can never be 100 percent secure," says Gold.

Some consumer-based applications make seemingly legitimate use of the data users have on their smartphones.

For example, laws against mobile phone use while driving have spurred the development of applications that offer text-to-voice services so that users can hear their incoming text messages. These applications take a copy of the message, send it off to a server that converts it to an audio stream, and send the audio stream back to the phone. These applications may be helpful to folks who are on the road a lot, but they release potentially sensitive corporate data to third-party sites.

Even if your organization chooses to block all third-party applications except for those pushed to users' devices by IT, you still have to manage data stored on the device itself. Increasingly, organizations are mobilizing CRM applications and outfitting field service representatives with smartphones capable of accessing back-office applications. These applications may be fully certified by the IT department, but their use means that corporate data is being stored on smartphones. Since smartphones are easy for users to lose and for thieves to steal, that valuable data can fall into the wrong hands. And smartphones are not exempt from disclosure laws if they are lost with unencrypted personally identifiable information (PII) in their memory. If a smartphone is lost with unencrypted PII, a business can face fines, negative publicity, damage to their reputation, and lost business. "It is a nontrivial issue losing data these days," says Gold.

## Protecting Corporate Data from Mobile Apps

Though it might be tempting to lock down smartphones to avoid data loss, this can negatively impact productivity. To ensure that users can take advantage of the functionality provided by smartphone applications and that corporate data is protected, smartphones should provide a number of security measures. Here are a few:

**CENTRALIZED MANAGEMENT:** First and foremost, look for a smartphone OS that offers centralized management—and in order for this to be effective, enterprise needs must be part of the product's DNA. That was a key criterion for Patrick Slesinger, director and CIO of Hong Kong-based diversified maritime group Wallem Innovative Solutions. "We are very concerned about security. We wanted a mobile platform that is designed for business. That's very much my feeling about the BlackBerry® platform. It's designed for the corporation," Slesinger says.



Research In Motion's (RIM) centralized policy and configuration management allows Slesinger and his team to easily manage operating system updates, enforce password use, and lock down devices, if necessary, across the entire company. Slesinger can also set more than 450 policies that block downloads of unauthorized software.

Slesinger originally deployed RIM's BlackBerry® smartphones at Wallem to provide users with mobile access to its corporate e-mail. Because of Slesinger's

of other operating systems can be difficult. Corporations should enforce a security baseline for user-owned smartphones. "Companies need to realize that [smartphones] are an evolution of the PC five years ago. It's not a completely different device. They're basically PCs on the network these days, and we have to think of them accordingly," says Gold.

Consider how you control desktops and mobility, and how you can extend that to the smartphones your users want to connect to the network. For example, you might

**"Companies need to realize that [smartphones] are an evolution of the PC five years ago. It's not a completely different device."**

—JACK GOLD, J.GOLD ASSOCIATES

confidence in RIM's security, users are now also using the devices to access backend databases. A mobile application called cDir®, by Tenet Computer Group, allows users to query databases that can be exposed with LDAP. Thus, users have access to corporate directories that hold vessel and contact information.

**ENCRYPTION:** Slesinger can rest easy knowing the data on his users' smartphones is secure—even if the devices are lost or stolen. All data transferred to and from the BlackBerry smartphones, as well as data stored locally on the handset, is encrypted with the highest level of encryption available. Encryption is turned on with the BlackBerry® Enterprise Server and is completely seamless to end users.

Slesinger is comfortable allowing users to download consumer apps onto their smartphones. "The reason for doing so is to promote usage. We want the BlackBerry smartphone to be the focal point of users' daily life," he says. Slesinger and his team carefully monitor network traffic. But they also have the option of establishing a limited sandbox where consumer-based applications can safely run without accessing corporate data.

**SECURITY BASELINE:** While standardizing on a single mobile OS is helpful in ensuring corporate data security and easing smartphone management, preventing the use

require that passwords be 12 characters or that the account locks after two minutes of inactivity. The important thing is to have a clear set of requirements. This removes the emotion behind the decision to connect any one person's smartphone to the network.

Wallem allows its employees to use their personal smartphones on a WEP basis, but they can only visit the same sites its laptop users would visit at an Internet kiosk. If they want to access corporate data beyond that, then they need to do so from a [corporately managed] BlackBerry smartphone. "We have a very simple IT structure. We don't have PCs, we have CCs. There's nothing personal about the computer. It belongs to the company. It's for company use. You use company tools to do company work," says Slesinger.

This simplicity is important given the fragmentation in the smartphone market. "Keep it as simple as possible," says Slesinger. "If you try to be all things to all people, you end up being a master of none."

