



February 1, 2010  
(c. online)

## **On the go: Mobile security**

*An explosion in smartphones, laptops, USB sticks and other portable devices has brought new security challenges, reports Greg Masters.*

Greg Masters  
February 1, 2010

The rise of the smartphone has done more than bring convenience to the hundreds of millions of consumers who use them. It has forced a realignment in the way IT administrators go about protecting enterprise networks. Where once their commandments about user policies were unquestioned and strictly adhered to, the so-called consumerization of the mobile device has, in many cases, obliterated their power to dictate the rules.

Employees have been bringing technology into the enterprise for quite a while now, says John Dasher, senior director of data protection at McAfee. "The day is long gone where employees use office-specified tools," he says. The time has come where executives can tell the IT department that they want to use their personal computers and other mobile devices. Employees have more influence about these matters and their power to circumvent what had been set rules will become more common, he says.

Much of this popularity has been driven by Apple's iPhone and other touchscreen smartphones, says Mikko Hyppönen, chief research officer at Helsinki-based computer security software company F-Secure. The iPhone already has more than a 10 percent share of the smartphone market.

As well, in just a few months, Android [Google's mobile OS] has gained traction, joining the iPhone as a highly demanded alternative to BlackBerry devices, says John Herrema, chief marketing officer at Good Technology.

"We're seeing Android as potentially the biggest mobility platform over the course of the next year," he says.

And, it is not just road warriors and enterprise users who have made smartphones so prevalent. Students and consumers on the go continually use their devices to stay connected via text and

social networks, such as Facebook, and their need for secure transmission of data is a rising concern as well.

The downside to all this growth in the mobile space is that the popularity is inevitably attracting the attention of malware writers. And, says Herrema, initial Android devices have not had a lot built into them as far as security. (For its part, a spokesperson at Google responds, “We pragmatically designed Android to help protect consumers from modern security threats, and we're looking to build and support security features for enterprise consumers on top of our existing structure. As this focus on enterprise grows, security will be a natural area for us to develop further.”)



When it comes down to it, consumers and organizations need to secure the pathways in and out of their networks, says Susan Callahan (left), chief marketing officer at Mobile Armor, a St. Louis-based data protection company.

“People are working from the road and out of their homes, and they are transporting valuable company information via these mobile devices,” she says. “In order to work efficiently, data needs to flow seamlessly and securely between mobile devices and the organization's servers.”

This rise in the mobile workforce has, in fact, changed the conversation on security methods from device-centric protection to data-centric security, she says, and the *Cybersecurity Act of 2009* means that protecting data will be even more crucial.

In the final months of 2009, for example, jailbroken iPhones (which give users the capability to install pirated apps), became a target for the first profit-motivated malware on this platform. The news of a Dutch hacker exploiting a jailbroken iPhone vulnerability was quickly followed by an Australian hobbyist writing the Ikee worm that tried to “teach people a lesson” for not changing their default SSH password. The worm changed the wallpaper on infected iPhones to a picture of 1980s pop star Rick Astley, a common web prank.

The first for-profit worm for jailbroken iPhones then emerged almost in the Netherlands. The worm was designed to create a mobile botnet and thereby gain access to online banking information. Customers trying to access their online bank from an infected iPhone were rerouted to a phishing site.

### **And the good news...**

F-Secure's Hyppönen expects this kind of organized criminal activity involving smartphones to increase in 2010. But, despite the fact that things will get worse in the mobile sector, there is good news as well. Mobile security can be a success story, he says.

“If you think about what could have gone wrong, there's been a lot of work by vendors to filter the technology. We've been able to if not avoid, at least delay major attacks.”

The reason for this disparity, he explains, is that third-party apps for smartphones must be certified and approved before they're made available on iTunes or other distribution networks.

“Compare that model to what's being done on the PC side where there are no restrictions and no code-signing,” he says.

In fact, there have only been about 450 mobile phone trojans over the last five years. “This is a good indication of how small the problem is for the mobile sector,” says Hyppönen, adding that none of the developers of the operating systems used in smartphones wanted to repeat mistakes made in the PC world. When the OS was developed for Windows, there wasn't much consideration given to security issues, he says. This is owing to the fact that the sector was on the margins, not worth bothering with for attackers after bigger shares of the marketplace.

The grace period mobile security has enjoyed out of the spotlight is likely coming to an end, Hyppönen concedes, as the proliferation of smartphones continues. “The problem is only going to get worse,” he says.

But Microsoft smells the coffee. Hyppönen expects the Redmond, Wash.-based software giant to bring out something similar to Apple's popular and profitable App Store to distribute approved software.

### **Competitive advantage**

While mobility is a fact of business today, helping to create a competitive advantage and efficiency for organizations, it invariably presents significant security challenges, agrees Michael Oldham, CEO of Marlborough, Mass.-based Portcullis Systems, a vendor of network and applications security.

“Gone are the days when the good people were on the inside, the bad people were on the outside and we put a firewall in between to keep everyone where they should be,” he says. “Mobility has shattered the perimeter of the corporate network. The border now exists in each iPhone, BlackBerry, smartphone, laptop, employee home PC, internet kiosk, partner PC, etc. that a corporation allows to connect to their network. Security to protect this has become more important than ever and has taken on new aspects.”

Today, companies are moving toward stronger security around access to their critical data and applications, says Oldham. Organizations are also working to control the data and applications that reside on the actual mobile devices. Use of encryption technologies to help protect the actual data, in case a device is lost, is becoming increasingly common. Username and passwords are being augmented by forms of two-factor authentication to restrict access to the device, information and applications.

As well, digital rights management technologies are being implemented to protect the data itself from unintended use even beyond the bounds of the corporation, Oldham says. And, access to information from devices, like USB keys, is being restricted to prevent unauthorized copying of data and to protect the device from unintended risk from executable code.

### **Mobility challenges**

The variety of mobile devices and carriers presents another set of challenges. Smartphones are surely an accident waiting to happen, warns John Adams, CTO at ChosenSecurity, a provider of on-demand PKI security services. He explains that while there are a variety of tools in the world of PCs to decrypt memory sticks, when it comes to smartphones, the technology is still

emerging. PCs share common sets of technologies, such as basic Windows utilities, but in the smartphone segment, there are multiple OS vendors and devices. As well, the rapid development cycle in hardware and software creates a lack of consistency.

"A professional carries personal music, photos and videos along with proprietary company data while traveling," says Edy Almer (*left*), vice president of product management of Philadelphia-based endpoint security vendor Safend. "With so much time spent on the road, mobile technologies provide some of the comforts of home. To limit company exposure, a content-aware, selective data protection solution must be put in place."

Major airports accumulate over 1,000 lost laptops a week, according to Ponemon Institute. Almer says that with today's hardware prices, it may be more economical to abandon the computer, rather than embark on a futile journey of locating it and risk losing a flight or paying rebooking fees. "Of course, this is true ONLY if the laptop is encrypted," he explains.

Since removable storage brought into a company by an employee may be the property of the employee, it is not inventoried, he adds. "If such a unit is lost, and contains sensitive data, it can be even more dangerous than losing a laptop that is, at least, accounted for with the security manager having a general idea of the type of data on the machine."

The mobility evolution is not going away. "It's a bit impractical to epoxy-shut the USB ports on computers," says McAfee's Dasher.

There are some, however, who take a hard line approach. Columbus, Ohio-based State Auto Insurance is strict with USB thumb drives – they're not allowed. In fact, the company disables the USB port in their computers so employees "will avoid getting into trouble," as Nancy Edwards, the company's chief security officer, explains it. "We can't figure out what you need a USB stick for. There are other ways to share a document, either via email or bring it on the laptop, all of which are encrypted."

For her work environment, the password is the ultimate in protection. "If you connect to our network, you have to be password-protected," says Edwards. And this includes all of the company's many road warriors doing business from their laptops, BlackBerries and other mobile devices.

To protect enterprise assets, Edwards says anyone using their BlackBerry is facing a time-out provision. In other words, the device will lock after 10 minutes, or when it is not used for a period of time. Users will then have to re-enter their four-digit code.

"We think if a company enables mobile devices, they need to protect it, same as a laptop, she says.

### **Employee migration**

And then there's one more aspect to this discussion. Good Technology's Herrema points out that from an enterprise perspective, users are paying out of their own pockets for these productivity tools because of their personal benefits. Smart CxOs can reduce the costs of mobility implementations as users prefer to use their iPhones for personal as well as business use. Herrema suggests it is possible to cut deals with employees to let them use their personal

smartphones, as long as they follow corporate policies, and the employee pays for the data plan.

Al Subbloie, CEO of Tangoe, a company based in Orange, Conn., which offers communications lifecycle management solutions, agrees that corporations are seeing a cost benefit owing to the migration by employees to using personal devices for work-related tasks. However, he says, the caveat is that security policies must be enhanced to protect corporate assets.

The primary defense against intrusions and data loss is setting strict usage policies and making certain all transmission activity uses some form of encryption.

“We’re seeing a lot more devices become inexpensive and available,” says David Ferre, product manager of ZENworks Endpoint Security Management at Novell. “A corporation needs to set policies to allow or disallow particular devices,” he says, adding that enterprises must make sure the data on these devices is encrypted. Novell customers are required to use a VPN. This way, once a user is authenticated and the VPN connection invoked, any data is encrypted, says Ferre. The next step is making sure policies are a big underpinning for security.

McAfee's Dasher agrees. Enterprises must think through what policies should be, what is permissible, and make conscious decisions, not assumptions, he says. “Put policies in place without any adverse effect on the business.”