

Tech Potpourri

Stirring Up Something Good

ILTA White Paper December 2011

Protecting the Unprotected: Encryption for Mobile Devices

MICHAEL GINSBERG ECHOWORK

The rapid evolution of smartphones in recent years has dramatically increased the use of mobile devices for confidential communications in law firms. With that comes an equally compelling need to protect email messages and other content exchanged on these ubiquitous devices. While encryption technology to protect communications has been widely used by business operations for many years, there is an alarming lack of encryption solutions for mobile devices. And what does exist is too complicated and too difficult to manage, or consists of piecemeal solutions that only address specific functions or platforms.

What we are facing is a new frontier for encryption — one that is expected to expand in short order. RBC Capital Markets forecasts that by 2012, 35.1 percent of global handsets (or 504 million units) will be smartphones, largely as a result of an anticipated shift to email messaging, browsing, applications and content.

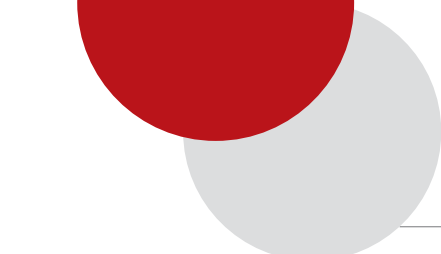
MOBILE INSECURITY

Risk is rising on two different fronts in the mobile arena. First, the use of smartphones for business correspondence and other sensitive communications is for the most part unmonitored. This was not a concern when mobile phones were primarily used for

voice and personal communications. Now, however, employees at law firms are using their smartphones to send and receive text and email messages and forward files — all activities that used to be managed by desktop functions where security processes are well in hand. But that's simply not the case for mobile communications.

Alongside the increased use of smartphones for business communications and advanced functionality is a significant increase in technology that can intercept mobile messaging. There are countless off-the-shelf, publicly available, free software and firmware resources for the hacking community. These perpetrators line their pockets by participating in a highly profitable market that thrives on intercepting confidential information exchanges. It is only made that much easier for them by the vast number of publicly available, unsecured Wi-Fi networks.

Even within the law firm walls, managers are challenged by something less malicious, but nevertheless insidious: employees using a wide range of unaccounted-for mobile devices to conduct day-to-day business communications. This is reminiscent of the early days of wireless networks, when staff took to installing their own routers. This rogue activity undermines the traditional centralized IT management approach. If an iPad or BlackBerry is stolen, there's very little an IT manager can do to safeguard the information on it.



All of this means that IT managers are facing less control and increased risk. Even if IT can find a way to control a device at the point of origin, it can't police the unprotected Wi-Fi network that a person might be using during their travels, or the devices and/or users to which the information is sent. In addition, if information is sent over a protected network, what network it ends up on at the recipient's end is anyone's guess.

This issue definitely came to light when the iPhone and Android came into the picture. In fact, over the last year, growth numbers for the Android platform have outstripped the iPhone, which represents a huge opportunity — and a huge threat. The Android brings an added risk to the equation, since applications can be downloaded from any location, rather than a centrally managed application store. At this point in time, the general assumption is that every phone is potentially a business device and therefore a danger to security.

MANAGING THE CHAOS

There have been attempts at adopting a device lockdown policy. But this has had little to no effect. Granted, it was easily accomplished when the BlackBerry Enterprise Server was the predominant business platform of choice, because of centrally provisioned data. But with the multiple devices, operating systems, networks and security measures being used today, the situation has escalated out of control. On one hand, you have an insatiable appetite on the part of end users for more access to information and applications. On the other hand, the IT managers are trying to impose limits to protect sensitive data. These two factors seem to be deadlocked in an ongoing tug-of-war.

As mentioned earlier, piecemeal solutions do exist, such as remote “wiping” of content from lost or stolen devices, disabling services or applying encryption tools that require complex authentication procedures. These only resolve a limited portion of the overall threat. What is needed to manage the chaos is an entirely new perspective for mobile security.

In fact, the best approach is perhaps the simplest: using the cloud to manage credentials, and using the mobile device to store encrypted email data.

Encrypted email messages are quickly becoming a requirement for law firms and businesses, and their IT managers are inundated with the “bring your own device” (BYOD) phenomenon. Firms need a powerful enterprise solution to manage the email infrastructure and an easy-to-use solution for staff.

If IT can have an over-the-air solution to manage these devices, where they can revoke or suspend the user's credentials and issue keys and digital IDs through a centrally managed console, they will have more time to focus on other IT issues.

At the same time, employee data will be protected as on-the-device encryption addresses the lack of

comprehensive security on smartphones and tablets. This on-the-device solution is a native email messaging experience that lets the user compose, send, download and read messages directly on the device. It doesn't require any additional components because it works with an existing business email address.

IMPACTING YOUR APPROACH TO SECURITY

When choosing a mobile encryption solution, be sure to choose one that is backed by a comprehensive public key infrastructure (PKI) credential-management platform and a globally recognized certificate authority. While smartphone and tablet technology has been an incredible enabler for business communications, there is no question that the proliferation in usage is challenging a law firm's ability to put the appropriate security measures in place to protect sensitive information.

A secure on-the-device encryption solution, however, promises to have a significant impact on how IT managers approach email messaging security on mobile devices. **ILTA**

MICHAEL GINSBERG is the Chief Executive Officer of Echoworx Corporation, the leading provider of managed encryption services for complete enterprise email and data protection. With 20 years of software experience, Michael is a seasoned operator with a proven track record; he has transformed the company's vision and product offerings, and is now leading its strategic direction and growth. Michael is known for his passion for business and software innovation and continuously challenges his employees and colleagues to deliver excellence. He can be reached at ginsberg@echoworx.com.