Why the next "ObamaBerry" might run Android or iOS

By Sean Gallagher | Published 4 days ago

Since US President Barack Obama took office in 2009, the mobile technology landscape has changed dramatically. When Obama was sworn in, there was no such thing as an iPad and the first Android phone (the HTC Dream) was just three months old. About the only technology that hasn't changed since Obama took office is the kind of phone he can use. But even that may change soon.

Two years ago, Obama fought a battle to keep his BlackBerry, a tool that had become essential to him on the campaign trail. (In the end, he got *a* BlackBerry but had to give up his personal handset.) Most people would be due for a handset upgrade of some sort by now, but like many people in the corporate world, the president's choices are still fairly limited. That's starting to change as some government agencies allow employees to bring their own devices into the workplace and connect to federal government networks for e-mail and other applications. Today, the technology that could make it possible for Obama to keep his personal BlackBerry—or whatever other wireless device he chooses—has arrived. And pending some major adjustments in policy, the president could soon opt to upgrade to an Android or iOS device.

The "ObamaBerry"

When Obama took office, he vowed to keep his BlackBerry. At first, many assumed that he was using the word "BlackBerry" as a euphemism for some other secure device. Since White House communications are provided by the Defense Information Systems Agency (DISA), analyst bets were on one of the two National Security Agency-approved devices offered under DISA's SME-PED program: the L3 Communications Guardian and the General Dynamics Sectéra Edge.

General Dynamics Sectéra Edge
General Dynamics

Both of these devices are equipped with a host of features you'd expect from $3,200 defense-contractor designed phones, including Type 1 export-restricted cryptography for secure voice communications and access to sensitive e-mail and websites through DOD's classified SIPRNET and unclassified NIPRNET. They're also heavily ruggedized—designed to withstand repeated 6-foot drops and operate while being pelted with rain. They come with all the baggage of a phone built for "war fighters"—they're big, clunky, pocket-unfriendly, and run on a secure version of Windows CE.

Instead, Obama managed to land an actual BlackBerry, a modified version of the Research In Motion BlackBerry 8830 World Edition with additional crypto installed. The BlackBerry was a relatively easy pick because, just as in other highly regulated organizations, RIM's platform is a government favorite and has been approved for official e-mail for over a decade. RIM offers BlackBerry devices that meet the FIPS 140-2 federal cryptographic standard (albeit at Level 1, the most basic level), with support for AES, RSA, Triple DES, and a number of other encryption algorithms. That rating now extends to RIM's Playbook as well, making it the only tablet device approved for viewing sensitive (but not classified) documents. And the government version of the BlackBerry offers an S/MIME mail client and supports the use of smart cards for authentication and encryption of e-mail.

The government is so dependent on its BlackBerrys that in 2006, when RIM was facing an injunction to shut its network down as a result of NTP's patent infringement case, the Department of Defense filed a brief stating that cutting off BlackBerry service to the government was a threat to national security.

Obama's BlackBerry probably doesn't require him to authenticate with a smart card when he uses it. He's also not using it for classified e-mail or phone calls. So the biggest security measure he's taken is security through obscurity: his e-mail address is restricted to a small number of key staff members, and it changes regularly.

Beyond the BlackBerry

BlackBerry 8830
Research in Motion

While the BlackBerry is still the device of choice for government execs, RIM's grip on the government market has loosened. Many agencies are exploring ways to use iOS and Android devices for a range of applications, and some are starting to let employees bring their own

mobile devices as both a way to save money and as a way to leverage the commoditization of mobile hardware.

In the past two years, the Defense Department has shown a great deal of interest in both the Android and Apple iOS platforms. The Army sponsored a mobile development competition called Apps4Army last year, and is in the process of developing an Army app Marketplace—a private app store for the military that will launch in 2012. And the Department of Veterans Affairs is moving to let hospital staff bring their own mobile devices into the VA's networks, and use devices such as iPads for clinical data.

But that interest hasn't yet turned into a wholesale move away from BlackBerry. The problem government agencies face is similar to the one facing companies as they start adopting "bring your own device" policies: how to incorporate them into the device management structure. With the security policies in place at many agencies, those problems are amplified for government; it's not just a matter of requiring employees to get their apps from an internal official app store.

First, there's the fact that Apple and Android devices have lacked the encryption certification and support for government digital signatures that RIM has had since 2001. And then there's the issue of two-factor authentication. Homeland Security Presidential Directive 12 (HSPD12), a directive issued by the Bush administration, requires all government agencies to issue smart card IDs for government employees and contractors to control access to sensitive government facilities and systems—including e-mail. The DOD has its Common Access Card standard, while the rest of the federal government is adopting a National Institute of Standards and Technology specification called the Personal Identity Verification (PIV) card. Both use a PKI certificate embedded in the card for authentication and encryption, which is read into the device through a card reader each time a user session begins. While RIM has a smart card reader for the BlackBerry, until recently there haven't been many alternatives for Android and iOS devices.

Without FIPS 140-2 encryption and PIV card integration, Apple and Android devices have been stuck on the edge of the government enterprise. "The bring-your-own-device world has generated a dilemma for the US government in that a large proportion of the government's employees are reading and sending e-mails from mobile devices," said Julian Lovelock, vice president of ActivIdentity, an identity management software company that does about 42 percent of its business with the federal government. "Those users can't decrypt e-mails that were encrypted on a laptop or another device. And add to that the introduction of tablets, and people bringing them into the government environment and wanting to read internal documents on them—while the iPad is a decent device for document review, that adds another whole set of security and authentication requirements for agencies to deal with."

The first hurdle, FIPS 140-2 crypto, was finally cleared last week. A Virginia company called Protected Mobility received the first FIPS 140-2 certification for a cross-platform crypto software module that can be used with Android 2.2 ("Froyo"), 2.3 ("Gingerbread"), and 3.0 ("Honeycomb"), as well as with iOS 4.2 and 4.3 devices. (Sorry, feds: no iCloud for you.) In September, San Francisco-based Mocana also got FIPS certification for its Froyo crypto software. That means that the government should be able to buy iPhones, iPads, and Android devices for official use next year.

The remaining hurdle is a more practical one: how to allow government employees to use their PIV cards to digitally sign, encrypt, and decrypt e-mails with PKI just as they do from their desktop e-mail systems? That's something Lovelock said ActivIdentity has partially solved, and is continuing to work on in partnership with Good Technology, which makes S/MIME-based secure e-mail clients and a secure container framework for mobile devices. ActivIdentity's identity "middleware" is already used on 5 million desktops to accept PIV card PKI certificates for desktop computer user authentication and to integrate that PKI with e-mail and other applications.

"What we are doing is taking that middleware and creating a version that can be embedded in the Good for Government mobile client to enable customers to read encrypted e-mails," Lovelock said.

One part of the solution already developed by ActivIdentity is a way to store the user's PKI certificate in a micro SD card or an embedded secure chip on the mobile device so that there's no need to have a smart card reader for the device. A middleware applet could be used to "clone" the certificate and store it for the user, essentially turning the mobile device into a virtual PIV or CAC card. The micro SD solution is easily applied to many Android devices that have slots for the storage format; for iPad users, it requires an adaptor, but one that's a lot less expensive than a secure Bluetooth-based smart card reader.

It may just be a matter of time, then, before Obama can trade in his BlackBerry for a presidential tablet—and switch from BrickBreaker to Angry Birds as the official First Time Waster.

Photograph by www.acclaimimages.com

EmeraldArcana | 4 days ago | permalink

Quote:

It may just be a matter of time, then, before Obama can trade in his BlackBerry for a presidential tablet—and switch from BrickBreaker to Angry Birds as the official First Time Waster.

Well, with enough time, anything can happen. The question is, will Obama still be the President by then?

Ostracus | 4 days ago | permalink

EmeraldArcana wrote:

Quote:

It may just be a matter of time, then, before Obama can trade in his BlackBerry for a presidential tablet—and switch from BrickBreaker to Angry Birds as the official First Time Waster.

Well, with enough time, anything can happen. The question is, will Obama still be the President by then?

Which will not change a thing the article talks about. Now my question is since ARM has some security features built-in to the processors. Are they used by these firms?

Budoinbatu | 4 days ago | permalink

Ha! Yo dawg, I'm up in tha white house, calling for a tee-time!

jalexoid | 4 days ago | permalink

Ostracus wrote:

Which will not change a thing the article talks about. Now my question is since ARM has some security features built-in to the processors. Are they used by these firms?

Considering they that they need to implement an export restricted variants of encryption algorithm, I don't believe that a UK company has the free access to those.

MAFIAAfire | 4 days ago | permalink

EmeraldArcana wrote:

Quote:

It may just be a matter of time, then, before Obama can trade in his BlackBerry for a presidential tablet—and switch from BrickBreaker to Angry Birds as the official First Time Waster.

Well, with enough time, anything can happen. The question is, will Obama still be the President by then?

I hope not.

Although I have nothing against Obama his second in command sucks on the media industries teats (among other things) a little too hard and totally supports them when they want to pass anti-consumer and ever more draconian laws.

Then again your options of who comes next is pretty f'ed up as well.