Pipeline
Your OSS/BSS Information Source.
www.pipelinepub.com Volume 7, Issue 4

RIM's War

By John Wilson, Associate Editor

It is easy to say that it has not been a very good month for Research in Motion (RIM), the Canadian manufacturer of popular BlackBerry mobile devices. First, RIM's first ever touch-screen phone with BlackBerry's newest OS update, the BlackBerry Torch, debuts to middling reviews. Then, numbers released by research firm NPD show Android phones ahead in market share for the first time. But the most glaring problem, and the one that may seal BlackBerry's fate, is the growing unrest in the Middle East aimed at BlackBerry.

> **"Many players in the West would see any concessions from BlackBerry as a blow to democracy."**

A Growing Problem

On August first, the United Arab Emirates announced a proposed suspension of RIM's email and instant messaging services, with an October deadline, citing security concerns over the encrypted network used by BlackBerry handsets. Similar shutdown threats were soon announced by Saudi Arabia and India, while an even longer list of countries admitted they were considering making the same demands. All of the countries wanted one thing: full access to BlackBerry's network.

Interestingly, it is the Middle East's own security issues that have led to this latest round of "security concerns" for BlackBerry. The Indian government has claimed that the 2008 Mumbai terror attacks, which left 173 dead, were coordinated using BlackBerry

handsets. In January of this year, Hamas official Mahmoud al-Mabhouh was assassinated in a Dubai hotel room; again, rumors swirled that the assassins had used BlackBerry phones. The assassination is said to have led directly to the U.A.E.'s ultimatum. The reasoning goes that by accessing the encrypted network, concerned governments could more easily track down and prosecute suspected criminals and terrorists. There remain two unanswered questions; can these governments be trusted with this data? And, if so, is it even technically possible to give it to them?

Unanswered Questions

It is no secret that many Middle Eastern governments have had long and combative relationships with their citizen's own right to privacy. The information age has given rise to a boom in political activism and organization in the Middle East, facilitated by internet enabled mobile devices. Authoritarian regimes in the region have repeatedly attempted to inhibit the political use of internet technologies and the fear is that some governments would use any access to BlackBerry's email and messaging services to spy on their own people and quash political dissent. Many players in the West would see any concessions from BlackBerry as a blow to democracy.

The U.A.E.'s initial challenge set off a flurry of negotiations between, and press releases from, BlackBerry and the governments of the U.A.E., Saudi Arabia, and India. The Saudis and India backed off on their initial threats after reportedly making progress in talks with RIM. For its part, RIM denies any cooperation. Adding to the confusion is the persistent rumor that RIM routinely grants Western and European governments access to any data they require. RIM has repeatedly denied these claims, but Middle Eastern governments remain unconvinced. But even if RIM did decide to cooperate, it remains to be seen if it is even technologically feasible.

> **"Even if a third party were to intercept the message, they would have to spend considerable time and resources to crack the encryption."**

Technical Problems

With all the attention placed on BlackBerry in the last month, it is easy to overlook a fundamental question; why is all this negative attention placed on BlackBerry devices and not Apple or Android phones? The answer lies in the way BlackBerry handles email and messaging technologies. On an iPhone or Android phone, all information, including email and messaging, is sent through regular internet channels. These applications are as secure or insecure as regular internet traffic. It is relatively easy for governments to intercept typical internet communications. The reason that BlackBerry is different, and faces so much scrutiny, is that they have established their own encrypted network to handle email and messaging data.

When a BlackBerry user sends an email, it is encrypted using a private key and sent through a BlackBerry Enterprise Server (BES) with a corresponding key. Even if a third party were to intercept the message, they would have to spend considerable time and resources to crack the encryption. There are two types of BES, those owned by RIM, and those owned by private businesses. Herein lies the problem for RIM; even if they wanted to, they would be unable to provide governments with any user's encryption key. If a user connects through a privately owned BES, RIM doesn't have access to the hardware, and if the BES is owned by RIM, they still do not know which encryption key the client is using.

RIM has attempted to clarify their position, from a technical standpoint, saying "RIM does not possess a 'master key,' nor does any 'back door' exist in the system that would allow RIM or any third party, under any circumstances, to gain access to encrypted corporate information … All data remains encrypted at all times and through all points of transfer between the customer's BlackBerry Enterprise Server and the customer's device (at no point in the transfer is data decrypted and re-encrypted)."

This raises an interesting point, from a lawful intercept perspective. If RIM's method for handling data is problematic, perhaps there is a wider message to be gleaned by all handset manufacturers or service providers who shy away from standardized or fully web-based computing in favor of proprietary networks. Security is ensured, but at what cost?

Perception is Reality

Several deadlines for Blackberry have already passed. Saudi Arabia let their August 10th deadline expire without taking action, and just recently, India has granted a 60-day stay while the India telecommunications department tests a proposed monitoring system. But individual victories do not address the biggest problem for RIM going forward: public perception. They claim that they cannot provide access to encrypted data, but Middle Eastern governments insist that RIM colludes with Western powers. RIM states that they have not bowed to foreign pressure, but Saudi Arabia and India tout their successes in receiving concessions.

If RIM does not meet government demands, they may be shut down in some countries; if RIM does meet government demands, they may lose the faith of their customers. In the stock market, an entity operating almost entirely on public perception, RIM has lost more than 20% of its value in a month. It is an unsettling reality that BlackBerry may be brought low by being unable to fulfill requests that they do not wish to honor anyways.

Furthermore, the case sheds light on the complexity faced by handset manufacturers and communications service providers operating globally. Lawful intercept is one facet that must be considered, but everything from billing regulations to local marketing preferences must become key considerations for growing companies.

RIM is now learning these tough lessons as they are forced to simultaneously think globally and act locally.