Was BlackBerry encryption really defeated?

Tuesday, September 23, 2008

- Jack Falkner

The Economic Times has reported that the Indian government has developed the ability to read BlackBerry messages. If this is actually true, there are at least three ways in which this could have been done. Some are more likely than others. It's unlikely that the Indian government will tell us exactly how it can read BlackBerry messages, but we can probably get a good idea of what they actually can do.

The least likely way is that the Indian government actually developed a way to beat the encryption used by the BlackBerry devices. This is extremely unlikely. The encryption used by these devices(AES 256 bit) from Blackberry device to Blackberry Enterprise Server(BES) is so strong that it's probably impossible for the Indian government to beat it and from all reports and sources-there are no backdoors. The maximum strength which reports suggest the Indian Govt has the ability to crack is 64 bit, possibly 128 bit.

Another possibility is that they might have found a way to defeat the key management used by the BlackBerry devices. It's almost always easier to attack key management that to attack encryption. It's possible that they found a way to do this, but it's still unlikely.

A third way is that the Indian government found a way to intercept BlackBerry messages when they're unencrypted. In most cases, the BlackBerry encryption just protects messages when they're transmitted wirelessly and doesn't protect them once they've moved off a wireless network. This means that there are lots of opportunities to intercept and read plaintext messages. This is relatively easy, and is probably what the Indian government managed to do, or insist that Blackberry service be provided by Wireless Carriers on a BIS.

Most corporations have a BES positioned behind the corporate firewall because it allows IT managers the ability to implement over 400 IT policies across the enterprise network and enforce policy compliance rather than leave it up to the end user. If a corporation has a BlackBerry Enterprise Server (BES), all corporate emails are encrypted at all points between the device and the corporation's BES, and are not accessible by the local service provider or RIM (or any other law enforcement agency) until after the BES decrypts it. The AES 256 bit encryption utilized is regarded as strong. ***The key point of vulnerability is when the email message exits from the BES it is decompressed and decrypted and forwarded to the Email Server where it is stored for access by the end user in plain readable text format. Typically, IT employees with access to corporate email servers or anyone with sufficient access to change a password on your account can login and view your content that is in your email store.*** With the existence of this vulnerability, the confidential operations of a company could become prematurely public or even the target of a profit-oriented interceptor.

Hence, corporations have an internal threat to address.

Telecom Carriers also provide Blackberry service via the Blackberry Internet Service (BIS) to the general public. A BIS does not have the rich palette of IT policies available for subscribers.

BlackBerrys bought directly from a telecommunication provider by small companies or by individuals operate on the wireless carrier – hosted BlackBerry Internet Service (BIS) server of the local country concerned (e.g., Rogers in Canada or Hutch in India). When leaving a device, all BlackBerry emails are sent to the local cellular service network provider and then routed through the RIM Network Operations Centre(NOC); the main one is in Waterloo, Ontario.

From the Blackberry device itself to the RIM NOC, the email is encrypted with 128 bit Secure Socket Layer(SSL) encryption on the Transport Layer for that portion of the call routing. At the NOC, the message is decrypted into a plain text file and transmitted via un-encrypted SMTP over the internet, possibly through several network gateways, to the Carriers BIS server and then routed to the carriers mail server. From the NOC onward, these email messages are NOT encrypted, and if the local gov't needs access to these emails, they need only to legally request them from the service provider, as all these emails are stored in a plain text webmail account. They could also be intercepted and read at any number of interim network gateways, and Datacenter employees of the wireless carrier would also have access to them. Therefore, if you are a subscriber on a BIS, a public user cannot expect any greater email security when using a BlackBerry than if using Hotmail or other webmail service.

The BIS does not support triple DES or 256 bit AES encryption as integrated and deployed for transmission between Blackberry devices and a corporate BES. The 128 bit SSL encryption deployed with the BIS, is regarded as weak by today's standards, and if enough horsepower is thrown at it, it could potentially be cracked.

Implementing end-to-end email encryption is the way to ensure your confidential information stays that way until decrypted by the authenticated recipient.

###