

Blackberry e a Segurança Nacional

01/07/2007

Nelson Murilo

<nelson@pangeia.com.br>

Segurança Nacional é um tema pouco discutido e existem bons motivos para isso. Não se deseja expor publicamente detalhes de segurança, que afetam toda uma nação, por mais pacífica que ela seja. Porém é possível observar, vez por outra, no noticiário, alguma referência que lhe diz respeito.

A mais recente é que o governo Francês proibiu o uso de *aparelhos* blackberry por funcionários de primeiro escalão. Foi alegado que estes aparelhos fazem uso de servidores que ficam em solo americano e portanto as informações trafegadas estariam, ao menos teoricamente, disponíveis aos serviços de inteligência americanos. Em resposta a isso a RIM, empresa que produz os aparelhos e os serviços de conectividade e sincronia, disse que os seus dados trafegam cifrados com os algoritmos modernos e atualmente seguros (no caso o AES 256), o que inviabilizaria qualquer escuta não autorizada.

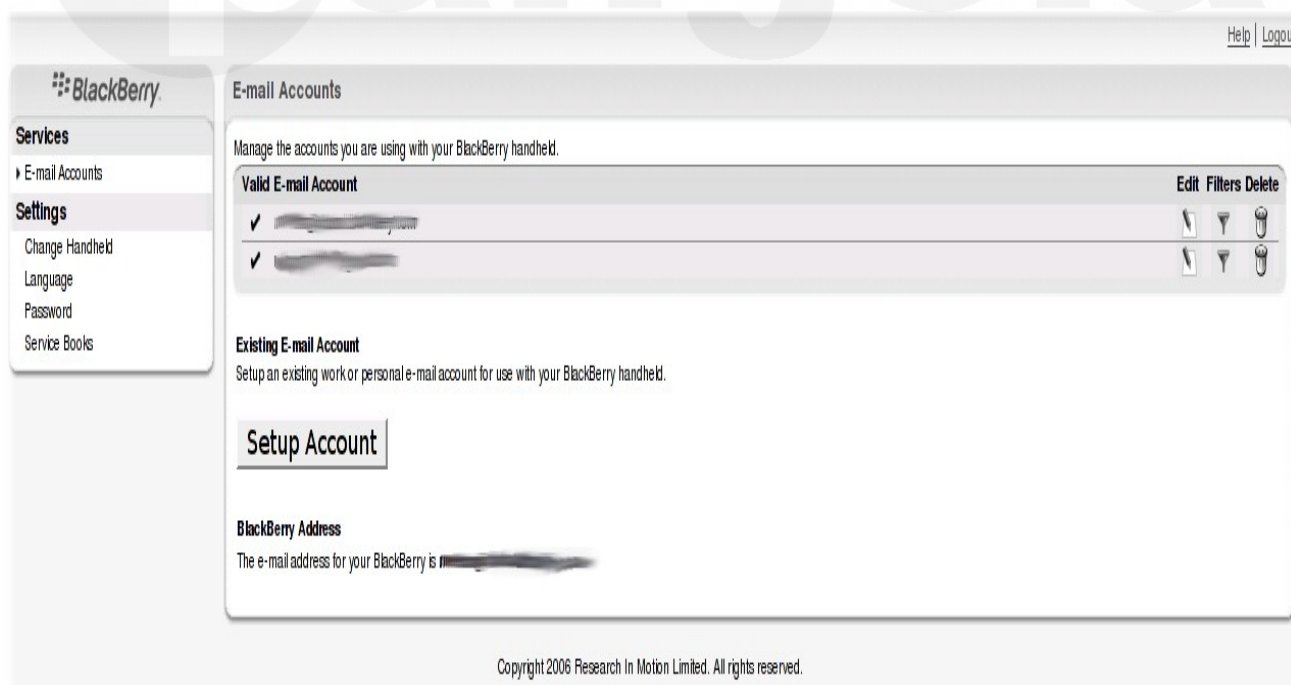
Por se tratar de um serviço mais ou menos novo e que agora vem ganhando volume no Brasil, seria conveniente entender um pouco melhor a arquitetura e os componentes do serviço para permitir uma avaliação mais embasada.

RIM em poucas palavras

O serviço consiste basicamente de uma estrutura que se utiliza da rede de dados da operadora de celular GSM, qualquer que seja o padrão de dados disponível. No Brasil temos GPRS e EDGE disponíveis atualmente. O objetivo é permitir a sincronia de informações pessoais, tais como: Calendário, Agenda de contatos, Notas, Lembretes e, principalmente, sincronia de mensagens de correio eletrônico. Esta sincronia, no caso do e-mail pode ser feita baseado em períodos de tempo pré-determinados e configuráveis ou, como é mais comum, usando um recuso de entrega imediata, chamado em inglês de *push-mail*. Para entregar imediatamente é necessário estar conectado no canal de dados em tempo integral (ou só em horário comercial e/ou durante a semana). Neste caso já existem, em várias operadoras brasileiras, planos de dados ilimitado, alguns inclusive restringindo ao serviço "*blackberry*". Existe ainda um serviço de navegação (acesso WEB) incluído neste serviço, apesar de pouco comentado, veremos mais adiante, porque em uma visão de segurança, este recurso precisa ser considerado.

O RIM é um serviço cliente/servidor, o cliente roda em celulares tipo *blackberry*, ou em outros celulares que permiter rodar o serviço *blackberry connect*, disponível para vários modelos de celulares, porém atualmente o serviço de navegação está disponível apenas nos *blackberries* nativos. O cliente é responsável por estabelecer a conexão com servidor RIM, quer seja ela periódica ou dedicada.

Outro aspecto importante diz respeito à gerência das contas de e-mail do usuário. Ao assinar o serviço, o usuário cria uma conta no próprio servidor da RIM, para gerenciar seu perfil. Esta conta tem um e-mail associado, que pode ou não ser usado pelo cliente. Independentemente da conta ser ou não utilizada como e-mail, o cliente poderá cadastrar a(s) conta(s) que ele deseja que seja(m) gerenciada(s) pelo servidor RIM. O procedimento é simples: ele indica o protocolo (IMAP ou POP3), indica se vai usar ou não criptografia (SIMAP/SPOP3), aponta o IP ou nome dos servidores (incluindo SMTP) e, por fim, informa o usuário e a senha que serão usados para coletar as mensagens no servidor IMAP/POP3 indicado. Existem ainda outros detalhes, como deixar ou não uma cópia no servidor (no caso de POP3), se existe necessidade de autenticação para envio de e-mail, e ainda outros.

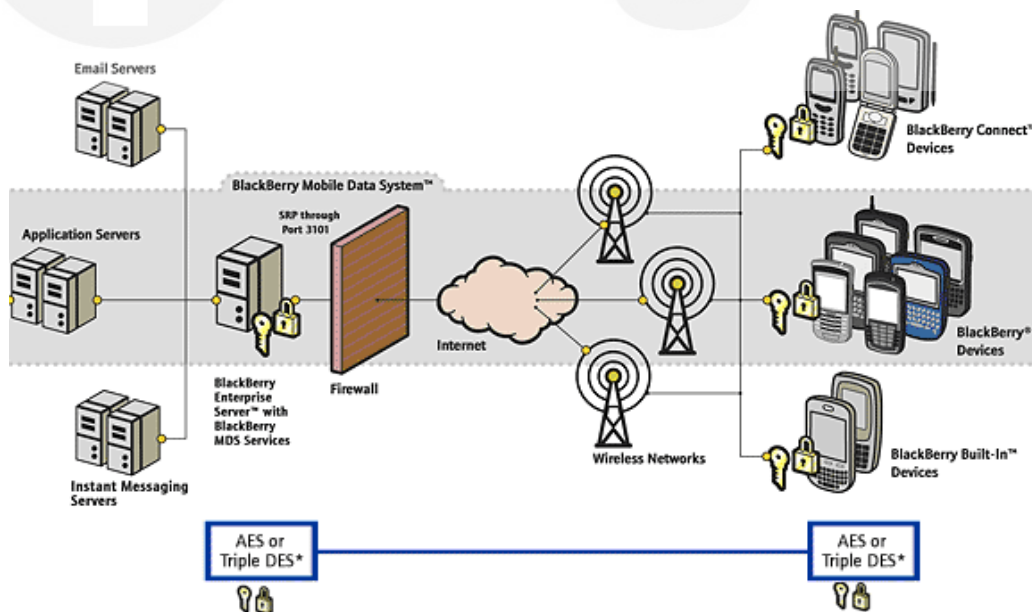


RIM em funcionamento

A configuração mais comum é a que estabelece a comunicação ininterrupta, através do canal de dados operadora de celular, possibilitando a recepção e o envio de mensagens em tempo real. Desta maneira uma mensagem chega ao servidor de correio que o usuário cadastrou, daí é transferido para o servidor RIM e encaminhado ao celular do usuário. Na resposta, ou composição de uma nova mensagem, esta fará o caminho inverso. Os demais serviços de sincronia trafegam apenas entre o cliente e o servidor RIM

O uso do canal de dados da operadora tem algumas particularidades, eles normalmente estão divididos em pontos de acesso (access points ou APs), esta divisão facilita na hora da conexão pois cada AP pode ter características particulares, como a qual servidor e porta conectar, protocolo e outras necessidades. No caso do serviço *blackberry* existe um ou mais APs associados a este, e é essa associação que permite a operadora tarifar, de forma diferente tráfego igual saindo por APs diferentes. Por exemplo: uma sincronia de e-mail diretamente do servidor POP3/IMAP, pode não estar definida no pacote de dados ilimitado, que seria possível apenas via os APs do serviço *blackberry*.

Portanto percebe-se que todo o tráfego de mensagens e de resto, os outros serviços de sincronia, são reconhecidos como serviços *blackberry* por conta do uso dos APs associados, e neste caso são as únicas possibilidades.



Uso do RIM em atividades sensíveis

Quais seriam então os principais pontos de falha do serviço?

O primeiro ponto, e que foi amplamente noticiado, é o da insegurança (após o incidente) quanto à estabilidade do serviço, e como todos sabemos, um dos pilares da segurança é a disponibilidade. Na verdade isso não pode ser garantido pela RIM, pois como foi visto a entrega ao dispositivo é feito pela operadora de celular, completamente fora da área controlada pela RIM. E mesmo que ela consiga manter sua rede no ar, o mesmo não se pode dizer do serviço de dados das operadoras, já seus *sites* são projetados estimativa de uso, para cada região, e por vezes e em situações especiais, vemos o serviço falhar por falta de recursos para serem alocados. Quedas no serviço de dados também são freqüentes no Brasil, mas talvez por conta da, ainda, pequena demanda.

Ainda nesta linha, outros componentes estão sujeitos a falha, o link entre o servidor *blackberry* e a Internet, impossibilitando a recepção e o envio das mensagens, ou de maneira isolada a conectividade da rede onde se encontra o servidor POP3/IMAP do usuário pode sofrer problemas, ou mesmo o servidor pode ter alguma parada ou mal-funcionamento que dificulte o processo.

Com vários pontos de falha que não estão sobre o controle da RIM, este pode fornecer garantias apenas sobre o que lhe cabe neste processo. Observa-se que são tantos os pontos de falha que, por vezes torna-se difícil uma identificação imediata de onde, exatamente, está o problema. Imagino que esta dificuldade de diagnóstico tenha possa ter ocorrido no evento em que parte da rede da RIM ficou fora por algumas horas.

O segundo ponto seria sobre a questão da criptografia. Apesar da empresa dizer que usa padrões de mercado, no caso o AES 256, a implementação é propriedade da RIM. Desta maneira não se pode garantir que não existem aberturas, intencionais ou não, que permitam entender as informações em trânsito.

Mas o servidor RIM faz backup? Se sim, o que é provável, como este backup é mantido seguro?

Por quanto tempo as informações ficam armazenadas?

As mensagens são armazenadas se forma segura até serem enviadas ao cliente, quando então deveriam ser apagadas?

Como é o processo de apagamento?

Todo especialista em forense computacional sabe que em uma remoção simples de conteúdo, os dados ficam disponíveis até serem sobrepostos e, em alguns casos, até por mais tempo.

Não existe atualmente, por parte da RIM, nenhum recurso de segurança nas mensagens armazenadas, como antivírus ou antispam. Nem mesmo na caixa nativa criada para gerenciamento do perfil. O que abre uma brecha para contaminação do dispositivo, caso o atacante tenha um alvo particular, o que não é impensável em se tratando de informações que podem afetar a segurança de países. O mesmo problema pode ocorrer no serviço de navegação, que não conta, atualmente, com nenhum tipo de proteção mais robusta. Aparelhos do tipo *blackberry* geralmente contam com recursos *bluetooth*, o que possibilita, ao menos teoricamente, ataques de acesso não autorizado às informações armazenadas e envio de informações, utilizando o dispositivo sob controle do atacante. Evidentemente estes tipos de ataques (ao dispositivo) não são exclusividades dos equipamentos tipo *blackberry*, mas devem ser considerados numa eventual escolha de dispositivos que oferecem menor risco.

Para enviar as mensagens que chegam ao cliente em sua caixa pessoal ou de trabalho, hospedada com terceiros, o servidor *blackberry* necessita se conectar a estes servidores e resgatar estas mensagens e, se for o caso, apagar as que foram apagadas no celular do cliente, sincronizando portanto, as caixas postais do cliente. Para que seja feito este acesso o servidor *blackberry* necessita das credenciais do cliente, seu usuário e sua senha de acesso. Que são informadas quando o usuário inclui uma determinada conta de e-mail para ser gerenciada. Lembrando ainda que o servidor remoto pode ou não usar criptografia (TLS/SSL), caso não haja criptografia as informações pode ser capturadas por escutas (*sniffers*) em qualquer ponto entre o servidor remoto e o servidor RIM. Mas mesmo que exista criptografia, o fato das credenciais ficarem armazenadas em um servidor, e mesmo que de forma cifrada, precisam ser decifradas para serem usadas, portanto o processo é conhecido e pode ser reproduzido.

Este último item, por si só, imagina-se, já seria suficiente para afastar o uso deste dispositivo das figuras alto escalão dos governos.

E, se nenhuma dos argumentos anteriores for suficientemente convincente, podemos supor que assuntos de Segurança Nacional não deveriam ser armazenados fora do país, qualquer que seja o tipo de armazenamento.