Is RIM too secure for governments?

UAE and India wanted access to encrypted data
• Banning Blackberrys
• Blackberry encryption
• Decrypting the data (or not...)
• BIS vs. BES
• Discussion
Spying on your people

• Governments want to have access to your data

• Encrypted services are a good defense against that

• Certain incidents provide the reason...

• How does this relate to smartphones? Especially Blackberry?
Blackberry/Governments 2010 to 2011

• In 2010 to 2011 many news articles regarding Blackberrys and governments

• Certain governments don’t want their users to encrypt their communication

• Blackberry offers a wide range of encryption services
Reports

- UAE, Saudia Arabia: judicial, social and national security concerns
- India: Attack in Mumbai in 2010
- United Kingdom: Riots in 2011
- Indonesia: Other reasons: adult content
How to?

- Governments approach RIM
- Want access to the data, or asks for ways how to gain access
- This was often reported in the news
- Further reports: RIM agreed to the requests
- Conclusions: “RIM can access your encrypted data”
Getting Information

- **Problem**: News coverage, most of the newspapers do not know the technical details

- **Problem**: RIM uses different methods for providing services,

- **Problem**: Proprietary protocols by RIM

- **Problem**: Mixing up different techniques and coming to conclusions (even Bruce Schneier did this in his blog: see links at the end)
Am I missing something here? RIM isn't providing a file storage service, where user-encrypted data is stored on its servers. RIM is providing a communications service. While the data is encrypted between RIM's servers and the BlackBerrys, it has to be encrypted by RIM -- so RIM has access to the plaintext.

5. For the record, I have absolutely no idea what this quote of mine from the Reuters story really means:

"If you want to eavesdrop on your people, then you ban whatever they're using," said Bruce Schneier, chief security technology officer at BT. "The basic problem is there's encryption between the BlackBerrys and the servers. We find this issue all around about encryption."

I hope I wasn't that incoherent during the phone interview.
Blog...

A comment by a user:
Sums up many news articles regarding this and other issues...

@ Bruce Schneier

"I hope I wasn't that incoherent during the phone interview."

Me too, as I have no idea what the hell you were talking about. More accurately, it made no sense. That's unusual for you. I wonder if you actually said that or if it's a misquote. I'm leaning on the latter unless you had a major hangover. Perhaps too much wine during a rave restaurant review...? :P
Services

• via Blackberry Enterprise Server (BES), BES Express, Hosted BES, Cloud Services

• via Infrastructure provided by RIM (for small businesses): Blackberry Internet Service

• PIN Messaging (Instant Messaging), similar to WhatsApp, iMessage... The telcos and governments don’t like this...
Services

- **BES**: Blackberry Enterprise Server
  - emails, web traffic, etc.

- **BIS**: Blackberry Infrastructure Service
  - emails, web traffic, etc.

- **PIM messaging** (similar to iMessage, replaces SMS, bypasses telcos)
  - via BES
  - via BIS
Blackberry Encryption

Diagram showing the encryption process:
- User provides an ephemeral key (from password).
- Ephemeral key encrypts the content.
- ECC public key encrypts user data received while locked.
- ECC private key decrypts user data stored while unlocked.
- Content protection key encrypts stored user data.
- Grand master key encrypts master encryption key.
- Master encryption key encrypts message (session) keys.

Key components:
- User
- BES/Blackberry
- Blackberry

Encryption flow:
1. User provides ephemeral key.
2. Ephemeral key encrypts content.
3. Content protection key encrypts stored data.
4. Master encryption key encrypts message keys.

Security layers:
- ECC public and private keys
- Content protection key
- Grand master key
- Master encryption key
- Message keys

Dataflow: User -> Ephemeral key -> Content -> ECC public/private keys -> Content protection key -> Grand master key -> Master encryption key -> Message keys.
Blackberry Encryption
to/from BES

• Masterkey generated during initialization process of Blackberry, stored on BES and Blackberry

• Masterkey changed periodically
Blackberry Encryption

- Encrypted with content protection key
- for messages (decrypted with grand master key, master key, session key)

Blackberry UNLOCKED
Blackberry Encryption

- Blackberry LOCKED and message comes in
- Encrypted with ECC public key (actually a shared key)
- When unlocked, decrypted with private key
- Re-encrypted with content protection key
- for messages (decrypted with grand master key, master key, session key)
Looking back to BES, BES Express

- BES server
- Handles communication with Blackberrys
- Handles connection to email server
- Configures Blackberrys (Policies etc.)
Blackberry Internet Service

- No BES involved
- RIM connects to your POP3/IMAP accounts, checks for mails and pushes them on your Blackberry
- Communication via special APNs of mobile networks
Gov Access

• Assumptions:
  • No access to infrastructure in other countries
  • No malware installation on smartphones (how?)
  • Access to mobile networks, providers, companies according to the law
• Technical possibilities?
BIS Communication

Canada

RIM Infrastructure in Canada (KEY)

U.S.

POP3

IMAP

Germany

POP3

IMAP

UAE

RIM Infrastructure in UAE (KEY)

Provider in UAE

Blackberry (KEY)

UAE GOV
PIN Messaging

• Via BIS: One encryption key for all Blackberrys

• Via BES: Additional encryption can be enabled (similar to other BES security): no one can read your PINs when within the BES domain

• Via BES: Policies, PIN Logging...
United Arab Emirates (UAE)

• in 2009: Update with Spyware by telco in UAE, RIM identified this and provided its own update

• 08/10: Blackberry services will be banned in 10/10

• Desire to monitor communication (criminal, terrorist, national-security...)

• Kuwait, India, China have also asked RIM
UAE Solution/Discussion

• Only companies with more than 20 Blackberrys are allowed to use BES and content-protection, otherwise BIS

• Discussions about shunting the emails to ISPs after decrypted on corporate servers

• BIS: assuming there are local Blackberry servers now in UAE an other countries: Access to data...

• BES security: NOT COMPROMISED
UAE

• Solution:
  • Ban BES Express (less than 20 subscriptions), need to switch to BIS
  • Allow BES but only for companies with trade licenses (requests for lawful interception of emails)
India

- Access to encrypted mails etc. (Mumbai attacks)
- 10/10: RIM willing to set up server in India that allows the government limited access
Saudi Arabia

- Threatened RIM to shutdown the service
- Special BIS server set up in Saudi Arabia
Indonesia

- 01/11
- Webfilter for pornographic sites (law)
- Adult content was filtered by Blackberry
- Local Blackberry infrastructure
Discussion

• BES service is secure: Only Blackberry and company have access (NOT RIM, NOT the government etc.)

• HOWEVER: Proprietary software, infrastructure, we do not know whether there is a “Super Ultimate Grand Masterkey” somewhere...


Bottom line, if you're not on a BES treat your BlackBerry like it is Facebook and assume nothing is private. If you are on a BES and send and receive email within your company it is secure, all other communications can be seen by others.
Links

• http://www.schneier.com/blog/archives/2010/08/u

Links

• http://us.blackberry.com/ataglance/security/features.jsp

• http://crackberry.com/blackberry-encryption-time-talk-turkey

• http://www.mauskar.com/index.php/browse-news/11-news/32-blackberry-internet-service-or-blackberry-enterprise-server-for-blackberry
Links


• http://www.intomobile.com/2010/10/08/rim-evades-uae-ban-blackberry-services-are-now-compliant/

• http://www.bitblock.com/content/view/165/65/