

Security on Mobile Devices: Threats, vulnerabilities, challenges and solutions



Gert Vanhaeght
Technical Account Manager
Vodafone Business Unit
Benelux region
Research in Motion



Agenda for today

- Research In Motion
- BlackBerry architecture
 - BlackBerry Infrastructure(s)
 - BlackBerry Enterprise Server in detail
- Secure connectivity
 - How the BlackBerry enterprise Server connects to RIM
 - How OTA provisioning works
 - Encryption mechanism
- Secured deployment of applications - Beyond mail
- BlackBerry handheld security
- Management and control tools (policies) on the BlackBerry Enterprise Server
- Security threats
- View on future...

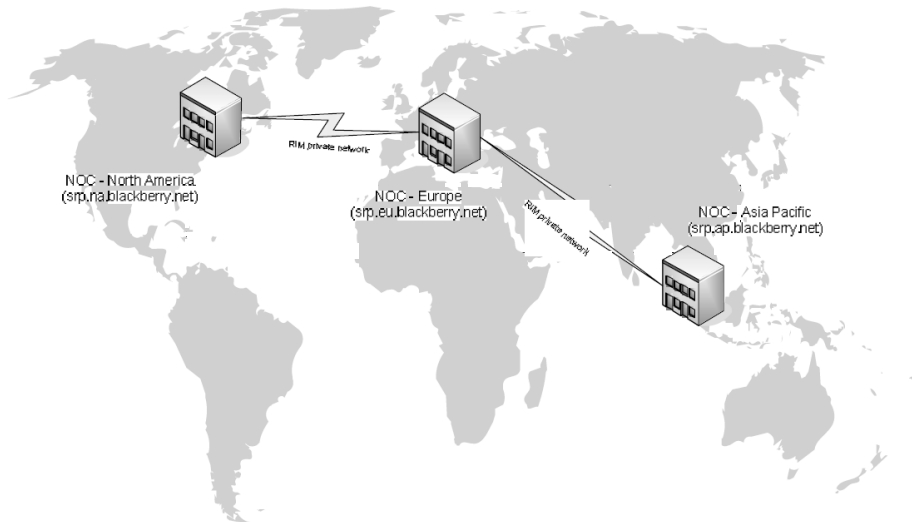


Research In Motion - Corporate Overview

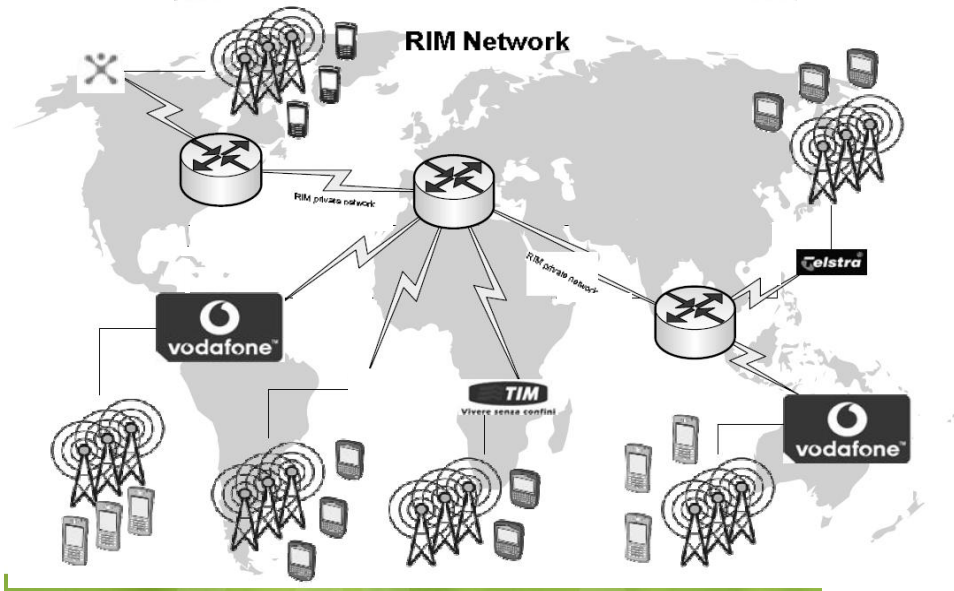
- Company founded in 1984
- Headquarters in Canada with offices in Europe, Asia Pacific and the United States
- Public company; TSE: RIM; Nasdaq: RIMM
- Over 21 million global BlackBerry subscriber accounts, of which more than 33% is outside North America
- 2.6 million subscribers were added in Q3 FY2009
- Partnership with over 425 distribution partners in 150 countries across the globe
- Operations in The Americas, Europe, Middle East, Africa and Asia Pacific and has over 12,000 employees worldwide, after hiring approximately 4,000 new people in 2008
- Over 200000 BlackBerry Enterprise Server (BES) installations



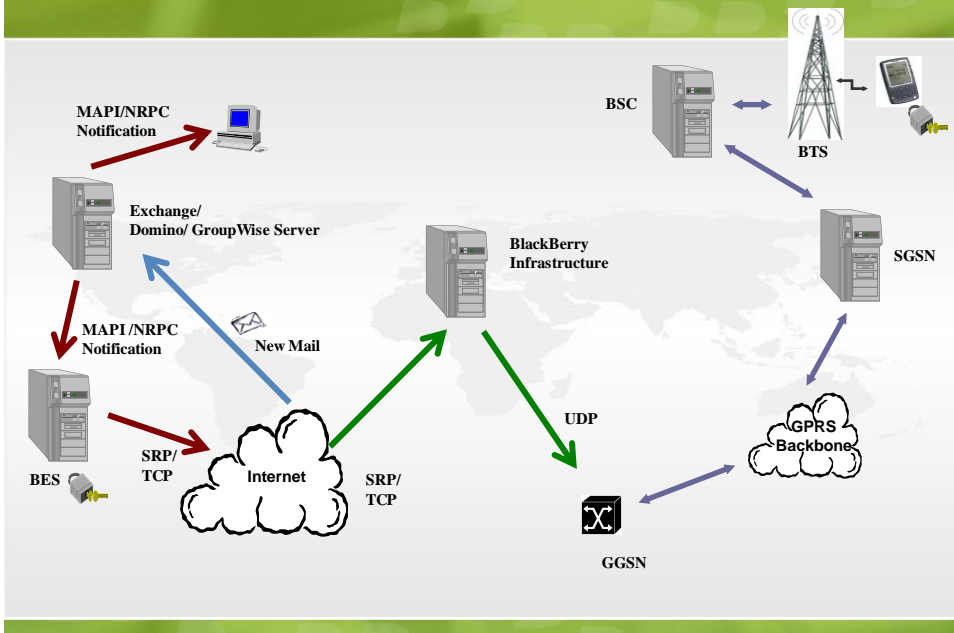
BlackBerry Infrastructure(s)



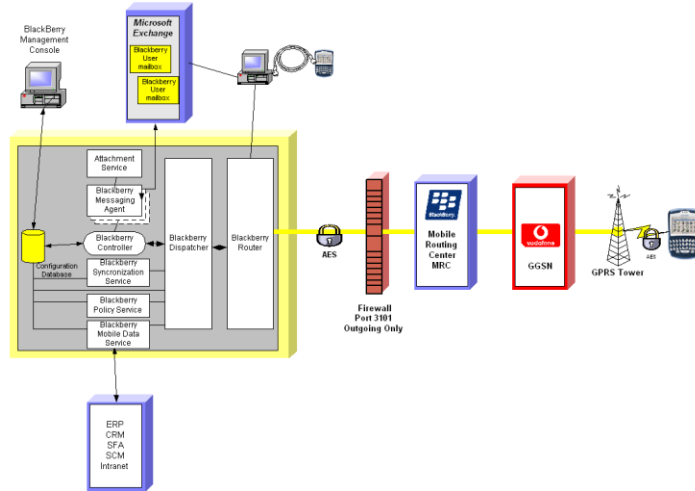
BlackBerry Infrastructure(s)



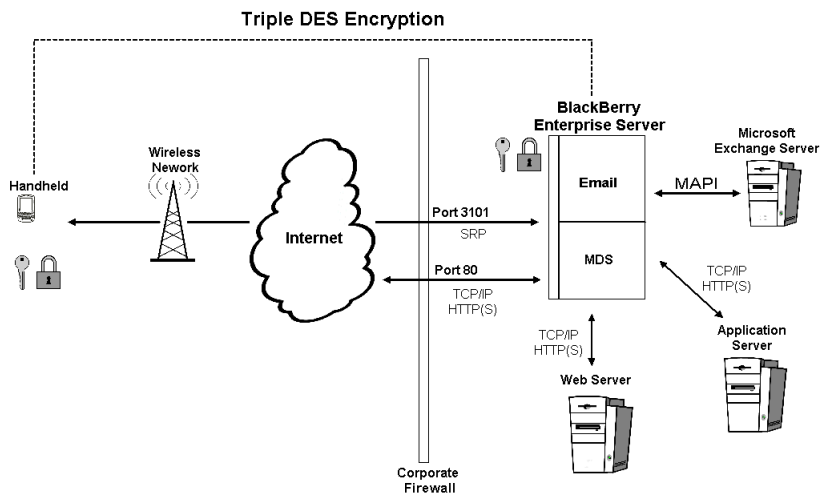
BlackBerry Enterprise Server



BlackBerry Enterprise Server in detail



BlackBerry Enterprise Server in detail



Secure connection



Each BES is identified with unique number, to be found on CD

SRP Identifier :

example S345656

With a 40-digit associated Authentication

SRP Authentication Key :

example y2jr-b8jn-kbea-rugp-bjvd-2xpe-5dfr-xgsd-249n-4nyq



This information is known and shared between customer and RIM

Each BlackBerry Handheld is identified with a hard coded, unique pin number

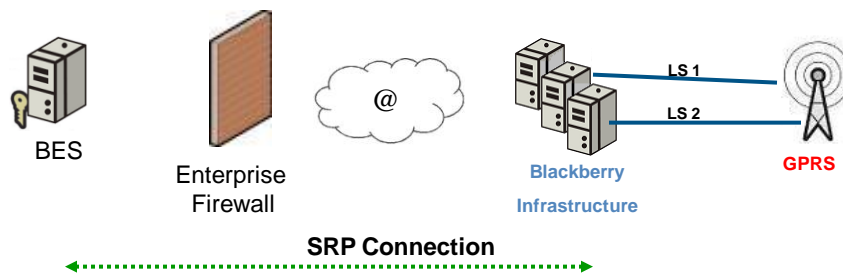
BBPin :

Example 2027668F



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

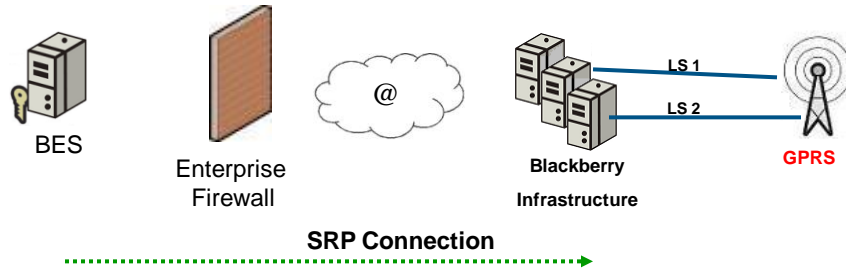


- First action of BES at startup is connecting towards the BlackBerry Infrastructure
- As firewall is set up with outbound initiated connection, only BES can initiate the connection
- SRP is a RIM specific protocol, end to end applied on top of TCP/IP



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

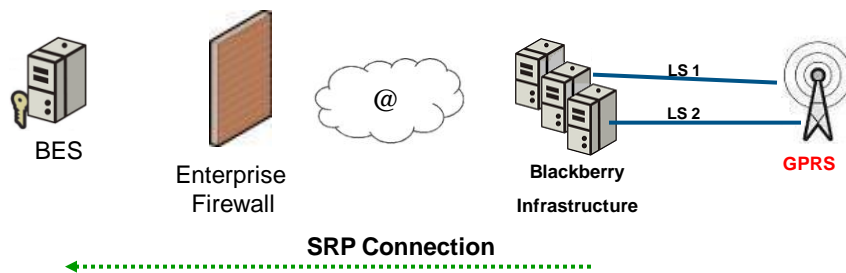


1. BES sends packet to BlackBerry Infrastructure, containing SRP Identifier



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

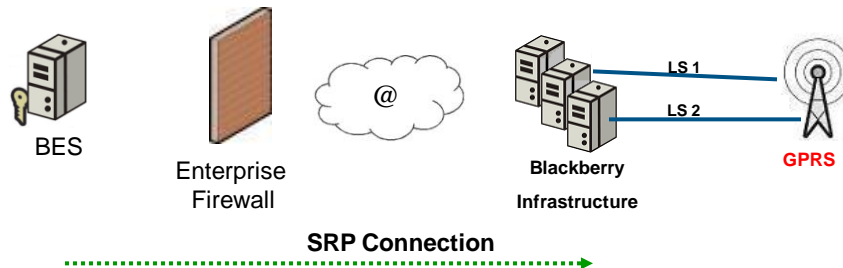


2. BlackBerry Infrastructure sends random response request package towards BES



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

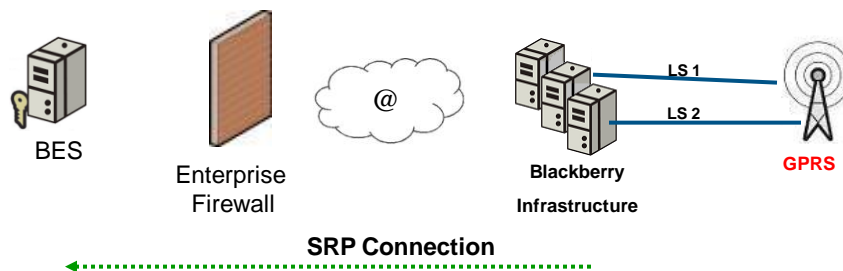


3. After receiving response request package, BES sends acknowledgment to BlackBerry Infrastructure



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

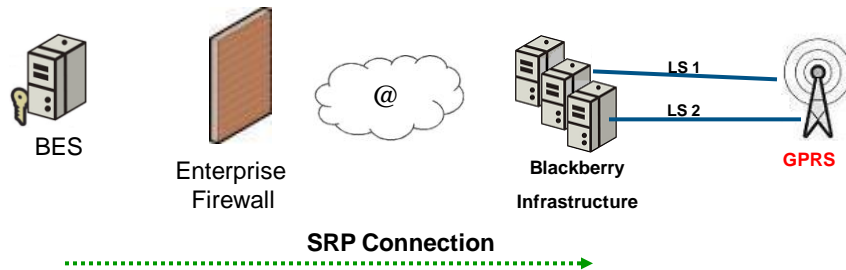


4. BlackBerry Infrastructure resends random response request package towards BES, this response request is hashed with the authentication key, using HMAC-SHA1. The 20 bit result is then send to BES



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

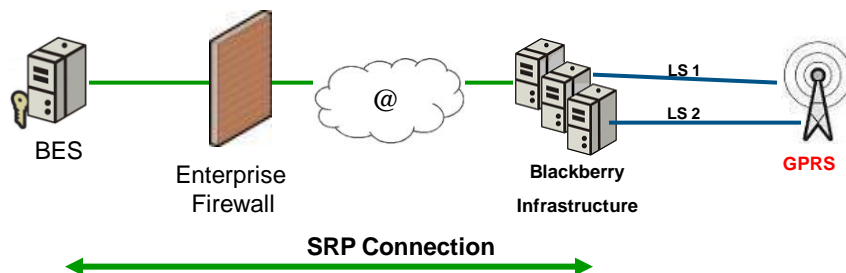


5. BES responds to random response request package, hashes it with shared authentication key



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

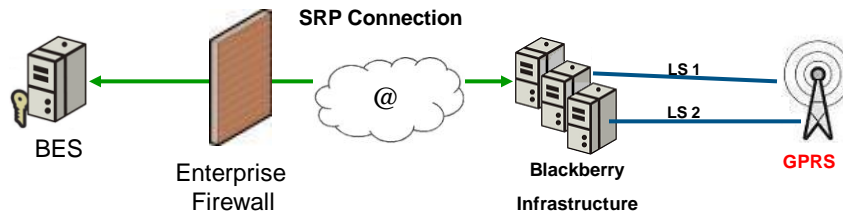


6. If BlackBerry Infrastructure accepts the response from BES, a confirmation will be sent and authentication process finishes. If BlackBerry Infrastructure rejects response, session stops and connection is dropped.



Secure connection

BlackBerry Enterprise Server connection towards BlackBerry Infrastructure

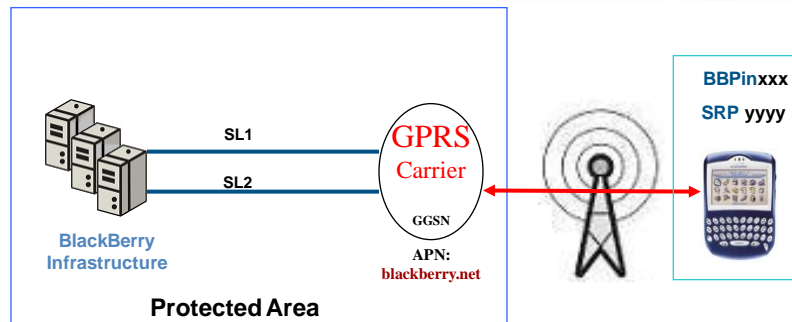


- The SRP Connection is set up via a shared (RIM & Customer) key: SRP Authentication key
- Authentication is mutual, 2-way between BES and BlackBerry Infrastructure
- If 2 simultaneous connections occur with same SRP Identifier, both connections will be dropped and the SRP Identifier will be locked out by RIM



Secure connection

BlackBerry Infrastructure connection towards Carrier



- The BlackBerry Handheld can only connect to the BlackBerry.net APN, hard coded
- The BlackBerry Handheld Creates a pdp GPRS context
- BlackBerry authentication is done via BBPin BBPin, then gets IP address from carrier DHCP pool (Carrier Private pool – not published on Internet)
- BBPin and IP address passed over secure line to BlackBerry Infrastructure



OTA provisioning

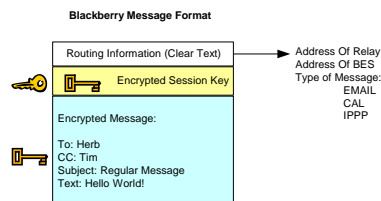


- When activating, a password is entered and used to encrypt the ETP.DAT file send to the BES
- BES reads ETP.DAT and checks password, if valid BES sends hashed packet to the Device with which the device can generate a Master Key
- Once both Device and BES have a shared Master Key, the data is send to the device, encrypted with a session key, which Device can decrypt.



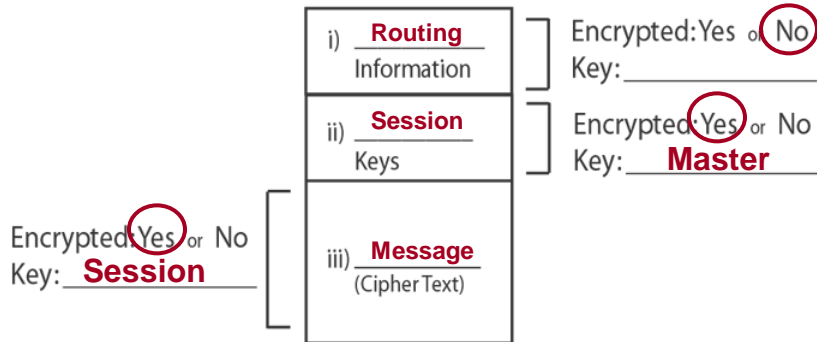
Encryption mechanism

- Messages delivered to and from the BlackBerry have a standard message format that includes routing information in clear text; a 3DES/AES encrypted session key and 3DES/AES encrypted message text.
- Routing information: Transmitted over the wireless network in clear text and contains minimal information : The address of the relay, the address of the BES and the type of message that is being sent. No information about the sender, message recipients or message content is contained in this layer.

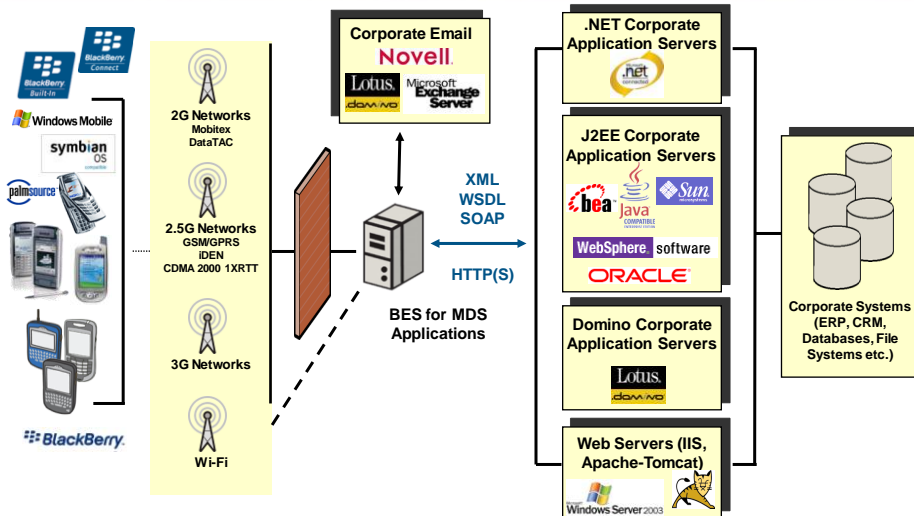


Encryption mechanism

BlackBerry Message Format



Secure application deployment



Applications on your BlackBerry

The diagram shows a central BlackBerry device with lines radiating to various application categories. To the left and right are lists of logos for various software providers.

Application Categories:

- Network & Systems Management
- corporate Intranet
- Business Intelligence
- Instant Messaging
- GAL/NAB Access
- Industry Vertical Applications
- Field Service Automation (FSA)
- Content
- CRM
- Database Access
- Sales Force Automation (SFA)
- Document Management
- Messaging & Collaboration
- SCM
- ERP

Logos: netIQ, SIEBEL, salesforce.com, Remyedy, SAP, IBM, NSET, PeopleSoft, Computer Associates, Flowfinity, salesnet, ONYX, Novell, Extended Systems, ECUTEL, XCELLENET, PointBase, sonic mobility, Time-tag, Wolfe Tech, RSUS, idokoromobile, Lotus, CONSILIENT, WebMessenger, active runner, mBiztech, Information Builders, COGNOS, BUSINESS OBJECTS, PRINTEROn, eAgency, Pocket Script, SEMOTUS, ORACLE, RETRIEVAL DYNAMICS, HillCast technologies, SANCHEZ INNOVATE.

BlackBerry

BlackBerry handheld security

The diagram shows a stack of BlackBerry handheld devices on the left and a detailed security architecture diagram on the right.

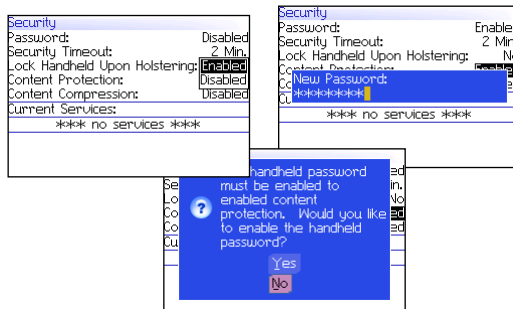
Security Architecture Layers:

- ROM OS** (Radio)
- Branding** (APN: Blackberry.net)
- Firewall**
- Java Virtual Machine (JVM)**
 - Blackberry Applications (Email, Calendar, Contacts, Phone)
 - Secure APIs
 - Third party Applications (Flowfinity, eOffice, etc.)

BlackBerry

BlackBerry handheld security

- Content Protection
 - Locally Encrypt All User Data
 - Leverages Existing Handheld Password Protection
 - Enforceable Via IT Policy
 - Extensible To 3rd Party Applications
 - AES 256 Encryption



 BlackBerry.

BlackBerry Enterprise Server Security

Remote password setup & lock

- BES Administrator Tool
 - MMC Management Console
- Set/Change Handheld Password
- Lock Handheld
- Set Owner Information

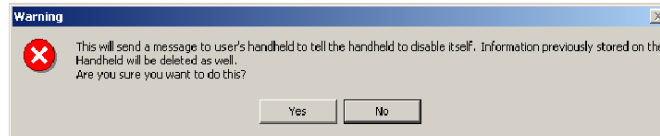
The screenshot shows the 'Set Handheld Password and Lock' dialog box. It contains the following fields and options:

- Set New Password:**
 - New Password: [text input field]
 - New Password Again: [text input field]
 - (Passwords are not set.)
- Set Owner Information as well:**
 - This will send a message to the user's handheld instructing it to set the Owner Information to the information entered below.
 - Owner Name: [text input field]
 - Owner Information: [text area]
- Are you sure that you want to send this command to this user's handheld?
- Buttons: OK, Cancel

 BlackBerry.

BlackBerry Enterprise Server Security

Remote Disable/Wipe



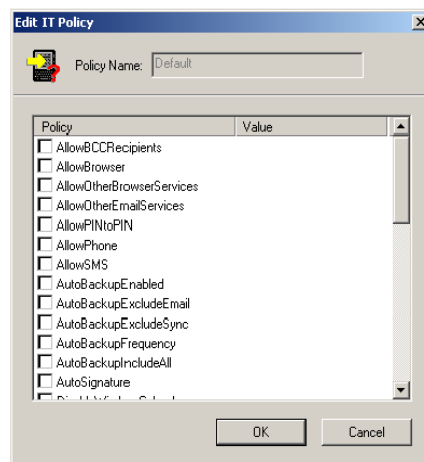
- BES Administrator Can Remotely Disable Handheld
 - Wipes All User Databases
 - Erases Encryption Key
- Device Must Be Synchronized
 - Same As Keying Password Incorrect X Times
- 4.0 Provides Same Wipe Function From Security Screen



BlackBerry Enterprise Server Security

Managing Security Policies

- Set Global, Group and/or Individual Policies
- Control Almost All User Configuration Options
- Pushed Over-The-Air
 - No User Overrides
- Desktop And Handheld Policies



BlackBerry Enterprise Server Security

Managing Security Policies

- Near 500 Policies
- Policy/Regulatory Compliance
 - Disable Cut/Copy/Paste
 - Disable Forwarding Between Services
 - Disable Out Of Band Communications (PIN to PIN)
- Device Security
 - Force Content Protection
 - Disable Persisted Plaintext
 - Enforce Password Rules
- Configuration Management
 - Wireless Synchronization Options
 - Default/Mandatory Settings
 - Application Controls



BlackBerry Enterprise Server Security

Managing Security Policies

- Passwords & Security
- Network Connections
 - Internal/External
 - Split Pipe
 - Browser / Phone
- Desktop
 - Automatic Handheld Backups
 - PIM Configuration
 - Force Software Upgrades
 - Disable Application Loader
- 3rd Party Application Controls
- Private PIN-to-PIN Key
 - Closed Messaging Community
- Message Transport
 - Plain Text, S/MIME
 - Enterprise, PIN-to-PIN
 - Other Email Services
 - Automatic BCC
- S/MIME Configuration
 - Ciphers
 - Key Length
 - Force Use For All Email
- Browser Configuration
 - Home Page
 - Connection Boundaries
 - Service Books



BlackBerry Enterprise Server Security

Managing Security Policies

IT Policies In 4.1

- FIPS level
- Periodic user challenge
- Disable 3DES transport
 - Forces AES Usage
- Content Protection strength
- Disable persisted plaintext
- Disable use of certs with stale revocation status
- Certificate revocation status stale age
- Accept unverified Certificate Revocation Lists
- Duress password email address
- Minimum security level for
 - Signing keys
 - Encryption keys
- Background colours
- Disable forwarding of messages between services
- Disable Cut/Copy/Paste
- Disable radio when USB cable is connected



BlackBerry Enterprise Server Security

Access Control Privileges

- Improved 3rd Party Application Management
 - Required, Allowed, Disallowed
 - Push Apps To Handheld
 - Extension To IT Policy
- Control Resource Access
 - Network Connections
 - API Access

Application	Version	Disposition	Delivery Mechanism	Policy Set
<input checked="" type="checkbox"/> System Software	<User Latest>	Required	Wireless Only	N/A
<input checked="" type="checkbox"/> Browser	<System Version>	Required	Wireless Only	N/A
<input checked="" type="checkbox"/> SSL/TLS Security Package	<System Version>	Required	Wireless Only	N/A
<input checked="" type="checkbox"/> WTLS Security Package	<System Version>	Required	Wireless Only	N/A
<input checked="" type="checkbox"/> Phone	<System Version>	Required	Wireless Only	N/A
<input checked="" type="checkbox"/> MemoPad	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 950/957	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 6200 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 6700 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 7200 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 7700 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> Tasks	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 6200 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 6700 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 7200 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 7700 Series	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> Calendar and Tasks	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> 950/957	<System Version>	Optional	Wireless Only	N/A
<input checked="" type="checkbox"/> Internal MSX App	1.0	Required	Wireless	Internal App Policies
<input checked="" type="checkbox"/> RIMCell	<Any>	Optional	Wireless	External App Policies
<input checked="" type="checkbox"/> RIMZee	<Any>	Optional	Wireless	External App Policies



BlackBerry Enterprise Server Security

Access Control Privileges

- Required Applications
- Excluded Applications
- Inter-Process Communication
- Internal Connections
- External Connections
- Local Connections
- Key Store Access
- Bluetooth API
- Email API
- PIM API
- Phone API
- Event Injector API
- Browser Filter API



BlackBerry Infrastructure

Threat Scenarios

Man in the Middle (MITM)

- “Traffic Laundering”
 - Used for stealing / planting information
- Traffic “Sniffing”
- BlackBerry Solution Answer:
 - Encryption using pre-shared secrets defeats this as adversary doesn't have the key



BlackBerry Infrastructure

Threat Scenarios

Spoofing

- Malicious injection of traffic
- BlackBerry Solution Answers:
 - Unencrypted Packets Are Discarded
 - Attacker Doesn't Have Access To Master Key
 - Worst Case Is A Replay Attack
 - Attacker Can't 'See' The Payload



BlackBerry Infrastructure

Threat Scenarios

Hijacking

- Taking over a communications channel while it is in use or being set up.
- BlackBerry Solutions Answers:
 - BES Will Drop Connection To Wireless Infrastructure
 - Connection Automatically Re-established When Needed
 - BES And BlackBerry Infrastructure Mutually Authenticate



BlackBerry Infrastructure

Threat Scenarios

Bluetooth

- Bluejacking
- Bluesniffing
- BlackBerry Solutions Answers:
 - BlackBerry handheld Bluetooth only to be paired with hardware like headsets etc...
 - No data transfer possible over Bluetooth
 - Bluetooth chip can be powered down via Policy



BlackBerry Infrastructure

Threat Scenarios

Rogue Code, Trojans, Viruses

- BlackBerry Solution Answers:
 - Trusted Application Execution Environment
 - Application Download Controls
 - Administrators Control What Applications Privileges
 - Signed Applications Ensure Integrity And Authenticity



BlackBerry Infrastructure

Threat Scenarios

Rogue Code, Trojans, Viruses

- BlackBerry Solution Answers:
 - Email Is Text Only - No Text Virus
 - Attachments Process In Binary Format
 - No Instantiation Of Office Components
 - No Macro Execution
 - XML Data To Handheld For Presentation
 - Messages Use Existing Corporate Infrastructure
 - Corporate Anti-Virus/Anti-Spam Measures In Effect



BlackBerry Infrastructure

Threat Scenarios

Data Siphoning Attacks

- Applications could “straddle” multiple communications channels pulling data from one channel and sending it through another

BlackBerry Solution Answers:

- IT Policy Can Prevent This
 - Disable Internal/External Connections
 - Disable Inter-process Communications
 - Only Approved Applications And APIs
- Device Firewall
 - No Unauthorized Network Access
 - End User Must Authorize Applications



BlackBerry Infrastructure

Necessity

- BlackBerry Infrastructure is essential for delivering a secure, efficient and scalable wireless solution
- NON- BlackBerry Infrastructure solutions have the following critical issues:
 - Consumes of 400-500% more network capacity than BlackBerry Infrastructure solution
(= much higher utilization and service costs).



BlackBerry Infrastructure

Necessity

- No ability to manage network traffic flow, forcing enterprises to establish direct connections with every carrier they deal with (= significant complexity and costs, especially for international organizations).
- Severely impacts battery life due to need for device to maintain persistent connection with corporate network (= poor end user experience and usability)
- Severely compromise network security as the requirement for continuous, multiple and unauthenticated inbound ports through the corporate firewall leaves the enterprise open to Denial of Service attacks (= high risk of corrupting network infrastructure).



BlackBerry Infrastructure

Facts

- Rim is NOT able to decrypt any messages passing on the BlackBerry Infrastructure, due to the Master/Session key Concept
- RIM Cannot access customer LAN, due to outbound initiated Firewall connection
- NO data packages are stored on the BlackBerry Infrastructure, Carrier sends out of coverage message to BlackBerry Infrastructure and from there to BES to stop sending once device is out of coverage



Q & A

- Questions?

