Technical White Paper
BlackBerry™ Security

For Microsoft® Exchange™
Version 2.1

Research In Motion Limited

Table of Contents

1. Introduction

This document explores the security of the BlackBerry™ wireless email solution and describes how corporate information stays secure even while transmitted over a wireless network to the BlackBerry Wireless Handheld™.

BlackBerry is a leading wireless email solution for mobile professionals. It is an innovation in simplicity for the user since it instantly provides a secure, continuous wireless link between the desktop and the handheld.

The BlackBerry solution:

- Monitors the user's inbox for new mail.
- Determines how and if a message is relayed to the user's BlackBerry Wireless Handheld through the application of user-defined filters.
- Compresses and encrypts messages and pushes them to the BlackBerry Wireless Handheld via the Internet and wireless network.
- Receives, via the Internet, messages composed on the BlackBerry Wireless Handheld, then decrypts and decompresses the messages and places them in the user's Outbox for delivery by the corporate Microsoft® Exchange Server.

The BlackBerry Enterprise Server provides a secure, two-way link between the user's Microsoft Exchange account and the user's BlackBerry Wireless Handheld. The BlackBerry Enterprise Server should be considered a conduit, rather than a mail server or a message repository. The Microsoft Exchange Server's message store is the only place a secure copy of the data is kept. Since it maintains a link to the messages in the user's Microsoft Exchange Inbox, the BlackBerry Enterprise Server has the following advanced features:

- After the first 2K of a message is delivered to the handheld, the user is able to request more of the message, delivered in 2K packets, up to a maximum of 32K.
- When "replying with text" from the handheld, the BlackBerry software appends the entire original message to the reply, not just the 2K that was sent to the handheld.
- When forwarding a message from the handheld, the BlackBerry software forwards the entire original message including all attachments.

2. Architecture

An overview of the system architecture for the BlackBerry Enterprise Server is provided in Figure 1. At the heart of this wireless email solution is the BlackBerry Enterprise Server (B). It uses the Microsoft Exchange Server's storage (C) for keeping unique information for each user, including security information, specialized forwarding rules and handheld identification.

Each user configures their own filter rules and encryption key information in the BlackBerry Desktop Manager, which runs on their own desktop (A). The BlackBerry Desktop Manager stores the configuration information in hidden folders in the user's Microsoft Exchange message store (C). The BlackBerry Enterprise Server also stores redirection statistics in the same location, so that either the desktop user or the IT department can view the statistics to determine if a given handheld is working correctly.

The BlackBerry Enterprise Server maintains a constant direct TCP/IP level connection (Server Routing Protocol or SRP) to the wireless network (E). A configuration change is required at the firewall (F) to allow an outbound-initiated connection on port 3101 using TCP. This is not a "hole" in the firewall because only an outbound connection is required.

Information is encrypted and decrypted by the BlackBerry Enterprise Server as well as on the user's BlackBerry Wireless Handheld. Assuming the company's server is secure within their building, the only two places the information is accessible within the BlackBerry solution are on the handheld and at the company (i.e. the user's desktop).

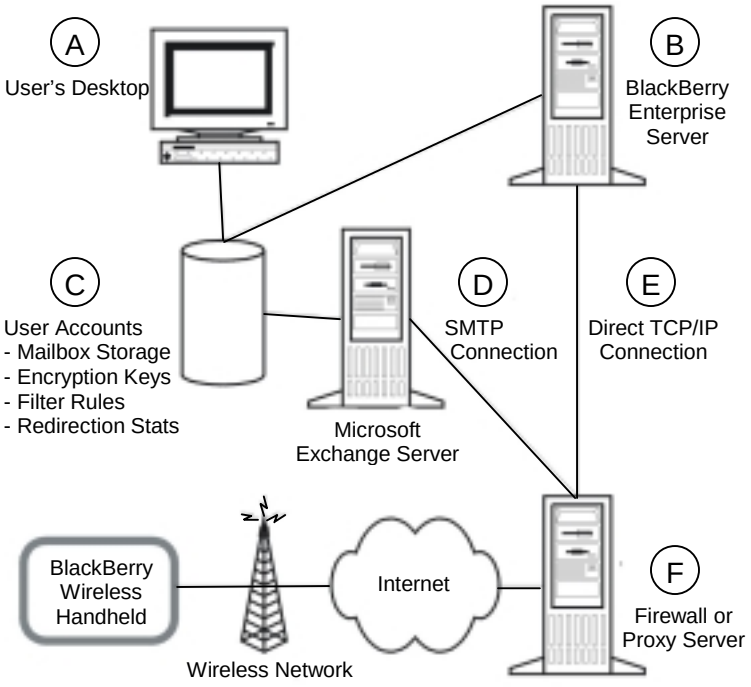

Figure 1: Architecture using BlackBerry Enterprise Server

3. Firewall Security

The BlackBerry Enterprise Server maintains a constant direct TCP/IP level connection to the wireless network. To do this, it requires a configuration change at the firewall to allow an outgoing connection on port 3101. This is an outbound-initiated connection initiated by the BlackBerry Enterprise Server.

To establish this connection, the BlackBerry Enterprise Server contacts the wireless network. If the authentication parameters are false, authentication will fail and the connection will not be established.

Once the connection is established, it remains a persistent session created for communication only between the BlackBerry Enterprise Server and the wireless network to the BlackBerry Wireless Handheld. Outbound traffic from the BlackBerry Enterprise Server has no destination other than the BlackBerry Wireless Handheld through the wireless network. Any inbound traffic to the BlackBerry Enterprise Server from any other destination will be discarded.

Many IT departments are uncomfortable about making firewall configuration changes. The connection through port 3101 is completely secure.

- The connection to the wireless network is outbound-initiated by the BlackBerry Enterprise Server and must be authenticated. No inbound traffic is permitted from any other source host.
- The BlackBerry Enterprise Server is only a redirector of messages to and from Microsoft Exchange: it stores no messages and therefore has no access to messaging or corporate information of any kind.
- All messaging traffic between the BlackBerry Enterprise Server and the user's wireless handheld is encrypted using Triple-DES encryption. All messages remain encrypted along the entire path from source to destination. There is no staging location where the message is decrypted and encrypted again. All communications between the BlackBerry Enterprise Server and the wireless network are fully protected from unwanted third parties.
- The BlackBerry Enterprise Server itself runs as a service under Windows NT®. The service will only accept data that it can decrypt using a valid encryption key. No communication of any kind can occur between the BlackBerry Enterprise Server and Microsoft Exchange unless this condition is met. As a result, as only the server has a valid encryption key, no commands will be accepted from any outside source.

4. Technical Overview

The BlackBerry Wireless Handheld gives users mobile access to messaging and personal organizer information located on their desktop computers. The security system is intended to ensure that the information exchanged between the handheld and the desktop computer or company LAN occurs without compromising the confidentiality of that information.

The objectives of the security system are as follows:

1. **Protecting Data on the Handheld:** Company information stored on the handheld should be as secure as information stored on the company LAN.

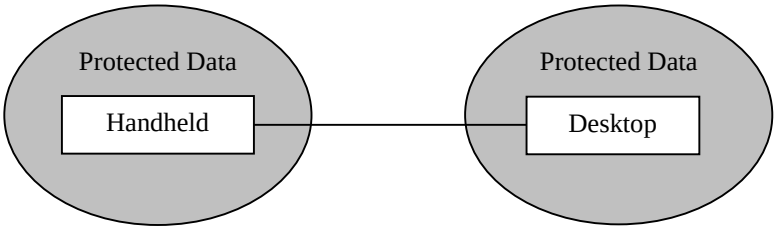

Figure 2. Protecting data on the handheld

2. **Securing the Wireless Link:** The information travelling on the link between the handheld and the desktop or company LAN should not be retrievable by an unauthorized third party. A Virtual Private Network (VPN) should effectively connect the handheld to the desktop.

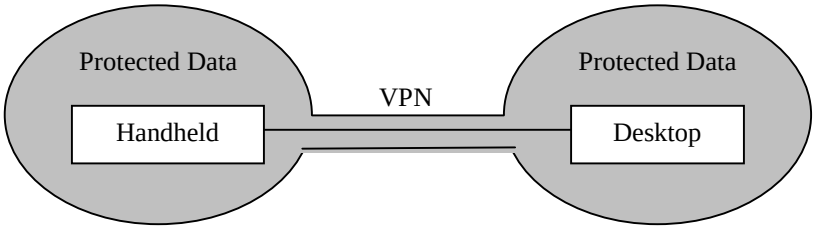

Figure 3. Securing the wireless link

3. **Minimal user impact:** The user should not be inconvenienced by the presence of the security system.

5. Handheld Information Protection

Users can use various handheld features to protect their information. Each user can set an individual password that is between 4 and 14 characters long. The aim of the password is to ensure that only the owner has access to the information stored on the handheld.

The handheld rejects weak passwords, such as those composed of identical characters or those that consist of a natural sequence (i.e. 1, 2, 3, 4, etc.). With the password set, a screen saver appears after a set period of inactivity; the screen saver can be customized to display contact information. Once the password is in place, there is a lock function available that causes the immediate appearance of the screen saver. When the screen saver appears, access to data on the handheld, through both the keyboard and the serial port, is prevented until the user enters the correct password. If an incorrect password is entered ten consecutive times, all user-specific data on the handheld is cleared.

The password itself is protected by storing only an SHA-1 hash of the password on the handheld. This ensures that even if someone had the contents of the memory, it would not be possible to determine the password. When the user enters the password, the handheld performs a one-way hash of the entered characters using SHA-1, and then compares the hashed input to the stored hashed password.

Security-conscious companies will value this added feature. Using the password ensures that users always require at least two pieces of security to access their corporate email. In this case, they physically have the security of the handheld as well as the knowledge of a private password.

6. Wireless Link Protection

BlackBerry was designed to ensure that information sent over the wireless link is also secure. Data sent between the handheld and the desktop or company LAN is encrypted using the Triple-DES algorithm. The Triple-DES algorithm is the most time-tested encryption algorithm available and is the algorithm favoured by the banking industry to electronically transfer confidential financial data.[1]

Security is derived from an encryption key shared by the handheld and the desktop. The key used by the handheld is generated on the desktop by extracting random information from mouse movements then hashing the collected random bits. The key is then exchanged with the handheld through a port connection. This exchange can only be done once so that the key is available in two places: on the desktop and on the handheld. The advantage of this symmetric key encryption system using a secure key exchange is that the encrypted data exchanged between the handheld and the desktop is guaranteed to be confidential and authenticated since it comes from a source holding the shared key.

Once this key has been generated, a copy of it is stored in Microsoft Exchange and the other copy is stored on the handheld. For messaging to occur, these keys must match at both the server and the handheld, or the message is discarded.

In the BlackBerry solution, information transferred between the handheld and the desktop or company LAN is not decrypted at any intermediate point. This means that only the desktop and handheld user have access to the information sent between them. In particular, it means that the service provider does not have access to any potentially sensitive company information.

Since the exchange of the symmetric key is allowed only when the handheld is plugged into the user's desktop there is an authenticated link for exchanging the key. This authenticated link creates an unbreakable bond, assuming the user's desktop is in a secure area. Users are also encouraged to use a password protected screen saver to ensure their desktops are secure.

[1] Distributed.net, a coalition of computer enthusiasts, was able to work as a connected worldwide computing team and decipher a message encrypted with the Single-DES algorithm in 22 hours and 15 minutes. As an illustration of the power of Triple-DES, consider the following example: according to experts, if Single-DES could be broken in one second, it would still take over 1 billion years to crack Triple-DES.

7. Wireless LAN Protection

The protection of existing information found on the desktop or company LAN is the responsibility of the corporate IT department. Information stored on the desktop is not specifically protected by the BlackBerry security system. The BlackBerry security system is intended to extend the existing security of information on the desktop to information being transmitted to, and available on, the BlackBerry Wireless Handheld. Users' desktops must be protected by a secure company firewall in order for the BlackBerry solution to offer a reliable security system. If the user sends email from the handheld to someone outside the company firewall, the message first travels to the "firewall protected" desktop. This is the limit of the BlackBerry security system's domain.

To ensure the email forwarded from a desktop to the Internet is encrypted, users and IT departments must use another solution, such as installing a secure Internet mail system like PGP or using S/MIME. Suggestions to enhance desktop security are included later in this document to assist non-technical users.

8. Details of the System

In this section, a more detailed description of the entire BlackBerry solution is provided. The solution consists of handhelds, a wireless data network communicating with the Internet and various computers (servers or desktops) running the BlackBerry software. The handhelds transmit and receive messages over a wireless network. The wireless data network sends messages to and receives messages from the handheld, as well as receiving and sending messages from a LAN server or desktop computer via the Internet. The BlackBerry software sends messages to and receives messages from the wireless network via the Internet, and interfaces with the desktop mailbox. The two modes of email communication used in the BlackBerry solution are handheld-to-desktop and desktop-to-handheld.

Handheld-to-desktop: When the handheld transmits a message, the message is encrypted and then sent to the wireless network. The network forwards the encrypted message across the Internet to the user's corporate email mailbox associated with the handheld. The BlackBerry software decrypts the message and then displays it on the user's desktop, in the Sent Items folder, in its original form.

Desktop-to-handheld: When a message is received at the user's corporate email mailbox it is encrypted and then sent across the Internet to the wireless network. The wireless network forwards the encrypted message to the handheld where it is decrypted and displayed for the handheld user. Information on the handheld is stored unencrypted.

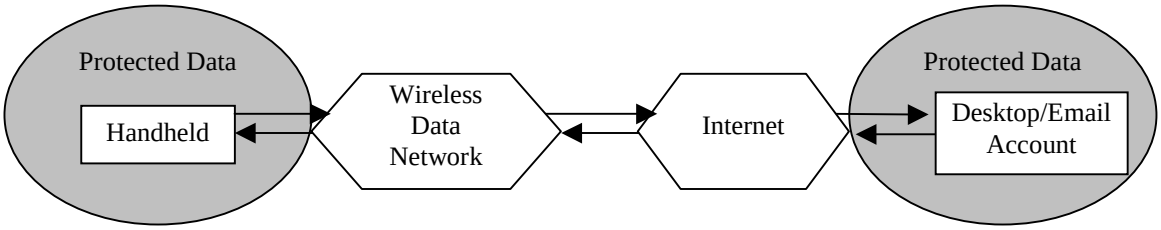

Figure 4. Message delivery between desktop and handheld

Security - Wireless Email

Using the email method of communication (handheld-to-desktop, desktop-to-handheld), there is only the need for the exchange of two identical keys per handheld and PC pair. (i.e., one key is created at the desktop and shared with the handheld). Since only one key must be generated (two identical keys are shared), it is efficient and effective to use symmetric key encryption in this mode.

Note To keep your information secure, it is recommended that this key be changed once a month. By default, the BlackBerry Desktop Manager generates a new key each month.

9. Frequently Asked Questions

The following list summarizes frequently asked questions regarding ways in which the user or IT department can ensure a secure system.

- **How do I get the security system working?**
  Set the password and security timeout period on the handheld. Optionally, set the owner information on the handheld in case the handheld is lost. When installing the BlackBerry Desktop Manager software, place the handheld in the cradle connected to the desktop and then run the software. During installation, a secret key is exchanged between the desktop and the handheld.

- **What happens if I forget the secret key?**
  The handheld user does not have access to the secret key and therefore does not need to remember it. If the handheld or desktop memory is corrupted, then a new secret key must be exchanged between the desktop and handheld using the BlackBerry Desktop Manager software. During the manual key generation, the user only needs to move the mouse to ensure an effective random key is created.

- **What do I need to do to achieve a completely secure operation?**
  Set the password and timeout option on the handheld. Ensure the screen saver is engaged before the handheld is set down. These actions help to secure data on the handheld. Link the handheld to the desktop using the BlackBerry software to allow the exchange of secret keys, then only use the handheld to send email (i.e., do not use SMS). This secures any data sent over the wireless link. Finally secure the desktop/LAN against unauthorized access.

- **How can I secure the desktop?**
  This is not part of the BlackBerry security system, but security at the desktop can be enhanced by (a) activating a password-protected screen saver; (b) installing firewall software; and by (c) installing PGP or S/MIME-protected email systems.

- **What happens if I forget the password?**
  There are no backdoors to circumvent the password protection on the handheld. If the password is unknown then the information on the handheld cannot be retrieved. The BlackBerry Desktop Manager software does, however, include a Backup and Restore feature, which can be used to periodically save the handheld information on the desktop. (Note: It is not possible to backup the handheld while it is locked and waiting to be enabled by the password.) In the event that the password is forgotten, the information on the handheld is cleared after ten incorrect password attempts. The information must then be restored from the desktop using the Backup/Restore tool located in the BlackBerry Desktop Manager software.

  Since most of the information is originally from the desktop personal organizer, the real owner of the handheld can resynchronize all information when the handheld is plugged back into their desktop.

- **What do I need to do in order to achieve protection against casual eavesdroppers?**
  There are no configurations required in order to achieve protection against casual eavesdroppers. The BlackBerry is capable of preventing these types of invasions for all email messages (not SMS).

10. Glossary

BlackBerry Desktop Software
The software that includes the four tools (Application Loader, Intellisync™, Backup/Restore, and Redirector Configuration) as well as the first screen that appears when the desktop software is launched.

BlackBerry Enterprise Server
The software that centralizes the management of BlackBerry into a server solution that the IT department can monitor and control.

Decryption
The process of restoring encrypted data to its original form.

Encryption
The process of encoding data to prevent unauthorized access, especially during its transmission. The data is encoded using a key (akin to a password).

Key
The secret data used to encrypt or decrypt data.

One-way Hash
The programmatically irreversible, yet reproducible, mangling of data. For example, if the passwords on a system are hashed, then whenever a user attempts to enter a password it can be hashed and the result compared to the stored value. Given the hashed password, it is unfeasible for anyone to compute the original password.

SHA-1
A U.S. government approved one-way hash algorithm.

Single-DES
The Single-Data Encryption Standard is a U.S. government standard symmetric-key encryption method that provides an almost unlimited number of ways to encrypt documentation.

Symmetric Key Encryption
An encryption scheme where two parties who want to exchange data confidentially must share the same key.

Triple-DES
A U.S. government approved symmetric key encryption algorithm that requires the generation and use of three keys. It is by far the most thoroughly tested encryption algorithm. No successful invasions on this encryption method have been found.