Table of Contents

INTRODUCTION ............................................................................................................................... 1
ARCHITECTURE ............................................................................................................................. 2
FIREWALL SECURITY ..................................................................................................................... 3
TECHNICAL OVERVIEW .................................................................................................................. 3
HANDHELD INFORMATION PROTECTION .................................................................................. 4
WIRELESS LINK PROTECTION ....................................................................................................... 5
WIRELESS LAN PROTECTION ....................................................................................................... 6
PEER-TO-PEER ADDRESSING ....................................................................................................... 6
DETAILS OF THE SYSTEM ............................................................................................................. 7
FREQUENTLY ASKED QUESTIONS ............................................................................................... 8
ASSOCIATED DOCUMENTS .......................................................................................................... 10
GLOSSARY ....................................................................................................................................... 11
Introduction

This document explores the security architecture of the BlackBerry Enterprise Edition™ for Lotus® Domino™ and describes how corporate information stays secure even when transmitted over a wireless network to the BlackBerry™ handheld.

The BlackBerry Wireless Email Solution is one of the most unique wireless product offerings for the corporate user. This solution is also an innovation in simplicity for the user, since it provides a secure, continuous wireless link between the desktop and the handheld.

BlackBerry Enterprise Edition for Lotus Domino is available as an enterprise server solution. The product performs the following tasks:

- Monitors the user’s mailbox for new mail;
- Determines how and if a message is relayed to the user’s BlackBerry handheld through the application of user-defined filters;
- Compresses and encrypts messages and delivers them to the BlackBerry handheld via the Internet and wireless network;
- Receives, via the Internet, messages composed on the BlackBerry handheld, then decompresses and decrypts the messages and places them in the MAIL.BOX for delivery by the Domino router task. Additionally a copy is placed in the Sent folder of the user’s mail database.

The BlackBerry Enterprise Server provides a secure, two-way link between the user’s Domino mail server and the user’s BlackBerry handheld. 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 up to a total of 32K to be delivered in 2K packets.
- 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.
Figure 1: Architecture using BlackBerry Enterprise Server.

Architecture

An overview of the system architecture for the BlackBerry Enterprise Server product is provided in Figure 1. At the heart of this mobile email solution is the BlackBerry Enterprise Server (A). The BlackBerry Enterprise Server is installed on a Windows NT or Windows 2000 server running Lotus Domino. Installing the BlackBerry Enterprise Server software will create two Domino databases used for managing wireless messaging. BlackBerryOutbox.NSF acts as the outbound queue for wireless email. BlackBerryProfiles.NSF contains configuration information for BlackBerry users such as security information, specialized forwarding rules and handheld identification information. The security on the individual databases is controlled by the database Access Control List (ACL). Additionally, some fields that require more security are encrypted within the database.

Users control their own filter rules and encryption key information using the BlackBerry Desktop Manager software. The Desktop Manager runs on its own PC or laptop (B) and writes the configuration information in the BlackBerryProfiles.NSF database on the BlackBerry Enterprise Server (A). The BlackBerry Enterprise Server also stores redirection statistics in this database so that the IT staff 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 (via Server Routing Protocol or SRP) to the wireless network (C). The BlackBerry Enterprise Server requires a configuration change at the firewall (D) to allow an outgoing connection on port 3101. This is not a “hole” in the firewall; it is rather an outbound-initiated connection which cannot be initiated by any host except the BlackBerry Enterprise Server.

Once delivered, information can only be decrypted by the BlackBerry handheld associated with the individual’s Domino Mail database. Information is encrypted and decrypted directly on the BlackBerry Enterprise Server as well as on the user’s BlackBerry handheld.
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 outbound-initiated connection on port 3101. This outbound-initiated connection is initiated only 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. Authentication on both sides takes place to ensure that the BlackBerry Enterprise Server is authenticating with the wireless network and that the wireless network is authenticating with the BlackBerry Enterprise Server.

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

The connection through port 3101 is completely secure, requiring configuration only for outbound-initiated traffic. The following characteristics of the connection and the traffic which passes across it further maintain the port’s security:

- The connection to the wireless network is outbound-initiated by the BlackBerry Enterprise Server and is authenticated via Challenge/Response. No inbound traffic is permitted from any other source host.
- 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 re-encrypted. All communications between the BlackBerry Enterprise Server and the wireless network are fully protected from interference by third parties.
- The BlackBerry Enterprise Server itself runs as a Lotus Domino add-in task. The task will only accept data that it can decrypt using a valid Triple DES encryption key. No communication of any kind can occur between the BlackBerry Enterprise Server and Domino unless this condition is met. As a result, no commands will be accepted from any outside source.
- Because the Triple DES encryption key is stored only on the BlackBerry Enterprise Server and in the user’s BlackBerry handheld there is no way for Research In Motion®, or any other third party, to introduce extra commands or “subversive” messages via the link.

Technical Overview

The BlackBerry handheld gives users mobile access to messaging and personal information located on their desktop computers. The security system is intended to ensure that the information exchange 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](protected_data_handheld_desktop)

2. **Securing the Wireless Link**: The information traveling 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](vpn_protected_data_handheld_desktop)

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

**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 either the keyboard or 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 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.
Wireless Link Protection

BlackBerry was designed so that information sent over the wireless link is 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 on the BlackBerry Enterprise Server 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.

BlackBerry security has received the FIPS 140-1 Validation for its embedded encryption technology. FIPS 140-1 Validation is an important, and often, mandatory, purchasing criteria for many organizations, especially within the government sector.

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.
Wireless LAN Protection

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 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” BlackBerry Enterprise Server. This is the BlackBerry security system’s domain.

Peer-to-Peer Addressing

In addition to messages sent by email, which are sent securely, the handheld offers a peer-to-peer option allowing users to send messages directly to another handheld using that handheld’s PIN. Messages sent peer-to-peer are scrambled to protect against casual eavesdropping, but are not fully secure. If the user requires a secure link, the PIN addressing mode should not be used.
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 Desktop Software. The handhelds transmit and receive messages over a wireless network (i.e., Mobitex or DataTAC® networks). The wireless network sends messages to and receives messages from the handheld, and also sends messages to and receives messages from a LAN server via the Internet.

The two modes of communication used in the BlackBerry solution are email and peer-to-peer.

1. **Email**:

   **Handheld-to-server**: 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 BlackBerry Enterprise Server. The BlackBerry Enterprise Server then decompresses and decrypts the message and deposits it in the MAIL.BOX on the BlackBerry Enterprise Server. Domino’s native routing mechanism then delivers the message to the destination.

   **Server-to-handheld**: When a message is received at the server it is compressed, encrypted and then sent across the Internet to the wireless network. The wireless network then forwards the encrypted message to the handheld where it is decompressed, decrypted and displayed for the handheld user. Information on the handheld is stored unencrypted.

2. **Peer-to-peer**: When the handheld transmits a message using the peer-to-peer mode, the message is scrambled (not encrypted) then sent to the intelligent wireless network. The network then forwards the scrambled message to the destination handheld(s). The destination handheld unscrambles and displays the message for the handheld user.
Frequently Asked Questions

The following list summarizes the frequently asked questions regarding ways in which the user or IT department can enable 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 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 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 maximize security?**
  Set the password on the handheld and set the timeout option. Ensure the screen saver is engaged before the handheld is set down. These actions 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 the peer-to-peer mode). 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 back doors to circumvent password protection on the handheld. If the password is unknown then the information on the handheld cannot be retrieved. The BlackBerry Desktop 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 Software.

  Since most of the information is originally from the desktop PIM storage areas, 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 messages.

• **What should I do if my handheld is lost and not retrieved?**
  If the device is stolen the user can contact BlackBerry Technical Support (1-877-255-2377) and request that the device be deactivated.

• **What should I do if my handheld is lost and then returned?**
  If it is suspected that the screen saver was not active when the handheld was lost, the handheld should be linked to the desktop using the BlackBerry Desktop Software and the handheld contents should be backed up. The handheld should then be erased to avoid the possibility of rogue code existing on the handheld. Once the contents are erased, use the loader and the backup/restore utility to reinstall the handheld code and contents onto the handheld.

• **What should I do if my handheld keys are made available to a third party?**
  This can only happen if someone gains access to the user’s desktop or to the company LAN. In this case two new keys should be generated to replace both the current and the previous encryption keys, which are kept on the handheld.
Associated Documents
As illustrated in Figure 1, there are several components in the complete BlackBerry product set. Associated documents describe each component in detail. To learn more about the BlackBerry Enterprise Server consult the BlackBerry Enterprise Server Technical White Paper, also available at www.blackberry.net.
Glossary

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

BlackBerry Enterprise Server
Is the software that is installed on a server and performs email redirection. It provides IT departments with centralized management and control of BlackBerry handhelds.

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.

Message Scrambling
The process of rendering a message unintelligible by anyone who does not possess the common scrambling key. When the handheld transmits a message using the peer-to-peer mode, the message is scrambled (not encrypted) then sent to the intelligent wireless network. The network then forwards the scrambled message to the destination handheld(s). The destination handheld unscrambles and displays the message for the handheld user.

One-way Hash
The programmatically irreversible, yet reproducible, scrambling 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.