Research in Motion: BlackBerry Cryptographic Kernel Policies

DOCUMENT CLASS:	Overview
CODE NAME:	FIPS
SECURITY LEVEL:	Level One
ORIGINATOR:	Aron Pinto
DEPARTMENT:	Technical Presales
DATE ORIGINATED:	27 November 2000
PRINTED BY:	Scott Bailey
PRINTED ON:	11/27/00 at 10:34 AM

APPROVALS		
Don McMurtry	VP Sales	Date
Herb Little	Software Development Director	Date
Scott Bailey	Technical Account Manager	Date
Anthony LeBlanc	Government Solutions Manager	Date
Aron Pinto	Product Specialist	Date

Table of Contents

Table of Figures

1.0 Introduction

1.1 Purpose

This document describes the security policies implemented by the BlackBerry crypto-kernel v2.1 (present in the BlackBerry 950 and 957 units) and specifically how the design of its firmware enforces these policies.

Figure 1.0: BlackBerry 950 (on the left) and the BlackBerry 957 (on the right)

1.2 Scope

This document addresses the RIM crypto-kernel v2.1's security policies.

1.3 Intended Audience

The intended audience for this document is: the Research in Motion BlackBerry Engineering and Product Management Team, external agencies for the validation or endorsement of the Research in Motion BlackBerry product and BlackBerry customers with significant concerns about messaging security including governments and the military.

2.0 BlackBerry Crypto-Kernel Overview

The BlackBerry crypto-kernel is an application initially loaded onto the BlackBerry product at the manufacturing site. To obtain the FIPS-approved version, please contact Research in Motion at 1-877-BLK-BERRy or visit their website at www.blackberry.net.

The BlackBerry crypto-kernel is messaging-system independent. To see which messaging systems are currently supported by the BlackBerry product, please consult the RIM website at www.blackberry.net.

In order to maximize security we shall assume that the BlackBerry handheld screensaver is always active whenever the handheld is left idle or locked by the user. The BlackBerry crypto-kernel v2.1, common to both the BlackBerry 950 and the BlackBerry 957, securely compresses and encrypts messages with triple DES. Following this procedure, the ciphertext is transmitted over the Internet to the user's mail server. Upon receiving the message, the mail server decrypts and decompresses the ciphertext back to the original plaintext.

A valid master key must be stored in the device in order for encryption to commence. The master key is generated while the BlackBerry device is connected to the user's desktop serial port by a RIM BlackBerry cradle. This is achieved via RIM's Desktop Manager Software. While the BlackBerry device is secured to the user's desktop by use of the cradle, the user assumes the crypto-officer role and must prompt the Desktop Manager software for the generation of a master key. After doing so, the software will guide the user through the key generation. The randomness of the key is derived from random movement of the mouse on the desktop. The coordinates of the mouse pointer are stored at random time intervals in a data buffer. Once sufficient data is stored, a SHA-1 hash algorithm is applied to the buffer, resulting in a 16-byte master key.

3.0 Security Roles Performed by the Crypto-Kernel

The owner of the BlackBerry has two roles when using the device:

3.1 User Role

The user is the cryptoblock.dll. The user role is invoked each time the user sends or receives a message. Sending a message involves compression of the plaintext, followed by encryption. Receiving messages involves decryption of the ciphertext, followed by decompression. The user role includes the following services: show status, create session key, encrypt and decrypt.

3.2 Crypto-Officer Role

The Desktop Manager Software performs the role of a crypto-officer through the management of keys on the mail server and on the device. The crypto-officer has the option to generate new master keys at will. The procedure involved in key loading and zeroization is further explained in section 4.3. The crypto-officer role includes the following services: self-tests, firmware initialization, master key initialization, show status and master key zeroization.

4.0 Security Service Performed by the Crypto-Kernel

The BlackBerry crypto-kernel v2.1 includes the following services:

4.1 Encryption

Prior to transmission, the BlackBerry crypto-kernel v2.1 compresses the plaintext to increase efficiency by reducing the size of the data to be transferred. Following compression, it encrypts the plaintext into ciphertext using a session key. The session keys are randomly generated for each message. Following the initial encryption, the session keys are encrypted using the master key stored on the device or mail server. Both the ciphertext and session keys are then transmitted to the mail server. Decryption does not occur until the message is received within the secure mail environment.

4.2 Decryption

The BlackBerry crypto-kernel v2.1 begins by decrypting the session keys by use of the corresponding master key, stored in the mail server. Once the session keys are retrieved, they are used in the decryption of the corresponding ciphertext. Following decryption the text is decompressed and stored as plaintext. The session key is then zeroed and discarded.

4.3 Master Key Generation, Loading and Zeroization

To initialize, master keys are generated and loaded onto both the device and mail server. One copy of the key is stored in the device's Flash Memory while the second is stored on a server in the user's secure messaging environment.

Zeroization of both master and session keys will occur following ten consecutive incorrect password attempts at which point the contents of the device are cleared and returned to the factory defaults.

5.0 Security Relevant Data Items Available to the BB Crypto-Kernel v2.1

- **DES session keys:** used in the encryption and decryption of individual messages.
- **DES master keys:** used in the encryption and decryption of session keys.
- **Handheld screensaver password:** used to limit access to the handheld.

6.0 Access to the Security Relevant Data Items of the BB Crypto-Kernel v2.1

Access to the security relevant data items is limited to the following scenarios:

6.1 Transferring messages from a BlackBerry to the mail server

The user must first deactivate the handheld screensaver in order to make the device functional. To do this, a password must be entered on the device. The master key being accessed is stored in the Flash memory of the device.

6.2 Transferring messages from the mail server to a BlackBerry

The master key is stored in the user's production messaging system. The BlackBerry messaging redirector accesses the key from this messaging system each time a message is sent to the handheld.

7.0 FIPS Mode Usage

All messages sent or received via email addresses are triple DES encrypted. Messages sent from PIN address to PIN address are not. FIPS mode usage is limited to sending or receiving messages via email addresses.