BlackBerry Java Handheld Application Security

Originally posted: February 2003

Introduction

Corporate data access capabilities supported by the BlackBerry platform enable wireless device connectivity through standard protocols and languages, while maintaining the solid architectural components that already allow BlackBerry™ to provide a secure, manageable and complete wireless email solution behind the firewall.

The BlackBerry 5800 Series™, BlackBerry 6500 Series™, and BlackBerry 6700 Series™ of wireless handhelds are based on an open, Java™-based platform. With support for Java 2 Micro Edition (J2ME™), and the Mobile Data Service feature of the BlackBerry Enterprise Server, the BlackBerry solution enables a wide range of software application development based on open standards.

BlackBerry handheld software version 3.6 or later enables users to download Java applications wirelessly, using the handheld browser. Standard BlackBerry security features protect corporate data on the handheld and on the network. Additional security features minimize the potential risk of adding third-party applications to the handheld.

This document discusses features that protect the security of corporate data on the handheld and on the network from the following security risks:

- loss or theft of the handheld
- interception of data on the network
- malicious attacks to steal corporate data
- identity theft
- malicious application code, such as viruses

Loss or theft of the handheld

Each user can set an individual password that is between 4 and 14 characters long so that only the owner of the handheld has access to information that is stored on it. The handheld rejects weak passwords, such as those composed of identical characters or those that consist of a natural sequence (for example, 1234).

When the password is set, a screen saver appears after a set period of inactivity. The user can customize the screen saver to display contact information. The user must type the correct password to gain access to the handheld. By default, if an incorrect password is typed ten consecutive times, the user-specific data on the handheld is cleared to prevent unauthorized access.

The password itself is protected by storing only an SHA-1 hash of the password on the handheld. Even if someone had the contents of the handheld memory, the password could not be determined from handheld memory.

System administrators can set IT policies to enforce corporate security policies, including:

- requiring that users set a password
- setting a minimum password length
- requiring that passwords have at least one number and one letter
- setting a password security timeout

With the BlackBerry Enterprise Server 3.5 or later for Microsoft® Exchange, if a handheld is lost or stolen, system administrators have several options:

- If the user expects to recover the handheld (for example, the handheld was left in a restaurant), the system administrator can set a password and lock the handheld so that no one else has access to the handheld.
- If the user does not expect to recover the handheld (for example, the handheld is stolen), the handheld can be wiped so that no user or corporate data remains on the handheld.

Interception of data on the network

All data that is sent between the BlackBerry Wireless Handheld and the corporate LAN over the wireless network through the BlackBerry Enterprise Server is encrypted using the Triple DES algorithm. Data is not decrypted at any intermediate point. All data is encrypted, including email, calendar appointments, and web data, for both standard BlackBerry applications and third-party applications.

A common encryption key is shared by the handheld and the corporate server. The BlackBerry Desktop Manager generates this encryption key by extracting random information from mouse movements and then hashing the collected random bits. By default, the desktop software generates a new key each month. The key is transferred from the desktop computer to the handheld over the serial or USB connection to the handheld cradle. After the key is generated, it is stored in two places: one copy is stored on the handheld, and the other copy is stored on the Microsoft Exchange or Lotus® Domino™ server. For messaging to occur, the keys at the server and the handheld must match, or the message is discarded.

Refer to the *BlackBerry Security* technical white papers for more information. These white papers are available at http://www.blackberry.com/knowledgecenter.

Theft of corporate data

The BlackBerry solution provides several features to help prevent third-party applications from gaining inappropriate access to data on corporate networks. In particular, security features are in place to prevent malicious applications from stealing data from the corporate network and sending it to external parties.

The BlackBerry Wireless Handheld includes a built-in firewall to prevent third-party applications from sending or receiving data over the network without the user’s knowledge. When a third-party application attempts to open a connection, a dialog box prompts the handheld user to allow or deny the connection. The handheld firewall gives users control over how applications on their handheld access the network.

System administrators can set IT policies to control how third-party applications are allowed to access the network. Administrators can control the following items:

- type of network connections that a third-party application can establish (for example, using a wireless application protocol (WAP) gateway, BlackBerry Enterprise Server, serial or USB port)
- whether third-party applications can establish an internal connection within the corporate network or an external connection outside the corporate network
- whether a single application can use both internal and external connections (a “split pipe”)

When an application attempts to open a network connection, IT policies are checked to determine whether this type of connection is allowed. Administrators can enable or disable connections that use a WAP gateway and connections that use the BlackBerry Enterprise Server.

Split-pipe connections are disallowed by default. After an application establishes the connection, it can only make connections of this type for as long as it remains on the handheld. Preventing split-pipe connections helps to protect corporations from a situation in which an application could retrieve corporate data using an internal connection and then send it outside the corporate network covertly.

With the BlackBerry Enterprise Server version 3.5.2 for Microsoft Exchange or BlackBerry Enterprise Server version 2.2 for Lotus Domino, administrators can set the following IT policies to control network access by third-party applications:

IT policy	Description
ALLOW_USE_MDS	controls whether third-party applications can establish an HTTP connection using the Mobile Data Service
ALLOW_USE_WAP	controls whether third-party applications can establish an HTTP connection using a WAP gateway
ALLOW_USE_SERIALPORT	controls whether third-party applications are allowed to use the serial port
ALLOW_INTERNAL_CONNECTIONS	controls whether third-party applications can establish a connection inside the corporate network (for example, using the Mobile Data Service or the serial port)
ALLOW_EXTERNAL_CONNECTIONS	controls whether third-party applications can establish a connection outside the corporate network (using a WAP gateway or direct TCP connection)
ALLOW_SPLIT_PIPE_CONNECTIONS	controls whether the same third-party application can open both internal and external connections (also called a split-pipe connection)

Identity theft

The Mobile Data Service supports standard network authentication mechanisms to control access to the intranet, including Basic Authentication and NT LAN Manager (NTLM), and Kerberos. You can set up your intranet so that users are required to provide their user identification and password before logging into specific web content or services.

Malicious application code

The BlackBerry solution provides several types of protection against third-party application that cause problems on the handheld:

- control of application downloads
- protection of handheld and application memory
- control of access to handheld resources

Application download control

Applications cannot be downloaded to the handheld without the user’s knowledge. The user must select an application using the handheld browser, and confirm the download before it proceeds.

With the BlackBerry Enterprise Server version 3.5.2 for Microsoft Exchange or BlackBerry Enterprise Server version 2.2 for Lotus Domino, system administrators can use IT Policy to control whether users can install and run third-party applications. For example, system administrators can install approved applications before deploying the handhelds in the organization, and then prevent users from installing additional applications.

Protection of handheld and application memory

The BlackBerry platform is designed to prevent applications from causing problems, either accidentally or maliciously, in other applications or on the handheld. Applications that are based on the Mobile Information Device Profile (MIDP), called MIDlets, cannot write to handheld memory that is not allocated specifically for use by the Java virtual machine (JVM). MIDlets cannot access the virtual memory of other applications, or the persistent data of another MIDlet suite. The remaining security concern—a denial-of-service (DOS) attack, in which a malicious application fills up the virtual memory to render the handheld unusable—is a concern that exists in standard Java programs.

Controlled access to handheld resources

BlackBerry applications can share persistent storage, interact with each other, and access user data, such as calendar appointments, email messages, and contacts. This open and flexible framework for application development might increase security concerns. Those security concerns are addressed in two ways:

- Third-party applications can only access persistent storage or user data, or communicate with other applications, through specific APIs.
- Applications that use these APIs must be digitally signed by Research In Motion (RIM).

The purpose of digitally signing third-party applications is to provide an audit trail of the applications that use sensitive APIs. RIM does not inspect or in any way verify third-party applications.

Conclusion

RIM is committed to providing an open and flexible platform for developing wireless applications, with robust security features to protect the integrity of the handheld, the network, and corporate data.

Part number: TAE-00083-001

RESEARCH IN MOTION LIMITED (RIM) ON BEHALF OF ITSELF AND ITS AFFILIATES MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION OR GRAPHICS CONTAINED IN THIS ADVISORY FOR ANY PURPOSE. THE CONTENT CONTAINED IN THIS DOCUMENT, INCLUDING RELATED GRAPHICS, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. RIM HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL RIM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED HEREIN. THIS DOCUMENT, INCLUDING ANY GRAPHICS CONTAINED WITHIN THE DOCUMENT, MAY CONTAIN TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. UPDATES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN AND RIM MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED HEREIN AT ANY TIME.