



Security for BlackBerry Devices with Bluetooth Wireless Technology

Contents

Executive summary	3
Audience	3
About BlackBerry Enterprise Solution security	3
About Bluetooth wireless technology	3
Supported Bluetooth profiles	3
BlackBerry devices that are enabled for Bluetooth wireless technology	4
Risks of using Bluetooth wireless technology on mobile devices	4
Bluejacking	5
Bluesnarfing	5
Bluebugging	5
Protecting Bluetooth-enabled BlackBerry devices	5
Bluetooth wireless technology security measures on BlackBerry devices	5
IT policy rules for Bluetooth wireless technology	6
How users can protect their BlackBerry devices	9
How you can protect BlackBerry devices	9
Related resources	10

Executive summary

This document provides information about the following topics:

- Bluetooth® wireless technology and its uses with BlackBerry Device Software
- potential vulnerabilities in Bluetooth wireless technology
- security measures and strategies that help to protect Bluetooth-enabled BlackBerry® devices from attacks
- information about how to reduce the risk of attacks when using Bluetooth wireless technology on a BlackBerry device
- IT policy rule configurations designed to control the use of Bluetooth wireless technology on BlackBerry devices

Audience

This document is intended for system administrators and system managers. It assumes that you have a working knowledge of the following topics:

- BlackBerry Enterprise Server™ installation, configuration, and administration
- corporate security issues
- wireless devices and networks
- Bluetooth wireless technology

About BlackBerry Enterprise Solution security

The BlackBerry Enterprise Solution™ (consisting of a BlackBerry device, the BlackBerry Device Software, and the BlackBerry Enterprise Server software) is designed to provide a wireless extension of the corporate messaging and collaboration environment.

The BlackBerry Enterprise Solution uses either the Advanced Encryption Standard (AES) or the Triple Data Encryption Standard (Triple DES) encryption methods to encrypt data while it is in transit between BlackBerry devices and the BlackBerry Enterprise Server.

Visit www.blackberry.com/knowledgecenterpublic/ and read the *BlackBerry Security* document for more information.

About Bluetooth wireless technology

Bluetooth is a standard for a personal area network (PAN) short-range wireless technology that enables two devices to communicate using radio waves operating at 2.4 GHz. Using Bluetooth wireless technology, a BlackBerry device can establish a wireless connection with other Bluetooth-enabled devices, such as a hands-free car kit or a wireless headset, that are within a 10-meter range.

The wireless industry considers Bluetooth wireless technology a non-secure wireless channel. If Bluetooth wireless technology is poorly or improperly implemented, security vulnerabilities might exist.

The BlackBerry Enterprise Solution includes features and settings that help you control how mobile professionals use Bluetooth wireless technology and help you protect Bluetooth-enabled BlackBerry devices from potential attacks.

Supported Bluetooth profiles

Bluetooth profiles specify how applications on the BlackBerry device and on Bluetooth-enabled devices connect and are interoperable.

Bluetooth profiles provide use case scenarios and information about how to configure applications that are interoperable. There are many Bluetooth profiles available for implementation. BlackBerry devices currently support only the following three profiles:

- **Serial Port Profile (SPP):** This profile provides procedures that describe how to configure serial connections between a BlackBerry device and a Bluetooth-enabled peripheral that uses a virtual serial port. The Bluetooth-enabled peripheral accesses the serial port through the BlackBerry Software Development Kit.
- **Hands Free Profile (HFP):** This profile works with the SPP to enable wireless voice capabilities with most headsets and some car kits. Because the HFP offers more functionality and performance than the HSP, it is the preferred user profile if both the HSP and HFS profiles are available. For example, the HFP can support wireless address book transfer for car kits that use AT commands (commands that control most modems).
- **Headset Profile (HSP):** This profile works with the SPP to enable wireless voice capabilities with most headsets and some car kits. Use the HSP for wireless voice transmission only if the target peripheral does not support the HFP.

BlackBerry devices that are enabled for Bluetooth wireless technology

Bluetooth wireless technology is available on the following BlackBerry devices:

- BlackBerry 7100 Series
- BlackBerry 7130 Series
- BlackBerry 7290 Wireless Handheld™
- BlackBerry 7250 Wireless Handheld™
- BlackBerry 7520 Wireless Handheld™
- BlackBerry 8700 Series

Risks of using Bluetooth wireless technology on mobile devices

The wireless industry considers that Bluetooth-enabled devices have three potential areas of vulnerability:

- Attackers can obtain confidential data from Bluetooth-enabled devices without the user's knowledge or consent.
- A previously trusted (or paired) source that has been removed from the Trusted list can access the memory contents of some Bluetooth-enabled devices.
- Attackers can gain access to higher-level commands and to voice, data, and messaging channels.

Security threats to Bluetooth wireless technology can be user-based or device-based.

Type of threat	Description	Example
User-based	User-based threats occur when the user changes a setting or performs (or fails to perform) an action that leaves a mobile device vulnerable or open to an attack.	bluejacking
Device-based	Device-based threats are the result of incorrect implementation of Bluetooth wireless technology on the mobile device that leaves the device vulnerable or open to an attack.	bluesnarfing bluebugging

Any Bluetooth-enabled device is at risk for attack when all of the following conditions are present:

- The Bluetooth radio is enabled.
- The device is set to Discoverable (visible) mode.
- The device is physically located within range of an attacker.

Bluejacking

Bluejacking is a user-based threat. It is the act of sending a text message anonymously to Bluetooth-enabled devices that are set to Discoverable mode and are within 10 meters of the attacking device. Attackers can target individuals or broadcast anonymous messages to all discoverable devices in the area. Because Bluetooth-enabled phones, personal device assistants, and laptops can search for other devices within a short range, attackers in crowded public areas can easily send anonymous messages without detection.

Bluesnarfing

Bluesnarfing is a device-based threat that occurs when device manufacturers incorrectly implement the specification for Bluetooth wireless technology.

Bluesnarfing occurs when attackers use Bluetooth wireless technology to connect to a user's device without notifying the user, and access device information without that user's knowledge or consent. Typically, the attacker gains access to the user's contact list, although all object exchange (OBEX)-addressable data that is stored on the device is vulnerable. Bluesnarfing attackers can obtain sensitive information, such as the unique network identifier of a device. They might send text messages, initiate phone calls, or create false address book entries.

Research In Motion® (RIM) does not implement OBEX functionality on BlackBerry devices, which helps to protect BlackBerry devices against bluesnarfing attacks. The Bluetooth interface that RIM implements plugs into the phone application for voice use only. This helps to prevent attackers from gaining access to core BlackBerry device data.

Bluebugging

Bluebugging is a device-based threat that occurs when device manufacturers poorly implement Bluetooth wireless technology security mechanisms.

Bluebugging occurs when attackers use Bluetooth wireless technology to access mobile phone commands on a user's device without notifying or alerting the user. This vulnerability enables the attacker to initiate phone calls, send and read text messages, access and add phonebook contacts, eavesdrop on phone conversations, and connect to the Internet, all without detection or authorization.

Protecting Bluetooth-enabled BlackBerry devices

Protecting corporate data is a primary concern for any organization. The following measures and strategies are designed to protect Bluetooth-enabled BlackBerry devices.

Bluetooth wireless technology security measures on BlackBerry devices

Security measure	Benefit
BlackBerry devices support only three of the available Bluetooth profiles.	This limits the ways that BlackBerry devices are vulnerable to attack. See "Supported Bluetooth profiles" on page 3 for more information about the three profiles.
BlackBerry devices have limited support for the Bluetooth SPP. This profile works only with the BlackBerry phone program to provide voice capability using Bluetooth-enabled headsets and car kits. Even though BlackBerry devices support the SPP for third-party peripherals and application development, this profile is not set up to work with other BlackBerry applications.	BlackBerry device users can control pairing requests, and the number of devices with which a user can pair is limited.
The Disable Discoverable Mode IT policy rule is set to False, which means that BlackBerry devices are not visible to other Bluetooth-enabled devices.	It is more difficult for potential attackers to locate BlackBerry devices and compromise them.

Security measure	Benefit
Use the Disable Bluetooth IT policy rule to turn off the Bluetooth radio on BlackBerry devices.	When you turn off the Bluetooth radio, Bluetooth wireless technology is not operational, and the BlackBerry device is not open to attack.
BlackBerry users must type a passkey to complete a connection or pairing with a Bluetooth-enabled device. A passkey must be anywhere from 1 to 16 characters long and is dependent on the target peripheral.	Users are aware of attempts to connect or pair with a Bluetooth-enabled device because the BlackBerry device prompts them for a passkey.
When the BlackBerry device attempts to pair with a Bluetooth-enabled device, it requests a combination key for authentication. The combination key is unique to the BlackBerry device and the Bluetooth-enabled device with which it is paired. Note: The BlackBerry Smart Card Reader™ uses an Elliptic Curve Diffie-Hellman key exchange, which is designed to enable wireless digital signing and encryption of wireless email messages. See the <i>BlackBerry Smart Card Reader Security</i> document for more information.	Combination keys are designed to prevent the interception of wireless communication between two devices by a third device that was previously paired with one of the devices.
The BlackBerry device prompts the user each time that a Bluetooth-enabled device attempts to connect to it.	BlackBerry users can decline connection requests from Bluetooth-enabled devices.
The Disable Desktop Connectivity IT policy rule prevents connections between the BlackBerry device and the BlackBerry Desktop Manager using Bluetooth wireless technology.	The BlackBerry Desktop Manager does not open the Bluetooth-based virtual serial port at regular intervals to attempt to establish a connection with a BlackBerry device that is within range. This security measure is designed to reduce the risk of unauthorized access to the BlackBerry device through the open port.
The Disable Wireless Bypass IT policy rule requires a BlackBerry device to use a serial port to exchange information with the BlackBerry Enterprise Server, instead of using a virtual serial port and a wireless connection.	The BlackBerry Device Manager does not open the Bluetooth-based virtual serial port at regular intervals to attempt to establish a connection with a BlackBerry device that is within range. This security measure is designed to reduce the risk of unauthorized access to the BlackBerry device through the open port.

IT policy rules for Bluetooth wireless technology

If you are using BlackBerry Enterprise Server version 4.0 or later, use IT policy rules to configure the behavior of Bluetooth-enabled BlackBerry devices. Visit www.blackberry.com/knowledgecenterpublic/ and read the *BlackBerry Enterprise Server IT Policy Reference Guide* for information about setting IT policy rules.

You can manage all Bluetooth-enabled BlackBerry devices simultaneously, or you can manage individual BlackBerry devices.

IT policy rule	Default setting	Configuration notes	BlackBerry Device Software	BlackBerry Enterprise Server software
Allow Outgoing Calls	0: Always By default, a user can place outgoing phone calls from a Bluetooth-enabled BlackBerry device.	The following configuration options are available: 0: Always 1: Only when unlocked 2: Never If you select an option instead of accepting the default setting, you can reduce the risk that an attacker can initiate phone calls from a Bluetooth-enabled BlackBerry device.	4.0.2	4.0.2
Disable Address Book Transfer	False By default, a user can exchange address book information wirelessly between a BlackBerry device and a Bluetooth-enabled device.	When you set this rule to True, it can prevent address book data exchange using AT commands with supported Bluetooth-enabled car kits.	4.1	4.0.3
Disable Bluetooth	False By default, Bluetooth wireless technology is enabled on the BlackBerry device.	When you set this rule to True, you turn off the Bluetooth radio. Use this policy rule to prevent BlackBerry devices from using Bluetooth wireless technology. Warning: If the Bluetooth wireless radio is active when you apply this rule, you must reset the BlackBerry device for the change to take effect.	4.0	4.0
Disable Desktop Connectivity	True The default setting prevents connections between the BlackBerry device and the BlackBerry Desktop Manager using Bluetooth wireless technology.	—	4.1	4.0.3
Disable Discoverable Mode	False The default setting prevents the use of Discoverable mode on Bluetooth-enabled BlackBerry devices.	—	4.0.2	4.0.2
Disable Handsfree Profile	False By default, the Bluetooth HFP is enabled on the BlackBerry device.	When you set this rule to True, you prevent connections that use the Bluetooth HFP.	3.8	4.0
Disable Headset Profile	False By default, the Bluetooth HSP is enabled on the BlackBerry device.	When you set this rule to True, you prevent connections that use the Bluetooth HSP.	3.8	4.0

IT policy rule	Default setting	Configuration notes	BlackBerry Device Software	BlackBerry Enterprise Server software
Disable Pairing	False By default, users can establish a pairing between a Bluetooth-enabled device and a BlackBerry device.	When you set this rule to True, it prevents users from pairing new Bluetooth-enabled devices with their BlackBerry devices. Note: You can pair BlackBerry devices with corporate-approved Bluetooth-enabled devices and then set this IT policy rule to True so that users can use the approved devices.	3.8	4.0
Disable Serial Port Profile	False By default, the Bluetooth SPP is enabled on the BlackBerry device.	When you set this rule to True, you prevent connections that use the Bluetooth SPP.	3.8	4.0
Disable Wireless Bypass	True The default setting requires a BlackBerry device to use a serial port to exchange information with the BlackBerry Enterprise Server, instead of using a virtual serial port and a wireless connection.	—	4.1	4.0.3
Require Encryption	False By default, a Bluetooth-enabled BlackBerry device does not use Bluetooth encryption on all connections.	When you set this rule to True, Bluetooth-enabled BlackBerry devices use Bluetooth encryption. Note: Setting this rule to True might restrict compatibility with other Bluetooth devices.	4.1	4.0.4
Require Password for Discoverable Mode	False By default, a BlackBerry device password is not required to enable the BlackBerry device to enter Discoverable mode. Note: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True.	When you set this rule to True, users are aware of when their BlackBerry devices are discoverable, because they must type a BlackBerry device password to enable Discoverable mode.	4.1	4.0.3
Require Password for Enabling Bluetooth Support	False By default, a BlackBerry device password is not required to turn on Bluetooth support. Note: The BlackBerry device uses this IT policy rule only if the Password Required rule is set to True.	When you set this rule to True, users are aware when Bluetooth functionality is turned on, because they must type a BlackBerry device password to turn on Bluetooth support.	4.1	4.0.3

How users can protect their BlackBerry devices

To help protect BlackBerry devices from bluejacking, bluesnarfing, and bluebugging attacks, users can perform the following actions:

- Leave the BlackBerry device set to non-Discoverable mode.
- If the BlackBerry device is set to Discoverable mode, deny requests to pair with unknown Bluetooth-enabled devices.
- When pairing a BlackBerry device with a Bluetooth-enabled device, set the BlackBerry device to Discoverable mode only for as long as it takes to complete the pairing.
- Complete device pairings in private, uncrowded areas only.
- Choose to encrypt data traffic to and from the BlackBerry device. The BlackBerry Enterprise Solution uses the passkey to generate encryption keys. BlackBerry devices use Bluetooth Security Mode 3 and the highest encryption key length available on the paired device (minimum = 8 bits/maximum = 128 bits).
- Protect the assigned name of your BlackBerry device. If an attacker knows the name of the BlackBerry device, the device is vulnerable to an attack, even when it is set to non-Discoverable mode.

How you can protect BlackBerry devices

To help prevent attacks, you can perform the following actions:

- Upgrade to BlackBerry Enterprise Server version 4.0 or later to access the IT policy rules that control the use of Bluetooth wireless technology on BlackBerry devices. Beginning with version 4.0, the BlackBerry Enterprise Server supports sending IT policy rule updates to BlackBerry devices over the wireless network.
Note: IT policy rules for Bluetooth wireless technology are also available in BlackBerry Enterprise Server version 3.6 Service Pack 3 or later for Microsoft® Exchange.
- For BlackBerry Enterprise Server version 4.1 and later, you can create a separate IT policy group for users who must use Bluetooth wireless technology. Turn off Bluetooth functionality for all other IT policy groups. Visit www.blackberry.com/knowledgecenterpublic/ and read the *BlackBerry Enterprise Server Administration Guide* for information about assigning IT policies to a group.
- Review the BlackBerry IT policy rules for Bluetooth wireless technology, and make sure that they are set correctly for your environment. If a user does not require access to Bluetooth wireless technology, set the Disable Bluetooth IT policy rule to True to turn off access to both Bluetooth wireless technology and the Bluetooth radio on the user's BlackBerry device.
- If you are concerned about unauthorized access to a user's BlackBerry device, but you still want to permit that user to use Bluetooth wireless technology, pair the BlackBerry device with the Bluetooth-enabled device, then turn off the pairing functionality. After you perform this action, only the approved peripheral can pair with the user's BlackBerry device.
- Stay current on viruses and worms that are threats to mobile devices. Assess whether BlackBerry devices are vulnerable to an attack, and then take steps to inform the appropriate individuals in your organization and to protect your corporate BlackBerry devices.
- Educate users about how to safely use Bluetooth wireless technology on their BlackBerry devices.

Related resources

Resource	Description
<i>BlackBerry Enterprise Server Administration Guide</i>	<ul style="list-style-type: none"> generating and changing master encryption keys enabling encryption security best practices
<i>BlackBerry Enterprise Server Feature and Technical Overview</i>	<ul style="list-style-type: none"> BlackBerry Enterprise Server architecture overview
<i>BlackBerry Enterprise Server IT Policy Reference Guide</i>	<ul style="list-style-type: none"> using BlackBerry Enterprise Server IT policy rules
<i>BlackBerry Security</i> document	<ul style="list-style-type: none"> BlackBerry security architecture encryption algorithms security settings
<i>BlackBerry Smart Card Reader Security</i> document	<ul style="list-style-type: none"> BlackBerry Smart Card Reader security
KB-03389 What is—Bluetooth	<ul style="list-style-type: none"> Bluetooth wireless technology overview
KB-03390 How To—Enable and disable Bluetooth	<ul style="list-style-type: none"> turning Bluetooth wireless technology on or off on a BlackBerry device
KB-03391 How To—Pair Bluetooth devices	<ul style="list-style-type: none"> pairing a BlackBerry device with a Bluetooth-enabled device
KB-03392 What is—Bluetooth Device Properties	<ul style="list-style-type: none"> changing the paired device name setting the Trusted field setting the Encryption
KB-03396 What Is—Bluetooth indicators	<ul style="list-style-type: none"> turning Bluetooth wireless technology on or off on a BlackBerry device
KB-03397 How To—Prevent Bluetooth device discovery when within range	<ul style="list-style-type: none"> making a Bluetooth-enabled BlackBerry device non-Discoverable (invisible) to other Bluetooth-enabled devices
KB-04009 What Is—Supported headsets and car kits for Bluetooth-enabled BlackBerry devices	<ul style="list-style-type: none"> compatible Bluetooth wireless technology car kits and headsets
www.blackberry.com/knowledgecenterpublic/	<ul style="list-style-type: none"> BlackBerry device documentation
Bluetooth wireless technology membership site www.bluetooth.org	<ul style="list-style-type: none"> development resources (specifications, qualifications, regulatory knowledge base) development groups research and papers
Bluetooth wireless technology web site www.bluetooth.com	<ul style="list-style-type: none"> web site of the Bluetooth special interest group

Part number: SWD_X_BES(EN)-178.000

© 2006 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, BlackBerry, "Always On, Always Connected" and the "envelope in motion" symbol are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Research In Motion is under license. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current list of RIM (as hereinafter defined) patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume no responsibility for any typographical, technical, or other inaccuracies in this document. In order to protect RIM proprietary and confidential information and/or trade secrets, this document may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information, hardware or software, products or services and/or third-party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third-Party Information or the third party in any way. Installation and use of Third-Party Information with RIM's products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM's products and services is provided "as is." RIM makes no representation, warranty, or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.