

# Bluetooth Security

## White Paper

BlackBerry Device Bluetooth Interface  
Security



**Fraunhofer** Institut  
Sichere Informations-  
Technologie

## Executive summary

Research In Motion (RIM) engaged Fraunhofer SIT to perform a security assessment of the BlackBerry® Enterprise Solution for mobile email-push-services. The aim of the assessment is to evaluate the security of the BlackBerry Enterprise Solution components, interfaces, software platforms, environments and communication protocols.

The assessment of the BlackBerry Enterprise Solution by Fraunhofer SIT was split into three consecutive projects. The first project focused on the BlackBerry Infrastructure and the communication between the BlackBerry Enterprise Server and BlackBerry devices, as well as general security mechanisms. The second project examined the BlackBerry Enterprise Server, the communication between its internal components, and the interaction with the corporate environment. Finally, the third project targeted the BlackBerry device and evaluated the accessibility of information on the BlackBerry device regarding standard applications and device interfaces within the BlackBerry Enterprise Solution and to external entities.

This white paper provides an overview of the results regarding the Bluetooth interface security characteristics evaluated in the third project. It has to be considered that the evaluation of the BlackBerry device Bluetooth interface security has been one work item during the overall assessment. The evaluation depth of the Bluetooth interface security evaluation therefore has to be considered in the context of the overall project and not as a single investigation of the Bluetooth interface itself.

The Bluetooth interface security evaluation found that the evaluated Bluetooth communication stack is very robust and constructed according to a state of the art security design. It is resistant to commonly known Bluetooth attacks and remains stable when handling malformed packets. Furthermore the communication stack provides proper Bluetooth access control implementation and configuration. This refers to both access to data stored on the BlackBerry device and access control attributes of Bluetooth services provided by the device.

# Introduction

Bluetooth is a very helpful and easy to use technology however security issues have to be taken into serious consideration in case of managing sensitive data. Lately some Bluetooth stacks have been vulnerable to specific attacks, but several risks which can arise using Bluetooth are inherent to any wireless technology.

The emerging complexity of Bluetooth communication stacks, such as the support of new profiles and vendor configuration, are significant reasons for a security analysis of the Bluetooth interface. The newly added OBEX support to BlackBerry devices, which enables file transfer, is an example of this emerging complexity. Furthermore good default vendor configuration and user enabled configurability of Bluetooth security characteristics are standard, and very effective, security measures.

The default configuration and communication stack stability were the starting points for the BlackBerry Bluetooth interface evaluation conducted by Fraunhofer SIT. The evaluation was performed as a work item in the overall BlackBerry Enterprise Solution security assessment.

The assessment of the BlackBerry Enterprise Solution was split into three consecutive projects. The first project focused on the BlackBerry Infrastructure and the communication between the BlackBerry Enterprise Server and BlackBerry devices, as well as general security mechanisms. The second project examined the BlackBerry Enterprise Server, the communication between its internal components, and the interaction with the corporate environment. Finally, the third project targeted the BlackBerry device and evaluated the accessibility of information on the BlackBerry device regarding standard applications and device interfaces within the BlackBerry Enterprise Solution and to external entities.

## 1 Methodology

Fraunhofer SIT described security requirements and assets that must be protected by the BlackBerry Enterprise Solution. A threat analysis determined the conditions under which vulnerabilities may arise and identified the corresponding parts of the evaluation target that could be exposed to those vulnerabilities. Based on these considerations and preliminary tests, Fraunhofer SIT developed realistic scenarios for potential attacks in typical deployment situations and performed targeted tests.

## 1.1 Test system

Fraunhofer SIT installed and configured a test system in their Testlab IT-Security in Darmstadt, Germany, using the latest software versions provided by RIM.

The test environment of the overall security assessment consisted of three computers, each of them with Microsoft® Windows® Server 2003 SE Service Pack 1 pre-installed and Microsoft Terminal Services enabled using the Remote Administration mode. Two computers were used to run the Microsoft Exchange server software and the BlackBerry Enterprise Server together with the Microsoft Database Engine (MSDE). The third computer was used as a client workstation and ran the BlackBerry Desktop Software and Microsoft Outlook®.

The tests in the third project used the following component versions:

- BlackBerry Enterprise Server v4.1.2.20
- Microsoft Exchange Server 2003 SP1, version 6.5.6944.0
- Microsoft (SQL Server 2003) Desktop Engine (MSDE)
- BlackBerry Device Manager version v4.1.2.25
- BlackBerry Desktop Software version 4.2

The BlackBerry devices which Bluetooth stack was evaluated reported the following component versions:

- Type: BlackBerry 8700 Wireless Handheld™ (EDGE)
- Firmware: v4.2.1.37 (Platform 2.3.0.33)
- Cryptographic Kernel: v3.8.4.34

The default IT policy settings related to the Bluetooth Security Group were used during the evaluation, as shown in Table 1-1.

IT policy rule	Setting
Allow Outgoing Calls	Always
Disable Address Book Transfer	False
Disable Bluetooth	False
Disable Desktop Connectivity	True
Disable Dial-Up Networking	False
Disable Discoverable Mode	False
Disable File Transfer	False
Disable Handsfree Profile	False
Disable Headset Profile	False
Disable Pairing	False
Disable Serial Port Profile	False
Disable Wireless Bypass	True
Require Encryption	False
Require LED Connection Indicator	False
Require Password for Discoverable Mode	False
Require Password for Enabling Bluetooth Support	False

Table 1-1 Bluetooth Security Group IT policy settings applied to test system

## 1.2 Test pattern

According to the security methodology at Fraunhofer SIT's Testlab IT-Security the analysis is based on defined security requirements and a comprehensive threat analysis, which determines the conditions under which vulnerabilities may arise and which components of the software or overall system may be exposed to them. The methodology for the identification of threats, protection goals and security characteristics is comparable with the accepted Common Criteria schemata.

The overall analysis of the BlackBerry Enterprise Solution was split into thematically focused work items. Each work item evaluated an interface, application, protocol, component or combination thereof. The evaluation depth of each work item was dependent on identified threats and the impact of a potential security issue. Therefore the evaluation depth of the Bluetooth interface security has to be considered in the context of the overall project and in relation to the evaluation depth of other work items and not as a single isolated assessment of the Bluetooth interface itself.

The general aims of the Bluetooth interface evaluation were to analyze the overall Bluetooth security characteristics and to perform vulnerability testing on the supported Bluetooth profiles and the Bluetooth communication stack. The evaluation regarding the overall Bluetooth security characteristics focused on basic Bluetooth stack configuration parameters, Bluetooth authentication and authorization, and Bluetooth service configuration. These have been investigated and compared to the documentation provided by Research In Motion.

Concerning vulnerability testing, Fraunhofer SIT has attempted to identify implementation errors in the Bluetooth communication stack or cause security issues by provoking the Bluetooth communication interface to depart from its proper or intended behavior.

Vulnerability tests in three categories were performed on the Bluetooth interface. The first category was stability, which included several link layer tests as well as Bluetooth profile checks. The link layer tests comprised, as an example, sending malformed and fuzzed packets on the Bluetooth transmission layer L2CAP and using L2CAP packets with a fuzzed L2CAP header, body or both. The second category was unprivileged access to information stored on the BlackBerry device using Bluetooth. These tests mainly targeted the OBEX profile, triggering attacker-defined unauthorized Bluetooth OBEX communication. The third category was most common and commonly known Bluetooth attacks, which included BlueStab, BlueSnarf, BlueSnarf++, and BlueSmack attacks.

## 2 Results

The Bluetooth interface of the BlackBerry device effectively limits the access to information resources to authorized Bluetooth devices.

Basic communication actions are protected by “Authentication required” attribute which results in authentication or pairing requests in case of external initiated communication. This restriction prevents attackers from obtaining information about the device Bluetooth configuration and services in an unauthorized state.

The default access control attributes of the provided services are well thought out. Based on the default access control attributes a user is able to configure discrete access control rights for other Bluetooth devices and their service usage at the BlackBerry device. This characteristic provides a good basis for protected services regarding both unpaired and paired Bluetooth devices.

Furthermore any unused Bluetooth channels were found closed and any active channels are presented to an authorized entity via a Service Discovery Protocol lookup. The evaluators did not find any unmapped or unprotected Bluetooth channels.

The tests for unprivileged access to stored information on the BlackBerry device showed that data confidentiality is preserved. In all circumstances, data was not accessible by unauthorized entities. Data in this context refers to stored user data as well as meta-data (e.g., file names or file sizes).

None of the stability tests had a negative effect on the Bluetooth stack availability, i.e. they did not result in a Bluetooth stack crash or a Denial of Service scenario. This demonstrates good stability of the Bluetooth communication stack.

Additionally the Bluetooth communication stack is not prone to any commonly known Bluetooth attacks.

### 3 Conclusion

Fraunhofer SIT testing of the specified BlackBerry Bluetooth stack showed good security measures and a robust and secure implementation based on a state of the art security design. The implementation provides proper Bluetooth access control measures with regard to implementation and configuration, and also provides stability during packet handling.

Nevertheless standard Bluetooth security measures have to be taken to protect Bluetooth communication, as with all Bluetooth enabled devices.

Visit [www.blackberry.com/security/](http://www.blackberry.com/security/) for more information on the security of Bluetooth-enabled BlackBerry devices and the BlackBerry Enterprise Solution.

# Appendix

## About Research In Motion Limited

Research In Motion Limited is a leading designer, manufacturer and marketer of innovative wireless solutions for the worldwide mobile communications market. Through the development of integrated hardware, software and services that support multiple wireless network standards, RIM provides platforms and solutions for seamless access to time-sensitive information including email, phone, SMS messaging, Internet and intranet-based applications. RIM technology also enables a broad array of third party developers and manufacturers to enhance their products and services with wireless connectivity to data. RIM's portfolio of award-winning products, services and embedded technologies are used by thousands of organizations around the world and include the BlackBerry wireless platform, the RIM Wireless Handhelds™ product line, software development tools, radio-modems and software/hardware licensing agreements. Founded in 1984 and based in Waterloo, Ontario, RIM operates offices in North America, Europe and Asia Pacific. For more information, visit [www.rim.com](http://www.rim.com) or [www.blackberry.com](http://www.blackberry.com).

## About Fraunhofer Institute for Secure Information Technology (SIT)

The Fraunhofer-Gesellschaft is the leading organization for applied research in Germany undertaking research of direct utility to private and public enterprise and of wide benefit to society. Its services are solicited by customers and contractual partners in industry, the service sector and public administration. The Fraunhofer Information- and Communication Technology Group within the Fraunhofer-Gesellschaft represents the biggest, coordinated capacity in the field of applied research in informatics within Europe.

As a specialist in IT Security Fraunhofer SIT offers highly reliable and individual services in assuring the protection of enterprise critical infrastructures and networks. A highly qualified staff of more than one hundred employees is active in all relevant fields of IT security and forms a broad base of competence for cross-technology development at the highest level of quality. SIT provides services for all branches of industry. Numerous successful projects at an international level visibly demonstrate our trustworthiness and reliability as a cooperation partner. In response to increased industry demand Fraunhofer SIT put up its TestLab IT-Security as a Competence Center for security assessments. The TestLab examines system designs, prototypes and products at all development stages.

## **Disclaimer**

This document does not warrant or guarantee the accuracy, completeness, or adequacy of the information herein, and this report makes no representations or warranties regarding the security of the BlackBerry Enterprise Solution or forward-looking statements regarding the effects of future events. Users of this information do so at their own risk and are urged to consult independent professional support regarding the deployment of the technology assessed. Nothing herein shall be construed as a warranty, guarantee or binding commitment on the part of RIM, nor as any authorization to perform any activities respecting the BlackBerry Enterprise Solution that are not expressly permitted by the applicable RIM licenses and/or end user agreements.

The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties and trademarks of Research In Motion Limited.