

@stake consultants

Chris Eng, Matthew Levine and Ollie Whitehouse conducted the testing and analysis of the RIM BlackBerry Wireless Solution.

Mr. Eng is a Senior Security Consultant with @stake. His primary areas of expertise include web application penetration testing, product penetration testing and network vulnerability assessments. He is co-leading @stake's Attack Simulation Center of Excellence.

Mr. Levine is a Senior Security Consultant with a focus on strategic security solutions, particularly in application security. He specializes in the secure design, deployment and risk assessments of emerging application technologies. He is currently leading strategic security initiatives with @stake's premier clients.

Mr. Whitehouse is a Senior Security Consultant and the lead of the @stake Wireless Security Center of Excellence. His primary expertise lies in architecture assessments, policy development and mobile-based attack & penetration testing of 2.0, 2.5g and 3g networks. Mr. Whitehouse is a recognized speaker on wireless security and also lectures on the security aspects of 802.11 and 802.11b.

NOVEMBER 2003

BlackBerry® by Research In Motion: An @stake Security Assessment

BlackBerry is the leading wireless enterprise solution developed by RIM that keeps mobile professionals connected to people and information while on the go. It is a proven platform that provides users around the world with secure, wireless access to a full suite of business applications, including email, corporate data, phone, SMS, web and organizer features. BlackBerry incorporates the industry's best software, services and hardware, providing the most comprehensive end-to-end wireless solution for corporate environments. It has become the corporate standard for wireless connectivity by properly addressing the needs of both mobile professionals and IT departments. For more information, visit www.blackberry.com.

Executive Summary

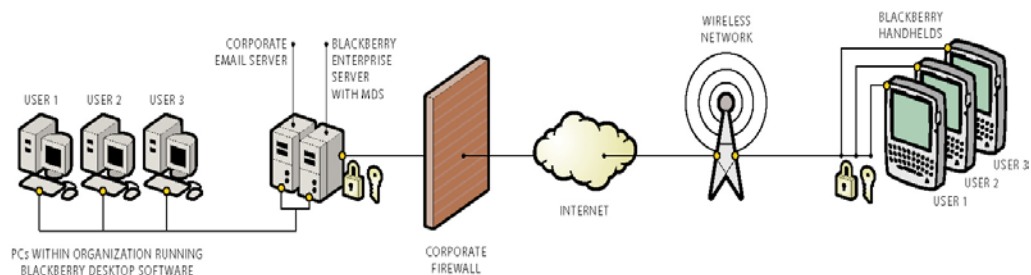
Research In Motion (RIM) engaged @stake, Inc. to perform a Product Penetration Assessment of the Java™ based BlackBerry Wireless Handhelds™ supporting components. Product Penetration Assessments model specific threat scenarios in a laboratory environment and provide insight into methods of attack against a product or application at a point-in-time. Using reverse-engineering and penetration techniques, @stake attempts to undermine the security features of the application from an informed position.

@stake's overall analysis indicates that the server to handheld communication security of the BlackBerry Wireless Handheld and BlackBerry Enterprise Server user input validation routines are robust. @stake was unable to forge messages from the handheld to the BlackBerry Enterprise Server environment.

Security Review Methodology

@stake installed and configured the BlackBerry Enterprise Server and supporting environment in the @stake Research & Development lab in Cambridge, Massachusetts. The test system consisted of BlackBerry users desktop computer and a dual-homed BlackBerry Enterprise Server, which faced both the Internet and an

internal test network consisting of the mail server (Microsoft® Exchange or Lotus® Domino™). A national 2.5G wireless network provider supplied the wireless connectivity. The diagram below denotes the simple test network with the portion behind the corporate firewall representing the @stake lab environment:



@stake's analysis included in-depth examination of the installed BlackBerry Enterprise Server components and the interaction and interdependencies between the BlackBerry Enterprise Server and the supporting corporate mail server. Decompilation of the BlackBerry Enterprise Server software was performed in order to identify instances of implementation errors, particularly buffer overflows or format string vulnerabilities. During the course of this assessment @stake did not discover any code related vulnerabilities such as buffer overflows or format string vulnerabilities.

In addition to analyzing binaries for improper buffer handling, @stake approached the BlackBerry Enterprise Server architecture from the user perspective and attempted to circumvent proper functionality of user interfaces. Through the use of overly long strings and other malicious inputs @stake attempted to force the BlackBerry Enterprise Server to mishandle user supplied data and cause an exception that might lead to a security issue. @stake was unsuccessful during the course of this engagement to impact any security related exceptions via manipulating user interfaces. Poorly formatted and overly long strings were handled gracefully with appropriate error reporting and logging.

The Java based BlackBerry Wireless Handheld was also analyzed during the security assessment. The goals of this analysis were to:

- Conduct attacks to gain physical access to the device circuitry
- Reverse engineer the various components
- Gain access to critical information from the microprocessor or external memory via physical access, serial port, or test interfaces.

Analysis Baseline

Introduction

The analysis baseline presents an overview of the technology used by RIM in the development of the BlackBerry security model. This section describes the data gathered during the engagement to provide context for the analysis.

@stake examined the following areas to assess the overall security of the BlackBerry wireless solution. Each of these areas is discussed in detail in the sections below:

- **BlackBerry Wireless Handheld**
- **BlackBerry Enterprise Server**
- **BlackBerry Desktop Software**
- **Security Model Matrix**

Baseline Overview

Overall the security of the BlackBerry wireless solution is sound. The BlackBerry wireless solution provides extensive end-user functionality with minimum risk in comparison to similar wireless solutions. Through a combination of common infrastructure security defensive measures and proper deployment of the BlackBerry wireless solution, any exposure can be mitigated. The nature of wireless services is to extend the perimeter of a network and expand the risk profile for such solutions. With the BlackBerry wireless solution, RIM has anticipated and mitigated these risks through the construction of the handheld itself, the means by which software runs on the handheld and the communications used to interact with the BlackBerry Enterprise Server. While the engagement team identified risks over the course of the engagement, these can be mitigated through relatively simple policies and strategies summarized at the end of this document.

BlackBerry Wireless Handheld

@stake examined the handheld to determine how it functioned and what security controls and elements existed to ensure that data delivered to and retrieved from the handheld was protected. Overall, the hardware design is well engineered. The engagement team conducted testing in the following two areas:

- **Physical Analysis.** Focuses on the physical housing, tamper detection/evidence mechanisms and identification of external interfaces. The handheld is designed to prevent access to cryptographic keys, system passwords, and other critical information so long as the casing remains intact.
- **Electrical Analysis.** Examines the physical circuit board, schematic, and external interface.

The hardware design is well engineered. This will limit the risk of attack from less skilled attackers, due to issues such as the location and tight spacing of components, which make probing attacks very difficult.

BlackBerry Enterprise Server

The server to handheld communication security of the BlackBerry Wireless Handheld and BlackBerry Enterprise Server user input validation routines are robust. @stake was unable to forge messages from the BlackBerry Wireless Handheld to the BlackBerry Enterprise Server environment. During the course of the evaluation, @stake installed BlackBerry Enterprise Server components and tested the interaction and interdependencies between BlackBerry Enterprise Server and the supporting corporate mail server.

The team also used a packet sniffer to capture traffic between the BlackBerry Enterprise Server and the BlackBerry Infrastructure, and then analyzed the captured data for observable patterns that might yield information about framing and contents. Since all traffic is encrypted except for the initial handshake, it would be extremely difficult to extract useful information from passively captured traffic without knowledge of the encryption key.

BlackBerry Desktop Software

@stake examined the BlackBerry Desktop Software to determine how the application responded to various application layer attacks. The focus of the assessment was on synchronization and backup, handheld-PC communication, and injected code attacks. Through protocol analysis and information provided by RIM, @stake prepared several specific low-level protocol attacks against the handheld and the synchronization mechanism used with the desktop software. @stake did not identify any clear vulnerabilities with the desktop software through the course of this assessment.

Security Model Matrix

The following matrix identifies the top security questions received by RIM from the client base and the @stake point of view, based on the security assessment, for each question.

BlackBerry Security Matrix	
TOPIC	@STAKE POINT OF VIEW
Comparison of the BlackBerry security model to a VPN for mobile solutions	<ul style="list-style-type: none"> BlackBerry provides similar security mechanisms to a traditional VPN solution. Traditional VPNs use IPSec to create an encrypted tunnel between the end user and the corporate network. BlackBerry uses end-to-end encryption between the handheld and the BlackBerry Enterprise server, preventing sensitive data from traveling across the Internet and wireless network unencrypted. Unique encryption keys are used for each handheld to prevent impersonation. Traditional VPNs generally require Access Control Lists (ACLs) to restrict the extent of individual users' access into the corporate network. BlackBerry's security model only allows handhelds to communicate with the BlackBerry Enterprise Server, removing the need for user-specific ACLs. <p>Conclusion: The BlackBerry security model provides the same level of security as a traditional VPN connection.</p>
Confidentiality, integrity and authentication of traffic in the BlackBerry security model	<ul style="list-style-type: none"> Authentication between the BlackBerry Enterprise Server and the BlackBerry Infrastructure is initiated with a 2-way challenge response mechanism. Data between the BlackBerry Wireless Handheld and the BlackBerry Enterprise Server is triple DES encrypted using a previously established shared secret key that can be changed periodically. <p>Conclusion: The BlackBerry security model provides the necessary confidentiality, integrity, and authentication.</p>
Message readability – can RIM view message content?	<ul style="list-style-type: none"> BlackBerry implements a triple DES layer of encryption over the wireless network between the BlackBerry Wireless Handheld and the BlackBerry Enterprise Server. This secures the contents of the messages while in transit between the handheld and the BlackBerry Enterprise Server. <p>Conclusion: RIM cannot view message content.</p>
Likelihood of a TCP session hijack attack	<ul style="list-style-type: none"> The level of effort required to hijack the connection between the BlackBerry Enterprise Server and wireless network is extremely high. <p>Conclusion: The likelihood of a TCP session hijack attack is extremely low.</p>
Impact of a TCP session, particularly: <ul style="list-style-type: none"> Injection of malicious email or calendar events Ability to mount a buffer overflow attack 	<ul style="list-style-type: none"> Even if an attacker were able to hijack the TCP session between BlackBerry Enterprise Server and the wireless network, they would require access to a BlackBerry Wireless Handheld's current encryption key. During the course of the assessment, @stake did not identify any buffer overflow vulnerabilities in the BlackBerry Enterprise Server. <p>Conclusion: Even if a TCP session was hijacked (extremely difficult) an attacker could not perform any malicious activity without having the current encryption key for a specific handheld.</p>

BlackBerry Security Matrix	
TOPIC	@STAKE POINT OF VIEW
BlackBerry Enterprise Server architecture: should the BlackBerry Enterprise Server be deployed in a demilitarized zone (DMZ)?	<ul style="list-style-type: none"> ■ Users are discouraged from deploying BlackBerry Enterprise Server in a DMZ, as the BlackBerry Enterprise Server does not need to accept incoming connections from the Internet. Installing the BlackBerry Enterprise Server in a DMZ would also necessitate the creation of firewall holes for communication with the corporate mail server. <p>Conclusion: The BlackBerry Enterprise Server should not be deployed in a demilitarized zone (DMZ) for security reasons.</p>
The ability for malicious handheld-side applications to access the corporate network over the wireline BlackBerry Desktop Manager connection	<ul style="list-style-type: none"> ■ The BlackBerry Desktop Manager connection only provides a mechanism for synchronizing data between the BlackBerry handheld and the PC; it does not allow a handheld to directly access the corporate network. ■ The BlackBerry handhelds proprietary Java Virtual Machine (JVM) requires any code that can run outside of the J2ME sandbox on the handheld to be cryptographically signed by RIM. <p>Conclusion: There is no way for malicious handheld-side applications to access the corporate network over the BlackBerry Desktop Manager connection.</p>
General security posture of the BlackBerry J2ME implementation and the overall JVM architecture	<ul style="list-style-type: none"> ■ The overall security posture of the BlackBerry J2ME and JVM architecture is sound. ■ The architecture and implementation meet existing industry best practice. <p>Conclusion: RIM's implementation of J2ME on the BlackBerry handheld is sound from a security and industry standards perspective.</p>

Secure Use of the End-to-End BlackBerry Wireless Solution

Based on the results of the assessment, @stake recommends security conscious BlackBerry customers follow these best practices for the installation and setup of the BlackBerry Enterprise Server:

- Do not store database credentials unencrypted in an unprotected registry key on the BlackBerry Enterprise Server. This practice makes it very easy for internal attackers to compromise the security of the database server. The likelihood of an external attack, however, is very low.
- Develop a hardened server environment for the BlackBerry Enterprise Server and test secure deployment of the BlackBerry Enterprise Server, BlackBerry Desktop Software and the corporate mail server (Microsoft Exchange or Lotus Domino)
 - Consult Microsoft documentation on hardening strategies for Windows 2000. The following URL can be used as a starting point for understanding Windows 2000 host hardening:
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56>
- Develop secure development guidelines and developer training for the BlackBerry Java Development Environment (JDE). This will help to ensure that developers observe secure coding practices when designing handheld-side applications.

About Research In Motion Limited

Research In Motion 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 Handheld™ 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. RIM is listed on the Nasdaq Stock Market (Nasdaq: RIMM) and the Toronto Stock Exchange (TSX: RIM). For more information, just visit www.rim.com or www.blackberry.com.

About @stake, Inc.

@stake provides corporations with digital security services that secure critical infrastructure and electronic relationships. @stake applies industry expertise and engages in pioneering research to design and build secure business solutions. As the first company to develop an empirical model measuring Return On Security Investment (ROSI), @stake works where security and business intersect. Headquartered in Cambridge, MA, @stake has offices in London, New York, Raleigh, San Francisco and Seattle. For more information, go to www.atstake.com

The information contained herein has been prepared by @stake in connection with the security assessment of the current state of the BlackBerry wireless solution. @stake has taken every effort in collecting, preparing and providing quality information and materials, but 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 the BlackBerry wireless 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 professionals regarding the deployment of the technology assessed. @stake is not an agent of RIM and is not authorized to bind RIM in any way. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of and trademarks or registered trademarks of Research In Motion Limited - used by permission. 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 wireless solution which are not expressly permitted by the applicable RIM licenses and/or end user agreements.