Global Information Assurance Certification Paper

Robin Killeen

Assessment of the Blackberry Enterprise Solution

Global Information Assurance Certification
GSEC Practical Assignment
Version 1.4b
Option 1

August 30, 2004

Table of Contents

Abstract

The BlackBerry wireless platform is broken down into its individual components and each of these are explain. The main focus is on the BlackBerry Enterprise Server (BES) and how it functions to maintain the security of the data being transferred.

Presently the BlackBerry solution is secure but the future of this security is uncertain as more applications and products make maintaining a secure system more complicated.

Introduction:

This paper discusses the BlackBerry Wireless Platform which includes the BlackBerry Enterprise Server solution, the wireless network and the BlackBerry unit itself.

The main focus will be the BlackBerry Enterprise Server, its current configuration, discuss the current challenges, point out some potential problems that BB is facing and make a few predictions on the future of Blackberry

RIM is the company that created and owns BlackBerry. BlackBerry is the name of the wireless platform, the name of the handheld itself, and the name of the software. To avoid confusion I will specify the server I am referring to.

The BlackBerry Wireless Platform

Research in Motion (RIM) is the company that, in 1994 created the BlackBerry handheld. Founded in 1984 and based in Waterloo, Ontario, RIM operates offices in North America, Europe, and Asia Pacific. As of February 2004 they have over 1 million subscribers to the Blackberry service making it one of the most used mobile e-mail devices in the world.

The components needed to use the service are referred to collectively as the BlackBerry wireless platform. This platform has three distinct parts.

The first is the messaging service which can be the BlackBerry Enterprise Server used in conjunction with a corporate mail server, the Blackberry web client or the BlackBerry Desktop Redirection Software. As previously stated, this paper will primarily focus on the BlackBerry Enterprise Server and it's communication to BlackBerry enabled handhelds. More information about the use and configuration of the web client and the Desktop Redirection/Desktop Manager software can be found on the website www.blackberry.com.

The second component is a wireless network service that supports both data and voice. This type of service can now be found in 30 countries worldwide using one or more of the following five wireless voice and data networks: CDMA2000 1X network, DataTAC network, GSM/GPRS network, Mike/Nextel on iDEN network, and Mobitex network.

The final component is the unit itself. RIM sells ten model series incorporating a total of nineteen models of the BlackBerry wireless handhelds[1]. Each model is well laid out on their website (www.blackberry.com). There are other units apart from RIM's BlackBerry that can be used; these will be outlined further on in this paper.

With all of these components secure access to wireless email is achieved. Only when using the BES is secure access available to corporate data, calendar, web servers, and phone. There are now eighty-two companies[2] listed as BlackBerry Partner Solutions providing mobile data service and third party applications which expands the uses of the BlackBerry to a stunning assortment. Some of these uses are remote telnet sessions, sales quotations, data gathering, CRM, helpdesk software, remote server control, spreadsheets, and games.

Blackberry Enterprise Server Architecture Overview

The BlackBerry Enterprise Server operates with the Microsoft Exchange messaging server and the Lotus Domino messaging server. The similarities between these to server are outlined below[3]:

> *The BlackBerry Enterprise Server centralizes e-mail redirection for BlackBerry Wireless Handheld users in an organization and performs the following functions for each user:*
>
> 1. *Monitor the user's Inbox for new mail.*
> 2. *Applies filters to new messages to determine if and how to redirect them to a user's BlackBerry handheld.*
> 3. *Compresses and encrypts new messages and delivers them to the Blackberry handheld over the Internet; and*
> 4. *Receives, decompresses and decrypts new messages composed on the BlackBerry handheld and places them in the user's Outbox for deliver by the corporate mail server.*[4]

There are two more similarities between the BES for Microsoft Exchange and the BES for Lotus Domino. The first is that both of the BlackBerry Enterprise Servers

[1] BlackBerry, URL1.
[2] BlackBerry, URL2
[3] BlackBerry-Kernel, 1
[4] BlackBerry-Kernel, 3

do not store a copy of the messages that they processes. By storing a message outside of the corporate messaging server you are decreasing the security of the solution by increasing the number of attack vectors available to the assailant. The second is neither of the BlackBerry Enterprise Servers change the way that the mail systems operate. By not changing the way that the mail server operates, RIM is lowering the impact of installing their product into an existing organization.

Although it is beyond the scope of this paper, it is equally important to note that there are differences in the way the BlackBerry Enterprise server for Microsoft Exchange internally secures, handles, and routes the messages when compared to the BES for Lotus's Domino server. There are several papers from BlackBerry that give an excellent detailed look at the inner workings of the BES server on both the Lotus Domino, and the Microsoft Exchange versions[5].

Note: At time of writing this paper, the final details of the BlackBerry Enterprise Server for Novell GroupWise have not been released. However, the server is expected to ship in late 2004.

To summarize the role of the BES server: In its most basic form the BES serves as a conduit for messages to and from the BlackBerry enabled handheld.

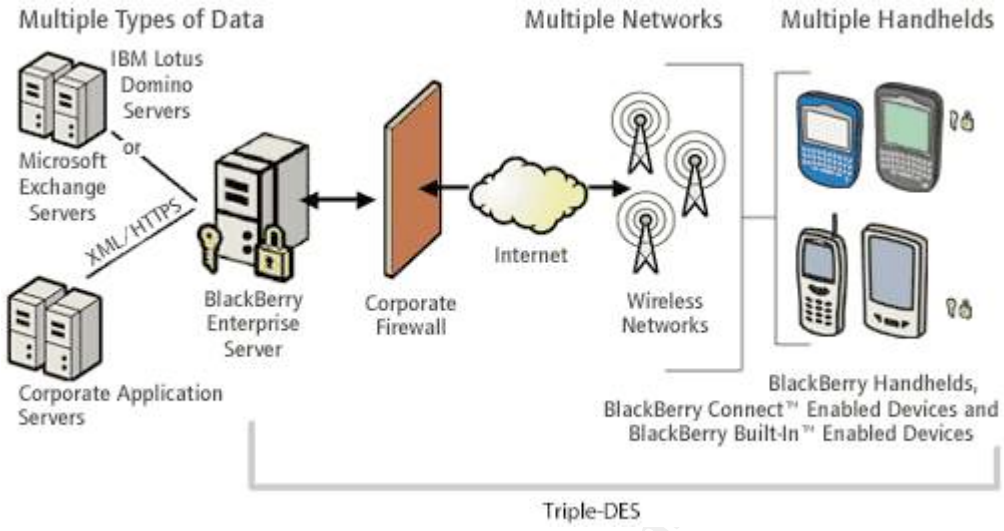
There are messaging solutions for other mail systems through RIM's Partner Solutions web page[6]. Just one of the many solutions is from a company called Consilient[7]. Their product Consilient2 Mobile Mail for BlackBerry extends the BB enterprise service to include the Oracle Collaboration Suite, Sun Java System Messaging Server, Sendmail Mailcenter, and Novell GroupWise. The Consilient2 Mobile Mail for BlackBerry solution sets up a server between the BES and the corporate mail server. So all communications to and from the HH and the BES are left altered. It basically acts as a third party mailroom. Monitoring and forwarding mail that is found in the user's mailbox in the corporate mail server to the BES and reverse.

Security Overview of the BlackBerry Wireless Platform

Figure 1 shows communication between the BES and the possible BB enabled handhelds.

[5] BlackBerry, URL3
[6] BlackBerry, URL2
[7] Consilient, URL4

Figure 1: BlackBerry Network Architecture[8]



As shown in figure 1, communication between the BES and the BlackBerry supported handhelds is encrypted with Triple-DES encryption. The Triple-DES encryption scheme used for the BlackBerry solution is specified in the FIPS publication 46-3[9]. This encryption is initiated with a 2-way challenge and response mechanism. The pre-shared key used in the encryption of the data can be changed periodically. With the framework of a solid security policy this will ensure the confidentiality, integrity, and authentication of the data travelling back and forth between the BES and the BlackBerry.

Blackberry server and handheld share a predetermined encryption key (also know as a symmetric key). The key is placed on the hand held through the BlackBerry cradle connected to a desktop computer running the BlackBerry Desktop Manager Software during the initial synchronization process or during a subsequent synchronization. At no time is the key sent across the BlackBerry wireless network. Once the pre-shared key has been established and transferred to the hand held it will only accept data sent from the BlackBerry Enterprise Server that uses its particular key. Like wise, the BES will only accept data from this particular hand held that match its respective key. Thus ensuring the authenticity of the data sent between the BES and the HH and vice versa.

The BES server and hand held cannot communicate wirelessly until the pre-shared key has been transferred to the BlackBerry hand held. Once the key has been transferred all wireless communication will be encrypted with Triple-DES encryption using the pre-shared key, thus ensuring the confidentiality of the data during transmission.

[8] Figure, 1
[9] FIPS-PUB-46-3

When the data arrives at the hand held it is decrypted and decompressed. Once this process is complete the information is checked with a Hashed Message Authentication Code (HMAC) to make sure that it has not changed during transport. If it passes the HMAC check it will be passed on to the user. If the data fails the HMAC check, it is rejected. Again, this happen in both directions. The HMAC check ensures integrity of the data during transport. The HMAC specification used in the BlackBerry solution is specified in FIPS publication 198.

The Blackberry wireless family of handhelds play an important role in the security of the solution. Because of the handhelds portability, they are prone to damage, theft and loss. The handheld can be password protected and this can be enforced by the BlackBerry Policy Manager[10]. The password is protected by running it through a SHA-1 hash and storing only the hashed value on the handheld. To unlock the handheld the user must enter a password that complies with the complexity requirements outlined in the BlackBerry Policy Manager. The SHA-1 hash algorithm used in the BlackBerry solution is specified in FIPS publication 180-2.

RIM states that BlackBerry has a secure encrypted end-to-end solution for wireless email[11]. End-to-end means from the BES to the HH as shown in Figure 1. Not from the messages origin until it reaches the BB. If the message originated from outside of an organization, the message has still traversed the Internet, usually in plain text, to arrive at the organizations server.

Security Assessment by @stake.

Using our understanding of the BlackBerry Wireless Platform, we can now examine security. A well known leader in the computer security business is @stake Inc.

@stake conducted a Security Assessment of the Blackberry Architecture. Their findings from the security assessment solidified the fact that RIM has built a first class secure wireless solution. Some of the findings are from the report are reviewed in this section.

During the security assessment, @stake systematically went through the different components that make up the BlackBerry Wireless Platform. Through the course of their assignment @stake could not identify any clear vulnerabilities with the desktop software, the hardware design of the BlackBerry handheld, or the Enterprise Server software. They also mentioned that the BB security model provides the necessary confidentiality, integrity, and authentication to ensure

[10] Policy Manager, 1

that the data passed between the handheld and the BES was secure and could be trusted.

Some of the more interesting questions that were posed to @stake centered around the possibility if RIM was able to view the contents of a message when it was on their network. @stakes findings stated that at no time on RIM's network was the message in its decrypted form and because of the nature of the key exchange RIM is does not have a copy of the symmetric key to be able to decrypting the message.

@stake also examined the risk of hijacking the Transmission Control Protocol (TCP) session between the BES and the BlackBerry and found that "The likelihood of a TCP session hijack attack is extremely low"[12]

If an assailant managed to actually hijack a TCP session the Triple-DES encryption and HMAC hashing of the contents of the TCP session would not allow the attacker to read or change the data unless he/she were also able to acquire the current encryption key used to communicate with that particular handheld.

The following is a quote taken from the @stake Security Assessment of the BlackBerry. This is a very good summary of the security of the BlackBerry wireless platform.

> "*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."* [13]

Overall, @stake's conclusions were positive, however the recommended a few potential security improvements. The first recommendation was to secure the credentials for the databases on the BES. It was found that an internal attacker can very easily comprise the security of the server if the credentials are stored in an unprotected registry key. The second recommendation was to develop a hardened server environment for your BES server, corporate mail server, and desktop software.

[12] Eng, Levine, Whitehouse, 5
[13] Eng, Levine, Whitehouse, 3

There are many recommended hardening tools and websites available to assist in the lock down of your server product. Microsoft Windows 2000/XP ships with a number of pre-configured security templates that are accessible through the Microsoft Management Console.[14] There are many additional, freely available templates and whitepapers to download from the U.S. National Security Agency (www.nsa.gov), the Center for Internet Security (www.cisecurity.org), Microsoft (www.micrsoft.com), and the U.S. National Institute for Standards and Technology (www.nist.gov) to name a few. .

In addition to the hardening of the server environment, @stake also recommends testing the secure rollout of the BlackBerry applications in a test environment before installing them in the working environment. Furthermore, if a company is developing applications that will be used on the BlackBerry, make sure to train the developers and create guidelines for secure development of the applications.

Securing a Changing Environment

The Blackberry Wireless Platform is changing. RIM is opening up its BlackBerry solution to other vendors. The perceived company focus was to push the BlackBerry hand held as a device that extends the corporate office to where ever the user may be. But as RIM COO Larry Conlee stated in 2002 while being interviewed by Brighthand[15] that “RIM is not a device company but an "enabler" of other companies' wireless strategies.” Mr. Conlee pointed out that wireless email was his companies core business, not devices, and that his companies popular BlackBerry handheld is "simply a viewing agent.”

Following up on the 2002 comment, RIM has opened the doors for other vendors to use the famous BlackBerry Wireless Platform on their own units. RIM has created two licensing models for this end. The BlackBerry Built-in and the BlackBerry Connect licensing agreements. The BB Built-in[16] licensing agreement allows vendors to use the full BB software suite on their devices. The BB Connect Licensing agreement has all of the same functionality but is missing the BlackBerry Applications suite (BlackBerry Email, BlackBerry Calendar, and BlackBerry Browser). The missing applications will be replaced with the vendor’s respective, and competing products.

There are several vendors that are now signed on to either the BB connect or BB built-in licensing model. These vendors include Nokia, Motorola, Siemens[17]

[14] Sans Institute, 136
[15] Brighthand, URL6
[16] BlackBerry-Built-in, URL7
[17] Yahoo News, URL8

Symbian OS, Palm OS, Pocket PC, and HTC[18] with more signing up almost monthly.

The Blackberry Wireless Platform as it is known today is changing. The addition of the licensing agreements will drastically increase in the number of handhelds using the BlackBerry solution to transport email and services across the airwaves of the world. This increase could cause problems in the following ways:

1. Control. Currently RIM controls the quality of product that works with their platform. The new hand held units that are going to be used are not manufactured by RIM nor are they controlled by RIM. This will impact the security of the network.
2. Viruses. There are no viruses that operate on the Blackberry. At least two of the vendors that have signed up have had viruses found on their systems.[19]
3. Vendors. RIM lists 82 companies that write software for the BlackBerry. There are literally thousands of companies and individuals that write software for the Palm OS alone. RIM has now allowed a massive market of developers and buggy code to come in contact with their product. Now, RIM has taken steps to minimize the risk of third party apps taking control of the BlackBerry enabled hand helds. Programs that access the sensitive Application Programmers Interfaces (API) that control the data on the Blackberry must be digitally signed by RIM. However, RIM only signs apps for tracking purposes; they do not check the code in any way.

Looking forward with the BlackBerry Enterprise Server

Version 4.0 of the BlackBerry Enterprise Sever will make a few changes to the general operation of the server and handheld. There will be support for AES as specified in FIPS publication 197 for communication between the Enterprise Server and the handheld. The handheld also receives a security improvement with the ability to encrypt all of the user data stored on the unit with “state-of-the-art” encryption technology. The IT departments will also be albe to have “cradle-less” synchronization for the handheld. This will reduce the number of installs of Desktop Manager and synchronization cradles on users desktop computers.

Conclusion

One saying about security is that the larger and more complex the system is, the harder it will be to manage and secure. In @stake’s security assessment of the

[18] Internetnews, URL1
[19] BBC-HHVirus, URL1

BlackBerry they stated that the design of the BB hand held added to the security of the solution. Now that RIM has opened up the number of devices that can run the BB software, will this not weaken the security of the solution? Only time will tell.

References:

BlackBerry, URL1, BlackBerry Wireless Handhelds, 2004
http://www.blackberry.com/products/handhelds/index.shtml (2004.08.22)

BlackBerry, URL2, BlackBerry Partner Solutions, 2004
http://www.blackberry.com/products/handhelds/index.shtml (2004.08.22)

BlackBerry-Kernel, BlackBerry Enterprise Server Cryptographic Kernel, Version 1.0.0.2, November 2003.
http://csrc.nist.gov/cryptval/140-1/140sp/140sp445.pdf (2004.08.30)

BlackBerry, URL3, BlackBerry Products, 2004
http://www.blackberry.com/products/index.shtml (2004.08.30)

Policy Manager, BlackBerry IT Policy Manager, July 29, 2002
http://whitepapers.zdnet.co.uk/0,39025945,60047995p-39000428q,00.htm
(2004.08.30)

Consilient, URL5, Wireless Solution for Novell Groupwise and BlackBerry, Unknown date
http://www.consilient.com/products/novell-solution-bb.html (2004.08.20)

Eng, Levine, Whitehouse, BlackBerry by Research In Motion: A Security Assessment. November 2003.
URL:http://www.blackberry.com/knowledgecenterpublic/livelink.exe/An_@stake_Security_Assessment.pdf?func=doc.Fetch&nodeId=644990&docTitle=An+%40stake+Security+Assessment (2004.08.28)

Cole, Fossen, Northcutt, Pomeranz, Windows Security, Sans Institute, January 2004. pg 131-138

Brighthand, URL6, BlackBerry: Device or Technology?, April 8, 2002
http://www.brighthand.com/article/Blackberry_Device_Or_Technology
(2004.08.30)

BlackBerry Built-in, URL 7, BlackBerry Licensing Programs, 2004
http://blackberry.com/licensing/index.shtml?CPID-ILC=nahrcbi (2004.08.30)

Nobel, Carmen, URL8, RIM Widens BlackBerry Server Support, August 9 2004 http://story.news.yahoo.com/news?tmpl=story2&u=/zd/20040809/tc_zd/132871 (2004-08-30)

Internetnews, RIM 'Connects' with Microsoft, Symbian, March 17, 2003

http://www.internetnews.com/ent-news/article.php/2110381 (2004-08-30)

BBC News, First Pocket PC virus discovered, July 19, 2003 http://news.bbc.co.uk/2/hi/technology/3906823.stm (2004.08.15)

BlackBerry, BlackBerry Security Overview, Unknown date. http://www.blackberry.com/products/software/server/exchange/security.shtml#wireless (2004.08.16)

Figure 1: Figure is the result of compilation of several different images found on the **www.blackberry.com** website. The image is an original piece of work which uses icons and fonts from on the BlackBerry website.

Last Updated: May 22nd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event