BlackBerry PlayBook Security: Part two
BlackBerry Bridge

Gavin Jones
Managing Consultant
gavin.jones@ngssecure.com

An NGS Secure Research Publication

15th November 2011

http://www.ngssecure.com

Table of Contents

1. Introduction

This is the second in a series of white papers regarding the security of the BlackBerry PlayBook, the first tablet device released by Research in Motion (RIM). The primary goal of the research that led to this paper was to gain an understanding of the functionality and security applied to the BlackBerry Bridge. Although the main body of work is primarily aimed at a reasonably technical audience, the key findings and conclusions drawn from these are presented at the end of the document.

2. Background

2.1. Overview

The BlackBerry Bridge is an application that allows users to connect the PlayBook tablet to a BlackBerry Enterprise Server via a smartphone and enables the use of applications on the tablet through the phone such as email, contacts and calendar, all of which are currently not included natively on the device. As a minimum requirement, version 5.0 of the smartphone software is required to use the BlackBerry Bridge functionality [3].

The application can also be used for tethering the tablet to a mobile network through the smartphone's mobile connection since the first version of the tablet devices are Wi-Fi only devices.

The tablet and smartphone perform two pairing processes in order to open an encrypted and authenticated connection between each of them:

- A Bluetooth pairing process to open a Bluetooth connection
- A BlackBerry Bridge pairing process to provide an additional level of security to the connection.

During the Bluetooth pairing process the tablet and smartphone share a Bluetooth key that is used to encrypt and decrypt data that is sent between the tablet and smartphone. In the BlackBerry Bridge pairing process the tablet and smartphone share a BlackBerry Bridge pairing key which is used to both authenticate the connection and encrypt and decrypt data that is sent between the tablet and smartphone. If the smartphone was activated on a BlackBerry Enterprise Server the tablet and smartphone also share the BlackBerry Bridge work key. Full technical details of the encryption algorithms used during this process are described in RIM's BlackBerry PlayBook Security Technical Overview[4].

The tablet has been designed to reconnect automatically to a smartphone that it was previously connected to if the tablet did not delete either the Bluetooth key or BlackBerry Bridge pairing key.

2.2. Previous Work

This paper follows on from the previous NGS Secure whitepaper "BlackBerry PlayBook Security: Part one" [1] by Daniel Martin Gomez and Andy Davis.

2.3. Caveats

It should be noted that the BlackBerry Bridge functionality is not currently supported by the PlayBook simulator (where "root" level access can be achieved by patching the VMDK file [2]). Therefore, the research performed was restricted due to the fact that the PlayBook tablet device was only accessible over SSH using the "devuser" low privileged account with limited access to the tablet's file system.

3. Research

3.1. BlackBerry Bridge Connection

After a user connects the tablet to a smartphone (See section 3.1.1 of [1]) requiring an unlock password, the tablet automatically requires that the user provides the password before the tablet accesses any smartphone data.

Smartphone data can include email messages, calendar entries, tasks, memos, BlackBerry Messenger messages, intranet content, files or attachments that the user views on the tablet.

The tablet requires that the user provide the smartphone password regardless of whether the applications are running in work mode or personal mode. Applications on the tablet can run in work mode, personal mode, or both, depending on the metadata that is associated with them. By default, all applications on the tablet run in personal mode. After the tablet user connects the tablet to a smartphone that is activated on a BlackBerry Enterprise Server (BES) an application can then run in "work" mode and the tablet permits the user to view and interact with "work" data.

"Work" data consists of all email messages, calendar entries, and attachments that a BES and a smartphone send between each other and any additional data that is associated with work applications. A media card must be present in the paired smartphone to permit the user to interact with the "work" data e.g. to open attachments on the tablet or save updates to files.

To help protect "work" data the tablet automatically creates a "work" file system in the BlackBerry Tablet OS that isolates the "work" data and "work" applications from "personal" data and "personal" applications.

The tablet caches "work" data locally using the "work" file system and is designed to prevent "work" data from persisting in flash memory in its cleartext form by encrypting the "work" file system using XTS-AES-256 encryption. The tablet queues any "work" file updates for sending to the media card that is inserted in the smartphone and sends the updates to the smartphone frequently.

The tablet is designed to prevent the user from accessing the “work” file system directly on the tablet by requiring them to use a bridge application to access the work file system as shown below:

Figure 1: Files Application

When the tablet runs the “Bridge Files” application the user can access the files that are stored on the media card that is inserted in the smartphone. The tablet opens these files using “work” applications and classifies the files as “work” data.

When the user connects the tablet to the smartphone using the BlackBerry Bridge the tablet displays the BlackBerry Bridge panel. The user can then use this panel to access “work“ applications as shown below:

Figure 2: BlackBerry Bridge Panel

The image below shows how the work file system is implemented on the device [4]:

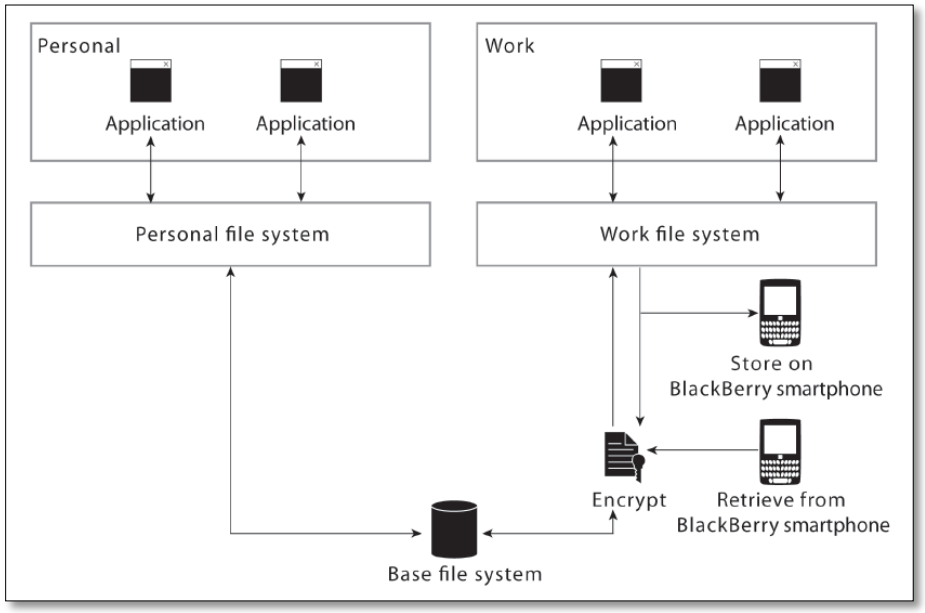

Figure 3: File System Configuration

The tablet does not allow the user to move data from the "work" file system to the "personal" file system and the user cannot cut, copy, or paste data from a "work" file in to a "personal" file. Similarly, the tablet does not allow a user to move data from the "personal" file system to the "work" file system and the user cannot cut, copy, or paste "personal" data into a "work" file. The user can however attach a personal file to a work email message or work calendar entry.

All the password features that apply to the smartphone are also extended to the tablet e.g. the tablet uses the same security timeout as the smartphone that it is connected to.

3.2. PlayBook Screenshot Functionality

The tablet allows a user to take a screenshot of the current screen by holding the “Volume Up” key and “Volume Down” key at the same time. The user can only take screenshots when the tablet is running in “personal” mode. The tablet saves screen shots in the Camera application and displays them in the Photo viewer application.

The tablet treats screen shots as “personal” files so it prevents the user from taking screen shots of “work” data when a “work” application is open and unlocked.

3.3. Bridge Browser Functionality

If the “Allow Browser” IT policy rule on a BlackBerry Enterprise Server is set to “Yes” and the user configures the BlackBerry MDS Connection Service to connect a smartphone to the Internet and intranet, a tablet connected to the smartphone can use the Bridge Browser to browse the Internet or intranet in “work” mode.

The BlackBerry MDS Connection Service connects wireless applications on BlackBerry devices to the applications on an organization’s application servers or web servers. After a wireless application is installed on BlackBerry devices, the application can receive data from “push” applications accessible on web servers. The application can also receive data by sending “pull” requests from BlackBerry devices. The BlackBerry MDS Connection Service processes “push” and “pull” requests and delivers data and updates to BlackBerry applications.

The Bridge Browser does not use the Wi-Fi connection to connect to the Internet or intranet. Instead, it uses the smartphone's connection to the BlackBerry MDS Connection Service.

By default, when a user clicks on a link in a “work” application (for example, a link in “work” email messages, calendar entries, the contact list, tasks, memos, or BlackBerry Messenger messages), the tablet opens the link in “personal” mode using the browser. However, the tablet opens the link in “work” mode using the Bridge Browser if any of the following conditions exist:

- The link is to an address that is not routable on the public Internet, such as a private IP address as specified in RFC 1918 or an address that does not contain periods.
- The link is to a domain that is included in the MDS Browser Domains IT policy rule that applies to the smartphone that the tablet is connected to.
- The Wi-Fi Internet Access Path IT policy rule that applies to the smartphone that the tablet is connected to is set to "Access through BlackBerry MDS Connection Service".
- No Wi-Fi connection is available.

To open a link using the Bridge Browser, the tablet must be able to access the BlackBerry MDS Connection Service.

Although, as stated above, the PlayBook will attempt to open a link to an RFC 1918 address using the Bridge Browser it was discovered that if a known hostname is hijacked and in turn pointed to an RFC 1918 address the (non-Bridge) Browser is used in its place.

The following hostname was configured with a static entry within the DNS server.

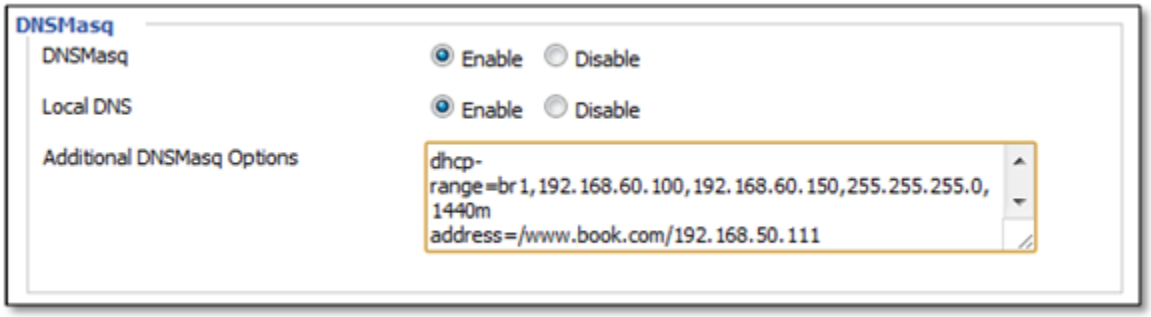

Figure 4: Static DNS Entry

This was confirmed with a simple nslookup command showing that the configured IP address was being returned by the DNS server:

```
C:\>nslookup www.book.com
Server:  drop-off
Address:  192.168.50.1

Name:    www.book.com
Address:  192.168.50.111
```

Figure 5: DNS Response

A listener was then started on the destination host and as can be seen the PlayBook connected using the browser when a link was sent to the target and clicked.

```
$ nc -lp 80 -vv
listening on [any] 80 ...
192.168.50.125: inverse host lookup failed:  : Operation not permitted
connect to [192.168.50.111] from (UNKNOWN) [192.168.50.125] 65191
GET / HTTP/1.1
Host: www.book.com
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (PlayBook; U; RIM Tablet OS 1.0.0; en-US) AppleWebKit/534.11+ (KHTML, like Gecko) Version/7.1.0.7 Safari/5
34.11+
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en_GB, en;q=0.8

Hello Playbook!
 sent 20, rcvd 344
```

Figure 6: Simple TCP Listener

The listener response was a simple text string (“Hello Playbook!”) which instead of being rendered by the browser as text as expected, a prompt was displayed requesting a filename to save the response.

As shown below the file was saved as “m.txt” and contained the following contents.

```
$ less ../1000/shared/downloads/m.txt
Hello Playbook!
../1000/shared/downloads/m.txt          (END)
```

Figure 7: Saved File Contents

The permissions of the saved file on the PlayBook are shown below.

```
$ ls -l ../1000/shared/downloads/m.txt
-rw-rw-rw-    1 100001000 10000           20 Sep 29 10:25 ../1000/shared/downloa
ds/m.txt
$
```

Figure 8: Saved File Permissions

It was also possible to respond to the initial request with an HTTP redirect to any arbitrary host in place of the text response.

From the end user perspective, apart from the caption displayed when switching between applications, there appears to be no way to differentiate between whether the Bridge Browser or (non-Bridge) Browser is being executed as both applications appear visually identical.

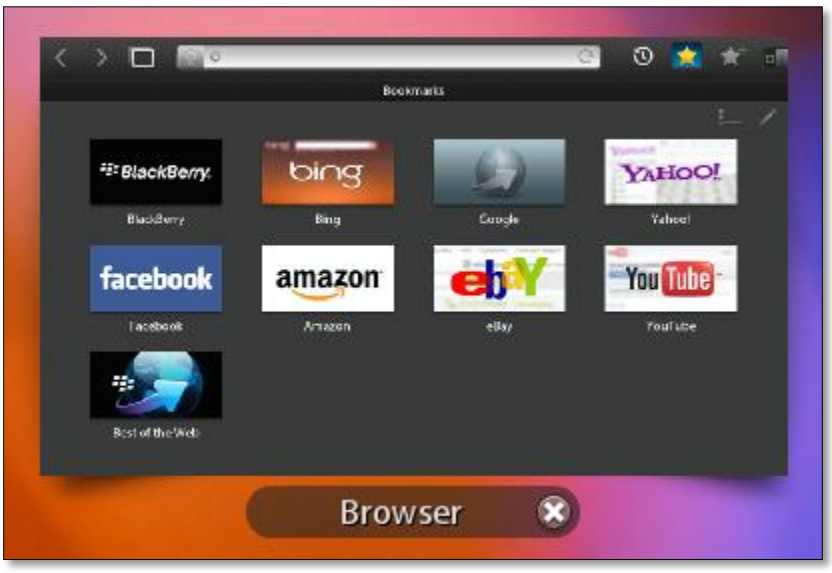

Figure 9: Browser Caption

Therefore it would be possible to coerce a user to follow a link whereby their expectation is that the link is for an internal "work" host and therefore it is inherently trusted by the user, although it is in fact accessed using the (non-Bridge) browser application and is a host controlled by the attacker.

4. Conclusion

Overall the security surrounding the BlackBerry Bridge functionality appears to have been well implemented, with the additional layer of protection offered by the BlackBerry Bridge pairing process on top of the Bluetooth pairing process. This provides a robust authenticated and encrypted connection between the tablet and the smartphone.

The separation of "work" and "personal" data has been well segregated by using storage on the BlackBerry smartphone and appropriate encryption for any data temporarily stored on the PlayBook. In addition, steps have been taken to prevent users from copy any pasting "work" and "personal" data between different applications when the BlackBerry Bridge is activated. However, further research into the separation of data between both the "work" and "personal" file systems would be possible with more privileged access to the QNX operating system running on the device.

The encryption used to protect data traversing the BlackBerry Bridge is considered to be adequate. The encryption algorithm currently used to generate the BlackBerry Bridge pairing key is currently considered robust enough to render brute force attacks computationally infeasible[4].The attacker only has a single attempt to guess the shared secret. If the guess is incorrect the tablet user must restart the BlackBerry Bridge pairing process which in turn creates a new shared secret, before the attacker can make another guess.

One recommendation that has been made to RIM was that a visual differentiator should be added to the "Bridge Browser" application to ensure the user is made aware of which browser is being launched when following a link. RIM has agreed with this recommendation and their development team is considering implementing the feature in a future software release.

5. References

1. http://www.ngssecure.com/Libraries/Document_Downloads/BlackBerry_PlayBook_Security_-_Part_one.sflb.ashx
2. http://cmw.me/?q=node/47
3. http://docs.blackberry.com/en/smartphone_users/deliverables/27018/About_Bridge_1266476_11.jsp
4. http://docs.blackberry.com/en/admin/deliverables/26992/BlackBerry_PlayBook-Security_Technical_Overview--1315426-0407044208-001-1.0-US.pdf