governmentattic.org
"Rummaging in the government's attic"

Description of document:	Department of State internal agency memos, correspondence, documents that review or discuss the merits and/or disadvantages of iPads and/or similar pad/tablet computer devices for employee use, 2011
Requested date:	18-August-2011
Released date:	10-July-2013
Posted date:	16-December-2013
Source of document:	Freedom of Information Act Request Office of Information Programs and Services A/GIS/IPS/RL Department of State, SA-2 Washington, DC 20522-8100 Fax: (202) 261-8579

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

United States Department of State

Washington, D.C. 20520

JUL 10 2013

RE: Freedom of Information Act Case No.F201107319

Reference is made to your August 18, 2011, FOIA request to the Department of State for a copy of internal agency memos or other correspondence or documents that review or discuss the merits and/or disadvantages of iPads and/or similar pad/tablet computer devices for employee use. The Office of Information Programs and Services (A/ISS/IPS) has referred three documents numbered 001 - 003 to the Bureau of Diplomatic Security for review and direct reply to you.

Portions of these documents have been withheld pursuant to 5 USC 552 (b)(7)(C), and (b)(7)(E).

Under the Department's regulations, you may appeal any denial of information to the Department's Appeals Review Panel. Appeals should be addressed to the Assistant Secretary for Public Affairs, c/o the Information Access Programs Branch, A/RPS/IPS/PP/IA, Department of State, SA-2, Washington, DC 20522-6001. A copy of the Department's Appeals Procedures is enclosed.

If you have questions regarding any aspect of this case, you should contact the Office of Information Programs and Services (A/ISS/IPS), Department of State, SA-2,Washington, DC 20522-8100. In any communication, please refer to the case number.

Sincerely,

William R. Terrini
Deputy Executive Director
Bureau of Diplomatic Security

Enclosure(s):
Documents
Appeal Procedures
Explanation of Exemptions

Subpart F – Appeal Procedures

§ 171.52 Appeal of denial of access to, declassification of, amendment of, accounting of disclosures of, or challenge to classification of records.

(a) *Right of administrative appeal.* Except for records that have been reviewed and withheld within the past two years or are the subject of litigation, any requester whose request for access to records, declassification of records, amendment of records, accounting of disclosures of records, or any authorized holder of classified information whose classification challenge has been denied, has a right to appeal the denial to the Department's Appeals Review Panel. This appeal right includes the right to appeal the determination by the Department that no records responsive to an access request exist in Department files. Privacy Act appeals may be made only by the individual to whom the records pertain.

(b) *Form of appeal.* There is no required form for an appeal. However, it is essential that the appeal contain a clear statement of the decision or determination by the Department being appealed. When possible, the appeal should include argumentation and documentation to support the appeal and to contest the bases for denial cited by the Department. The appeal should be sent to: Chairman, Appeals Review Panel, c/o Appeals Officer, A/RPS/IPS/PP/LC, U.S. Department of State, SA-2, Room 8100, Washington, DC 20522-8100.

(c) *Time limits.* The appeal should be received within 60 days of the date of receipt by the requester of the Department's denial. The time limit for response to an appeal begins to run on the day that the appeal is received. The time limit (excluding Saturdays, Sundays, and legal public holidays) for agency decision on an administrative appeal is 20 days under the FOIA (which may be extended for up to an additional 10 days in unusual circumstances) and 30 days under the Privacy Act (which the Panel may extend an additional 30 days for good cause shown). The Panel shall decide mandatory declassification review appeals as promptly as possible.

(d) *Notification to appellant.* The Chairman of the Appeals Review Panel shall notify the appellant in writing of the Panel's decision on the appeal. When the decision is to uphold the denial, the Chairman shall include in his notification the reasons therefore. The appellant shall be advised that the decision of the Panel represents the final decision of the Department and of the right to seek judicial review of the Panel's decision, when applicable. In mandatory declassification review appeals, the Panel shall advise the requester of the right to appeal the decision to the Interagency Security Classification Appeals Panel under § 3.5(d) of E.O. 12958.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552 (FOIA):

(b) (1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information, (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of aright to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a (PA):

(b) No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains,

(d)(5) information compiled in reasonable anticipation of a civil action proceeding.

General Exemptions:

(j)(1) applies to CIA records and information provided by foreign governments;

(j)(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, except records of arrest.

Specific Exemptions:

(k)(1) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal which did not result in loss of a right, benefit or privilege under Federal law, or which would identify a source under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;

(k)(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suit ability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, the disclosure of such material would reveal the identity of a source under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality;

(k)(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the testing or examination process; or

(k)(7) evaluation material used to determine potential for promotion in the armed services, the disclosure of such material would reveal the identity of a source under an express promise of confidentiality, or, prior to the effective date of this section, under an implied promise of confidentiality.

TRANSFERRED FOR DIRECT REPLY DS

*** Sensitive But Unclassified ***

The United States Department of State

Diplomatic Security—Countermeasures Program—Technology Evaluations Branch

DS/CMP/TEB

Apple® iPad® as an Electronic Reader Evaluation Report

(Draft 3)

April 7, 2011

Authors: Christopher H. Leonard
Evaluators: Christopher H. Leonard;

DS/CMP/TEB Branch Chief: Fred G. Everdale _____

DS/ST/CMP Division Director *(Acting)*: Karl Covington _____

*** Sensitive But Unclassified ***

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY:

The Technology Evaluations Branch (TEB) keeps abreast of emerging information technologies and their trends to prepare for potential use within the Department. The Office of the Executive Secretariat (S/ES) has expressed interest in using Apple iPads to support its mission. On October 6, 2010, the DS/ST/CMP Division Director received an electronic mail,

The purpose of this document, *"Apple iPad as an Electronic Reader Evaluation Report"* is to provide the results of the evaluation.

The evaluation was based on the device hardware (model MC497LL; OS version 3.2) and the available security controls provided by the iPhone Configuration Utility (version 3.0.1.256) which also supports the iPad. The hardware scope involved identifying active circuit components contained in the iPad. The evaluation included a comparison of the security controls available on the iPad versus the preexisting controls available on the BlackBerry.® And, most importantly, the evaluation focused on determining any vulnerabilities

Regarding the comparison to the BlackBerry, out of the 236 security controls considered in the evaluation, 54 of them are associated with features currently not supported by the iPad. Out of the remaining 182 (all of which are supported by the BlackBerry) only 21 are supported by the iPad to some degree. Therefore, it should be noted that the iPad supports only 11% of the security controls that are instrumental to the Department's countermeasures for mobile devices. Details of each control are provided in

Control Type	BlackBerry Support	iPad Support
Disable Location Based Services	Full	Full
Disable Applications Center	Full	Full
Disable Screen Shot Capture	Full	Full
Disable Wi-Fi	Full	Limited
Disable Bluetooth	Full	Limited
Password	Full	Limited
Disable Application Downloading	Full	Limited
PC/Desktop	Full	Limited
Disable Third-Party Browser	Full	[redacted]
Disallow External Networks	Full	
Disable IP Modem	Full	
Disable Serial Port/USB from Third-Party Apps	Full	
Force Content Protection & Level	Full	
Force Memory Cleaning	Full	
Restrict Use Based on Certificate Status	Full	
Disable Instant Messaging and other Services	Full	
Disable SMS/MMS	Full	
Software Configuration & Application White List	Full	

The following is a list of the vulnerabilities found with the iPad

1. **There is no forced configuration for disabling Wi-Fi and Bluetooth**—A user-provided manual configuration is the only configuration allowed for disabling Wi-Fi and Bluetooth. Users are capable of adjusting the setting (allowed/disallowed) at his/her discretion.

   If either Wi-Fi or Bluetooth is enabled, there exists a risk for the loss of data or audio in or around the device.

2. **Third-party applications are not prohibited**—Disabling the installation of applications via the configuration profile simply removes the "Apps Store" icon from the iPad; thereby disallowing the installation of applications *via the icon method.* Applications may still be installed indirectly using a PC connection to the Apple configuration tool or iTunes; and any pre-existing third-party applications (prior to the installation of the configuration profile) are still available to the user. The iPad does not provide a white-listing feature for applications; as a result, users are either allowed to execute all applications or they are not allowed to execute any applications.

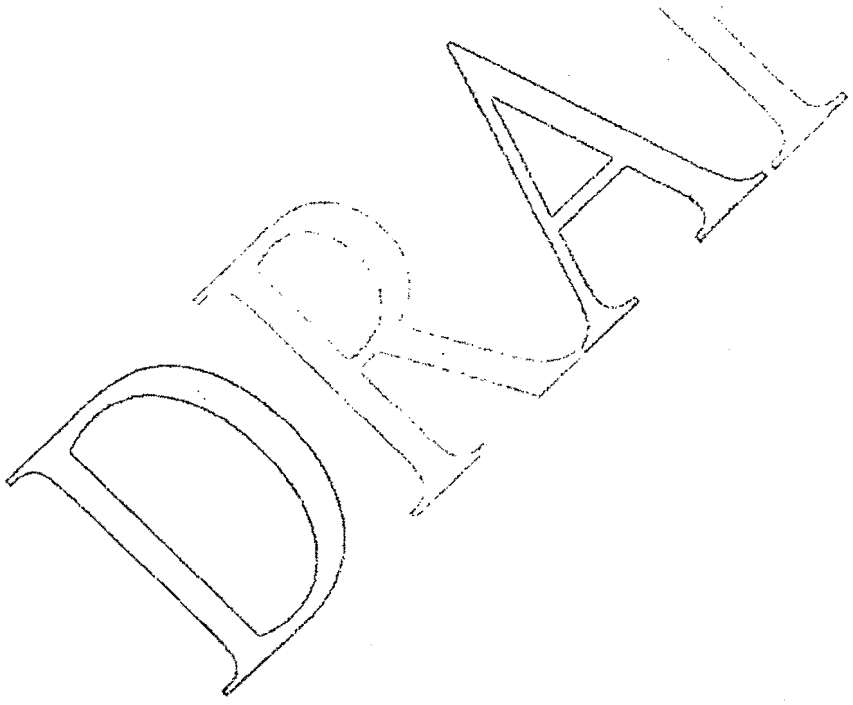
3. **Airplane mode does not necessarily disable Wi-Fi and Bluetooth**—The Airplane Mode feature (only configurable manually by the user) provides a method to disable the cellular data radio and initially disable the Wi-Fi and Bluetooth radios. It is only an "initial" disablement; however, because while Airplane mode is turned "on," the user may enable Wi-Fi and Bluetooth at his/her discretion without altering the Airplane mode status. The S/ES-IRM proposed configuration includes an operational procedure that users must follow to assure that the Airplane mode is enabled. Operating the iPad with Airplane mode disabled allows the iPad to communicate with the cellular network and potentially provide an avenue for the exfiltration of data to unauthorized networks. Similarly to the first vulnerability described the likelihood of an unintended disablement of the Airplane mode is unlikely.
4. **Good Reader Application content can be exported**—The proposed configuration for the iPad allows users the ability to perform screen capture functions while Good Reader documents are visible. Even though SBU information is intended to be contained within the Good Reader application and transferrable only via the iTunes Good Reader synch function, it is conceivable that SBU (and possibly PII) information may be copied to the Photos area of the iPad and therefore available to additional PC synchronization methods. Content can also be copied from Good Reader onto an external SD card via a hardware/software combination (i.e., ZoomIt).
5. **iPad password does not protect against PC access to the device**—Even though the iPad is configured with a password and may be in a locked state,

a correct password entry is not required when connecting to a PC for the import or export of data. Therefore, anyone obtaining physical access to the device will be capable of exporting content.

1. Although the Wi-Fi, Bluetooth, and Airplane mode vulnerabilities raise some concern, the likelihood of an unintended enablement of these wireless technologies is unlikely. Nonetheless, a recommended countermeasure would be to assure that the authorized users are familiar with wireless vulnerabilities and confirmation that users will not intentionally enable them.
2. Develop and administer user training to emphasize that the Airplane mode icon visible on the iPad does not necessarily mean that all wireless has been disabled. Users should periodically check for the faint Bluetooth icon on the iPad that is a visual indicator that the feature has been enabled. More proactive checking of the Wi-Fi setting would be required because the iPad does not provide a visual indicator that the Wi-Fi has been enabled.
3. Maintain physical control of the iPad at all times to circumvent unauthorized reconfiguration of the device, PC connectivity, or installation of third-party applications.

5. Although not evaluated by TEB, upgraded software (iPad and iPhone Configuration Utility) might provide controls that address some of the vulnerabilities in the evaluated version (i.e., iPad v3.2). Consider upgrading the software to make use of newer controls; in particular, the ability to remotely wipe the iPad if it is determined that it has been stolen or compromised.

DECLASSIFIED



1. INTRODUCTION

1.1 Background

Over the past few years Apple has taken the personal electronics device (PED) market by storm with its introduction of the iPhone®. Early this year Apple released its next wave of PEDs in the form of a tablet personal computer (PC) called the iPad™. With the introduction of the iPad, Apple has slowly begun to cross between the consumer market and the business market. The company has even taken a step further to attempt to capture the corporate market. As a result, Apple maintains focus on identifying and implementing controls and safeguards to address the security issues that are ubiquitous among all corporate networks while offering enterprise applications that are conducive to the rising demands of corporate users—all without sacrificing the "coolness" of the device which plays a major role in the users' attractiveness to the products. Just as quickly as Apple makes strides to embrace the corporate market, corporate enterprises are gearing up to support Apple products. The Department of State is no exception.

1.2 Purpose and Scope

The Technology Evaluations Branch (TEB) keeps abreast of emerging information technologies and their trends to prepare for potential use within the Department.

The evaluation was based on the device hardware and the available security controls provided by the iPad security configuration files currently supported. The hardware scope involved identifying active circuit components contained in the iPad. For the security controls perspective, the evaluation included a comparison of the controls available on the iPad versus the controls available on the BlackBerry.®

UNCLASSIFIED

1.3 Objectives

Specific objectives for the Apple iPad evaluation were as follows:

1. Identify and list the iPad Device Operating System and software installed or made available out of the box.
2. Identify vulnerabilities that may exist in the iPad based on the device's feature, technology, hardware component, and security capabilities.
3. Evaluate applications and features proposed for use on the iPad and identify potential vulnerabilities.
4. Recommend countermeasures that may be employed to mitigate identified vulnerabilities.

DRAFT

UNCLASSIFIED

2. EVALUATION RESULTS

The iPad evaluation was accomplished in four phases. Because there was a single iPad available for the evaluation, phase 2 and phase 3 were performed in series.

2.1 Phase One: Research and Data Gathering

This phase encompassed identifying any resources or websites that list the hardware components used within the iPad as well as specifications of those components. In addition, the evaluators researched proper methods for disassembling and reassembling the iPad.

First, a description of the iPad high level software architecture is provided (refer to Section 2.1.1) as well as a description of the configuration profiles available on the iPad (refer to Section 2.1.2. Next, the evaluators identified resources that assisted with the disassembly of the device (refer to Section 2.1.3).

2.1.1 Identification of Device and Pre-Installed Applications

The following lists the details regarding the iPad used for the evaluation as well as its pre-installed applications.

- iPad Model: MC497LL
- Version: 3.2 (7B367)
- FCCID: BCG-E2328A
- Capacity: 59.2 GB
- Cellular Data Number: 12024361225
- IMEI: 01 222400 250893 7
- WiFi MAC: E8:06:88:9C:FA:E0
- Bluetooth MAC: E8:06:88:9C:FA:E1

The following table, Table 2-1, lists the iPad's pre-installed applications.

iPad Pre-Installed Applications	Description
Safari	Traditional web browser
Mail	Mail client; Supports MobileMe, Microsoft Exchange, popular webmail services (e.g., Yahoo! Mail, Google Mail, AOL) and most industry standard POP3 and IMAP e-mail services.
Photos	Photo/Video Viewer and Slideshow. Allows quick assignment to wallpaper, mail messages, and/or contacts.
Videos	View video clips, movies, TV shows, and podcasts from your iTunes library.
YouTube	Connect to www.youtube.com to view videos and manage your YouTube account.
Calendar	Traditional calendar for scheduling appointments.
Contacts	Traditional address book for maintaining contact names, phone numbers, addresses, etc.
Notes	Traditional notepad for creating memorandums
iPod	Provides access to typical iPod feature such as the ability to play/shuffle digital music files.
Maps	Provides access to Global Positioning System mapping capabilities to support navigational applications.
iTunes	Provides access to Apple's exclusive iTunes application which provides a means to play and synchronize media (such as music, movies/videos, apps, RSS feeds, etc.)
App Store	Provides access to Apple's exclusive repository of applications compatible with the iPhone and the iPad.
Settings	Provides access to global configuration settings applicable to the iPad.

Table 2-1: Apple iPad Pre-Installed Apps

2.1.2 Apple Configuration Profiles

Apple provides a free utility (Apple iPhone Configuration Utility) that was originally designed to configure the iPhone. The utility however, was modified to support the iPad and was therefore used for this evaluation. The following sections describe configuration options available for the iPhone Configuration Utility (version 3.0.1.256) used for the evaluation.

2.1.2.1 General Settings

The General Settings section contains mandatory settings: (e.g., identifier field). It also allows provisioning of the overall Security Control which indicates when the profile can be removed (Always, When Authentication, and Never) and provides additional information such as (Profile Name, Org Name, and Description).

2.1.2.2 Passcode Settings

The Passcode section allows for the configuration of a password for securing the iPad. The administrator may configure the iPad to require a password as well as the following options: Simple or Alphanumeric type; Minimum Length (1-16); Minimum number of complex/non-alphanumeric characters (1-4); Maximum Passcode age (1-730 days or none); Auto Lock Timeout (1-5 mins. or none); Passcode history (1-50 or none); Grace Period for Device Lock (1, 5, or 15 mins., 1 or 4 hours, or none); and Maximum number of failed entry attempts before wipe (4-16, or unlimited/no wipe).

2.1.2.3 Restrictions

The Restrictions section allows for the configuration of various device functions such as Safari browser, camera, purchasing and installation of applications, voice dialing, backups, and encryption. More details regarding the specific restrictions are provided in Table 2-3 of Section 2.2.2.

2.1.2.4 Wi-Fi Settings

This section allows for the configuration of the WLAN networks authorized for connectivity. Provisioning parameters include SSID, "Hide SSID", encryption type (None, WEP, WPA/WPA2, Any (Personal), WEP Enterprise, WPA/WPA2 Enterprise, Any (Enterprise)) and Password for authentication to the network.

When configuring this section the SSID is mandatory. There appears to be no limit to the number of wireless networks that can be configured.

2.1.2.5 Virtual Private Network (VPN) Settings

This section allows for the configuration of the VPN networks authorized for connectivity. Provisioning parameters include Connection Name, Connection Type (L2TP, PPTP, IPSec (Cisco), Cisco AnyConnect, Juniper SSL), Server IP Address or Hostname, User Account, Authentication Type (Password, RSA SecureID), Shared Secret, Send All Traffic (Checkbox), and Proxy (None, Manual, Automatic). There appears to be no limit to the number of VPNs that can be configured.

2.1.2.6 E-mail Settings

This section allows for the configuration of e-mail accounts for the iPad. Provisioning parameters include Account Description, Account Type (IMAP, POP), User Display Name, E-mail Address, and incoming/outgoing mail server information (IP Address or Hostname and port# [required], user name, authentication type (none, password, MDS challenge-response, NTLM, HTPP MDS Digest), password for incoming server, and use SSL (Checkbox).

2.1.2.7 Microsoft Exchange ActiveSync Settings

This section allows for the configuration of an MS Exchange e-mail account for synchronization. Provisioning parameters include Account Name, Server IP Address or Hostname (required), Use SSL (Checkbox), domain name, user name, e-mail address, password, Past days of Mail Sync (Unlimited, One Day, Three Days, One Week, Two Weeks, One Month), Authentication Credential Name (i.e., certificate), Include Authentication Credential Passphrase (available only when Authentication Credential Name is provided).

2.1.2.8 LDAP Settings

This section allows for the configuration of the LDAP networks authorized for connectivity. Provisioning parameters include Account Description, Server IP Address or Hostname (required), User Account name, password, Use SSL (Checkbox), and LDAP Search Settings. There appears to be no limit to the number of LDAP servers that can be configured.

2.1.2.9 CalDAV Settings

This section allows you to configure the CalDAV server authorized for connectivity. Provisioning parameters include Account Description, Server IP Address or Hostname and port (required), Principal URL, User Account name, password, and Use SSL (Checkbox).

2.1.2.10 Subscribed Calendar Settings

This section allows you to configure subscribed calendars authorized for connectivity. Provisioning parameters include Account Description, URL of Calendar File, User Account name, password, and Use SSL (Checkbox).

2.1.2.11 CardDAV Settings

This section allows you to configure the CardDAV server authorized for connectivity. Provisioning parameters include Account Description, Server IP Address or Hostname and port (required), Principal URL, User Account name, password, and Use SSL (Checkbox).

2.1.2.12 Web Clip Settings

This section allows you to configure web link information and associated icons to be made available on the iPad. Provisioning parameters include Label, URL, Removable (Checkbox), Icon (file selection), Pre-composed Icon and Full Screen.

2.1.2.13 Credentials Settings

This section allows you to configure PKCS1 and PKCS12 certificates to be installed on the iPad.

2.1.2.14 Simple Certificate Enrollment Protocol (SCEP) Settings

This section allows you to configure settings for SCEP which allows over-the-air-provisioning of the configuration profiles. Provisioning parameters include the URL for the server, Name, Subject, Challenge, Key Size, and Fingerprint HEX

2.1.2.15 Mobile Device Management (MDM) Settings

This section allows you to configure information regarding the mobile device manager that will be used to supplement the management of the iPad. Provisioning

parameters include the URL for the MDM server, Check In URL, Topic, Identity, Access Rights, and the Queries that the MDM server will be allowed to make.

2.1.3 Supporting Resources for Hardware Assessment

Prior to actually disassembling the iPad, the TEB evaluators consulted various websites, including http://www2.electronicproducts.com/Apple_iPad_Wi_Fi_16GB-whatsinside-92.aspx to learn of anticipated interworking components. Detailed photographs of the iPad interworking were extracted from: http://www.ifixit.com/Teardown/iPad-Wi-Fi-Teardown/2183/1 and http://www.ifixit.com/Teardown/iPad-3G-Teardown/2374/1.

In addition, the following is a list of videos from www.youtube.com that TEB consulted for disassembling procedures:

1. Teardown Intro: http://www.youtube.com/watch?v=87jL-ybg9To
2. Opening Up: http://www.youtube.com/watch?v=UllD3-Rmhgs
3. LCD & Digitizer: http://www.youtube.com/watch?v=KvdNqiTtFik
4. Battery: http://www.youtube.com/watch?v=KvdNqiTtFik
5. Speaker: http://www.youtube.com/watch?v=ntZvcB0rjB4
6. Vol/Hold/Pwr Button: http://www.youtube.com/watch?v=mKLEz9faEG8
7. Headphone Board: http://www.youtube.com/watch?v=juevWd07EA4
8. Logic Board: http://www.youtube.com/watch?v=2sfjdKmJ094
9. I/O Cable: http://www.youtube.com/watch?v=fH5d69Jhjhs

2.2 Phase Two: Security Controls

In Phase II of the evaluation, the TEB evaluators executed test scenarios to measure the effectiveness of the iPad's security controls. This required new laboratory configurations which are described in Section 2.2.1. Section 2.2.2 describes the scenarios as well as their high level results. Also included in this phase, was a comparison of the iPad security controls and the BlackBerry security controls (

2.2.1 Preparation of Networking Environment and Resources

First, the TEB evaluators prepared the laboratory networking environment by obtaining and installing the required Apple resources (i.e., Apple Configuration

Utility, Apple iTunes). Next, in order to mimic the anticipated "real-world" environment, the evaluators built a web server and associated web pages for the distribution and download of Apple configuration profile files. This required an augmentation and reconfiguration of the lab Dedicated Internet Network (DIN). In addition, a new Multipurpose Internet Mail Extensions (MIME) type had to be created on the web server: The file extension (.mobileconfig) had to be setup for type "application/x-apple-aspen-config;" otherwise, the web server and the iPad were not able to open the configuration files.

2.2.2 Creation, Execution, and Results of Test Scripts

The evaluators identified various methods to control (i.e., enable/disable) specific iPad functions and applications (refer to Table 2-2). Considering this information as well as the restrictions provided by the configuration utility (refer to Table 2-3), the TEB evaluators developed test scenarios. Refer to Appendix A for the description of the scenarios as well as the specific results.

Function/Application	Potential Ways to Enable/Disable
Wi-Fi	1. Settings Icon – Wi-Fi: (Directly from the iPad) 2. Settings Icon – Airplane mode: (Directly from the iPad) 3. iPhone Configuration Tool 4. Application/Website: (Via an application/tool) 5. Docking: (Will docking automatically disable feature?) 6. Root Access: (Modifying data file stored on the iPad) 7. Hardware IC: Removing Hardware (Wi-Fi) Component
Cellular	1. Settings Icon – Cellular Data: (Directly from the iPad) 2. Settings Icon – Airplane mode: (Directly from the iPad) 3. Application/Website: (Via an application/tool) 4. Docking: (Will docking automatically disable feature?) 5. Root Access: (Modifying data file stored on the iPad) 6. Hardware IC: Removing Hardware (Cellular) Component 7. Hardware External: Removing SIM Card
Bluetooth	1. Settings Icon – General – Bluetooth (Directly from the iPad) 2. Settings Icon – Airplane mode: (Directly from the iPad) 3. Application/Website: (Via an application/tool) 4. Docking: (Will docking automatically disable feature?) 5. Root Access: (Modifying data file stored on the iPad) 6. Hardware IC: Removing Hardware (Bluetooth) Component
Apple Proprietary I/O Port	1. Root Access 2. Hardware IC: Remove I/O Port

Speaker	Speaker enabled by default with no configurable means to disable. Sound Controlled by the following: 1. Settings Icon – General – Sounds 2. Docking: (Will docking automatically disable feature?) 3. Root Access: (Modifying data file stored on the iPad) 4. Hardware IC: Removing Hardware (Speaker) Component
Browser/Safari	1. Settings Icon – General – Restrictions (Directly from the iPad) 2. iPhone Configuration Tool 3. Docking: (Will docking automatically disable feature?) 4. Root Access: (Modifying data file stored on the iPad)
YouTube	1. Settings Icon – General – Restrictions (Directly from the iPad) 2. iPhone Configuration Tool 3. Docking: (Will docking automatically disable feature?) 4. Root Access: (Modifying data file stored on the iPad)
iTunes	1. Settings Icon – General – Restrictions (Directly from the iPad) 2. iPhone Configuration Tool 3. Docking: (Will docking automatically disable feature?) 4. Root Access: (Modifying data file stored on the iPad)
Installing Apps	1. Settings Icon – General – Restrictions (Directly from the iPad) 2. iPhone Configuration Tool 3. Docking: (Will docking automatically disable feature?) 4. Root Access: (Modifying data file stored on the iPad)
Location Based Services	1. Settings Icon – General – Restrictions (Directly from the iPad) 2. iPhone Configuration Tool 3. Docking: (Will docking automatically disable feature?) 4. Root Access: (Modifying data file stored on the iPad) 5. Hardware IC: Removing Hardware (GPS) Component
Microphone	1. Root Access: (Modifying data file stored on the iPad) 2. Hardware IC: Removing Hardware (Microphone) Component

Table 2-2: Alternatives for Enabling/Disabling Functions

Control	Apple Verbiage	Available Settings:	Default Setting
DEVICE FUNCTIONALITY			
Installation of Applications	Allow Installing Apps	Checkbox (yes/no)	YES
Camera	Allow use of camera Allow FaceTime	Checkbox (yes/no) Checkbox* *only if parent control is set to yes	YES YES
Screen Copy	Allow screen capture	Checkbox (yes/no)	YES
Roaming Synchronization	Allow automatic sync while roaming	Checkbox (yes/no)	YES
Voice Dialing	Allow voice dialing	Checkbox (yes/no)	YES
Purchasing via Applications	Allow In App purchase	Checkbox (yes/no)	YES
Multiplayer Gaming	Allow multiplayer gaming	Checkbox (yes/no)	YES
Backups & Encryption	Force encrypted backups	Checkbox (yes/no)	NO
APPLICATIONS			
YouTube	Allow use of YouTube	Checkbox (yes/no)	YES
iTunes Store	Allow use of iTunes Music Store	Checkbox (yes/no)	YES
Safari	Allow use of Safari Enable Autofil Force Fraud Warning Enable JavaScript Block Popups Accept Cookies	Checkbox (yes/no) Checkbox* Checkbox* Checkbox* Checkbox* Selection(Never, From Visited Sites, Always)	YES YES NO YES NO Always
	Allow explicit music and podcasts	Checkbox (yes/no)	YES
	Ratings Region	Selection (United States, Australia, Canada, Germany, France, Ireland, Japan, New Zealand, United Kingdom	United States
	Allowed content ratings Movies TV Shows Apps	Selection (Don't allow movies, G, PG, PG-13, R, NC-17, Allow All Movies) (Don't allow TV Shows, TV-Y, TV-Y7, TV-G, TV-PG, TV-14, TV-MA, Allow All TV Shows) (Don't allow Apps, 4+, 9+, 12+, 17+, Allow all Apps)	Allow All Movies Allow TV Shows Allow All Apps

Table 2-3: Restrictions Available via Apple iPhone Configuration

2.2.2.1 Installation of Configuration Profile Scenario Results

All of the test scenarios regarding the installation of configurations profiles completed with expected/favorable results. If two profiles (even with the exact filename and identifying information) are installed on the same iPad with conflicting restrictions, the most restrictive setting is enforced. Furthermore, a signed and encrypted profile was only capable of being installed onto one iPad.

2.2.2.2 Removing of Configuration Profile Scenario Results

All of the test scenarios regarding the removal of configurations profiles completed with expected/favorable results. If allowed, users may choose to remove profiles that are installed on their iPads. If not allowed, users are prohibited from removing installed profiles on their iPads.

2.2.2.3 Functional Controls Scenario Results

Perhaps the most significant finding resulting from the execution of the functional test scenarios is that control of the iPad via the configuration profile *does not necessarily* yield the same result as a manual control via the Settings icon directly from the device. In all cases, the manual controls were more effective in producing the desired control/result. And in some cases, the manual controls are the only option for there is no forced software configuration for disabling Wi-Fi and Bluetooth. Most of the functional test scenarios completed with expected/favorable results with the exception of the following:

- Camera controls—although not seemingly relevant to devices without cameras—may prove useful when considering applications that provide camera-like functions.

- Disabling the installation of applications via configuration profile simply removes the "Apps Store" icon from the iPad; thereby disallowing the installation of applications *via the icon method.* Applications may still be installed indirectly using a PC connection to the Apple configuration tool or iTunes.

- Disabling the ability to purchase content (e.g., articles, books, additional applications) within applications via the configuration profile does not work; however, if the user sets this restriction manually directly on the iPad, the restriction holds.

2.2.2.4 Application Controls Scenario Results

When properly configured (either manually or via configuration profile) to disable specific applications (e.g., Safari, iTunes, YouTube), the iPad will *hide* the icons relevant to those applications thereby disallowing access via that method. However, that limited control does not provide an effective means to block additional access. For example, when YouTube is disabled, users are still allowed to access the www.youtube.com website; when Safari is disabled, users are still allowed to install a 3rd party browser for web browsing; and when iTunes is disabled, users are still allowed to access iTunes via a PC connection. Furthermore, these test scenarios yielded these additional surprising results.

- Disallowing all application content via configuration profile has no effect on the users' ability to install and/or run applications; however, the same control administered directly from the iPad Settings icon yields the anticipated result—all 3rd party applications are not allowed.
- Applications may still be installed indirectly using a PC connection to the Apple configuration tool or iTunes.

2.2.2.5 RF Impact Scenario Results

All of the test scenarios designed to assure that the RF signals are indeed disabled when the wireless components (i.e., cellular, Wi-Fi, Bluetooth) are disabled were completed with expected/favorable results. The TEB RF team also determined that Bluetooth, cellular and Wi-Fi signals are disabled when the device is put in Airplane mode. Refer to Appendix C for the specific spectrum analysis findings for each of the RF test scenarios.

Of interesting note is the fact that switching the Airplane Mode to "On" will indeed disable the Wi-Fi, Bluetooth, and cellular; however, the Wi-Fi and Bluetooth may be re-enabled while the Airplane mode is "On."

Additional evaluations of the interaction between the iPad and the RF spectrum yielded interesting results. Any audio played from the iPad is capable of being intercepted and listened/recorded at various frequencies throughout the RF spectrum (20 MHz – 1 GHz), including those that are outside of the human speech range.

2.2.2.6 Root Access/"Jailbreak" Scenario Results

The TEB evaluators were successful in performing a jailbreak on an iPad that was configured to allow access without requiring a password. The evaluators were able to access all files on the iPad at the root level and make modification to the files. Specifically, configuration files and settings were identified and modified; however, the modifications were not reflected onto the device given the evaluators' inexperience in performing hacking functions. It is conceivable that experienced hackers would have minimal difficulty reconfiguring the iPad from root level once jailbroken.

this scenario, TEB attempted to perform a "clean" install of the OS and Apple would not provide a means to re-install the tested version of the OS (i.e., version 3.2 (7B367)) and therefore, the inability to jailbreak the device in this scenario may not necessarily be a result of the fact that it was password protected, but instead may be a result of the upgrade in the OS (i.e., version 4.1.1).

This section presents the results of the analysis of the initial, proposed configuration and use of the iPad. The analysis was based on the following assumptions:

b7E

DECLASSIFIED

b7E

DECLASSIFIED

DECLASSIFIED

The TEB evaluators installed the Good Reader application onto the iPad, performed the following tests:

A. Transferred .pdf and .txt files to and from the iPad's Good Reader App using iTunes and via a USB cable connection to a non-Internet-connected PC.

The TEB evaluators were able to successfully transfer files to/from the PC using the documented procedures through iTunes. Transfer successfully performed

B. Determined the potential to export Good Reader files from the Good Reader App using a mechanism other than iTunes.

The TEB evaluators determined two alternatives to exporting files from the Good Reader App. Any documentation on the screen while running the Good Reader App can be copied using the Screen Capture feature that is active and available using the proposed iPad configuration. This copied content is automatically saved on the iPad as an image under the Photos icon. Another method to extract documents from Good Reader is to use the ZoomIt external card reader. This required, however, the installation of the ZoomIt application.

C. Determine the potential to activate wireless (cellular, Wi-Fi, and Bluetooth).

Even though there will be a procedural policy to maintain the iPad in Airplane mode and with additional wireless (i.e., Wi-Fi, Bluetooth) deactivated; the user has the ability to deactivate Airplane mode at his/her discretion. Moreover, regardless of the Airplane mode setting, the user has the ability to activate Wi-Fi or Bluetooth. However, all user-controlled wireless settings are activated via various levels of the "Settings" icon on the iPad; as a result, an inadvertent activation of the wireless features is not probable. The TEB evaluators also used various wireless applications in an attempt to identify a specific application that would automatically enable the wireless features. No such application was found.

D. Determine the potential to install applications.

The TEB evaluators verified that users are not capable of installing applications onto the iPad via the Apps Store icon or via iTunes within the Safari web browser. However, if the user connects the iPad to a PC that is running the Apple Configuration Utility, the user is allowed to install applications via the utility.

E. Determine the potential to remotely pull Good Reader (or other) files from the iPad

The TEB evaluators were not able to establish a remote connection to the Good Reader App as a means to "pull" files.

F. Determine the potential to "jailbreak" the iPad, or otherwise gain unauthorized access to the iPad and its files.

The TEB evaluators were not able to jailbreak the iPad; however, it was indeterminable if this was because of the configuration settings or the unintentional upgrade in the iPad device OS (version 4.2.1 [8C128]) which occurred prior to this jailbreak attempt.

2.2.4 Comparison of Apple iPad Controls to BlackBerry Controls

The Department's BlackBerry Program has been in effect for approximately six years and, as a result, has set a precedent for the expected security posture for mobile devices. Considering the BlackBerry device control as the standard for the Department's device security "requirements," TEB evaluators performed an analysis of the iPad's security controls to determine if the device offers the same or similar security features.

Even though the BlackBerry offers approximately 500 security controls, only a fraction of those were considered in this comparative analysis. Only those controls for which the Department has provided a specific restriction and/or setting were factored into the analysis. As a result, a total of 236 security controls were evaluated. Due to the extensive amount of data, the specific results are provided in Appendix B. A summary of the specific results is provided in Table 2-4 where many of the controls were categorized. Table entries marked as "Full" means that

the iPad provides similar functionality for fully supporting the control type. "Limited" means that the iPad provides some limited controls for the control type; and None means that the iPad does not support the control type at all.

Overall, out of the 236 security controls considered, 54 of them are associated with features currently not supported by the iPad. Out of the remaining 182; 21 are supported by the iPad to some degree. Therefore, the iPad supports 11% of the BlackBerry security controls that are instrumental to the Department's countermeasures for mobile devices.

The iPad provides controls for forcing the use of passwords and their specific types; however, the device does not force a password entry when connected to a PC. Also, even though the iPad provides an auto lock and forces a password entry upon an idle timeout, it does not force a password entry at a security timeout interval for non-idle use.

The iPad provides a control for disabling Bluetooth; however, the control is only provided manually and the user can enable/disable Bluetooth at his/her discretion. Bluetooth cannot be configured via the iPhone Configuration Utility to force the feature into a disabled state. Furthermore, the iPad provides no additional controls for Bluetooth such as enabling/disabling discoverable mode, forcing encryption and authentication, and allowing/disallowing specific Bluetooth service profiles as well as the pairing function altogether.

The iPad provides a control for disabling Wi-Fi; however, the control is only provided manually and the user can enable/disable Wi-Fi at his/her discretion. Wi-Fi cannot be configured via the iPhone Configuration Utility to force the feature into a disabled state.

The iPad provides very little support for controlling features and capabilities available when connected to a PC/Desktop. Desktop connectivity is never restricted and users are capable of gaining access to files on the iPad via the Desktop regardless of the lock/unlock state of the iPad. The only control provided by the iPad is the ability to assure that all backups performed are encrypted. The device does not provide a means for disabling backups or specific backup types altogether and does not provide restrictions on device swapping and synchronization. Furthermore, the wireless radio is not capable of automatically disabling upon desktop connectivity.

The iPad provides limited controls for application downloading. In particular, the configuration utility does give the ability to remove the Apps Store access on the iPad (thereby blocking the user from installing new applications) and with an ability to manually disallow all applications, most typical methods for downloading and accessing application are addressed; however, there are loop holes to the configuration where users may connect the iPad to a PC to install applications.

Additional security controls that are instrumental to the Department's countermeasures for mobile

are not supported on the iPad. Moreover, the iPad does not provide a means to manage software configuration and third-party application white-listing.

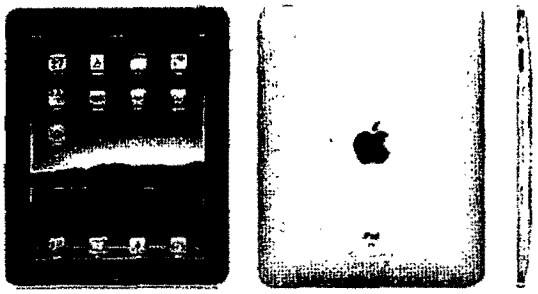
Control Type	BlackBerry Support	iPad Support
Disable Location Based Services	Full	Full
Disable Applications Center	Full	Full
Disable Screen Shot Capture	Full	Full
Disable Wi-Fi	Full	Limited
Disable Bluetooth	Full	Limited
Password	Full	Limited
Disable Application Downloading	Full	Limited
PC/Desktop	Full	Limited
Disable Third-Party Browser	Full	
Disallow External Networks	Full	
Disable IP Modem	Full	
Disable Serial Port/USB from Third-Party Apps	Full	
Force Content Protection & Level	Full	
Force Memory Cleaning	Full	
Restrict Use Based on Certificate Status	Full	
Disable Instant Messaging and other Services	Full	
Disable SMS/MMS	Full	
Software Configuration & Application White List	Full	

Table 2-4: Summary of iPad versus BlackBerry Analysis

2.3 , Phase Three: Hardware Assessment

In this phase, the TEB evaluators looked closely at the iPad's hardware components. The objective was to identify the expected components that support certain features or capabilities and to make note of any unusual circuit board configurations or unknown components.

2.3.1 The Apple iPad Hardware Description



- Dimensions: 9.56 in x 7.47 in x 0.5 in
- Weight: 1.6 lbs
- Display: 9.7 in LED-backlit Multi-Touch
- Memory: 32 or 64 GB Flash
- Processor: 1 GHz Apple A4
- Sensors: Accelerometer, Ambient Light
- Wireless: 802.11a/b/g/n; Bluetooth; 3 G Cellular
- Audio: Speaker, Microphone

The new Apple iPad is the company's first PC Tablet. The device supports tri-band High Speed Downlink Packet Access (HSDPA) and Wi-Fi (802.11a/b/g/n) networks, and has a 1-GHz mobile microprocessor with an Apple A4 platform for running 3rd party applications, e-mail, video, or web browsing. Its rechargeable built-in lithium polymer battery provides up to 10 hours of use. The Multi-Touch display uses Liquid Crystal Display (LCD) and implements In-Plane Switching (IPS) technology. It has a standard resolution of 1024 x768 and supports various audio and video formats such as .mp3, .m4a, .wav, .mov, .avi, .mpeg, .mp4, .m4v. Other key features of the iPad include assisted global positioning system (A-GPS), Bluetooth 2.0, and digital compass.

The following provides more descriptive information regarding the Apple iPad components:

- **Circuit Board (Main)**—AT&S (MX11110) 10 Layer lead-free, halogen-free 112.5 x 83 x 0.8
- **Processor**—Apple A4 (APL0398 33950084) ; and Apple A2 (33850805-82)

- **Display***—Wintek (WT-1294-01) Touch Screen Assembly 9.7" Capacitive ITO Glass on Glass 239.5 x 185 x 5); LG (LP097X02-SLA1) 262K-Color TFT 225 x 173 x 6.4; Broadcom (BCM5973KFBGH) Microcontroller for Touch Screen 9 x 9 x 1.5; Broadcom (BCM5974CKFBGH) Multi-Touch Controller 5 x 5 x .05
- **Internal Memory/Storage**—Samsung (K9PFG08U5M-LCB0) Flash NAND 64Gb, MLC, DDP 18 x 14 x 0.7
- **Internal Memory/Storage**—Samsung (K4X2G643GE-JGC8) SDRAM 2 Gb Mobile DDR 14 x 14 x 0.7
- **Accelerometer***—ST Microelectronics (LIS331DLH) 3-axis ±2g/± 4g/±8g 3 x 3 x 1
- **Ambient Light Sensor***—TAOS, Inc. (TSL2583xx) 3 Layer Flex Kapton lead-free 2.0 x 2.0 x 0.65
- **Digital Compass***—AKM Semiconductor (AK89735) Electronic Compass 3-axis 8-bit Digital w AD/DA Converter 2.50 x 2.50 x 0.50
- **Bluetooth WLAN/Wi-Fi**—Broadcom (BCM4329XKUBG) APN 339S0107 WLAN 802.11a/b/g/n /Bluetooth 2.1+EDR/FM Transmitter/Receiver; 6.5 x 5.6 x 0.5
- **GSM/GPRS**—Infineon 3G Baseband Processor (33753754); Infineon Quad Band GSM/GPRS and Tri-Band WCDMA/HSPDA RF Transceiver (33850353)
- **RF Amplifiers**—Skyworks GSM/GPRS Power Amp (SKY77340-21); SAW Low Noise Amp (RXCC 001 016); TriQuint Semiconductors WCDMA/HSUPA Power Amps (TQM616035A; TQM666032B; TQM678031A)
- **GPS**—Broadcom Assisted GPS (BCM47) S01065
- **Audio**—Loudspeaker Assembly (TLV320AIC31061ZQER) 1 Pair ½ in Voice Coil, Mylar Cone, 2.8mm high 26mm diameter*; Audio Jack In Apple Ft 8210795
- **Power**—Li-ion Polymer Battery (A1315) 3.75 V 24.8 WHr; APN 616-0477; VPN 969TA029H
- **Antennae**—Back Panel, Apple (621-0920-B) HF/el, SAA c1710

TRANSFERRED FOR DIRECT REPLY DS

I2 OCJ

(P)

b7C

b7E

The United States Department of State

Diplomatic Security—Countermeasures Program—Technology Evaluations Branch

DS/CMP/TEB

BlackBerry® PlayBook™ Evaluation

(Final Draft)

September 23, 2011

b7C

Author:

DS/CMP/TEB Branch Chief: Fred G. Everdale

DS/ST/CMP Division Director: Karl W. Covington

DECLASSIFIED

DECLASSIFIED

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Technology Evaluations Branch (TEB) keeps abreast of emerging technologies and their trends to prepare for potential use within the Department. The Department has been looking at tablet devices as a way to provide resources in support of the new trend toward Mobile Diplomacy. As a result, IRM/IA provided TEB with a BlackBerry PlayBook for a preliminary evaluation. The purpose of this document, *"BlackBerry PlayBook Evaluation"* is to highlight the methodology used for, and present the results of, the DS/CMP/TEB evaluation of the BlackBerry PlayBook product.

The evaluation was based on a hardware and software perspective. The hardware scope involved identifying active circuit components contained in the BlackBerry PlayBook.

The scope of this evaluation was limited to those features and/or security controls that have not yet been evaluated or would be changed as a result of the introduction of the PlayBook.

The main technical issue with the BlackBerry PlayBook is that it requires the use of Bluetooth technology which is currently not permitted in DOS facilities. The PlayBook is not a standalone device for work purposes; as such it is required to be connected (via Bluetooth) to a Department BlackBerry Smartphone. This is the only way to have access to Department related work data and email. This BlackBerry Bridge is only able to be performed through a Bluetooth connection.

Secondly, IEEE 802.11 Wi-Fi is required during the setup process. This Wi-Fi connection is used to download Operating System (OS) patches and updates. The update process takes place in the background, and the user does not have the option to avoid or eliminate the update process. Additionally the website that the download is being pulled from is not displayed, so one can only hope that it being pulled from a

Research In Motion (RIM) controlled server. There is no way to utilize a "known good" patch during the setup process. This makes DOS controlled patch management unfeasible.

Fourth, the OS does not adequately distinguish between the work file system and the personal file system for the same application. This could easily allow for the inadvertent creation and storage of Sensitive But Unclassified (SBU) data on the personal file system. In this location the file would be outside the protection of the FIPS 140-2 encrypted file system. This combined with the lack of administrative control over the device could easily allow for the file to be browsed, copied, or deleted by someone who connects to the device over Wi-Fi.

If in future models the Bluetooth radio is reduced to a class 2 or class 3 per DOD guidelines, then TEB will review this recommendation.

1. INTRODUCTION

1.1 Background

Recently the Department of State has begun to push the capabilities of the mobile diplomat. Expanding upon the already established base of BlackBerry devices, the Department has begun to investigate the possibility of using more feature-rich BlackBerry devices, and newer devices from other vendors. These new vendors are presenting the Department with new hardware and operating system platforms for mobile devices. With the goal of increasing the flexibility of the mobile diplomat,

. Pursuant to this goal, the Technology Evaluations Branch (TEB) has taken on the review of this device in order to provide comments regarding the feasibility of a secure implementation.

1.2 Purpose and Scope

TEB reviews emerging technologies and their trends and the Mobile Computing lab) expressed interest in pilot programs to evaluate tablet devices. TEB, in addition to working on other pilot projects with MC, is, at the request of and , providing this evaluation of the BlackBerry® PlayBook™

Unlike any other tablet or mobile phone devices, the PlayBook is a dedicated viewer for the BlackBerry device. As a result the evaluation was based on the device hardware and the available security controls for PlayBook and the BlackBerry it is connected to. The hardware analysis involved identifying active circuit components contained in the PlayBook; in particular, the Wi-Fi and Bluetooth® components. From the security controls perspective, TEB evaluated the hardware features of the device with respect to identifying the possible vulnerabilities of the device. Then TEB determined the changes that need to be made to the current BlackBerry® Enterprise Server (BES) policy to enable the PlayBook. TEB attempted to exploit these changes on the BlackBerry operating system. Testing centered on the Bluetooth and Wi-Fi connections to the BlackBerry and the PlayBook. TEB then evaluated the IRM/IA proposed implementation of the PlayBook (including the changes CS suggested to the BES security policy in its *"RIM BlackBerry PlayBook Evaluation Report"*).

1.3 Objectives

Specific objectives for the BlackBerry PlayBook evaluation were as follows:

1. Evaluate the identified features of the device in relation to the OS and if settings exist to enable and or disable these features. Determine if these features present any vulnerability based on the effectiveness of the setting that are able to be applied.
2. Evaluate the control the BES has over the PlayBook
3. Determine if features/capabilities of the user file system may present any vulnerability to the work file system on the PlayBook or the attached BlackBerry.
4. Evaluate the Bluetooth connection as a means to gain entry to the PlayBook or the BlackBerry
5. Evaluate the Wi-Fi connection as a means to gain entry to the PlayBook or the BlackBerry
6. Determine changes in BES policy needed to install the Bridge application and establish connectivity to the BlackBerry. Evaluate these changes for vulnerabilities in the PlayBook and BlackBerry devices.
7. Perform a hardware analysis of the PlayBook to correlate the components found in the device with the advertised features. Determine if the device chipsets hold undocumented features that can be exploited.
8. Perform a radio frequency (RF) analysis of the PlayBook to determine if the software controls for the Bluetooth radio set to off is in fact not emanating at all.
9. Perform an RF analysis of the PlayBook to determine if the software controls for the Wi-Fi radio set to off is in fact not emanating at all.
10. Recommend countermeasures that may be used to mitigate any identified vulnerabilities.

2 EVALUATION RESULTS

2.1 Hardware Assessment

The BlackBerry PlayBook is a lightweight portable electronic device (PED) that can be referred to as a tablet. The PlayBook represents Research In Motion's first foray into the tablet arena. The device that was evaluated includes the following Specifications:

Identification

- BlackBerry PlayBook 1.0
- Operating System 1.0.7.2670

Features

- Dual High Definition (HD) cameras (3 Mega Pixel (MP) front facing, 5 MP rear facing), supports 1080p HD video recording
- Stereo speakers and stereo microphones
- Magnetic three pin connector for Power charging

I/O Ports

- Audio Port: One Jack (Headphone Out)
- Micro High-Definition Multimedia Interface (HDMI)
- Micro Universal Serial Bus (USB)

LED Indicators

- Power Light Emitting Diode (LED), Wireless LED

Wireless

- Wi-Fi 802.11 a/b/g/n
- Bluetooth 2.1 +Enhanced Data Rate (EDR)

Due to time constraints of this evaluation TEB was unable to perform an in-house teardown of the PlayBook. The Internet however, is an excellent resource for obtaining information regarding the inter-workings of tablets and other Smartphone devices. Much of the information in this section was extracted from http://www.ifixit.com and http://www.chipworks.com.

Figure 2-1 through Figure 2-5 are pictures of the BlackBerry PlayBook Printed Circuit Board (PBC) components. Table 2-1 provides a list of all the chipsets found in the device, the markings on the chips and their functionality.

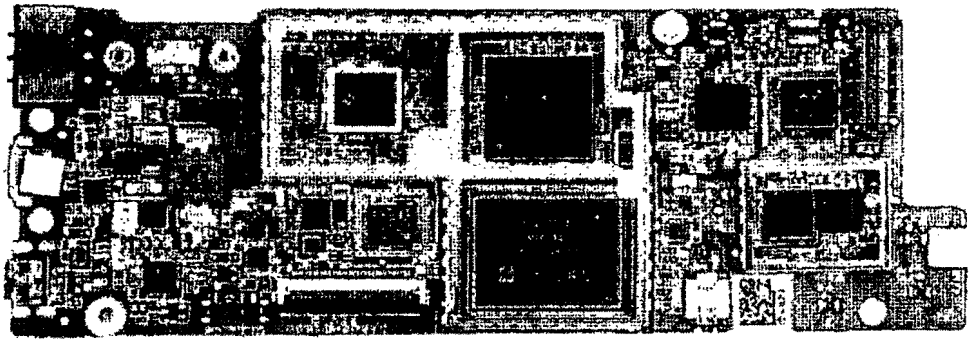


Figure 2-1: BlackBerry PlayBook PCB (Front)

- Front view of the motherboard.
  - (Red) Elpida B8064B2PB-8D-F 1GB DRAM & the TI OMAP4430 1GHz dual-core processor
  - (Orange) SanDisk SDIN5C2-16G 16 GB NAND Flash
  - (Yellow) Texas Instruments TWL6030 Power Management
  - (Lt Blue) STMicroelectronics XTV0987 5 MP mobile imaging processor
  - (Dark Blue) Wolfson WM8994E audio codec
  - (Purple) Texas Instruments WL1283 GPS/WLAN/Bluetooth/Bluetooth low-energy (BLE)/ANT/ANT+/FM
    - Supports Wi-Fi Direct
    - Supports Soft AP mode capabilities
  - **(Black)** TriQuint Semiconductor TQP6M9002 802.11a/b/g/n + BT front-end module
  - (Lt Green) **Unknown Chipset 358764G / 183888 / 1045 HAL / Japan**

Not Classified

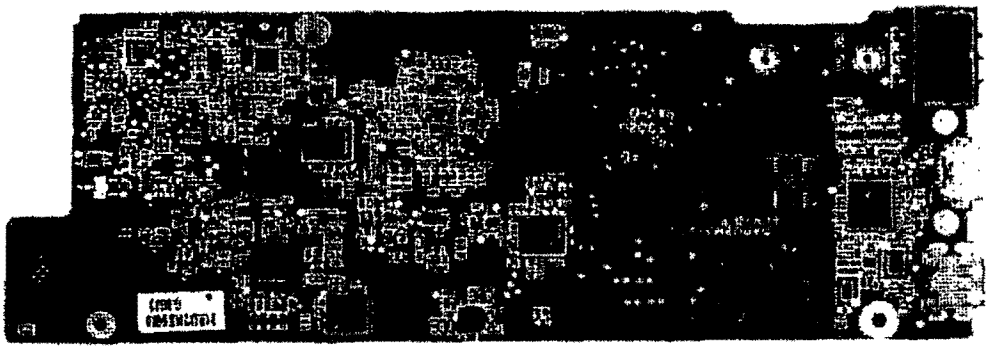


Figure 2-2: BlackBerry PlayBook PCB (Back)

- And the rear view of the motherboard.
  - (Red) Texas Instruments LMV339 Quad General Purpose Low-Voltage Comparators
  - (Orange) Texas Instruments SN74AVCH4T245 4-Bit Dual-Supply Bus Transceiver with Configurable Voltage Translation and 3-State Outputs
  - (Lt Blue) Bosch Sensortec BMA150 Digital 3-axis accelerometer
  - (Dark Blue) Invensense MPU-3050 3 axis gyroscope
  - (Purple) Texas Instruments PS63020 High Efficiency Single Inductor Buck-Boost Converter with 4A Switch

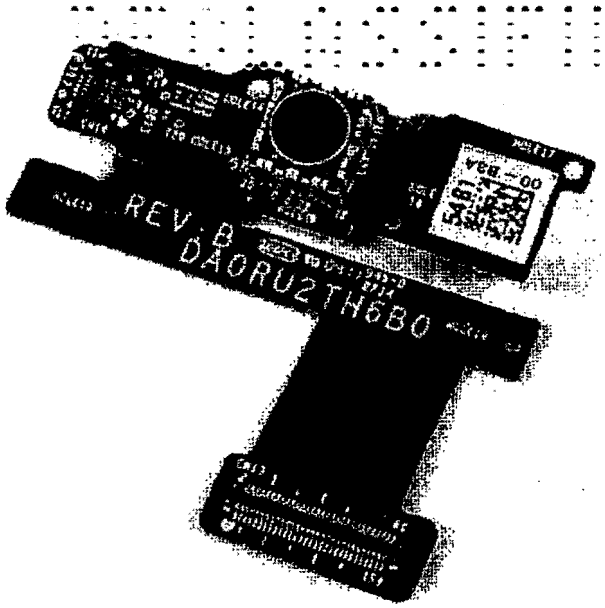


Figure 2-3: BlackBerry PlayBook Front and Rear Cameras and Top Control Buttons

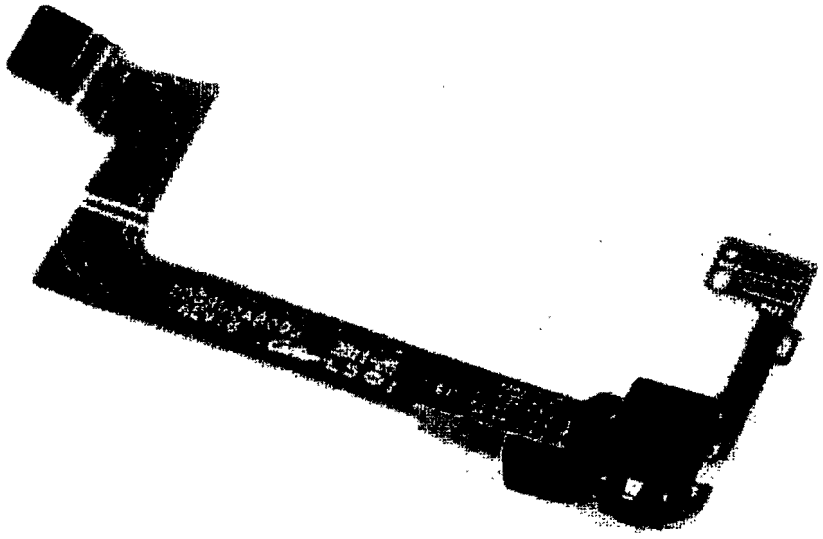


Figure 2-4: BlackBerry PlayBook Headphone Jack and Right Microphone

UNCLASSIFIED

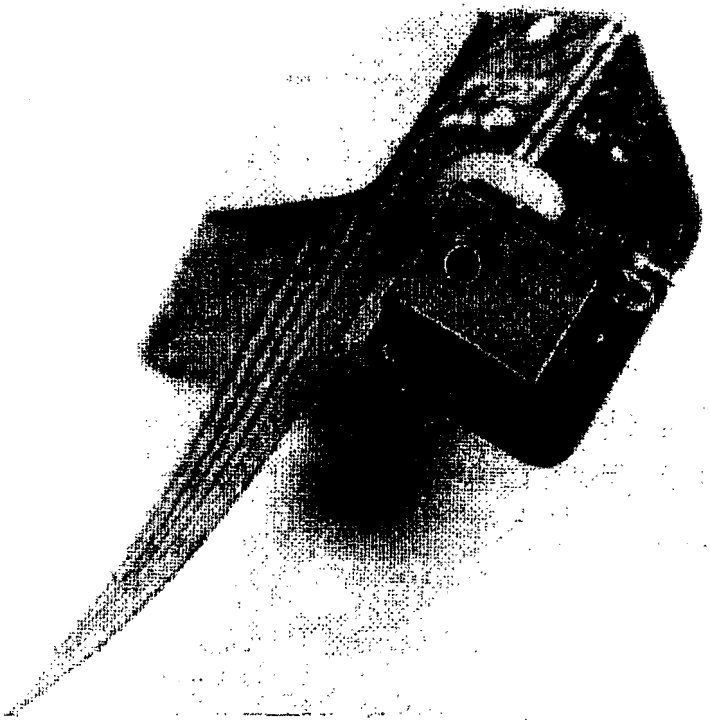


Figure 2-5: BlackBerry PlayBook Left Microphone Assembly

- Dual microphones presumably allow for noise cancelling to eliminate background noise or to provide stereo input.

UNCLASSIFIED

Manufacturer and Chip	Chip Nomenclature	Function
Texas Instruments OMAP4430	OMAP TM / X4430DCBS / R1 / 0CZFQW9 / G1	Application Processor
Texas Instruments TWL6030/TWL6040	PTWL6030BCMR / OCZFJD9 L / G1	Power Management
Texas Instruments WL1283	MCS / WL1283C / 11M1ED3	WLAN, Bluetooth (including 3.0 and BLE), ANT/ANT+, WiFi Direct and Soft AP, and FM (Rx and Tx), GPS. This is the WiLink 7 .0 solution
Wolfson WM8994E	Logo / WM8994E / 09GAAWB	The WM8994 is a highly integrated ultra-low power hi-fi CODEC
STMicroelectronics STV0986	XTV0987 / GK1XK9E / CHN 036 / Logo lead free B	5 Megapixel mobile imaging processor (same as in the BlackBerry Torch)
Elpida B8064B2PB-8D-F	Elpida Japan/ B8064B2PB-8D-F/ 10530N02100	8 Gb DRAM
SanDisk SDIN5C2-16G	SanDisk / SDIN5C2-16G / Taiwan / 0535S1G123	16 Gb NAND Flash / 32 Gb NAND Flash / (depending on model)
TriQuint Semiconductor TQP6M9002	6M9002 / 1045 / ACI104	802.11a/b/g/n + BT front-end module
Cypress Semiconductor CY8CTMA3	CY8CTMA3 / 01E-48LQX / 1025 D 04 / CYP634986 / PHI / 185	Multi-Touch All-Point TrueTouch™ projected capacitive touch screen controllers
STMicroelectronics STM5953BA	5953CA	4.9 Mp CMOS Image Sensor (primary sensor)
STMicroelectronics 58548A	58548A	3.1 Mp CMOS Image Sensor (secondary sensor)
Invensense MPU-3050	INVENSENSE / MPU-3050 / Q2R774-G1 / EL 1050 K	3 axis MEMS gyroscope
Texas Instruments PS63020	PS63020 / TI 0BK / E8KQ	High Efficiency Single Inductor Buck-Boost Converter with 4A Switch
Bosch Sensortec BMA150	043 / U023	Digital 3-axis accelerometer
Texas Instruments SN74AVCH4T245	WS245 / TI 0BW / ZF94	4-Bit Dual-Supply Bus Transceiver with Configurable Voltage Translation and 3-State Outputs

Texas Instruments LMV339	MV339I / logo 08K 04 / D23P	Quad General Purpose Low-Voltage Comparators
Texas Instruments TPD12S015YFFR	TI0CA4GQI / PN015	HDMI Companion Chip with Step-up Converter, I2C Level Shifter, and High-speed ESD Clamps
Intersil ISL9519/i951	Logo 951 / 9HRTZ / F024PV	Highly integrated Narrow VDC system voltage regulator and battery charger controller with SMBus interface
Texas Instruments TPS63031	CEF / TI / J / OCPN	High Efficient Single Inductor Buck-Boost Converter w/1-A Switches
Unknown	358764G / 183888 / 1045 HAL / Japan	Unknown

Table 2-1: Chip Manufacturer, Markings found on Chip and Chip Function in the PlayBook

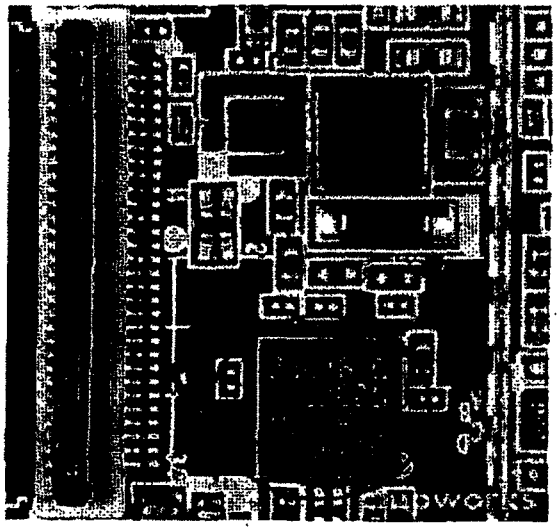


Figure 2-6 Highlight of the Unknown Chipset on the PCB Front

The TEB evaluation of the hardware found a couple areas of concern. First there is the unknown chipset featured above. Neither research nor Internet searches provided any information about the chip's function in the PlayBook or its capabilities. The lack of information about this chipset makes it impossible to yield

conclusions regarding specific vulnerabilities; however, the more uncertainty of the chipset raises concerns that any security professional would deem warranted. Second, during the analysis of the identified chipsets, TEB discovered that the Texas Instruments WL1283 chipset also supports Wi-Fi Direct and soft AP mode capabilities (each having the potential to impact network connectivity). While these features are not supported in the PlayBook's Operating System, they do exist on the chipset, and are one firmware patch away from becoming active. TEB does not have the infrastructure to activate the features on this chipset and evaluate it for vulnerabilities that their presence may cause. Since these features are dormant and can be activated by a firmware patch or possibly by malware, it is unknown what impact they would have to the BlackBerry Bridge and its associated data that it protects. If a future patch or upgrade activates these features, a new evaluation of the device must be performed.

2.1.1 Findings

The following represent the major findings of the hardware assessment.

- TEB identified an unknown chipset on the device with unknown functionality.
- TEB identified that the Texas Instruments WL1283 chipset possesses dormant features that cannot be evaluated for vulnerabilities.

2.2 Software Assessment of the Hardware Subsystems

The TEB evaluators performed 3 major steps in evaluating each objective. First, the RIM "out of box" default settings using just the PlayBook. Second, the PlayBook was attached to a BlackBerry Smartphone that was in RIM default mode and not connected to a BES. Third the PlayBook was attached to a BlackBerry Smartphone that was attached to the BES and running the CS modified version of the Department's OpenNet IT Policy. This section provides the results of this software hardware assessment. It is important to note that when evaluating BlackBerry devices there are typically several ways to access specific features. It is imperative that each of these pathways are considered to verify that features that are intended to be disabled are indeed disabled. The PlayBook recently received FIPS 140-2 certification of its encryption technology. As a result TEB did not concentrate on the security of the data in transit over the Bluetooth link nor on the Data at Rest. The evaluation centered on whether the needed changes to the IT

policy provided any new vulnerability to the approved BlackBerry Smartphone and could the PlayBook be used as a means to gain access to the data on the BlackBerry Smartphone or even on OpenNet.

The following subsections highlight the results of the software hardware assessment. Details of specific scenarios are provided in the Appendix.

2.2.1 The device controls of the identified features

TEB reviewed the administrative controls available for the PlayBook features. The features TEB concentrated on were:

2.2.1.1 The Bluetooth control

The Bluetooth functionality is required on both the PlayBook and BlackBerry Smartphone. This allows the PlayBook to connect to the BlackBerry Smartphone or access DOS work data and emails.

Prior to BES connectivity, the PlayBook control of Bluetooth was tested. First a Bluetooth connection between the PlayBook and another Bluetooth device (Bluetooth enabled cell phone) was established. Bluetooth was then turned off on the PlayBook. It was determined that the Bluetooth connection was indeed broken between the two devices. This test was performed again after the PlayBook was bridged to a BES activated BlackBerry. The second test produced the same result.

2.2.1.2 The Wi-Fi control

Prior to BES connectivity, the PlayBook Wi-Fi control was tested by first connecting the PlayBook to an IEEE 802.11 b/g/n access point (AP). The IP address of the PlayBook was ascertained from the AP. The ping command was used in continuous mode with the IP address to test connectivity. With the ping command showing a response from the PlayBook, the Wi-Fi was turned off. The ping command showed a loss of connectivity and the AP no longer show the PlayBook device as connected. This test repeated after the PlayBook was bridged to a BES activated BlackBerry with the same result.

2.2.1.3 File Sharing and Wi-Fi file Sharing

2.2.1.3.1 Prior to BES Connectivity

Prior to BES connectivity, the PlayBook control of *file sharing* and *Wi-Fi file sharing* was tested. First, a Wi-Fi connection between the PlayBook and the Wi-Fi AP was established. Next, the global *file sharing* and *Wi-Fi file sharing* options were allowed on the PlayBook. The PlayBook was identified on the network and scanned using a network port scanning tool. The result showed no open ports but did provide a NetBIOS workgroup. This allowed for future exploration by using the Universal Naming Convention (UNC) to create a file sharing connection to the Samba shares (a software that emulates a windows NetBIOS share, and allows windows systems to connect to UNIX or Linux systems) on the PlayBook. Upon opening the shares several folders are available. The folders were accessible and files in the folders were capable of being copied to or from the folders. *Wi-Fi sharing* was then turned off. As a result, the UNC shares were disabled and access to the shares was lost. The test was repeated with a connection to an IEEE 802.11 a/n access point and produced the same result.

With the *Wi-Fi file sharing* off and *file sharing* still on TEB tested the PlayBook by connecting it to a laptop using the micro USB cable. The device could be explored from My Computer on the Windows Laptop. The same files and folders seen in the previous test were available. The folders could be transverse and files could be created and copied to and from the folders to the computer. Using BlackBerry Desktop Manager the PlayBook could be backed up without issue.

The *file sharing* feature was then turned off and the test was rerun by reconnecting the PlayBook to the laptop. The file shares were still available and able to be modified. Whereas this may be a flaw in feature design, it does not present a vulnerability to the work data. With the PlayBook not attached to a BES activated BlackBerry there is no work file system to attempt to attack.

2.2.1.3.2 After BES Connectivity

The *Wi-Fi file sharing* test was performed again with the PlayBook after it was bridged to a BES activated BlackBerry and yielded the same results. The NetBIOS

shares were still accessible for file transfer. However, TEB was unable to gain entry into the work file system or view any work files.

TEB performed the same file sharing tests using the bridged PlayBook and a micro USB connection to the laptop. All of the folders that were previously available were accessible and the files were able to be moved, copied, deleted, or created. The PlayBook device could be backed up and no password was required to access the device. Again, TEB was unable to gain entry into the work file system or view any work files.

TEB performed this test again with the global user set password enabled. This prevented the PlayBook from automatically connecting to the computer. It also prevented any file or folder access until the password was entered.

Result: The *file sharing* features of the PlayBook do not present any vulnerabilities to the work file system (i.e. work files may not be shared over Wi-Fi or USB hardwire connections). However, the global file sharing setting is ineffective in providing control over accessing personal device files from the USB connection, including file manipulation and device back up. The global user password does provide some level of protection from this and should be enabled. Although due to the limitations of BES control it cannot be mandated.

2.2.1.4 Internet Tethering

Prior to BES connectivity, the PlayBook Internet Tethering control was reviewed using the just the Bluetooth connection, it was reviewed again after the Bridge was established, and again after the bridged BlackBerry was activated on the BES.

. Although TEB was able to perform Internet Tethering in pervious evaluations, TEB was unable to get the Internet Tethering to work with the BlackBerry PlayBook and BlackBerry Smartphone in this test configuration.

2.2.1.5 Speakers Controls

TEB reviewed the controls for speakers and system sound. Along with the nonexistent BES controls, TEB found only a volume control and no master control to turn off the speakers.

2.2.1.6 Microphone Controls

TEB reviewed the controls for the microphone device. TEB found no microphone control, and no way to turn off the microphone device, in addition to no control from the BES.

2.2.2 BES Direct Control of the PlayBook

TEB evaluated what BES policies have direct control over the PlayBook. There is only one BES policy that has any PlayBook control and that is the Companion Device Policy Group, which contains the BlackBerry PlayBook Log Submission Rule. This is the only policy rule in this policy group. The rule specifies whether the BlackBerry PlayBook tablet can generate and send log a file to the BlackBerry Technical Solution Center. Aside from controlling if the PlayBook creates a log file and if the log file is sent to RIM there are no other BES policies that directly control the PlayBook.

2.2.3 Features/Capabilities of the User and Work File Systems for Vulnerabilities

TEB evaluated if the features/capabilities of the user file system may present any vulnerability to the work file system on the PlayBook or the attached BlackBerry. (No work file system exists when the PlayBook is not connected to a BES enabled Smartphone.)

This evaluation took place in two parts. First, TEB evaluated the access control of the file system. This was done by attempting to access work files from personal applications and personal files from work applications. TEB determined that work applications could open files of other work applications and personal applications

could open personal files of other personal application. The personal applications could not access the work files at all.

Second, TEB attempted to move data from the work file system to the personal file system, and from the personal file system to the work file system. This was performed by attempting to use the cut/copy/paste functionality to move data between file systems. TEB was unable to move data by this method. TEB then attempted to attach work files to personal emails and personal files to work emails. TEB was able to attach a personal file to a work email but was unable to attach a work file to a personal email. The built in personal email clients do not support file attachments. TEB used the web version of the personal email clients but still was unable to attach a work file to a personal email.

2.2.4 Bluetooth connection vulnerabilities for the PlayBook and Smartphone

TEB evaluated the Bluetooth connection as a means to gain entry to the PlayBook or the BlackBerry Smartphone. The testing took place in three parts. First, TEB evaluated the PlayBook and BlackBerry Smartphone in an "out of the box" or default mode. The object was to see what devices could be paired to the PlayBook and what features and services does the PlayBook provide these devices and if any of these can be exploited.

Second, the BlackBerry was activated on the BES with the new CS configuration policy for the PlayBook. The BlackBerry Smartphone was again paired to several devices and the services and features that the Smartphone offered where evaluated for vulnerabilities.

Third, TEB utilized the BES activated BlackBerry and used the BlackBerry Bridge to connect it to the PlayBook. TEB then performed the same tests against both the PlayBook and the BlackBerry Smartphone that had been previously tested; again looking for changes in features or services that were offered that could create or pose a vulnerability.
Throughout the testing TEB utilized several Bluetooth enabled devices:

- A second BlackBerry Smartphone
- A Bluetooth Access Point (AP) – used to establish LAN connectivity for a device through the Bluetooth connection.
- A Bluetooth enabled non BlackBerry Smartphone

- A Bluetooth headset
- A Bluetooth enabled laptop

2.2.4.1 Prior to BES Connectivity

Prior to BES connectivity, TEB established just a Bluetooth connection between the BlackBerry Smartphone and the PlayBook (both devices are out of box). TEB found that neither device was offering any services or features to the other. TEB went on to test the non-BlackBerry Smartphone; again the PlayBook did not provide any services to the Smartphone. TEB then tested a Bluetooth enabled laptop and a Bluetooth AP, with the same negative result. The PlayBook did not offer any services to connected devices. TEB attempted file transfers but that was not possible with the PlayBook lacking services. The headset paired to the PlayBook but was not able to control it in any way; additionally the PlayBook showed no services for the headset.

2.2.4.2 After BlackBerry Smartphone is Connected to BES but not the PlayBook

This portion of the testing concentrated on the BlackBerry Smartphone and the changes made to the DS BlackBerry security policy that was required to connect to the PlayBook. The intent is to determine if the changes (mainly to the Bluetooth BES policy settings) present any general Bluetooth connectivity / access issues. TEB activated a BlackBerry Smartphone on the BES and applied the modified DS BlackBerry policy to the device. After BES connectivity was established, connected a laptop and Bluetooth AP to the BlackBerry Smartphone. Neither the laptop nor the Bluetooth AP showed any services for the BlackBerry Smartphone. Additionally, no files were able to be pushed to the Smartphone and the BlackBerry could not send any files out. Both the second BlackBerry and the non-BlackBerry Smartphone where connected to the BlackBerry under test. The test BlackBerry did show the serial port service but neither phone could send files to the test BlackBerry.TEB then tested the Bluetooth headset, it was unable to provide any control over the Smartphone (e.g. could not make, answer, or end any calls). The headset could not listen in on any calls. The only indicator was the

Bluetooth icon on the display would flash when the button on the headset was pressed.

2.2.4.3 After PlayBook is Connected to the BES activated BlackBerry Smartphone

Finally TEB connected the PlayBook to the BES activated BlackBerry Smartphone and retested the devices that were tested in the first two section. All devices performed the same as they did in the previous testing. The BlackBerry Smartphone offered a serial port but no services, so no data could be set to or from the Smartphone. Additionally the PlayBook Bluetooth connection did not provide and services that could be utilized.

In addition TEB utilized two BlackBerry Smartphones with the BlackBerry bridge software installed on each of them and that were both paired with the same PlayBook. Although the PlayBook supports multiple pairings it does not support simultaneous BlackBerry Bridge connections. With both phones able to pair to the same PlayBook, TEB attempted to gain access to the work files by moving the bridge from one device to the other. The PlayBook destroyed the connection to the first BlackBerry and created a new Bridge to the second BlackBerry. The second BlackBerry had no access to the bridge data of the first BlackBerry.

TEB then evaluated other controls to make sure that the changes required by the PlayBook did not open up vulnerabilities in other areas of the IT policy.

UNCLASSIFIED

2.2.6 Findings

The following represent the major findings of the software assessment.

- The Bluetooth paring provides good security out of the box and throughout testing. The PlayBook did not offer any service to paired devices.

- There is no Microphone control.
- There is no on/off control for the speaker only limited volume control.
- The password does provide some protection for personal data.
- TEB was unable to get the Internet tethering to work, possible due to cellular account restrictions.
- Wi-Fi is required during the setup process.
- The PlayBook downloads patches automatically during the setup of the device. The user/administrator has no control of where the patches are downloaded from.
- The Bluetooth functionality is required on both the PlayBook and Black Berry Smartphone. This allows the PlayBook to connect to the BlackBerry Smartphone or access DOS work data and emails.

- Throughout the testing the personal applications could not access the work files at all.
- The cut/copy/pate method was unable to move data from one file system to the other.
- Built in personal email clients does not support using file attachments.
- Use of the Web version of personal email clients was able to attach personal files but could not access work files.
- From work email client, a personal file can be sent as an attachment

- Although the PlayBook supports multiple pairings it does not support multiple simultaneous BlackBerry Bridge connections.

2.3 Radio Frequency Evaluation Results

This evaluation was conducted to identify potential vulnerabilities associated with the three radio technologies embedded within the PlayBook mobile device. Test setup consisted of using a radio frequency (RF) shielded enclosure to ensure a controlled RF environment. The PlayBook was placed in the enclosure along with the BlackBerry 9800 (Torch) that was configured and authorized to connect to the PlayBook. A log periodic antenna was place 3 meters (10 feet) away from the device(s) being tested. Outside the shielded enclosure the antenna was connected to the Rohde and Schwartz FSQ spectrum analyzer and a screen shot was captured for each test. A table of the testing conducted may be found in Table 1.

The first wireless technology evaluated was the Bluetooth (Figures 3-1 to 3-4). It was confirmed that when the Bluetooth was manually turned off on the PlayBook device the Bluetooth would not transmit. During testing of the Airplane Mode the Bluetooth would initially stop transmitting but the user may turn the transmitter back on by simply re-enabling the Bluetooth while the device still had the Airplane Mode option on.

The second wireless technology evaluated was 802.11b/g/n (2.4 GHz band) (Figures 3-5 to 3-6). The device appeared to immediately begin to transmit pings. There are no user controls for what technology or frequency should be used. The device will only connect to whatever Access Points are available to it. The user is unable to readily identify what frequency spectrum or technology is being used. When Airplane Mode is enabled the transmitter will turn off and cannot be re-enabled until the Airplane Mode is disabled.

The final wireless technology evaluated was 802.11a/n (5 GHz) (Figures 3-7 to 3-8). The device could not be detected transmitting on the 5 GHz spectrum. An 802.11a wireless Access Point (AP) was set up to accommodate further evaluation. Once the Access Point was detected by the PlayBook and a connection was made the PlayBook began continuous transmissions to the AP. Once the AP could no longer be detected, the PlayBook would continuously attempt to try to reconnect (transmit a ping) in the 5 GHz frequency. While the 2.4 GHz radio is the default as long as the PlayBook was connected to a 5 GHz AP it will continue to look in the 5 GHz range but does not change back to the previous 2.4 GHz default.

2.3.1 Background Information

BlackBerry PlayBook Federal Communications Commission (FCC) Identification (FCCID) number is - **L6ARDJ20WW**

2.3.1.1 IEEE 802.15 Bluetooth 2.1(+EDR)

Class 1 Bluetooth device, able to transmit up to 330 feet or 100 meters away. Enhanced data rate of 2.1 Mega Bits per second (MBps). Four Bluetooth profiles identified –

- **Dial-Up Networking (DUN)** – This is what allows for Bluetooth tethering to any phone that supports it
- **Serial Port Profile (SPP)** – This profile has multiple uses
- **Secure Simple Pairing (SSP)** – Allows easy pairing of the PlayBook to the BlackBerry or any device with Bluetooth 2.1+
- **Human Interface Device (HID) (keyboard only)** –Bluetooth Keyboards only but identified to work with mice too.

2.3.1.2 IEEE 802.11b/g/n Wi-Fi (2.4 GHz)

According to FCC report the maximum transmit power out of the device is 310 mW (24.9 dBm). Power levels cannot be controlled on the PlayBook device, thereby preventing the minimization of transmit power levels. Typical mobile devices transmit around 150 mW.

2.3.1.3 IEEE 802.11a/n Wi-Fi (5 GHz)

According to FCC report the maximum transmit power out of the device is 49 mW (16.9 dBm). The 802.11a/n radio will not transmit unless there is already an 802.11a/n (5 GHz) access point transmitting within the area. There was no ping observed within the 5 GHz frequency spectrum when there was no device detected

to connect to.

2.3.1.4 Airplane Mode

Airplane mode will initially disable all transmitters. Bluetooth can be enabled even when the PlayBook's Airplane Mode is enabled. Wi-Fi on the PlayBook does not allow the user to define what technology to use. Users cannot define the frequency spectrum to use be it the 802.11 b/g/n (2.4 GHz) or the 802.11 a/n (5 GHz). Airplane mode must be disabled to allow the Wi-Fi connection to transmit.

	PLAYBOOK	BLACKBERRY	SPECTRUM
Bluetooth	On	Off	Yes (Figure 3-1)
	Off	On	Yes (Figure 3-2)
	On	On	Yes (Figure 3-3)
	Off	Off	No (Figure 3-4)
Wi-Fi (2.4 GHz)	On	N/A	Yes (Figure 3-5)
	Off	N/A	No (Figure 3-6)
Wi-Fi (5 GHz)	On	N/A	Yes (Figure 3-7)
	Off	N/A	No (Figure 3-8)

Table 2-2 RF Tests Performed

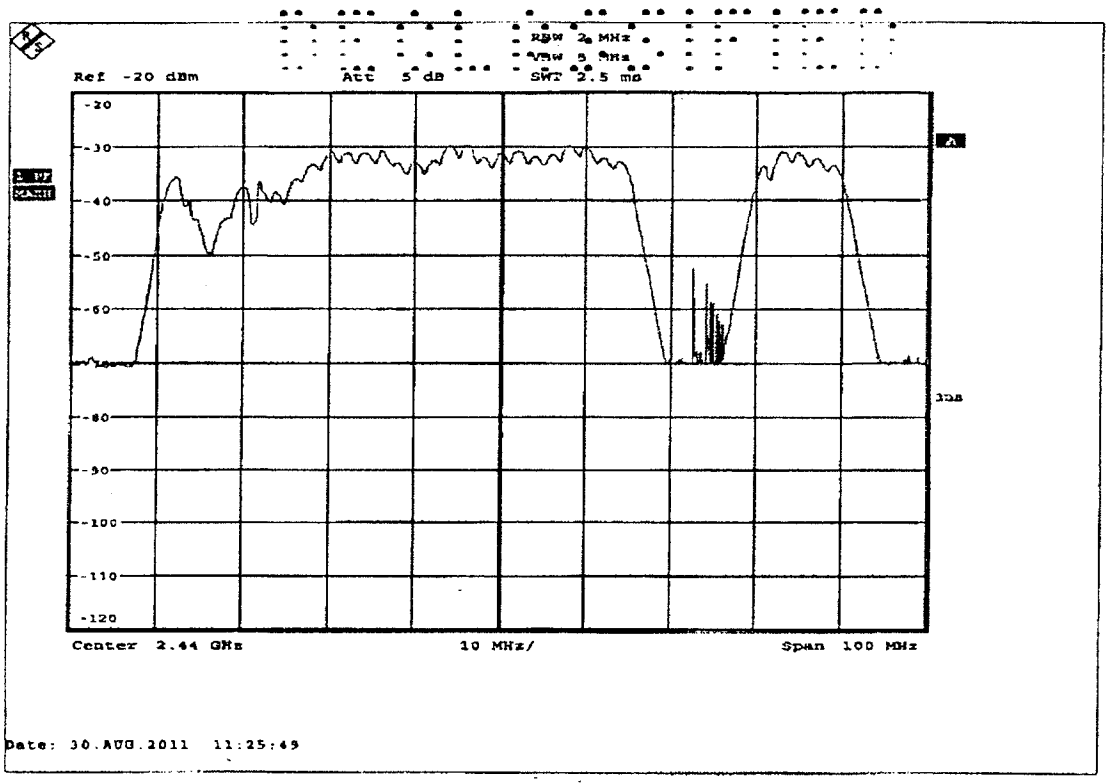


Figure 2-7 Bluetooth – PlayBook on / BlackBerry off

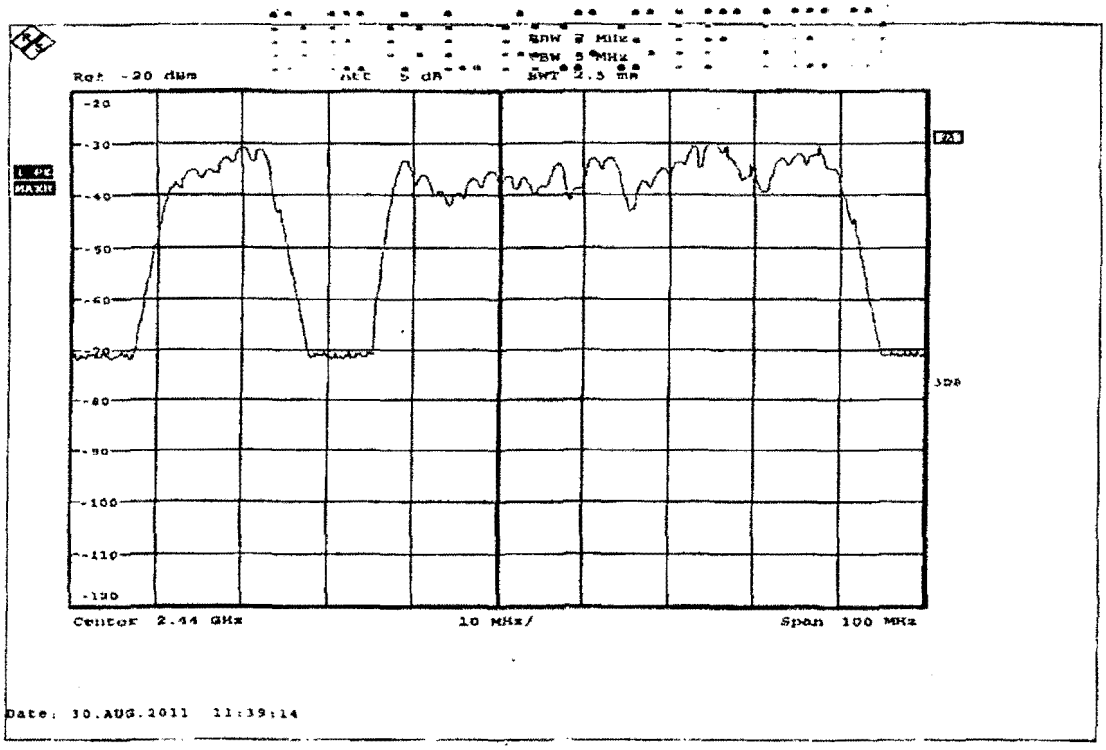


Figure 2-8 Bluetooth – PlayBook off / BlackBerry on

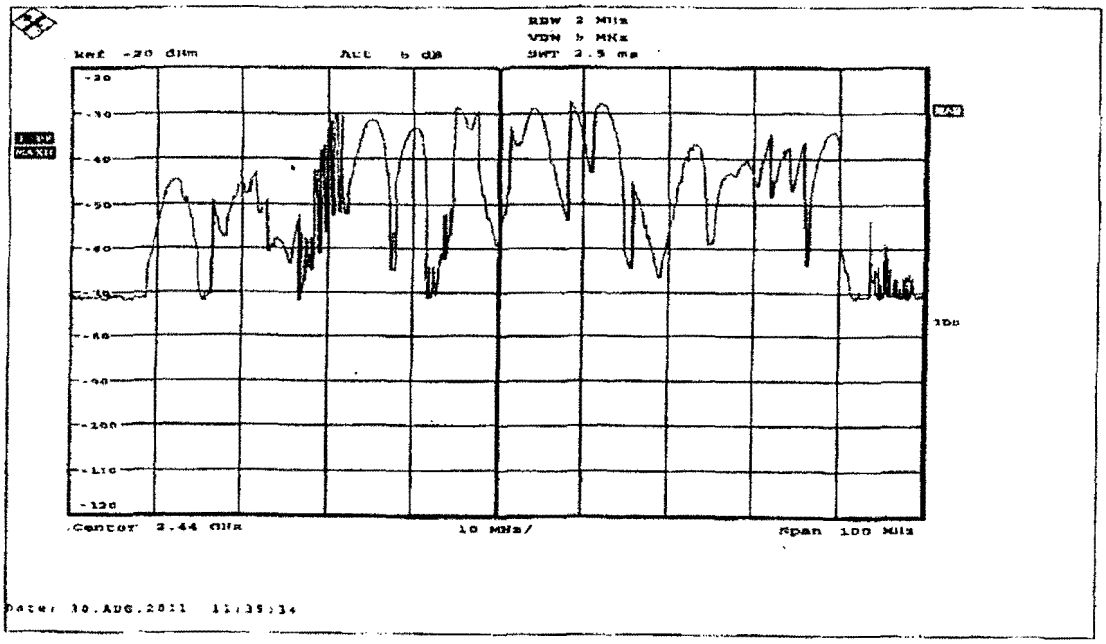


Figure 2-9 Bluetooth – PlayBook on / BlackBerry on while bridged

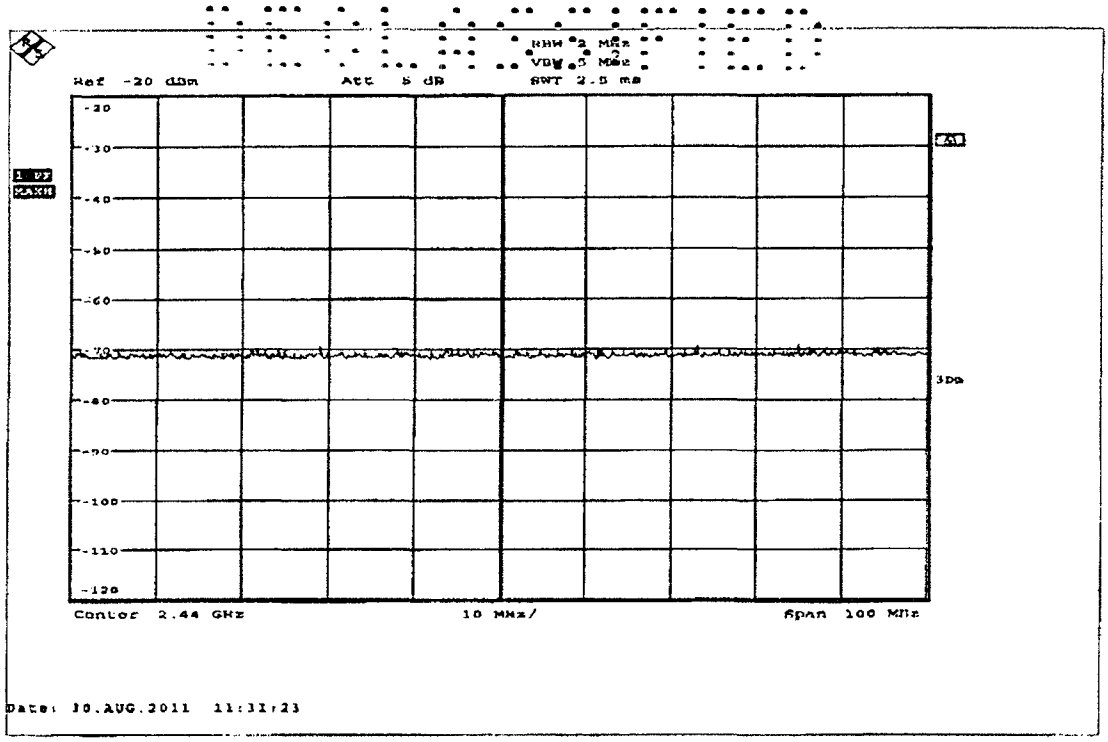


Figure 2-10 Bluetooth PlayBook off / BlackBerry off

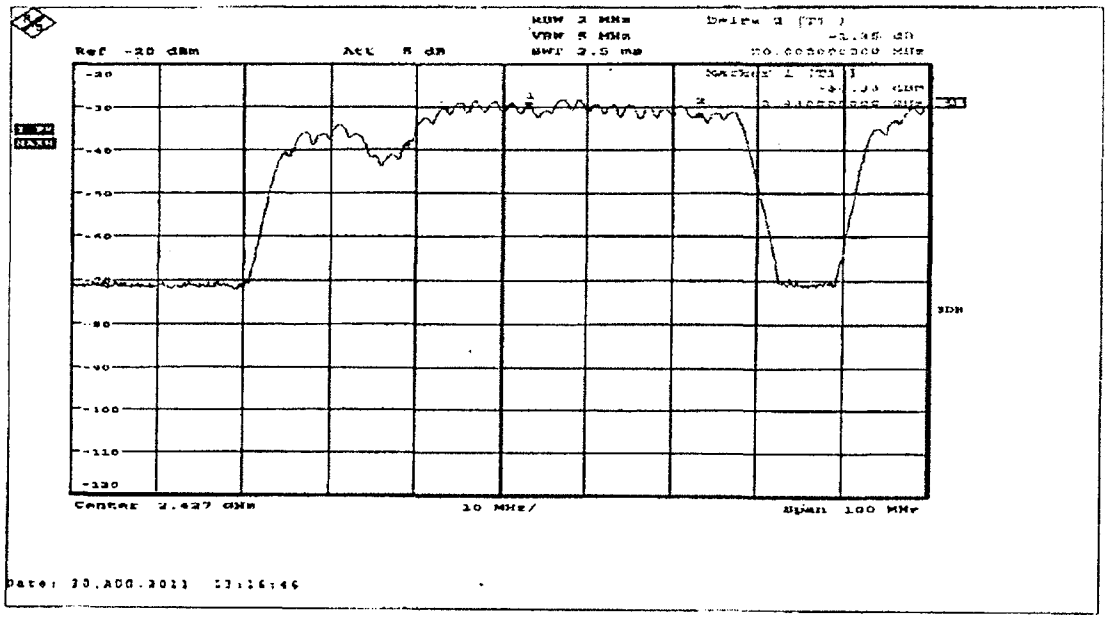


Figure 2-11 Wi-Fi 2.4 GHz PlayBook on (not connected)

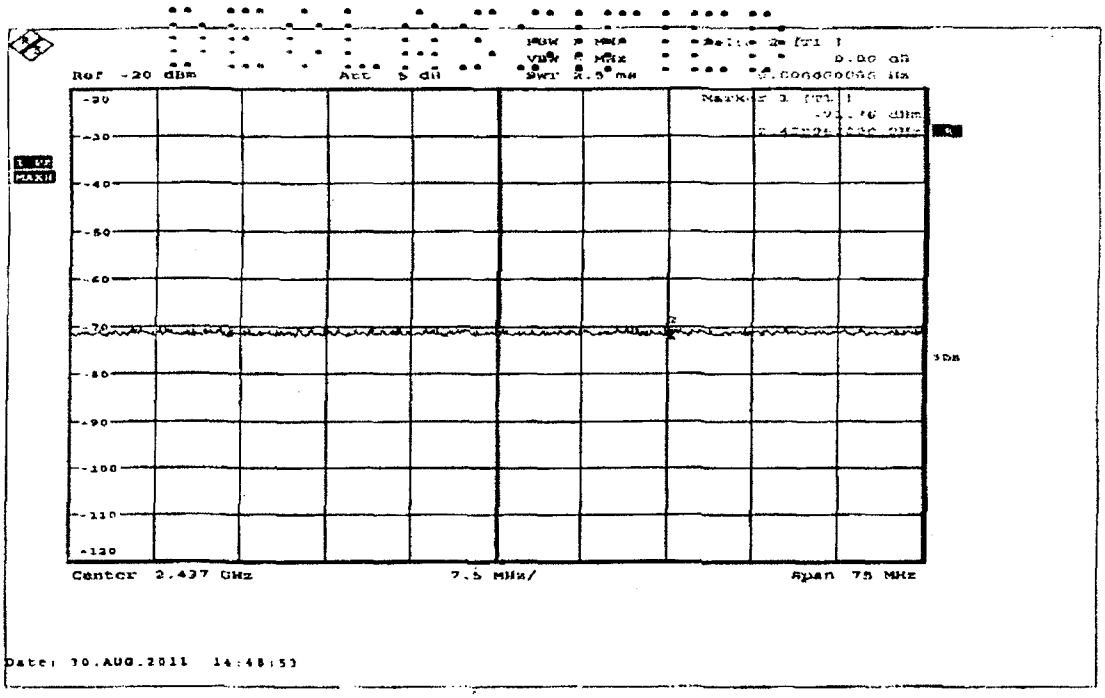


Figure 2-12 Wi-Fi 2.4 GHz PlayBook off

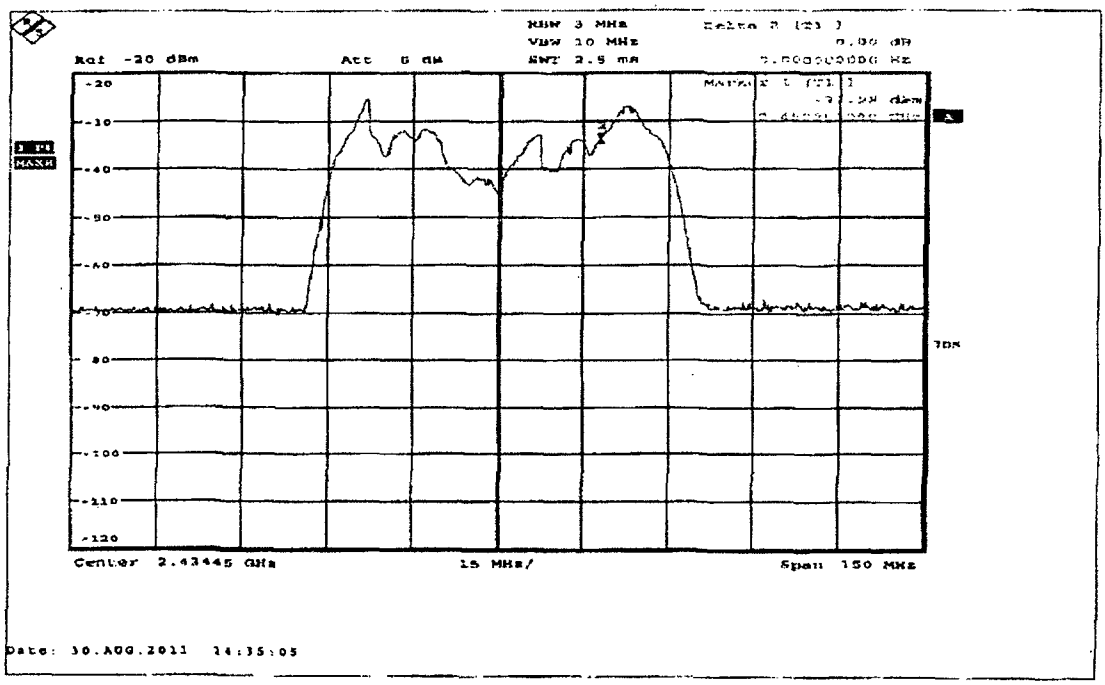


Figure 2-13 Wi-Fi 5 GHz PlayBook on connected to Access Point

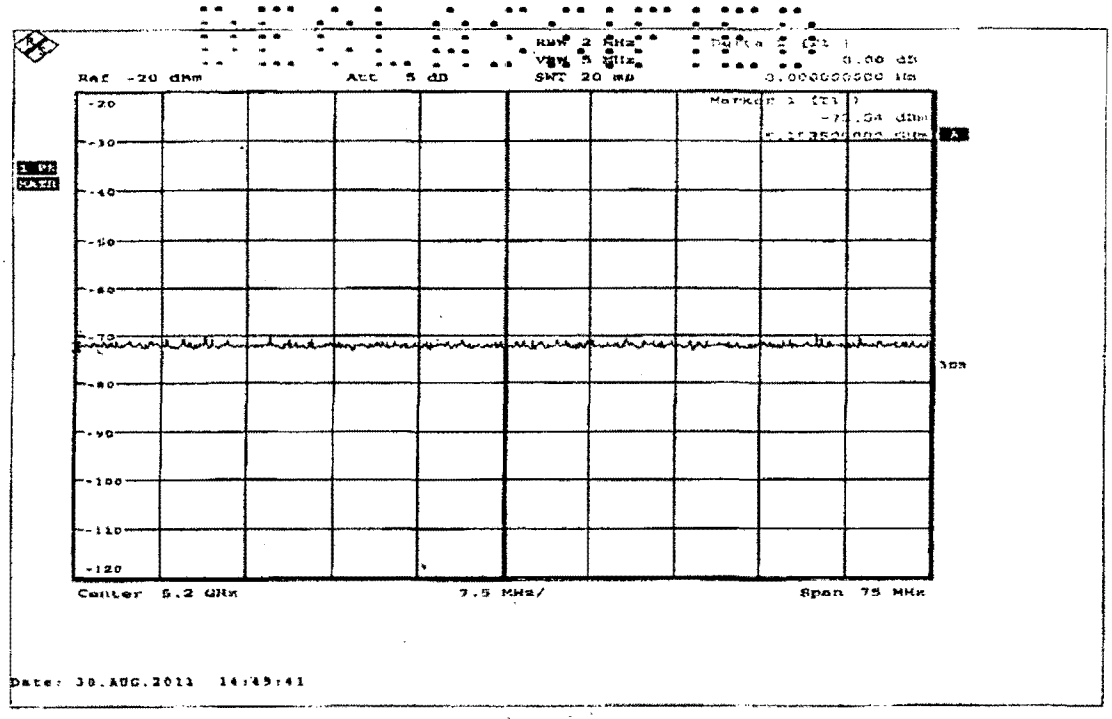


Figure 2-14 Wi-Fi 5GHz with the PlayBook off

2.3.2 Findings

The following represent the major findings of the RF assessment.

- TEB confirmed that when the Bluetooth was manually turned off on the PlayBook device the Bluetooth would not transmit.
- During testing of the Airplane Mode the Bluetooth would initially stop transmitting but the user may turn the transmitter back on by simply re-enabling the Bluetooth while the device still had the Airplane Mode option on.
- There are no user controls to specify what Wi-Fi technology or frequency should be used.
- The user is unable to readily identify what Wi-Fi frequency spectrum or technology is being used.
- When Airplane Mode is enabled the transmitter will turn off and cannot be re-enabled until the Airplane Mode is disabled.

- While the 2.4 GHz radio is the default as long as the PlayBook was connected to a 5 GHz AP it will continue to look in the 5 GHz range but does not change the 2.4 GHz default.
- Class 1 Bluetooth device, able to transmit up to 330 feet or 100 meters away.
- Four Bluetooth profiles identified – **Dial-Up Networking (DUN), Serial Port Profile (SPP), Secure Simple Pairing (SSP), and Human Interface Device (HID)**
- According to FCC report the maximum 2.4 GHz Wi-Fi transmit power out of the device is 310 mW (24.9 dBm). Typical mobile devices transmit around 150 mW by comparison.
- Wi-Fi power levels cannot be controlled on the PlayBook device, thereby preventing the minimization of transmit power levels.
- Airplane mode must be disabled to allow the Wi-Fi connection to transmit.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

4. Appendix

The following presents more detail to the results of the testing TEB performed

4.1.1 Evaluate the identified features and the OS control of those features

Evaluate the identified features of the device in relation to the OS and if setting exist to enable or disable these features. Determine if these features present any vulnerability based on the effectiveness of the settings that are able to be applied.

Prior to BES connectivity, the PlayBook control of Bluetooth was tested. First a Bluetooth connection between the PlayBook and another Bluetooth device was established. Bluetooth was then turned off on the PlayBook.

4.1.1.1 Does it break the Bluetooth connection? ***YES***

4.1.1.2 Can the other device still connect to the PlayBook? ***No***

Prior to BES connectivity, the PlayBook control of Wi-Fi was tested. First a Wi-Fi connection between the PlayBook and Wi-Fi Access Point (AP) was established. The Wi-Fi was then turned off on the PlayBook.

4.1.1.3 Does it break the Wi-Fi connection? ***YES***

4.1.1.4 Can the PlayBook be contacted over the Wi-Fi connection (using the Wi-Fi as a physical layer connection)? ***No***

Prior to BES connectivity, the PlayBook control of file sharing was tested. Establish a Wi-Fi connection between the PlayBook and the Wi-Fi AP. Turn on File Sharing and Wi-Fi Sharing on the PlayBook.

4.1.1.5 Port scan showed no new ports open but a NetBIOS workgroup was detected.

4.1.1.6 The Universal Naming Convention (UNC) provided a connection to the PlayBook with Samba shares.

The Following Shared folders were available

Certs

.metadata_never_index file found in certs directory. The file is blank when opened in Notepad.

Media -
Bookmarks folder (empty)
Books folder (empty)
Camera folder (empty)
Documents folder (empty)
Downloads folder (empty)
Misc folder (empty)
Music folder (empty)
Photos folder (empty)
Print folder (empty)
Videos folder (empty)
Voice folder (empty)
.metadata_never_index file -The file is blank when opened in Notepad.

4.1.1.7 Turning off the Wi-Fi sharing disables the UNC shares.

Connect the PlayBook to a computer over USB to test File sharing over USB.

With file sharing turned off:

- Performed a backup of the device
- Had full access to the media folder access from My Computer as a mapped drive.
  - Bookmarks folder (empty)
  - Books folder (empty)
  - Camera folder (empty)
  - Documents folder (empty)
  - Downloads folder (empty)
  - Misc folder (empty)
  - Music folder (empty)
  - Photos folder (empty)
  - Print folder (empty)
  - Videos folder (empty)
  - Voice folder (empty)
  - .metadata_never_index file

- Able copy/create files from desktop manager

4.1.1.8 With File sharing turned on the same feature are available over the USB connection to the computer.

4.1.1.9 Internet Tethering – not working just over Bluetooth (without a special data plan)

4.1.1.10 Sounds – The sounds section has only volume controls and no master control to turn off the speakers.

4.1.1.11 Microphone – There is no setting to control the microphone

4.1.2 Evaluate BES Direct Control of the PlayBook

- Evaluate the direct control the BES has over the PlayBook. Determine what BES policies control the PlayBook.
  - Only two BES policy groups apply directly to the BlackBerry PlayBook.
    - BlackBerry Bridge Policy Group
      - Enable BlackBerry Bridge
        - This is the only policy rule for this policy group. It applies to the BlackBerry Smartphone and not the PlayBook. The rule specifies whether a BlackBerry Smartphone can run the BlackBerry Bridge application. (This application is required for connection to the PlayBook; however it could be place in the same category as Bluetooth. It affects the BlackBerry smart phone and not the PlayBook itself.)
    - Companion Device Policy Group
      - BlackBerry PlayBook Log Submission
        - This is the only policy rule in this policy group. The rule specifies whether the BlackBerry PlayBook tablet can generate and send log file to the BlackBerry Technical Solution Center.

4.1.3 Evaluate features/capabilities of the user and Work file systems for Vulnerabilities

Determine if the features/capabilities of the user file system may present any vulnerability to the work file system on the PlayBook or the attached BlackBerry. (No work file system exists when the PlayBook is not connected to a BES enabled Smartphone.)

4.1.3.1 File System Access control

- Verify that Work application 1 has read-write access to a work file it created
  - **True**
- Verify that Work application 2 has read-write access to a work file it created
  - **True**
- Verify that Work application 1 has read-write access to a work file that Work application 2 created
  - **True**
- Verify that Personal application 1 has no access to a work file that Work application 2 created
  - **True**
- Verify that Personal application 2 has no access to a work file that Work application 2 created
  - **True**
- Verify that Personal application 1 has read-write access to a Personal file it created
  - **True**
- Verify that Personal application 2 has read-write access to a Personal file it created
  - **True**
- Verify that Personal application 1 has read-write access to a Personal file that Personal application 2 created
  - **True**
- Verify that Work application 1 has read only access to a Personal file that Personal application 2 created
  - **True**
- Verify that Work application 2 has read only access to a Personal file that Personal application 2 created

- **True**
- Verify that Work application 1 has read-write access to the private data of Work application 1
  - **True**
- Verify that Work application 2 has no access to the private data of Work application 1
  - **True**
- Verify that Personal application 1 has no access to the private data of Work application 1
  - **True**
- Verify that Personal application 2 has no access to the private data of Work application 1
  - True

4.1.3.2 Attempt to move data from the Work file system to the Personal file system:

- Try cut/copy/paste operations to copy Work data into Personal files
  - **failed**
- Try to attach work files to personal emails.
  - **Passed** - not able to attach any file (work or personal) to the personal email. The feature does not exist – Had to over ride by using the website version of personal email to use attachments. Could only attach personal files.

4.1.3.3 Attempt to move data from Personal files to Work data

- Try cut/copy/paste operations to copy Personal data into Work files
  - **Failed**
- Verify that a personal file can be attached to work emails.
  - **Passed**

4.1.4 Bluetooth connection vulnerabilities for the PlayBook and Smartphone

- Evaluate the Bluetooth connection as a means to gain entry to the PlayBook or the BlackBerry Smartphone.

4.1.4.1 Prior to BES Connectivity

- Prior to BES connectivity, establish just a Bluetooth connection between the Smartphone and the PlayBook. (both devices are out of box)
  - What services are available?
    - **No available services on either the phone or the PlayBook.**
- Prior to BES connectivity, establish just a Bluetooth connection between the Laptop and the PlayBook. (The PlayBook is out of box)
  - What services are available?
    - **No available services on either the Laptop or the PlayBook.**
- Prior to BES connectivity, establish just a Bluetooth connection between the PlayBook and the BlueTooth Access Point.
  - What services are available?
    - **The PlayBook showed no available services for the AP.**
  - Can the Bluetooth AP be used to connect to the Internet? **No**
  - Can the Bluetooth AP be used to gain access to the PlayBook or BlackBerry Smartphone? **No**
- Prior to BES connectivity, establish just a Bluetooth connection between the PlayBook and a Jabra BT 250v headset. (The PlayBook is out of box)
  - What services are available?
    - **The PlayBook showed no available services for the headset.**

4.1.4.2 After BlackBerry Smartphone is Connected to BES but not the PlayBook

- After BES connectivity is established, attempt to connect a Laptop to the BlackBerry Smartphone.
  - What services are available?
    - **The test BlackBerry Smartphone showed all the service of the attached Laptop**
    - **Connectivity was unstable and the laptop did not load all the drivers properly**
    - **The laptop was unable to connect to the Smartphone for anything**
- After BES connectivity is established, attempt to connect another Smartphone to the BlackBerry Smartphone.

- What services are available?
  - **The test BlackBerry Smartphone showed all the service of the attached Smartphone.**
  - **The attached Smartphone only showed the connection to the test BlackBerry.**
  - **An attempt to send data from the test phone to the attached phone failed**
  - **An attempt to send data from the attached phone to the test phone failed**
- After BES connectivity is established, attempt to connect a Bluetooth headset to the BlackBerry Smartphone.
  - What services are available?
    - **The test BlackBerry Smartphone showed all the service of the attached headset**
    - **The headset was unable to control the BlackBerry Smartphone**
      - **Could not answer calls**
      - **Could not make calls**
      - **Only activity is the Bluetooth icon flashes on the BlackBerry when the headset button is pressed**
- After BES connectivity is established, attempt to connect a Bluetooth AP to the BlackBerry Smartphone.
  - What services are available?
    - **The phone displays the service provided by the Bluetooth AP**
    - **The Bluetooth AP does not show the connection to the**
    - **BlackBerry in the connections table.**
    - **Not under PAN**
    - **Not under LAP & DUN devices**
    - **Not under SPP connections**
    - **The BlackBerry Smartphone does not appear to be providing any services**

4.1.4.3 After PlayBook is Connected to the BES activated BlackBerry Smartphone

- After BES connectivity is established, attempt to connect a Laptop to the BlackBerry PlayBook.
  - What services are available?
    - **None**
- After BES connectivity is established, attempt to connect another Smartphone to the BlackBerry PlayBook.
  - What services are available?
    - **BlackBerry Bridge service offered from the Smartphone**
    - **The PlayBook offered no services**
- Can data from one Smartphone be seen on the PlayBook by the other Smartphone?
  - **No the Data is remove when the Bridge is transferred.**
- After BES connectivity is established, attempt to connect a Bluetooth headset to the BlackBerry PlayBook.
  - What services are available?
    - **None**
- After BES connectivity is established, attempt to connect a Bluetooth AP to the BlackBerry PlayBook.
  - What services are available?
    - **None**
- Attempt to connect one Smartphone to another
  - What services are available?
    - **The BES BlackBerry only provided the serial port But we were unable to send a file to or from it.**

4.1.5 Possible Wi-Fi Connection Vulnerabilities

Evaluate the Wi-Fi connection as a means to gain entry to the PlayBook or the BlackBerry.

4.1.5.1 Determine what connection information could be found external to the PlayBook:

- Current IP address is **192.168.1.82**
- The MAC address is **E8:3E:B6:FA:9B:A9**
- Ping IP address – **device responds to ICMP ping requests**

- Attempt a telnet connection on common ports 20, 21, 22, 23, 24, 80, 81, 443, 8080 – **No connections were able to be established.**
- Use third party software to scan for vulnerabilities over the IP connection.
  - **A port scan of the PlayBook show only that the device responds to ping. It did not provide a hostname or show any open ports, nor show any web content, and no NetBIOS information was provided either.**

4.1.5.2 Turn on file sharing and Wi-Fi sharing.

- Port scan showed no new ports open but a **NetBIOS workgroup** was detected.
- The Universal Naming Convention (UNC) provided a connection to the PlayBook with Samba shares.

Certs

- .metadata_never_index file found in certs directory. The file is blank when opened in Notepad.

Media

- Bookmarks folder (empty)
- Books folder (empty)
- Camera folder (empty)
- Documents folder (empty)
- Downloads folder (empty)
- Misc folder (empty)
- Music folder (empty)
- Photos folder (empty)
- Print folder (empty)
- Videos folder (empty)
- Voice folder (empty)
- .metadata_never_index file -The file is blank when opened in Notepad.

*4.1.5.3 Turning off the Wi-Fi sharing **disables** the UNC shares.*

DECLASSIFIED

TRANSFERRED FOR DIRECT REPLY DS

UNCLASSIFIED

DECLASSIFIED

003 I 15 (P) b7E

RIM BlackBerry PlayBook Evaluation Report

FINAL DRAFT

United States Department of State
Bureau of Diplomatic Security
Directorate of Security Infrastructure
Office of Computer Security

Version 1.0
May 2011

DECLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FINAL DRAFT

UNCLASSIFIED

1 INTRODUCTION

1.1 Purpose

This document provides a hands-on analysis and review of the enterprise security capabilities available within the RIM Blackberry PlayBook tablet device and its suitability for use within the Department of State.

1.2 Scope

The following resources were used in this evaluation report:

- BlackBerry Style 9670 (Device OS v6.0.0.248)
- BlackBerry PlayBook 16GB (Device OS v.1.0.3.1868)
- BlackBerry Enterprise Server (v5.0.2)
- BlackBerry Bridge application for BlackBerry Smartphone (v1.0.0.83)

This review is limited to the applications, features and settings provided in the resources above. Any additional features/capabilities provided via third party applications are beyond the scope of this document.

1.3 Background

The Blackberry PlayBook is the first tablet device released by Research in Motion (RIM) utilizing a new Blackberry Tablet OS based on QNX Neutrino 6.5, a UNIX-like operating system. At a glance, QNX is a highly modular operating system that features a relatively tiny kernel and sandboxing of services to provide enhanced security.

From a hardware perspective, the PlayBook is powered by a 1 GHz Dual-core TI OMAP 4430 processor with 1 GB of RAM. Different PlayBook models are available that contain 16, 32, and 64GB of internal flash memory. The device features a 3 MP front-facing camera and a 5 MP rear-facing camera. Network connectivity is limited to Wi-Fi 802.11 a/b/g/n and Bluetooth 2.1 + EDR. Future models will include support for 4G cellular data capabilities (WiMax, LTE, and HSPA+).

The device includes a single 1/8" headphone jack, micro USB port, micro HDMI port, and a quick-charge port. There are no other USB ports or slots for memory cards.

Compared to Blackberry smartphones released to date, this device carries a greater emphasis on usability as a consumer device.

b7E

2 Analysis

2.1 Device Management

The PlayBook features limited integration with the Blackberry Enterprise Server (BES) via a Bluetooth solution called the *BlackBerry Bridge*. The BlackBerry Bridge is a 256-bit AES encrypted link over Bluetooth between the PlayBook and a BlackBerry smartphone running OS 5.0 or later. The BlackBerry Bridge app must be installed on the BlackBerry smartphone in order to setup the Bridge connection.

There are two new PlayBook-related IT policies added to the BES that control whether supported BlackBerry smartphones can bridge with **any** PlayBook. Other than these two settings, the BES has no direct control or management over any PlayBook devices. This effectively means the non-4G PlayBook in its current form can only be deployed as unmanaged device.

2.2 BES IT Policies

2.2.1 New Policies

The following are new BES IT policies that apply to the PlayBook tablet:

- BlackBerry Bridge Policy Group
  - "Enable BlackBerry Bridge" to specify whether a BlackBerry device can run BlackBerry Bridge
- Companion Device Policy Group
  - "BlackBerry PlayBook Log Submission" to specify whether the tablet can generate and send log files to BlackBerry Technical Solution Center

2.2.2 Modifications to Existing Policies

b7E

2.3 Data Protection

The PlayBook represents a major philosophy change from how data protection is implemented on BlackBerry smartphones. It utilizes a read-only base file system that contains the tablet OS system files. Upon boot up of the device, an integrity check is performed to detect tampering. On top of the base file system are two additional file systems, one for personal applications/data and one for work applications/data coming from a bridged BlackBerry smartphone. The creation of separate file systems is designed to ensure work data coming from a bridged BlackBerry device is kept protected.

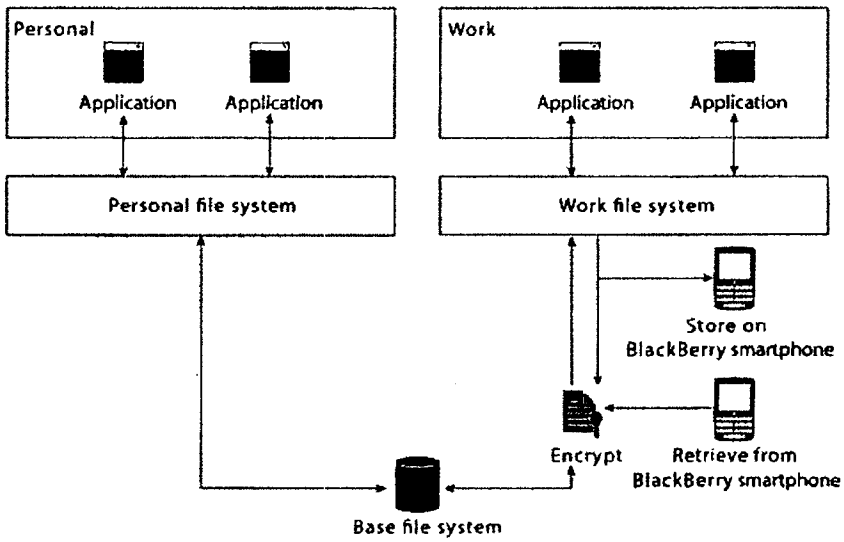


Figure 1. PlayBook File Systems

Breakdown of PlayBook file systems

1. Base file system
    a. Read only and contains system files
    b. Integrity checks are performed at boot time
2. Personal file system
    a. Contains the applications that run in personal mode and personal application data
    b. Users can move data from personal file system to the work file system
    c. Users cannot cut, copy, or paste personal data into a work file
    d. Users can attach a personal file to a work email message or work calendar entry
3. Work file system
    a. Contains applications that run in work mode and work application data
    b. The tablet encrypts (AES-256) the work file system and the decryption key is stored on the smartphone
    c. Work data consists of all email messages, calendar entries, attachments, and any data that is associated with work applications.
    d. Users cannot move data from work file system to personal file system
    e. Users cannot cut, copy, or paste data from a work file to a personal file

2.3.1 Personal Data

The PlayBook comes pre-installed with several applications typical of a consumer-orientated tablet device. This includes multimedia apps such as YouTube, video games like Need for Speed: Underground, and office productivity apps from Documents to Go. In addition to the pre-installed applications included with the PlayBook, additional applications can be downloaded and installed via the BlackBerry App World. Personal data stored on the personal file system is not encrypted. Any personal applications running on the tablet has no access to any work files.

2.3.2 Work Data

Once a BlackBerry Bridge connection has been established, the following bridge applications are available on the PlayBook:

- Messages – Allow users to send and receive messages using email account associated with the smartphone
  - Media card support must be enabled for accessing email attachments
  - Currently unable to edit and save email attachments with an encrypted media card
- Contacts – Allow users to check or edit contacts on the smartphone
- Bridge Browser – Allow users to browse the internet/intranet using the paired smartphone's data plan
  - Bridge Browser maintains separate browsing data from regular PlayBook browser
- Calendar – Allow users to check or edit calendar events on the smartphone
- MemoPad – Allow users to check or edit notes on the smartphone
- Tasks – Allow users to check or edit tasks on the smartphone
- Bridge Files – Allow users to browse and open files stored on the tablet and smartphone media card
  - Media card support must be enabled for browsing content on the smartphone
  - Currently unable to browse encrypted file content stored on smartphone media card
  - Currently only supports PDF and Microsoft Office documents as readable content on unencrypted media card
- BlackBerry Messenger – Allow users communicate virtually instantly with other BlackBerry users
  - Not tested due to incompatible BBM version on the smartphone

2.4 DoD Bluetooth Security Requirements

The following table provides an analysis of how the Playbook meets *Department of Defense (DoD) Bluetooth Peripheral Device Security Requirements (16 July 2010).* The requirements listed below are for the secure use of unclassified Bluetooth peripheral devices. There are 39 total requirements:

- 12 determined as not applicable (N/A)
- 5 cannot be determined (additional analysis may be needed)
- 22 determined to meet the requirements

DoD Bluetooth Security Requirements	PlayBook
Basic Requirements	
1.1 For personal area network applications, Bluetooth devices must use low-power Class 2 or Class 3 Bluetooth radios without external amplifiers or high-gain antennas.	Bluetooth Class 1
1.2 Devices must not use the Bluetooth 3.0 High Speed (3.0 + HS) alternate MAC and PHY or Bluetooth 4.0 Low Energy (LE) technology.	Bluetooth 2.1 + EDR
1.3 Devices must use easily-understandable connection, configuration, and link activity status indicators like LEDs or icons.	Yes
1.4 Devices must only support the minimum number of Bluetooth services required for operational use of approved Bluetooth peripherals. Services should be enabled only while needed. Devices or administrators must reliably disable or delete all unneeded Bluetooth services.	N/A
1.5 Devices or administrators must reliably disable or delete all unneeded Bluetooth user controls, drivers, application programming interfaces, executables, and applications.	N/A
1.6 Devices must use random number values and public/private key pairs that achieve maximum entropy for all cryptographic functions as mandated and defined in the Bluetooth specifications and based on applicable NIST guidelines.	Yes
1.7 Each Bluetooth device intended for use in the DoD should be subjected to an independent security implementation evaluation conducted by one or more qualified and objective individuals approved by DISA Field Security Operations. Evaluators must work with the vendor to mitigate any security deficiencies prior to approval for DoD use.	N/A
1.8 Once approved for DoD use, operational Bluetooth devices and piconets must be independently monitored for unauthorized Bluetooth activity.	N/A
1.9 Bluetooth devices must be transported and stored securely by users and administrators at all times.	N/A
Connectivity Requirements	
2.1.1 Bluetooth devices must not be discoverable (responsive to inquiry messages from other Bluetooth devices) unless absolutely necessary. Ideally devices should never be discoverable.	Yes (user controlled)
2.1.2 Devices must never be discoverable for longer than two minutes at any one time.	Yes
2.2.1 Bluetooth devices must not be connectable (responsive to incoming connection requests from other Bluetooth devices) unless absolutely necessary. Ideally devices should become unconnectable once the connection is established, or should never be connectable if operationally possible.	Yes (user controlled)
2.2.2 Devices should initiate Bluetooth connections only when absolutely necessary. Ideally only one device per Bluetooth piconet should initiate connections to other devices in that piconet.	Yes (user controlled)
2.3.1 Page frames from devices attempting to automatically re-establish Bluetooth links to peripheral devices must be transmitted periodically and not continuously.	unknown
2.3.2 Bluetooth devices must not transmit auto-reconnect frames longer than 30 seconds	unknown

DoD Bluetooth Security Requirements	PlayBook
at any one time or more frequently than once every five minutes.	
2.3.3 Bluetooth devices must never transmit auto-reconnect frames longer than 20 minutes total.	unknown
Authorization Requirements	
3.1 Bluetooth devices must prompt the user to authorize all incoming Bluetooth connection requests before allowing any incoming connection request to proceed.	Yes
3.2 Users must never accept connections, files, or other objects from unexpected, unknown, or untrusted sources.	N/A
Pairing and Authentication Requirements	
4.1.1 During initial Bluetooth connection requests, all Bluetooth devices must pair (mutually authenticate) and bond (store the resulting link key).	Yes
4.1.2 Devices must store link keys securely based on applicable NIST guidance.	Yes
4.1.3 Subsequent to pairing, all Bluetooth devices must again mutually authenticate each other during all connection requests.	Yes
4.1.4 Devices must not delete existing link keys until after a replacement link key is generated successfully.	Yes
4.1.5 All Bluetooth pairing should be done as infrequently as possible, ideally in a secure location (e.g., an indoor non-public area away from windows and behind physical access controls) where attackers cannot realistically observe entry of the passkey or intercept transmitted pairing messages.	N/A
4.1.6 Users or administrators must never enter or confirm pairing passkeys when unexpectedly prompted to do so.	N/A
4.1.7 Users or administrators must immediately remove unused, lost, stolen, or discarded Bluetooth devices from paired device lists.	N/A
4.1.8 Bluetooth devices must use either legacy pairing Security Mode 3 link level security or Secure Simple Pairing Security Mode 4 service level security. See Section 4.2 and 4.3 below for additional guidance on each.	unknown
4.2.1 Bluetooth 2.0 and earlier devices must use Security Mode 3 link level security during legacy Bluetooth pairing.	N/A
4.2.2 Bluetooth devices using legacy pairing must not use or accept unit keys and must use combination keys for link key establishment.	N/A
4.2.3 Devices must use completely random Bluetooth passkeys at least eight digits in length that are newly generated for each pairing exchange. Ideally devices should use random 128-bit binary passkeys. Passkeys must not be valid indefinitely.	Yes
4.3.1 Ideally Bluetooth 2.1 and later devices should use the Passkey Entry SSP association model. Devices may also use Numeric Comparison association model if each digit of the passkey is confirmed individually. Devices may also use the Out of Band association model but only with a tethered, non-wireless interface. Devices must never use the Just Works association model and therefore must immediately discard all unauthenticated Just Works link keys after pairing to terminate such connections.	Yes
4.3.2 Bluetooth devices supporting SSP must use Elliptic Curve Diffie-Hellman (ECDH) public/private key pairs that are unique for each device and must originate from a trusted source.	Yes
4.3.3 Bluetooth devices must store SSP ECDH public/private key pairs securely.	Yes
4.3.4 Host protocol stacks in devices using Security Mode 4 must be sufficiently robust to prevent denial of service and other attacks based on anomalous frames.	unknown
Encryption Requirements	
5.1 All Bluetooth links must use 128 bit Bluetooth encryption.	Yes
5.2 Devices must initiate Bluetooth encryption immediately after the successful completion of mutual authentication.	Yes
Additional FIPS-Certified Cryptography	
6.1 Where practically feasible, all Bluetooth devices must use FIPS 140-2-certified key	Yes

DoD Bluetooth Security Requirements	PlayBook
establishment and encryption layered atop the Bluetooth cryptography specified above for defense in depth.	
6.2 Bluetooth smart card readers intended for DoD use must use FIPS 140-2 certified cryptography.	N/A
6.3 Public/private key pairs used in FIPS-certified cryptography must be unique to each device and must originate from a trusted source.	Yes
6.4 Bluetooth devices must store public/private key pairs and all keys used in FIPS-certified cryptography securely based on applicable NIST guidance.	Yes

2.5 Observations and Concerns

The following are notable observations and security concerns identified with the PlayBook:

2.5.1 Observations

- Each time the BlackBerry Bridge connection is lost or locked, the user is prompted to enter the smartphone password again to access BlackBerry Bridge applications
- Screenshot capability is disabled once a BlackBerry Bridge connection is established with a BES activated device
- Unable to access media files (pictures, music, and video) stored on the smartphone from the PlayBook
- Files can only be downloaded onto the smartphone while browsing the internet/intranet with the Bridge Browser
- The tablet does not store any persistent work data. It caches the data and encrypts it with AES-256 encryption, where the encryption key is stored on the smartphone.
    - Note: Technical verification regarding the clearing of cache data was not performed as part of this evaluation.

2.5.2 Concerns

The following section covers noteworthy security issues with deploying the PlayBook and security controls built-in or available to mitigate those risks.

- **Personal data stored on the PlayBook is not encrypted**. The lack of encryption of personal data opens up the risk that information stored on the device's internal memory may be compromised. For example, users may e-mail SBU information to a personal e-mail account and access that data on the PlayBook. This issue is compounded by the lack of BES support for managing PlayBook devices and the inability to remotely wipe lost or stolen devices.
- **The PlayBook uses a web browser based on the WebKit engine and could be susceptible to future vulnerabilities.** For example, see KB26132.
- **Allowing media card on the smartphone could lead to malware being introduced onto the device and OpenNet.** By allowing removable media cards, users could unknowingly insert a media card that contains malware.

- **Enabling media card support on the smartphone could lead to potential loss of data.**
  - *Mitigation:* Encryption is enabled on the media card to protect data in case it is lost or stolen
- **Allowing Bluetooth connections could lead to potential interception of data between connected devices.**
  - *Mitigation*: The tablet and a smartphone perform two pairing processes to open an encrypted and authenticated connection between each other: a Bluetooth pairing process and a BlackBerry Bridge pairing process that is designed to enhance the level of encryption for the connection
- **Allowing Bluetooth pairing enables the capability for unauthorized Bluetooth devices to be paired with the smartphone.**
  - *Mitigation*: All Bluetooth functionalities are disabled by IT policy with the exception of pairing and serial port profile. A Bluetooth headset was successfully paired with the smartphone, but was non-functional due to headset profile being disabled in the proposed IT policy settings

3 Recommendations

3.1 Policy Recommendations

- **All PlayBook device inventory shall be maintained with the latest released firmware.** In order to ensure the greatest protection against known software vulnerabilities identified within the PlayBook Tablet OS, it is critical that all PlayBook devices consistently be up to date with the latest release of the PlayBook firmware provided by RIM.
- **No SBU information.** No SBU information is authorized to be stored and/or processed on the Personal side of the device.
- **Educate or provide security awareness training to authorized end users regarding acceptable usage of the PlayBook and security best practices.** Deployment and usage of the PlayBook should be consistent and in compliance with as much as possible.
- **Establish a policy for lost or stolen Department-owned PlayBooks.**

3.2 Device Security Recommendations

- Set up a separate BES IT policy group intended only for PlayBook users with the proposed modifications:

3.3 BES IT Policy Recommendations

This section covers the recommended settings for the Blackberry Enterprise Server related to Bluetooth and select security policies related to the PlayBook.

Bluetooth Policy Group

IT Policy Rule	Description	
Allow Outgoing Calls	Specify whether the user can place outgoing phone calls from a Bluetooth enabled BlackBerry device.	
Disable Address Book Transfer	Specify whether to prevent the BlackBerry device from exchanging address book data with supported Bluetooth enabled devices.	
Disable Advanced Audio Distribution Profile	Specify whether a Bluetooth enabled BlackBerry device can use the Bluetooth Advanced Audio Distribution Profile (A2DP) to perform audio streaming via Bluetooth.	

IT Policy Rule	Description	
Disable Audio/Video Remote Control Profile	Specify whether a Bluetooth enabled BlackBerry device can use the Bluetooth Audio/Video Remote Control Profile (AVRCP) to facilitate remote control of audio & video via Bluetooth.	
Disable Bluetooth	Specify whether support for Bluetooth technology is turned off on the BlackBerry device. If the Bluetooth wireless radio is active when the BlackBerry device receives this IT policy rule, the BlackBerry device must be reset manually for the change to take effect	
Disable Desktop Connectivity	Specify whether the BlackBerry device can use Bluetooth technology to connect to the BlackBerry® Desktop Manager.	
Disable Dial-Up Networking	Specify whether a Bluetooth enabled BlackBerry device can use the Bluetooth Dial-Up Networking Profile (DUN).	
Disable Discoverable Mode	Specify whether to prevent a Bluetooth enabled BlackBerry device user from turning on Discoverable mode on their BlackBerry device. Note: A BlackBerry device with Discoverable mode turned on can be discovered by other Bluetooth enabled devices in range of the BlackBerry device.	
Disable File Transfer	Specify whether the Bluetooth enabled BlackBerry device can exchange files with compatible Bluetooth OBject EXchange (OBEX) devices.	
Disable Handsfree Profile	Specify whether to prevent a Bluetooth enabled BlackBerry device from using the Bluetooth Hands Free Profile (HFP) required to enable wireless voice capabilities with most car kits and some headsets.	
Disable Headset Profile	Specify whether to prevent a Bluetooth enabled BlackBerry device from using the Bluetooth Headset Profile (HSP) required to enable wireless voice capabilities with most headsets and some car kits.	
Disable Message Access Profile	This rule specifies whether a Bluetooth device can retrieve email and SMS messages from a BlackBerry device. By default, a Bluetooth enabled device can retrieve email and SMS messages from a BlackBerry device. If you change the value to Yes, a Bluetooth enabled device cannot retrieve email or SMS messages from a BlackBerry device.	
Disable Pairing	Specify whether to prevent a Bluetooth enabled BlackBerry device from establishing a relationship (in other words, pairing) with another Bluetooth device. Note: Set this rule to Yes to prevent the BlackBerry device user from pairing with subsequent Bluetooth devices after the BlackBerry device pairs with an approved Bluetooth device (for example a headset).	

IT Policy Rule	Description
Disable Serial Port Profile	Specify whether to prevent a Bluetooth enabled BlackBerry device from using the Bluetooth Serial Port Profile (SPP) required to establish a serial connection between the BlackBerry device and a Bluetooth peripheral using a serial port interface.
Disable SIM Access Profile	Specify whether to prevent a Bluetooth enabled BlackBerry device from using SIM Access Profile (SAP). Some car kits require SAP to share the SIM card when the car kit initiates dialing.
Disable Wireless Bypass	Specify whether a Bluetooth enabled BlackBerry device can perform wireless bypass over Bluetooth.
Force CHAP Authentication on Bluetooth Link	Specify whether the Bluetooth serial connection to a Desktop must use CHAP authentication.
Limit Discoverable Time	Specify whether the BlackBerry device user can set the Bluetooth discoverable mode option to have no time limit. Set this rule to Yes to permit the user to set the Bluetooth discoverable mode option to have a time limit of 2 minutes or to turn off Bluetooth discoverable mode. The BlackBerry device uses this IT policy rule only if the Disable Discovery Mode IT policy rule is set to No.
Minimum Encryption Key Length	Specify the minimum encryption key length (in bytes) that the BlackBerry device uses to encrypt Bluetooth connections.
Require Encryption	Specify whether a Bluetooth enabled BlackBerry device uses Bluetooth encryption on all connections. Set to Yes to force Bluetooth enabled BlackBerry devices to use Bluetooth encryption on all connections. Note: Requiring Bluetooth encryption on all connections might restrict compatibility with other Bluetooth enabled devices.
Require LED Connection Indicator	Specify whether the LED is required to flash when the BlackBerry is connected to another Bluetooth device.
Require Password for Discoverable Mode	Specify whether the BlackBerry device requires that the user type the BlackBerry device password to enable Discoverable mode. Set to Yes to require the BlackBerry device to prompt the user for the BlackBerry device password to make the BlackBerry device discoverable by other Bluetooth devices. Set to No to permit the BlackBerry device user to turn on Discoverable Mode without entering the BlackBerry device password.

IT Policy Rule	Description	
Require Password for Enabling Bluetooth Support	Specify whether the BlackBerry device requires that the user type the BlackBerry device password to enable Bluetooth support. Set to Yes to require the BlackBerry device to prompt the user for the BlackBerry device password when enabling Bluetooth support. Set to No to permit the BlackBerry device user to enable Bluetooth support without typing the BlackBerry device password.	

Security Policy Group

IT Policy Rule	Description	
Disable External Memory	Specify whether to prevent the expandable memory (microSD) feature from working on supported BlackBerry devices.	
External File System Encryption Level	Specify the level of file system encryption that the BlackBerry device uses to encrypt files that it stores on an external file system. You can use this IT policy rule to require the BlackBerry device to encrypt an external file system, either including or excluding multi-media directories. Warning: This rule works with BlackBerry Desktop Manager Version 4.2 only. Note: The external file system encryption does not apply to files that the BlackBerry device user manually transfers to the external memory device (for example, from a USB mass storage device).	

BlackBerry Bridge Policy Group

IT Policy Rule	Description	
Enable BlackBerry Bridge	Specify whether a BlackBerry smartphone can run BlackBerry Bridge	

Companion Device Policy Group

IT Policy Rule	Description	
BlackBerry PlayBook Log Submission	Specify whether a BlackBerry PlayBook tablet can generate and send log files to the BlackBerry Technical Solution Center	

4 References

- Defense Information System Agency. (n.d.). *DoD Bluetooth Requirement Specifications.* Retrieved from http://iase.disa.mil/stigs/downloads/pdf/dod_bluetooth_requirements_spec_20100716.pdf
- Research In Motion. (n.d.). *BlackBerry Playbook Security Technical Overview.* Retrieved from http://docs.blackberry.com/en/admin/deliverables/26992/BlackBerry_PlayBook-Security_Technical_Overview--1315426-0407044208-001-1.0-US.pdf
- Research In Motion. (n.d.). *BlackBerry Playbook Tablet User Guide.* Retrieved from http://docs.blackberry.com/en/smartphone_users/deliverables/27019/BlackBerry_PlayBook_Tablet-User_Guide--1526983-0418113733-001-1.0-US.pdf
- Shimpi, A. L. (n.d.). *The BlackBerry Playbook Review.* Retrieved from AnandTech: http://www.anandtech.com/show/4266/blackberry-playbook-review