BLACKBERRY OPERATING SYSTEM (OS) 10.3.x SUPPLEMENTAL PROCEDURES

Version 1, Release 3

28 October 2016

Developed by BlackBerry, Ltd. and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. SECURITY READINESS REVIEW

1.1 General

When conducting a BlackBerry 10.3.x OS Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies and provide data from which to predict the effectiveness of the proposed or implemented security measures associated with the BlackBerry 10.3.x OS, its associated network infrastructure, and the individual devices comprising the system.

1.2 Mobile Policy Review

Detailed policy guidance is available on the DISA Information Assurance Support Environment (IASE) website located at:

http://iase.disa.mil/stigs/mobility/Pages/policies.aspx

Use the Mobility Policy STIG to review the General Wireless Policy asset and the Commercial Mobile Devices (CMD) Policy STIG to review the Smartphone Handheld asset.

2. CONCEPTS AND TERMINOLOGY CONVENTIONS

2.1 BlackBerry Enterprise Service

The BlackBerry Enterprise Service (BES) is the Mobile Device Management (MDM) solution for enterprise mobility management of BlackBerry 10 OS. BES allows enterprise security administrators to enforce security policies (e.g., password usage and rules), publish enterprise profiles (e.g., Wi-Fi, VPN, etc.), and manage (e.g., change work password and wipe the work space) BlackBerry 10 devices. Under management of BES, all enterprise data traffic is routed through the enterprise, applying enterprise network controls and traceability. The BlackBerry OS 10.3.x STIG covers the use of BlackBerry 10.3.x devices only when activated with the BES. The BlackBerry 10.3.x devices used in DoD must be activated and managed by the BES.

2.2 BlackBerry Balance

The BlackBerry OS 10.3x STIG is designed to allow users to use BlackBerry 10 devices for both work and personal use. BlackBerry Balance technology distinguishes and separates work and personal data on the device. DoD data is stored and processed in the work space only while device users manage their personal data in the personal space. The DISA SRG requirements apply only to the work space protecting DoD information, and the BlackBerry OS 10.3x STIG contains guidance for securing the work space, unless otherwise specified within this document.

2.3 BlackBerry Bridge

BlackBerry Bridge allows users to pair a BlackBerry smartphone and BlackBerry PlayBook tablet. When paired, users are able to use the BlackBerry PlayBook to access the Internet using the BlackBerry smartphone's connection, control the BlackBerry PlayBook tablet remotely using the BlackBerry smartphone, and share files and data between the devices.

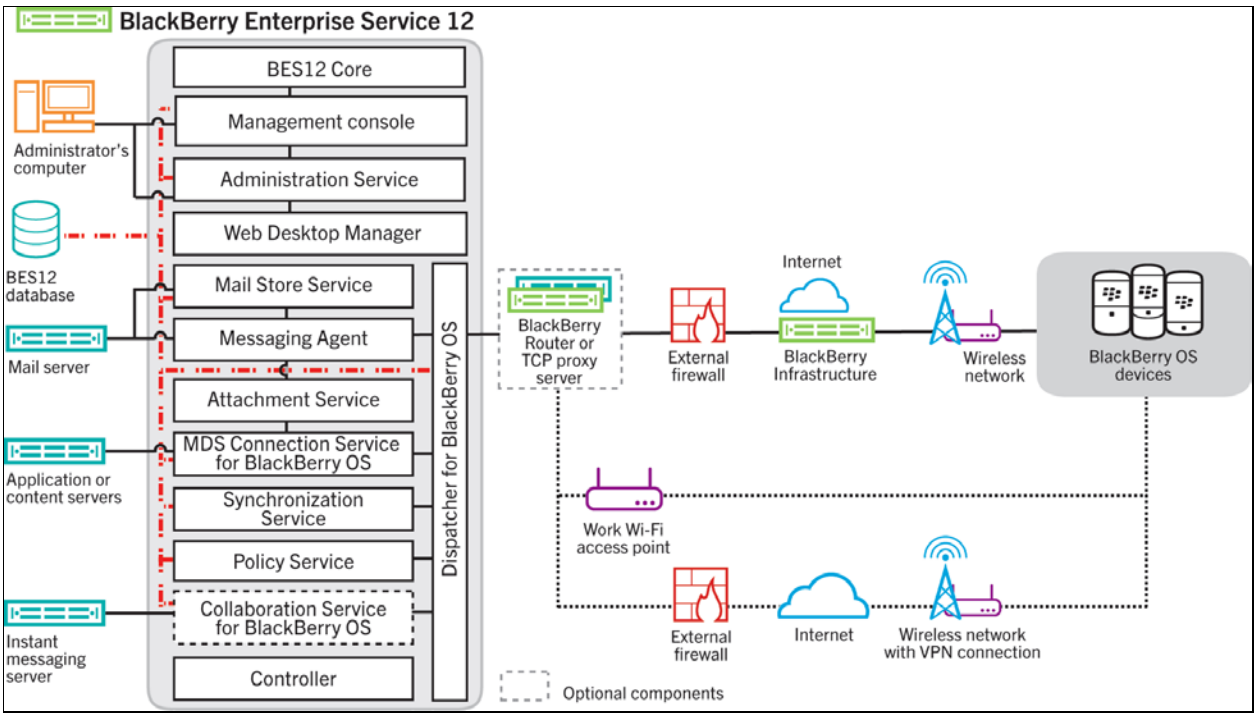
A tablet and a smartphone perform Bluetooth pairing and BlackBerry Bridge pairing processes to open an encrypted and authenticated connection, utilizing Elliptic Curve Diffie-Hellman (ECDH) and Advanced Encryption Standard (AES)-256. All data transferred from the smartphone to the tablet is stored temporarily and protected using XTS-AES-256. The data from the BlackBerry smartphone remains separated between personal and work spaces using BlackBerry Balance technology and is deleted when the Bridge connection is terminated.

Note: The use of a BlackBerry Playbook is not authorized in the DoD. Therefore, BlackBerry Bridge is disabled by this STIG.

3. GENERAL SECURITY REQUIREMENTS

3.1 BlackBerry Architecture

Figure 3-1: Components Used to Manage BlackBerry OS Devices



3.2 Access Control

3.2.1 Password for Personal and Work Space

There are two password protection mechanisms on the BlackBerry 10 device. Users must authenticate using:

- A device password to access the personal space
- A work space password to access the work space

The use of a work space password and its rules are enforced by the BES. The user must create (at minimum) a four-digit password without complexity for the device to protect the personal space, and a six-digit password is required for the work space.

3.2.2 Certificates

Certificates on the BlackBerry 10 device are used to authenticate using the public key when connecting to remote information systems, and with organizational resources such as a messaging server, Wi-Fi network, or VPN. When authenticating using certificates, the certificate

is validated by constructing a certification path with status information to a trust anchor. The OS also verifies the certificate's revocation status before verifying its authenticity. During this process, the BlackBerry 10 device alerts the user and provides the option to deny acceptance of the certificate when:

- The certificate is invalid
- The certificate is issued from an untrusted certificate authority
- The revocation status of the certificate cannot be verified

All private key materials in the key store are encrypted using AES-256 and stored in the encrypted domain of the file system. Files in the encrypted domain are protected by a hierarchy of encryption keys, stemming from the Key Encryption Key (KEK) embedded in the processor during the manufacturing process.

3.3 System and Information Integrity

The integrity of BlackBerry 10 OS is verified during boot-up. If an integrity check failure has been detected during this process, the OS does not boot, preventing a potentially malicious code from executing.

Information about the OS can be obtained on the device from the "Settings" menu by selecting "About". Information such as the OS version is also reported to the BES. When OS updates (including security patches to remediate flaws) are published, device users receive a notification of the availability, and upon user initiation, the updates are downloaded and installed. BlackBerry 10 device users are required to update the operating system to the latest DoD-approved software, currently at version 10.3.x.

The internal clock of BlackBerry 10 OS must be synchronized with an authoritative time server.

There are two separate browsers on BlackBerry 10 OS, one each for personal and work spaces. While the work space browser directs all its traffic through DoD infrastructure, the personal space browser does not. The personal space browser cannot be removed at this time.

3.4 Anti-Virus Software

BlackBerry OS devices do not require anti-virus software. BlackBerry OS devices meet the virus protection requirement of DoDI 8500.01 with a combination of security policies, application sandboxing, and code signing. These technologies help contain malware and control its ability to install itself on a BlackBerry OS device and gain access to applications and data, device resources, and DoD networks.

3.5 Software Updates

Keeping BlackBerry OS up to date ensures that it has the latest enhancements and security controls in place. BlackBerry OS is signed and activated by BlackBerry for each device to ensure

its integrity. This STIG requires that all updates come from an approved source. BlackBerry is considered a DoD-approved source. BlackBerry-provided updates can be installed on BlackBerry OS devices when available, with the exception that users should not install the next major release until authorized to do so.

4. CORE AND PREINSTALLED APPLICATIONS[1]

4.1 Disabled Applications

Table A-1 lists core and preinstalled applications that should be disabled. Risk in using these apps in the DoD environment is considered to be high. DoD Commands and Agencies should fully vet these apps, using the Application Software Protection Profile (APPSWPP), prior to approving their use.

4.2 Enabled Applications

Table A-2 lists core and preinstalled applications that are recommended for approval. DoD Commands and Agencies should consider vetting these apps using the APPSWPP.

4.3 Auditing/Reviewing Device Applications

Applications in the work space are controlled by an application whitelist (install/uninstall). Only those applications added to the enterprise application list (BlackBerry World – Work), by authorized administrators, can be downloaded and installed in the work space on managed devices. The use of IT Policies can help limit the risk of installing undesirable/unapproved applications, by restricting the use of development mode, and preventing the installation of applications from sources that have not been approved by DoD. In these cases, the "application" icon may still be present, but the user may not be able to activate some, or all, of the features of the application. For example, the BlackBerry Assistant can be used in both the personal and work space; however, the voice dictation functionality for the work space is disabled by IT policy. User-based enforcement may also be required for some applications, which may be available through approved application repositories, such as BlackBerry World. A Blacklist of applications should be maintained by administrators, as reference, to ensure that undesirable/ unapproved applications are not inadvertently added to BlackBerry World – Work, and to assist in auditing applications that have already been added to BlackBerry World – Work, or that have been downloaded and installed on BlackBerry devices, in either the personal or work spaces.

The following procedures are recommended for performing an audit/review of applications on BlackBerry devices:

1. Installed applications in the work space
   - Review the list of applications listed on the whitelist on the BES12 Administration console.

[1] A core app is defined as an app bundled by the operating system vendor, for example, BlackBerry Messenger. A preinstalled app is included on the device by a third-party integrator, including the device manufacturer or cellular service provider, for example, BlackBerry, Verizon Wireless, or AT&T.

- Verify all apps on the list have been approved by the Authorizing Official (AO)
  Note: Core and preinstalled applications included in Table A-2 are considered approved for DoD use unless expressly disapproved by the AO.

2. Core and preinstalled applications, and applications installed in the personal space
   - View the blacklist of applications maintained by the Enterprise Administrator:

     - Unlock the BlackBerry device and swipe through the application windows in the personal space.
     - Delete any applications installed on the device that are in the blacklist.
     - Switch to the work space and swipe through the installed applications.
     - Delete any applications installed in the work space that are in the blacklist.

   - Generate a list of applications installed on the BlackBerry device:

     - Unlock the BlackBerry device and swipe through the application windows in the personal space.
     - Switch to the work space and swipe through the installed applications.
     - Remove any app on the whitelist and any app in Table A-2 from this list.
       Note: The whitelist may include approved installed, core, and preinstalled apps.
     - Verify all apps remaining on the list of installed applications on the device have been approved by the AO.

APPENDIX A: APPLICATION LISTS

Table A-1: Applications Recommended for Disapproval

Application Package Name	Application Name	Installed in	
		Personal Space	Work Space

Currently there are no applications preinstalled on BlackBerry 10 OS devices that are recommended for Disapproval.

Note: This is a recommended list that can be changed based on local approval.

Table A-2: Applications Recommended for Approval

Application Package Name	Application Name	Installed in	
		Personal Space	Work Space
com.rim.bb.app.adobeReader	Adobe Reader	X	X
sys.search	Assistant	X	X
com.amazon.mShop.android	Amazon	X	
com.amazon.venezia	Appstore (Amazon)	X	
sys.bbm	BBM	X	
sys.fuse	BlackBerry Fuse (Blend)	X	X
sys.pim.messages	BlackBerry Hub	X	X
sys.appworld	BlackBerry World	X	
sys.enterpriseappworld	BlackBerry World - Work		X
sys.cfs.box	Box	X	
sys.browser	Browser	X	X
sys.calculator	Calculator	X	
sys.pim.calendar	Calendar	X	X
sys.camera	Camera	X	X
sys.clock	Clock	X	
sys.compass	Compass	X	
sys.cfs.dropbox	Connect to Dropbox	X	
sys.pim.contacts	Contacts	X	X
DTGLauncher_arm	Docs To Go	X	X
com.evernote	Evernote	X	
com.rim.bb.app.facebook	Facebook	X	
sys.perimeterbrowser	File Manager	X	X
com.foursquare.blackberry	Foursquare	X	
sys.help	Help	X	X

Application Package Name	Application Name	Installed in	
		Personal Space	Work Space
com.linkedin	LinkedIn	X	
bbmaps	Maps	X	X
sys.airtunes	Music	X	
sys.rim.bb.app.passwordkeeper	Password Keeper	X	
sys.phone	Phone	X	
sys.pictures	Pictures	X	X
sys.pim.remember	Remember	X	X
sys.settings	Settings	X	
sys.setupbuffet	Setup	X	
sys.simtoolkit_ui_app	SIM	X	
sys.smarttags	Smart Tags	X	
sys.movie_magic	Story Maker	X	
sys.chat	Text Messages	X	
sys.howto	Tutorials	X	X
com.twitter	Twitter	X	
sys.videoplayer	Videos	X	
sys.weather	Weather	X	
sys.uri.youtube	YouTube	X	
Com.synchronoss.BackupAssistant	Verizon Cloud	X	
com.vzw.hss.myverizon	My Verizon Mobile	X	
ATT_T_FamilyMap	AT&T Family Map	X	
myATT	myAT&T	X	
ATT_Classic_Help	Device Help	X	
ATT_Passport_Help	Device Help	X	