Is Blackberry Dead?

An Introduction to Blackberry 10 Security (BB10 - QNX)

Alex Plaskett - 2013
Introduction

• Technical Research Into BB10 (QNX Platform)
• Application Security Features
• Enterprise Features Introduction
## Blackberry Background

### Worldwide Smartphone Sales to End Users by Operating System in 4Q12 (Thousands of Units)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>4Q12 Units</th>
<th>4Q12 Market Share (%)</th>
<th>4Q11 Units</th>
<th>4Q11 Market Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>144,720.3</td>
<td>69.7</td>
<td>77,054.2</td>
<td>51.3</td>
</tr>
<tr>
<td>iOS</td>
<td>43,457.4</td>
<td>20.9</td>
<td>35,456.0</td>
<td>23.6</td>
</tr>
<tr>
<td>Research In Motion</td>
<td>7,333.0</td>
<td>3.5</td>
<td>13,184.5</td>
<td>8.8</td>
</tr>
<tr>
<td>Microsoft</td>
<td>6,185.5</td>
<td>3.0</td>
<td>2,759.0</td>
<td>1.8</td>
</tr>
<tr>
<td>Bada</td>
<td>2,684.0</td>
<td>1.3</td>
<td>3,111.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Symbian</td>
<td>2,569.1</td>
<td>1.2</td>
<td>17,458.4</td>
<td>11.6</td>
</tr>
<tr>
<td>Others</td>
<td>713.1</td>
<td>0.3</td>
<td>1,166.5</td>
<td>0.8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>207,662.4</strong></td>
<td><strong>100.0</strong></td>
<td><strong>150,189.9</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Source: Gartner (February 2013)
Blackberry 7

BB7 Features

- Blackberry Proprietary OS
- Java Applications
- CESG Approved (RESTRICTED)
- No Modern Exploit Mitigations - DEP/ASLR (pwn2own 2011)
- Never publically rooted
Blackberry Playbook

Playbook Features

• QNX (6.5 sp1) based
• Rooted via Samba (Dingleberry)
• Backups were unsigned!
Blackberry 10

BB10 Features
• QNX 8.0
• Playbook Similarities
• Not rooted (yet.. 😊)

BlackBerry software ruled not safe enough for essential government work
CESG rejects BB10 software in new Z10 handset, dealing blow to Canadian firm in key market
CESG’s response:

"Discussions with BlackBerry are ongoing about the use of the BlackBerry 10 platform in government. We have not yet performed an evaluation of the security of the platform, but we expect to be issuing Platform Guidance in the summer. This will cover a number of platforms, including BlackBerry 10 (and the use of 'Balance').

We have a long-standing security partnership with BlackBerry, and this gives us confidence that the BlackBerry 10 platform is likely to represent a viable solution for UK Government."
QNX Architecture
QNX History

• First version released in 1982
• Late 1980’s largely rewritten (QNX 4.0)
• 2007 QNX released its source code (QNX 6.*)
• 2010 RIM acquired QNX Software Systems (Source Code access restricted)
• 2013 BB10 (QNX 8.0) released
QNX Architecture

Operating system – QNX Neutrino RTOS

Advanced runtime technologies
- Adaptive partitioning
- Fast boot

Wireless and secure networking
- Multi-core

High availability
- POSIX utilities
- File systems

Memory protected applications

HMI technologies
- Device drivers
- Networking

Secure kernel space

Messaging layer

QNX Neutrino RTOS microkernel

QNX board support packages

Processor architectures
- x86
- SH-4
- PowerPC
- MIPS
- ARM
QNX Message Passing

Diagram showing the flow of message passing in QNX, with components such as Microkernel, POSIX Mqueue, Filesystem, Process manager, Serial driver, SCSI driver, and Application.
How this actually works

```c
mmap(void *addr, size_t len, int prot, int flags, int fd, off_t off)
{
  ..
  MsgSend(MEMMGR_COID,..);
}
```
Syscall Transition

LOAD:000483A0 MsgSend proc near ; DATA XREF: ...
LOAD:000483C3 jz short loc_483D8
LOAD:000483C5 mov ecx, esp
LOAD:000483C7 sysenter
Resource Managers

\target_10_1_0_1020\qnx6\usr\include\sys\memmsg.h

User Process

malloc()
mmap()
MsgSendv()
return msg.o.addr;

_Process Manager_

MsgReceivev()
memmgr_map()
vmm_mmap()
map_create()
MsgReplyv()
pa_alloc()
pte_manipulate()

community.qnx.com/...Microkernel.../Webinar_kernel_oct07_final.ppt
Process Manager
Resource Managers

- **Resmgr_attach** – Register for path in pathname space
- **iofunc_func_init** – Initialize the POSIX-layer function table
- **Message_attach** – Attaches a handler to a message range
Kernel Comparison

Monolith Kernel (Android)  Microkernel (QNX)
Microkernel Security Advantages

- Minimal Size of Trusted Computing Base (procnto)
- Principle of Least Privilege
- Division of Responsibilities
- Fault Tolerant
## Simulator Process Listing

<table>
<thead>
<tr>
<th>Process</th>
<th>Count 1</th>
<th>Count 2</th>
<th>Count 3</th>
<th>Count 4</th>
<th>Count 5</th>
<th>Count 6</th>
<th>Count 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>procnto-smp-instr</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>devc-con</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pci-bios</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>slogger2</td>
<td>26</td>
<td>25</td>
<td>26</td>
<td>25</td>
<td>26</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>pipe</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>devb-edge</td>
<td>132</td>
<td>132</td>
<td>132</td>
<td>132</td>
<td>132</td>
<td>132</td>
<td>132</td>
</tr>
<tr>
<td>m_resource_manager</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pps</td>
<td>339</td>
<td>86</td>
<td>339</td>
<td>86</td>
<td>339</td>
<td>86</td>
<td>339</td>
</tr>
<tr>
<td>perimeter_mgr</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>authman</td>
<td>0</td>
<td>0</td>
<td>505</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ves-server</td>
<td>99</td>
<td>0</td>
<td>99</td>
<td>0</td>
<td>99</td>
<td>0</td>
<td>99</td>
</tr>
<tr>
<td>battmgr</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>io-usb</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dumper</td>
<td>27</td>
<td>412</td>
<td>27</td>
<td>412</td>
<td>27</td>
<td>412</td>
<td>27</td>
</tr>
<tr>
<td>io-hid</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>devc-ser8250</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>screen</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>drmclock</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>random</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>coreServices2</td>
<td>0</td>
<td>32</td>
<td>31</td>
<td>32</td>
<td>0</td>
<td>32</td>
<td>0</td>
</tr>
</tbody>
</table>
But what does this actually mean?

- Microkernel attack surface minimised (77 syscalls vs Linux 338)

- However, 27+ processes running as EUID 0 (root!)

- Already found some issues (kernel panics)

- Cross-Process messaging based attacks in future?
Application Security
BB10

- C/C++ Native SDK
- C++/Qt Cascades
- HTML5/WebWorks
- Adobe Air

BB7

- Java
- Android Java Runtime
BB10 Application Security

• Application Sandbox
• Application Code Signing
• Application Permissions
Application Sandbox

• Applications are installed into /apps/

• Apps cannot read another applications code (/apps) or data (/accounts/*/appdata).

• OS permissions and Authman enforce this
## Application Sandbox

<table>
<thead>
<tr>
<th></th>
<th>BB10</th>
<th>iOS</th>
<th>Android</th>
<th>WP8</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPC</td>
<td>Yes</td>
<td>Disallowed</td>
<td>Yes</td>
<td>Disallowed</td>
</tr>
<tr>
<td>URL Handlers</td>
<td>No * (built in ones)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File Handlers</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Application Code Signing

- Applications need signed before they can run on a BB10 device
- Developer devices can side load and run unsigned code using a debug token.
- Blackberry World used for distribution
# Code Signing Comparison

<table>
<thead>
<tr>
<th></th>
<th>BB10</th>
<th>iOS</th>
<th>Android</th>
<th>WP8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unsigned Code</strong></td>
<td>Debug Token (Free)</td>
<td>Dev unlock (Non-Free)</td>
<td>Yes</td>
<td>Dev Unlock (Non-Free)</td>
</tr>
<tr>
<td><strong>Mandatory Application Code Signing</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (but self-signed is allowed!)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Code Signing Differences

• QNX executable binaries do not require code signing for devuser or a debug token
• Possible to SCP these to BB10 device
• Anyone can dev unlock a device and do this (free).

• Useful for testing local exploits / jailbreaks! 😊
Blackberry World Communication

- Downloads applications in Plaintext HTTP
- Applications are integrity checked (code signed)
- However, applications are not encrypted / obfuscated (iOS and WP8 are)
- Reverse engineer!
Application Permissions

• Security and privacy critical functionality

• User prompted on installation

• Developers specify permissions in the bar manifest

<permission>read_device_identifying_information</permission>
Application Permissions (Unique Feature)

Permission Details

Facebook
Research In Motion Limited
10.0.0.71

Location
On
Allows this app to access your device’s current or saved locations.

Shared Files
On
Allow this app to access your pictures, music, documents, and other files stored on your device, at a remote storage provider, on a media card, or in the cloud.
Application Permissions Implementation (MAC)

- `/etc/authman/sys.res` use_camera:
  - `prompt *` allow sys.*

Allow – means the identified apps can use the permission
Deny – means that capability cannot be used by the app
Prompt – means that the app must prompt the user first
Application Permissions Implementation (MAC)

- /etc/authman/sys.acl

use_camera
  MAC macro_access_camera_service

macro_access_camera_service
  ACL rw /dev/camera/front1
  ACL rw /dev/camera/rear1
Enterprise Security
BES 5

• Only supports BB7
• Granular device policies
• Blackberry attachment service (vulnerabilities)
BES 10

- Supports Android, iOS, BB10 MDM
- Not backwards compatible with BB7
- Can be installed on the same server as BB5 potentially.
Blackberry Balance

Personal

Work
Blackberry Balance

- Creates separate user accounts, groups and data stores for work data
- Separate ACL for Authman (/etc/authman)
- Even restricts copy / paste
- Classifies data based on source
- Remote wipe of only work data
Blackberry World for Work

• Enterprise Application Store

• Approved Work Applications / Company Applications
Data Protection

• Device Encryption (XTS-AES-256)

• SD Card Encryption

• Application Crypto APIs
Conclusions

• Early Days

• Large number of security controls implemented

• QNX architecture weaknesses?
Questions?