BLACKBERRY IOT SECURITY

OVERVIEW

January 2020
Problem: Ensuring Trust in an Evolving World of Connected Things
Inevitability → vulnerabilities will be found

BlackBerry Approach → defense in depth

• *create security in layers* that make leveraging vulnerabilities difficult/impossible
• *reduce the attack surface* so fewer vulnerabilities are accessible
• *introduce barriers and checks* that protect the platform even after an attacker finds a vulnerability
• *monitor for key signs of exploit* and supports remote *integrity attestation*
SECURITY FEATURES AND BEYOND

✓ BlackBerry platform hardening goes beyond end-point software features to address secure development, manufacturing and repair.

✓ Security features span the entire end-point software stack from bootchain to application software.

✓ Security is a principal concern even for non-security features.

✓ Beyond software features: BlackBerry platform hardening also address process via Secure Manufacturing.

BLACKBERRY PLATFORM HARDENING LAYERED ARCHITECTURE

SECURITY FEATURES SPAN STACK

DEVICE

- BlackBerry Security Suite
- 3rd Party Applications
- System Services
- Runtime
- libc
- init
- Boot Chain
- Hardware

BLACKBERRY

- Privileged Operations
- Secure Activation
- Device Identity
- Secure Manufacturing & Provisioning

✓ Security features span the entire end-point software stack from bootchain to application software.

✓ Security is a principal concern even for non-security features.

✓ Beyond software features: BlackBerry platform hardening also address process via Secure Manufacturing.
Platform Hardening

“Platform hardening is a litany of features spread across the Linux kernel and userland “

**KERNEL HARDENING EXAMPLES**
- Ensuring no kernel pages are RWX
- Ensuring kernel configuration for production devices has properly disabled debug interfaces
- Ensuring kernel modules can only be loaded from trusted filesystems
- ...

**USER SPACE HARDENING FEATURES**
- Ensuring executables only be loaded from trusted filesystems
- Randomizing the address space layout of processes
- Throttling service automatic restart with a sequential back off
- ...

...
In the first Secure IoT Accelerator drop

- BlackBerry will provide a subset of the kernel hardening features listed above.

- There will be an interface to the eSIM element.

- The OS security (in this release and later) should be transparent to the applications you develop, but should make it harder for attackers that might try to exploit the platform.

- OS security can only help when applications are designed and written securely. So please: create a threat model of your applications, end points and the back-end, and design mitigations that protect the system end-to-end from day one. Use mechanisms like discretionary access control, and firmware security to make your product robust.