BlackBerry
Intelligent Security. Everywhere.

Solution Brief

Embedded / Internet of Things Security Service

Business Challenge

By 2023, global spending on Internet of Things (IoT) devices will exceed $1 trillion annually[1]. By 2025, the number of IoT devices in the field will reach 25 billion[2] and generate over 79 zettabytes (ZB) of data[3]. These network-connected devices will be extremely diverse, ranging from smart home products, to medical devices, to autonomous vehicles, to factory-floor robotics systems that utilize networks of sensors to optimize manufacturing processes in real time.

Yet, widespread concerns remain about the vulnerability of IoT devices to cyber attacks. According to Bain and Company[4], "Security remains the leading barrier for IoT adoption". These concerns are well-founded. According to a Ponemon Sullivan Privacy Report[5], the number of organizations that sustained IoT-related data breaches increased from 15% of those surveyed in 2017 to 26% of respondents in 2019. The prospects of successful attacks can only increase as threat actors continue developing tactics, techniques, and procedures (TTPs) that are explicitly designed to compromise IoT devices.

As noted in the BlackBerry 2020 Threat Report:

- New versions of Mirai malware targeting enterprise-level IoT hardware[6] have surfaced since 2016, when Mirai was implicated in one of the world's most prolific distributed denial of service (DDOS) botnet attacks.
- First discovered in 2014, Gafgyt malware has been updated as recently as September 2019. The malware uses remote code execution exploits to access and recruit routers into its IoT botnet.

The National Institute of Standards and Technology (NIST) has urged federal agencies, IoT device manufacturers, and systems integrators to assess the risks to data security and data privacy posed by their IoT devices and to develop mitigation strategies to address them[7].

BlackBerry Embedded/IoT (E/IoT) Security consultants help organizations safely pursue their goals for digital transformation by providing in-depth security assessments and remediation solutions for IoT devices that span the chipset to the enterprise.

BlackBerry Approach To Embedded/IoT Security

To identify device vulnerabilities, BlackBerry E/IoT Security consultants employ the same penetration testing and reverse engineering methodologies utilized by real-world threat actors and security researchers alike. Both remote and local attack vectors are assessed during an engagement. Organizations sometimes assume, incorrectly, that their physical security controls prevent local attacks. Unfortunately,

well-funded threat actor groups can acquire devices relatively easily by posing as legitimate businesses or by purchasing them on eBay and other online sales platforms.

Threat actors can afford to spend months testing and reverse engineering a device. E/IoT consultants must achieve the same results in a matter of weeks. Therefore, BlackBerry recommends a white box testing approach that grants consultants access to all pertinent device firmware images, technical documentation, and source code assets at the beginning of every engagement. This makes it possible for consultants to acquire a deep understanding of the device quickly, which is essential for cost-effective vulnerability discovery and maximizing the client's return on investment.

Vulnerability criticality scores are based on the Common Vulnerability Scoring System (CVSS) standard, but also reflect the practicality of the exploitation vectors available and the potential impacts on data confidentiality, integrity, and device availability. Criticality factors include the levels of access required, the sensitivity of the device and its data, as well as the extent to which the device can access other systems and the supporting infrastructure.

Assessment Methodologies

E/IOT consultants test device components and systems both individually and in combination to ensure all significant vulnerabilities are identified and assessed. The following attack surfaces are analyzed in a typical assessment:

Hardware

E/IoT consultants enumerate the components on the device's printed circuit board (PCB), including the microcontroller unit (MCU), systems on a chip (SOC), flash memory, etc. Chipsets with known vulnerabilities are identified and flagged. For example, some chip-level components are known to be vulnerable to fault injection and side channel analysis. Fault injection, also known as clock or voltage glitching, can cause a device to skip an instruction, resulting in an authentication bypass. During side channel analysis, attackers attempt to recover encryption keys by measuring subtle variations in a chip's power consumption as they make correct and incorrect guesses about the encryption key's values.

Next, the E/IoT team examines the PCBs for debug interfaces on the production device that have been left in place without blowing the one-time programmable memory (OTP) security fuse. Typically, this includes such interfaces as Joint Test Action Group (JTAG), Serial Wire Debug (SWD), background debug mode (BDM), and universal asynchronous receiver/transmitter (UART).

By exploiting these interfaces, attackers can retrieve firmware, bypass a secure bootloader, and read or write instructions into memory. Depending upon how it's been implemented, UART can also provide attackers with valuable debug information or open a direct, serial-based command shell into the operating system. The E/IoT team also looks for simple flash chips that support Serial Peripheral Interface

(SPI) or Inter-Integrated Circuit (I2C). Chips like these are vulnerable because the contents can be accessed easily in-circuit or by de-soldering the chips and reading them in a programmer.

Tamper Prevention

Device makers often implement controls to prevent or detect tampering, such as filling the case or covering critical components with epoxy. This method can be defeated by removing the epoxy with heat and a razor knife or by applying chemical compounds that leave the PCB and components intact. A case switch may also be employed that deletes cryptographic keys from flash memory or renders the device inoperable when triggered. Case switches can be bypassed by inserting a fiber scope into an existing case opening (e.g., for the LCD screen), or by carefully drilling the case and modifying the tampering circuit so that it remains closed when the case is removed. If any tamper prevention or tamper-evident protection controls are found, the E/IoT team will attempt to bypass them.

Bootloader

The purpose of a secure bootloader is to prohibit unauthorized users from reprogramming a device. To defeat such controls, E/IoT consultants begin by inspecting the configuration of the bootloader and firmware update processes to ascertain whether firmware can be updated via an over-the-air (OTA) process or only locally. Next, the team analyzes the firmware to see if it's cryptographically signed and verified by the bootloader and if the firmware images are being encrypted. If not, an attacker can use reverse engineering methods to obtain them. If pre-execution environment (PXE) booting is enabled, the consulting team will check to see if the bootloader is verifying the certificate in the shim file, whether the shim file can be modified, and if a custom shim file can be inserted using Dynamic Host Configuration Protocol (DHCP) and a Trivial File Transfer Protocol (TFTP) server.

Consultants also determine whether an attacker could use a USB drive to boot the device to a live image. This is possible if the UEFI/BIOS has been left unlocked or if the boot order process doesn't prioritize external boot sources.

Firmware

To assess firmware, E/IoT consultants employ a combination of static and dynamic analysis methods. This begins with extracting the firmware image, reassembling the filesystems, identifying custom code, and analyzing configuration files and other product-specific artifacts. Next, the E/IoT team searches the firmware for the hardcoded keys used to encrypt data at rest and in transit, and for the credentials/keys used to authenticate the device to other systems.

Some functions are vulnerable to stack/heap-based buffer overflow errors due to improper bounds checking. Functions like these can be identified by disassembling and searching through product-specific binaries during static analysis.

The team also looks for Common Gateway Interface (CGI) injection vulnerabilities caused by improper handling of arguments, which can be exploited for local/remote command execution. The E/IoT team will also search for writeable set-user identification (SUID) type binaries or scripts that, if exploited, provide adversaries with privilege escalation opportunities.

The output of the static analysis phase provides the basis for the subsequent dynamic analysis. Once the firmware has been emulated, E/IoT consultants perform both local and remote fuzzing against the custom binaries and use debugging tools to pinpoint crash locations. Proof of concept code to recreate the crash is then written and code paths are followed to determine whether the crash can be controlled to allow local/remote code execution. If source code is made available by the client, the E/IoT team can utilize binary instrumentation to increase fuzzing efficiency and optimize code coverage.

Local Attack Surface

E/IoT consultants assess the operating system's local attack surface to see if it's optimally configured. For example, if the operating system presents the user with a limited shell or a service with a limited environment, the team will attempt to break out of the environment and acquire root level control. The team will also look for ways to escalate privileges by exploiting vulnerabilities in either the operating system, installed applications, and libraries.

Remote Attack Surface

E/IoT assessments of the remote attack surface are informed by the knowledge gained during the static firmware and binary analysis. All network-facing services are identified along with their authentication and authorization mechanisms. Areas of concern include unauthenticated web application programming interfaces (APIs), and web socket services, as well as embedded webservers that are vulnerable to exploits based on parameter manipulation, directory traversal, Structured Query Language (SQL) injection, and command injection.

Network Protocols

All wired and wireless network protocols used to connect the device to its supporting systems are assessed. This includes wired protocols such as Ethernet, CAN, and Serial, as well as wireless protocols such as 802.11, ZigBee, Bluetooth/BLE, Z-Wave, LoraWAN, cellular (GSM/CDMA), etc. If necessary, the E/IoT team will proxy traffic and disassemble/decompile the applications on each side of the communication stream in order to reverse engineer proprietary wired/wireless protocols. The team will also determine whether data in transit is being encrypted and uses proper message integrity checking to prevent man-in-the middle and replay attacks.

Supporting Systems and Applications

All systems and applications that a device can interact with are considered during this stage of an E/IoT assessment. This includes the protocols used to communicate with the device and backend cloud environments such as Azure IoT Hub and AWS IoT Core, vendor-managed backends accessed via Access Point Name (APN)

gateways, virtual private networks (VPNs), etc. The E/IoT team will also assess the thick applications used to interact with the device. In both cases, authentication and authorization mechanisms are key areas of focus. This includes determining how the device authenticates to the backend, whether symmetric/asymmetric cryptography is in use, and if hardcoded keys or credentials are being stored on the device. All backend systems and services that can be accessed and exploited by an attacker are identified. The E/IoT team will also assess how a key obtained from one device can be used to exploit remote devices via the cloud and backend platforms.

Engagement Deliverables

At the conclusion of every engagement, the E/IoT team presents its findings in a technical report. This includes a complete inventory of the systems and services tested, a prioritized list of vulnerabilities and their severity, descriptions of how the most critical vulnerabilities can be exploited to evade security controls and access restrictions, and the potential operational and business impacts for the client. The report concludes with an action plan for remediating the highest priority vulnerabilities and a set of tactical and strategic recommendations for optimizing the device's operational integrity. The tactical recommendations focus on individual components, the system as a whole, and its supporting systems. The strategic recommendations focus on secure engineering methods, device design, and development practices such as Security Development Lifecycle (SDL), software/hardware bill of materials (sBOM), as well as the importance of a secure supply chain.

Expected Business Benefits

BlackBerry E/IoT service engagements help clients preserve the integrity and availability of their embedded devices and prevent threat actors from using them as pivot points to attack enterprise systems and data. Benefits include:

- **Access to world-class consultants:** BlackBerry E/IoT Security teams are composed exclusively of principal-level consultants that have completed successful engagements for organizations of all sizes and in virtually every industry sector.
- **Completeness:** All local and remote attack surfaces are closely examined. Assessments encompass hardware, firmware, bootloaders, network protocols, tamper prevention capabilities, supporting/backend systems, and more.
- **Breadth:** All identified vulnerabilities and potential points of compromise are documented, including vulnerabilities the client may already have discovered and erroneously dismissed as insignificant.
- **Depth:** E/IoT consultants determine how vulnerabilities can be exploited to steal or escalate privileges, establish persistence mechanisms, and gain unauthorized access to other high value systems. Often, vulnerabilities must be chained together to achieve maximum device penetration.
- **Significant reductions in cyber risk exposure:** At the conclusion of every engagement, clients are provided with tactical and strategic recommendations for remediating device weaknesses before they can be exploited by threat

actors. Device manufacturers are empowered to lock down all layers of the security stack. Integrators gain confidence that the devices they deploy have been hardened correctly. Organizations that deploy embedded devices are protected from current and emerging threat actor TTPs.

- **Both business and technical perspectives:** In addition to a technical analysis, recommendations are contextualized in terms of their potential business impacts. This helps design and development professionals win executive support for necessary security investments or device upgrades.
- **Opportunities to optimize client endpoint defenses:** At the conclusion of an E/IoT engagement, clients have the option to optimize their endpoint defenses by purchasing one-year or three-year licenses for BlackBerry® Protect and BlackBerry® Optics. BlackBerry® ThreatZERO® consultants are available to help clients accelerate their transition from a reactive to a prevention-first security posture.

To Learn More

Whatever security challenge you may be facing, BlackBerry's consulting team stands ready to help. For more information about BlackBerry Red Team services, please visit the Red Team Services web page or call +1-888-808-3119 for immediate assistance. BlackBerry Red Team services portfolio also includes Attack Simulation. Please visit the consulting landing zone for the complete list of BlackBerry consulting solutions.

[1] Worldwide Internet of Things Spending Guide

[2] Gartner Identifies Top 10 Strategic IoT Technologies and Trends

[3] Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023

[4] Cybersecurity Is the Key to Unlocking Demand in the Internet of Things

[5] Third-party IoT risk: companies don't know what they don't know

[6] I Can't Believe Mirais: Tracking the Infamous IoT Malware

[7] Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB20-0231 | 200528