BlackBerry | IoT Solutions Group

BlackBerry IoT Services - Embedded Systems Penetration Test

Program Description ("Embedded Systems Penetration Test or "Project"), ("107423")

This document provides a general description of the Services to be provided. BlackBerry reserves the right to periodically change information in this document; however, such changes will only apply to Services contracted for after such change is made. All capitalized terms used but not defined in this Program Description have the respective meanings ascribed to them in the Professional Services Agreement ("PSA").

Embedded Systems Penetration Test

INTRODUCTION

BlackBerry will assess the security assurance of the target hardware and software by attempting to breach some or all of that system's security, using the similar tools and techniques employed by a potential adversary.

The specific techniques employed will be tailored to the system being assessed, the strategy being to understand weaknesses in the software's security design by inspection followed by defining and testing exploits. More complex systems may also require the definition of threat models such as misuse cases, attacker profiles and a threat testing plan.

RESPONSIBILITIES AND KEY AREAS OF FOCUS

Area	What	Activities
Analysis and Testing	Planning	• Confirmation of target for testing • Defining rules of engagement
	Information Gathering and Discovery	• Static firmware analysis focuses on application specific vulnerabilities (e.g. use of insecure system calls, insecure memory handling, processing of uncontrolled user input) as well as logic flaws in the applications. • Automated composition analysis of binary images • Mapping the software bill of materials and identifying the target materials • Auditing the operating system for all applications running on QNX stack • Open Source Software Analysis including Common Vulnerabilities and Exposures detection • Based on the identified weaknesses and vulnerabilities supporting further penetration testing activities • Hardware Analysis to determine Bill of material(s) and interfaces • Communication Interface discovery (MITM, CAN, BT, Wifi, Ethernet, etc.)
	Threat Modelling	• Weakness & Threat Analysis • Testing Plan • Attacker profiling • Misuse case analysis
	Testing	• Attack identified hardware interfaces • Reverse engineering on the extracted firmware • Software vulnerability exploitation • Software security controls testing including secure boot, code protection, key handling and protection

Deliverable	Report	In-depth report, broken down into 3 main parts:
		• Executive Summary
		• Technical Overview
		• Detailed Technical Findings highlighting:
		  ○ Vulnerabilities, Risks and potential impacts
		  ○ Detailed steps to reproduce
		  ○ Mitigation recommendations
		• 2 hour debrief with consultant (If requested)

DURATION

Customer must use the Services set out in this Program Description by the earlier of (i) the date set out in the applicable Order or (ii) within 2 months of from the date the Order is executed ("**Expiry Date**"), as tracked and reported on by BlackBerry. Any Services not used by the Expiry Date, shall be forfeited and no refunds or credits will be provided. BlackBerry's ability to perform Services is subject to Customer fulfilling the obligations set out below. A more detailed Project timeline will be confirmed during Project kickoff.

LIMITATIONS & EXCLUSIONS

a. This Project covers only the Services explicitly described in this Program Description and is subject to the terms and conditions of the PSA located here www.blackberry.com/legal. Additional consulting work not contained in this Program Description is deemed out of scope.
b. Services are provided Monday to Friday (excluding local bank/statutory holidays), 9am-5pm EST, with a 60-minute break for lunch.
c. BlackBerry is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities.
d. A hardware tear down is often required in order to complete the analysis. In this case one of the test devices will often be rendered inoperable by the testing.

CUSTOMER RESPONSIBILITIES

a. The Customer will provide BlackBerry access to the binary software image that resides on the device. In some cases, it might be advantageous to have early access as process begins with static analysis, the results of which inform later phases of the analysis
b. The Customer will provide BlackBerry with the agreed number of devices to be tested (generally 3 are required).
c. The planning stage sets the expectations for the level of information shared with the penetration testing team. In black box testing, very little (if any) information is shared.
d. In the case of grey box testing the customer is encouraged to share additional information such as design documentation or schematics.
e. Making the necessary arrangements to allow BlackBerry to perform the Services.
f. If the Services are performed at Customer's site, providing necessary access to its site including, but not limited to, appropriate access to Customer premises, computer systems and other facilities. In addition, Customer will provide all equipment required in the execution of duties i.e. laptop, desk, secure working space with suitable seating arrangements.
g. Providing any requirements for screening or security clearance of key BlackBerry Consultants in advance of the Project start date.
h. Appointing a contact person to supply BlackBerry with any necessary or relevant information and who shall have the authority to make decisions or obtain decisions from others expeditiously.
i. Providing BlackBerry with Project-relevant documentation in a timely manner upon request by BlackBerry.
j. Ensuring the Customer Project Manager and team members are assigned and available to meet for Project kick-off at Project start date.
k. Ensuring key stakeholders are available in a timely manner to undertake tasks such as change control and documentation review.
l. Ensuring any hardware requirements are met.

m. Providing full and free access, remote or otherwise, to Customer's system together with such information and assistance as is reasonably required by BlackBerry to enable it to perform its obligations under the Project.
n. Ensuring adequate backup copies are made of data, operating and application software such that the Customer's system and files may be restored in the event of corruption or other similar loss due to the performance of the Project or for any other reason, howsoever caused.
o. Unless expressly stated otherwise, restoring all data, operating and application software in the event of system failure or virus attack, regardless of the cause.
p. The Customer shall provide at least five (5) business days' notice for the cancellation or postponement of any work already scheduled as part of the Project. BlackBerry reserves the right to charge additional fees to Customer for any time lost due to cancellation or postponement resulting from Customer not meeting their responsibilities as defined herein.

BlackBerry offers additional consulting and educational offerings. To learn more about these offerings, please go to: https://blackberry.qnx.com/en/professional-services/services-overview