Risk Analysis of USB Communication for EOBRs

Rev. 1.4

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA. 92121-1714
U.S.A.

This document summarizes the results of a risk analysis performed by the Product Security team to inform project management and guide their risk management decisions. Because this analysis was performed using available information and resources, it cannot be an exhaustive review of all possible threats or attacks to the system and **is not approval or certification of the system security**. The conclusions in this document depend on details of the system and the environment in which it is deployed as well as the attack techniques known at the time of writing. The reader must assume an attacker is also aware of the information we used for our analysis, and will attempt to develop new attacks.

June 29, 2011

Table of Contents

1 Introduction

Qualcomm Product Security Initiative (QPSI) is a team of security experts at Qualcomm Inc. working with all Qualcomm's product divisions and responsible for security design and analysis of company's products. The team includes experts in multiple areas of computer security, ranging from applied cryptography and software security to secure hardware.

This document contains QPSI's feedback to certain aspects of Regulation 395.16 by Federal Motor Carrier Safety Administration (FMCSA). Regulation 395.16 describes a set of regulations by FMCSA for electronic on-board recording devices (EOBRs). More specifically, the regulation document proposes several forms of communicating driving records from an EOBR device to a law enforcement computer, one of which being a wired USB connection. This document presents QPSI's risk analysis of a USB communication method for transmitting driving records as proposed in Regulation 395.16.

2 Summary

QPSI strongly recommends against enabling a wired USB data connection as a channel for transmitting electronic driving records for EOBR devices. We believe that USB communication in this scenario is associated with a number of substantial risks. Our primary concerns include:

- *Lack of Secure Authentication. USB connection between two devices provides no way of verifying identities of either device.*
- *Unauthorized Read/Write/Code Execution. The most common ways of connecting devices via a USB connection do not provide sufficient protection against unauthorized data access on EOBR devices and requires additional security measures.*
- *Malware. USB malware is a highly likely attack vector which can infect or disable a large fraction of both EOBR devices and law enforcement computers.*
- *Physical Limitations of USB Connections. USB 2.0 standard specifies the maximal length of a USB cable to be 16.4 ft (5 meters), which might be insufficient for most intended uses of a USB connection with EOBR devices.*

We explain each of these risks below in more detail. While each of these risks can potentially be mitigated, addressing all of these risks represents a substantial technical and business challenge. Given availability of more secure transmission mechanisms – such as transmitting electronic driving records via a central server – we see no practical reasons why FMCSA should allow transmitting electronic driving records via wired USB connections.

3 Detailed Security Analysis

3.1 Lack of Secure Authentication

The primary security concern with using a USB connection for transmitting driving record is an inherent lack of secure authentication in the USB standard. That is, a USB connection between two devices, whether these are two computers or a computer and a USB storage device, provides no way of verifying identities of either device. This means that a law enforcement officer has no way of being assured that he is connected to a legitimate EOBR device and at the same time, the EOBR device cannot be assured that the recipient of driving records is a legitimate law enforcement officer. Given a history of adversarial behavior observed by the industry task force from both drivers and motor carriers we believe that a secure authentication for driving records transmissions is an absolute necessity.

We envision multiple scenarios where EOBRs that use unauthenticated USB connections are likely to be abused. An example attack would be a third party (either a malicious driver or a competitor) connecting a personal laptop to the EOBR in order to retrieve driving records. We believe it to be highly undesirable if an unauthorized third party could obtain driving record information from the EOBR.

Another example would be a malicious motor carrier equipping drivers with USB storage devices containing fake driving records or a malicious driver modifying driving records and storing them on a personal laptop or a USB storage device. At a traffic stop, a driver would connect a cable from the law enforcement computer not to the actual EOBR but to the USB device containing these fake records. With no secure authentication, a law enforcement officer has no means of verifying whether the driving records he obtained came from a legitimate source. Given a large variety of manufacturers of EOBR systems and a large number of EOBR form factors, we believe it to be easy for the driver to trick a law enforcement officer into connecting to a wrong device.

We considered two existing types of solutions available on the market to counter the lack of UBS authentication – a secure USB hardware and a software authentication protocol – and found both of this approaches to be infeasible for the case of EOBR authentication.

The first approach towards authenticating a USB connection is using a form of secure hardware, such as USB security tokens. Without going into much technical detail of available secure hardware solutions, all such solutions known to us are proprietary technologies and are not widely adopted. From QPSI's prospective, we see no way how any of such solutions can be accepted by an industry consortium.

Another alternative solution to the authentication problem includes developing a custom software protocol that will perform necessary authentication operations. This implies that every EOBR device and every law enforcement computer need be equipped with this

authentication software and provisioned with appropriate cryptographic keys. While such a solution is theoretically possible, it involves an outstanding amount of development work to account for all EOBR platforms and to distribute the software to all law enforcement computers. Given realistic budget and time constraints, we don't envision a software authentication component as a feasible solution.

To summarize, we believe that a USB connection with no secure authentication is unacceptable for the purpose of transmitting electronic driving records. At the same time we're unaware of feasible solutions to establish a secure authentication in this scenario.

3.2 Unauthorized Read/Write/Code Execution

The second important security consideration with a USB data connection is a possibility of an authorized access to the device. When a law enforcement computer is connected to an EOBR device via a USB connection, both devices need to be protected from an authorized data access. An unauthorized access can happen when one device attempts to perform data read, data write, code execution or a combination of these operations against the other device. The most common ways of connecting devices via a USB connection do not provide sufficient protection against unauthorized access and require additional security measures.

An exemplary attack exploiting unauthorized access to the device would be a malicious EOBR device attacking law enforcement computers. That is, a driver can load a malicious software into the EOBR device (or a laptop simulating the EOBR device) and attempt to attack a law enforcement computer during a traffic spot. When a law enforcement officer connects his laptop to the EOBR device, the driver executes malicious software which attempts to get an unauthorized access to the law enforcement machine.

A successful attack can result in the driver either stealing data from the law enforcement computer or installing malicious software that will give an attacker a full control over the law enforcement machine.

On the other side, an attacker – e.g. a competitor – could pose as a law enforcement officer and cause malicious software to be loaded onto EOBR devices. This links us back to the authentication problem. Without a secure authentication mechanism there is no way the EOBR device can tell a legitimate law enforcement device from a malicious machine of a hacker.

QPSI wants to highlight the need for preventing unauthorized access whenever a USB data connection is used with EOBR devices. Any proposal for USB data connection for driving record transmission should include measures for preventing any forms of unauthorized read, write and code execution operations.

3.3 Malware

A particular example of an attack exploiting unauthorized code execution via a USB connection is a wide availability of malware which is distributed via USB storage devices.

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. On many computing platforms, such a code from a USB device may be executed without the user's acknowledgment.

Threats of USB malware were well documented in the last decade. Since early 90's several viruses and worms have been known to infect millions of devices by distributing themselves via USB storage devices; most notable examples being *Agent.btz* and *Conficker* worms. For example, starting from year 2008 the US Army banned its personnel from using USB storage drives citing concerns for USB malware as a primary reason.

According to Symantec Global Internet Security Threat Report around 40% of malicious code that propagates between computing devices does so as shared executable files. USB storage devices account for a large portion of these cases. Shared executable files are the propagation mechanism employed by viruses and some worms that copy themselves to removable media, such as USB storage devices.

Given a large variety of computing platforms used in EOBR devices, QPSI considers malware to be a highly likely attack vector which can infect or disable a large fraction of both EOBR devices and law enforcement computers.

3.4 Physical Limitations of USB Connections

We also want to highlight an inherent physical limitation of a USB data connection. USB 2.0 standard specifies the maximal length of a USB cable to be 16.4 ft (5 meters). This might be insufficient for most intended uses of a USB connection in the case of EOBRs.

More specifically, a typical scenario for transmitting driving records involves a traffic stop, where a law enforcement officer needs to transfer driving records from a stationary EOBR device located in a truck's cab to a laptop located in a law enforcement vehicle. While we didn't conduct any field experiments on whether the cable length of 16.4 ft is sufficient, our estimates show that in most cases such devices cannot be connected by a cable under 25ft long.

4 Conclusion

In this report, QPSI provides a detailed justification for our recommendation against enabling retrieval of driving records from EOBR devices through USB. We believe that a much cleaner and secure solution involves law enforcement personnel retrieving driving records from a server that hosts this data. The driving records would have to be transferred over an encrypted and integrity protected link with appropriate mutual authentication implemented for both law enforcement team and EOBR server to prove that their identities.