Proceedings of the 19th International Symposium on the Packaging and Transportation of Radioactive Materials
PATRAM 2019
August 4-9, 2019, New Orleans, LA, USA

CYBER AND GLOBAL POSITIONING SYSTEM VULNERABILITIES AND MITIGATION STRATEGY FOR RADIOLOGICAL TRANSPORT VEHICLES

Michael R. Moore, PhD
Oak Ridge National Laboratory

Greg Phillips
STS Nuclear

Mason J. Rice, PhD
Oak Ridge National Laboratory

Frank L. Combs
Oak Ridge National Laboratory

Kimberly Anderson
Oak Ridge National Laboratory

ABSTRACT

Vehicles are increasingly cyber-physical systems which depend on networked control units and sensors. Consequently, modern transportation faces challenges to ensure security and safety from cyber-attacks. Specifically, modern vehicles include scores of on-board electronic control units (ECUs) communicating over in-vehicle networks to control safety critical systems. While these electronically controlled functions provide vastly improved capabilities such as collision avoidance and wireless connectivity, they also inherently introduce vulnerabilities such as demonstrated in the 2012 Jeep Cherokee attack (C Miller, 2014). Therefore, an assessment was conducted to analyze the global transport security of radiological materials. Several cyber-attack methods were evaluated that included direct access to vehicle electronics, remote attacks via the telematics or head unit, jamming of GPS and/or radio links, and spoofing of communications. These were applied to scenarios including redirecting the driver, disabling the vehicle, stealing the vehicle, and stealing the radiological devices. Common subsystems of a wide variety of relevant vehicles were chosen for in-depth analysis and one attack scenario was experimentally verified. Based on the vulnerability assessment, several mitigation methods were developed. These included: 1) a checklist used at the time of purchase of a vehicle, 2) the development and integration of CAN Bus monitoring tools, the hardening of RF/Telematics interfaces, and the development of embedded software/malware detection tools. This paper will cover general vulnerabilities and mitigation methods. These will span from low-tech adversarial methods to highly sophisticated attack vectors. It will then show how emerging commercial products and best practices augmented by cutting-edge research at ORNL can protect these vehicles.

INTRODUCTION

The rapid increase in electronically enabled functions on passenger and commercial vehicles has significantly raised the number and complexity of cyber-based vulnerabilities. A critical mission impacted by this increase is transport security for radioactive material. Thus, Oak Ridge National Laboratory (ORNL) was tasked to assess transport vehicle cyber security for the US Department of Energy National Nuclear Security Administration (DOE NNSA) Office of Radiological

Security (ORS). The purpose of the assessment was to analyze material transport security in partner countries given emerging threats from cyberattacks. One result of that effort was the report, "Radiological Transport Vehicle Cyber and Global Positioning System Vulnerability Analysis for the Office of Radiological Security Global Fleet," ORNL/SPR-2018/11 (Moore, 2018).

The analysis identified major vulnerabilities that could globally interrupt the transport of radioactive materials including vehicles ranging from small pick-ups to medium-duty trucks. Recent and near-future vehicles were also targeted for analysis given rapid changes to electronic profiles of vehicles as technology continues to evolve.

The goal of the analysis was to determine operational risks to radiological transport, as opposed to simply determining individual component-level vulnerabilities. Therefore, the report includes an evaluation of the following seven cyberattack scenarios:

- Scenario 1—Disrupting or tracking vehicles using a direct controller area network (CAN)/sensor bus injection device
- Scenario 2—Disrupting or tracking vehicles by compromising telematics or head unit communications
- Scenario 3—Disrupting or tracking vehicles by compromising head unit software
- Scenario 4—Disrupting or tracking vehicles by compromising electronic control unit (ECU) Software
- Scenario 5—Interfering with cooperative tracking by jamming or spoofing global positioning system (GPS)
- Scenario 6—Interfering with remote operations by denying or spoofing telematics communications of geolocation
- Scenario 7—Interfering with or spoofing driver assistance sensors

All subsequent vehicle, system, and subsystem analyses were performed with these seven scenarios in mind.

The findings of the analyzed vehicles showed attack susceptibility through low-cost CAN bus injection devices, advanced navigation head units, GPS jamming, and telematics reporting. The findings also indicated combined practical methods that can help mitigate these attacks.

ATTACK SCENARIOS

The scenarios were chosen after interviews with select subject matter experts who have provided protection analysis, technologies, and oversight for decades. Based on their input, these scenarios were used to determine which cyber-attacks would contribute to a successful attack and thus become part of a subsequent risk analysis.

Scenario 1—Disrupting or Tracking Vehicles Using Direct Can/Sensor Bus Injection Device

As stated previously, this adversarial approach is deemed to be the most likely scenario because it requires very modest resources and gives the attacker a method for taking total control of the vehicle from almost any distance.

Scenario 1 was assessed by recreating a typical CAN bus injection attack. Common Arduino hardware obtained for about $60 from internet sales sites as shown in Figure 1 were used. Then the Arduino-based hardware were loaded with C-like codes (Arduino codes), also readily available on the internet. This effort was repeated by staff and undergraduate interns three times and never took more than a few days of development.

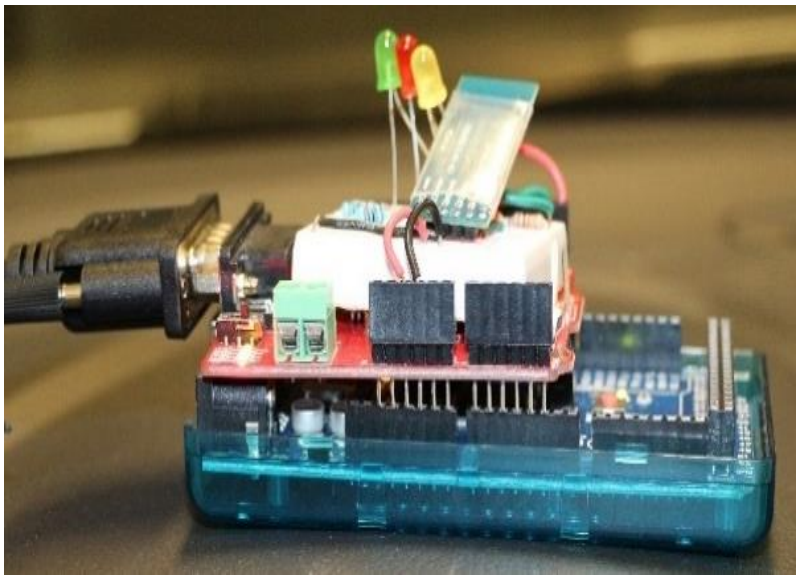

Figure 1. Arduino-based direct CAN bus injection hardware.

The Arduino system included a Bluetooth module that allowed short-range command and control (C2). It would be very straightforward to replace the Bluetooth module with a cell-modem, Wi-Fi, or other communication hardware to enable further standoff.

Installation into the vehicle requires only 5–10 minutes if proper connectors and wiring harnesses have been acquired. There are two general approaches: (1) attaching to the OBD-II diagnostic port or (2) attaching to the CAN-High and/or CAN-Medium speed busses elsewhere along the wiring harness. The first approach takes less than a minute but is easily detectable. The second approach can take up to approximately 10 minutes and is harder to detect from a casual visual inspection.

The execution of the attack consists of waiting until the vehicle is within a region of interest and within range of whichever communications relay method is being used (e.g., BT or cell modem) to provide C2 for the CAN bus injection. Depending on the speed of the vehicle and the exact

injection commands, the vehicle may take a few minutes to stop on its own, the driver may stop the vehicle, or the vehicle/driver may react in other ways.

As shown in Figure 2, the adversary would use a compatible transmitter for C2 (red arrow) with the device embedded in the transport vehicle. The device would then inject the commands into the CAN bus (blue arrow), causing the adversarial action.

Figure 2. Operational scenario for remotely activated direct CAN bus attack.

Scenario 2—Disrupting or Tracking Vehicles by Compromising Telematics Or Head Unit Communications

The longest distance attacks which require no direct access to the vehicle involve remote communication through the head unit (also called navigation system or telematics in various publications). This method gives global standoff but requires significant tailored development and extensive knowledge of the target vehicle and assumes that the vehicle has some of the telematics systems that are general options. This adversarial approach requires significant resources, development time, and compatible systems. However, it gives the attacker a method for taking total control of the vehicle from any remote transmitter.

Scenario 3—Disrupting or Tracking Vehicles by Compromising Head Unit Software

Some attacks can be enabled by inserting malware or compromised codes into the head unit via a USB port or other data port built into many navigation systems for updating software. This method could be used in combination with Scenario 2 or as part of Scenario 4. That is, it can be used to compromise the telematics to achieve global, regional, or national standoff, or it can be used to enable malware attacks within the ECUs connected to the sensor and CAN busses. This adversarial approach requires significant development time and compatible systems, but it gives the attacker a method for taking total control of the vehicle from any remote transmitter.

Scenario 4—Disrupting or Tracking Vehicles by Compromising Electric Control Unit Software

Some attacks can be enabled by inserting malware or compromised codes directly into the ECUs that convert commands transmitted over the sensor networks into physical actions or measurements. This requires maintenance technician–level access and training. This method could be used in combination with Scenario 1 or as part of Scenario 3. That is, it can be used to compromise the CAN bus commands directly or used to propagate malware to other subsystems within the vehicle. This adversarial approach requires significant development time and compatible systems and gives the attacker a method for taking total control of the vehicle from any remote transmitter.

Scenario 5—Interfering with Cooperative Tracking by Jamming Or Spoofing GPS

One of the easiest attacks to carry out is jamming the GPS signal. This can be accomplished by using any of several commercial-off-the-shelf (COTS) devices at close range. This attack, however, is not deemed to be high risk because consequences would be modest and mitigation via redundant location services would be easy to implement.

Scenario 6—Interfering with Remote Operations by Denying Or Spoofing Telematics Communications Of Geolocation

There are two basic approaches to interfere with the telematics or other automated reporting of the vehicle's location to the command center: (1) jamming (same as Scenario 5), and (2) a priori alteration of the telematics software to deny or spoof communications during operations. This latter method is addressed in Scenario 3.

Scenario 7 – Interference or Spoofing of Driver Assistance Sensors

With the rapid increase in driver assistance systems (e.g., collision avoidance, lane change control, etc.) comes vulnerabilities associated with the increased autonomy of the vehicle. For instance, if a signal is maliciously echoed back to an ultrasonic detector intended to sense pedestrians or roadway obstructions, the vehicle could be brought to a halt. This attack would take moderate to significant resources and would be very hard to detect.

SUBSYTEM ANALYSIS

As mentioned, subsystem analysis was chosen over vehicle make/model focused analyses for the following reasons:

a. There are too many trim variations on each vehicle to exhaustively analyze each possible vehicle
b. Subsystem analysis supports predictive risk analysis for future vehicle make/models that have not even been designed yet

Thus, if the risks of key subsystems are understood, then future vehicle purchases can be tailored (e.g., adding security features or disabling certain options such as Bluetooth or Collision Avoidance).

Electronic Subsystems

This section outlines the expected electronic devices associated with vehicles of interest. Figure 3 shows a typical vehicle electronic subsystem. These subsystems provide an array of features and services but also introduce potential vulnerabilities for both long-range intercept and direct attacks on components.

There are some relevant trends that are important for near future analysis of these subsystems. First, the attribution between messages on the CAN bus and their attendant sensors are protected intellectual property for most passenger vehicles but are well published for medium and heavy-duty trucks. This difference is a result of the final assembly of larger trucks with multiple OEMs (e.g., cab and engine by one OEM and load bed by another) thus requiring well-established addressing and protocols for sensor data. However, passenger vehicles with one OEM in the final assembly can make their data messaging proprietary.

Second, the OBD-II port is gradually being hardened and/or phased out. In some cases, it no longer gives access to all CAN-bus messages but only the diagnostic command and responses. In other cases, it is being replaced with a Bluetooth link that could either help or harden or make the system more vulnerable depending on the implementation.

Third, the ability to hack the rolling codes of keyless entry systems and long-range head unit attacks have been well established for several years. However, other attack vectors that control the whole vehicle are less well known. A complete subsystem analysis was undertaken to ensure that complete vehicle attack surface was addressed.

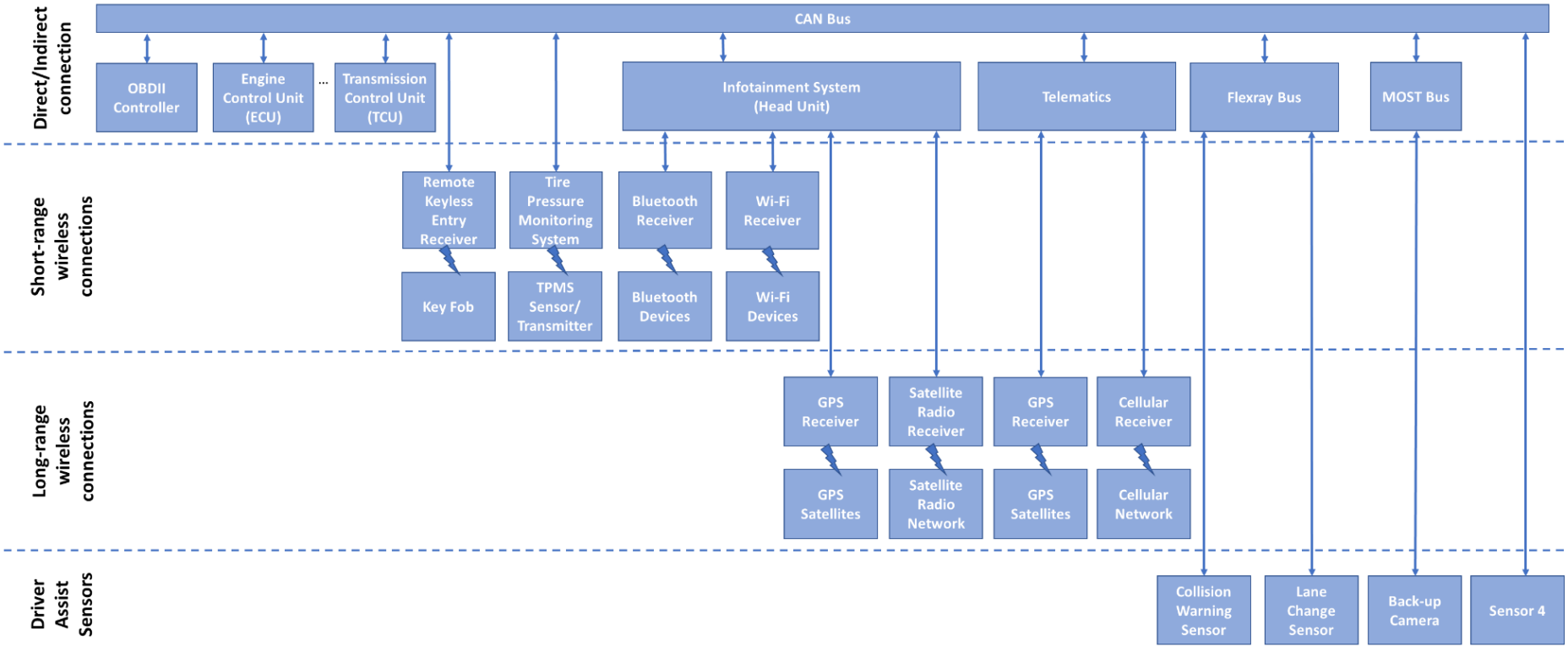

Figure 3. Overview of typical vehicle electronic subsystems and their connections to the control busses.

Telematics

In addition to the vulnerabilities associated with cyber attacks on the electronic subsystems, attention should also be given to the interception or exploitation of the emerging data links between vehicles, OEMs, and other centrally located databases. For example, the amount of data accessible to criminal elements and other malicious actors has greatly increased through automatically transmitted data (e.g. OnStar and others) that OEMs are requesting, and governments are requiring.

Based on our examination of the incentives to gather and re-identify data, we developed our own incentive taxonomy. Some of the categories require low-level analysis. These incentives are based on passive data collection: the data generator does not know data have been exchanged.

- Information compromise (e.g., finding out a person's home address)
- Driver behavior
- Feature/application use profiling
- Risk assessment
- Disruption
- Threats to person or family (e.g., finding out where a person and his/her family members live)
- Physical harm (e.g., location, times, opportunities for crime)

MITIGATION OF CYBER ATTACKS

As a part of the analysis, some preliminary mitigation strategies were developed. Since it was determined that no one technique or technology could protect the vehicles that support radiological transport, the following methods should be used in combination.

Prevention

1) Inventory or specify the complete list of electronically enabled options and features of a given vehicle, so that options that introduce unacceptable risks can be disabled or removed.
2) Add CAN-bus monitoring capabilities.
3) Harden/Manage head unit devices. This includes both navigation (e.g., GPS) and communication (e.g., WiFi or cell phone) connections.
4) Protect/Check the software in the ECUs periodically or after any maintenance or repair events.
5) Institutionalize data security for all telematics services.

Complementary Tactics, Techniques, and Procedures (TTPs)

6) Provide drivers with redundant navigation aids.
7) Provide drivers with redundant communication resources (e.g., push-to-talk radios).
8) Provide escort vehicles with redundant communications.

CONCLUSIONS

The findings on the vehicles analyzed are as follows:

- All vehicles analyzed are susceptible to an attack that involves placing a low-cost CAN bus injection device on the vehicle's wiring harness or second-generation on-board diagnostics (OBD-II) port.
- Vehicles with advanced navigation head units are susceptible to very long-range attacks, although it will take more adversarial resources than other technical attacks.
- All vehicles are susceptible to an attack that involves GPS jamming, which denies both the driver and any remote command center reliable geolocation information.
- Commercial solutions for mitigating the GPS jamming scenarios are available; however, complementary TTPs need to be developed and operators need to be trained.
- Targeted development of commercial or government off-the-shelf capabilities could mitigate the CAN bus attacks regardless of whether they involve long-standoff or direct-connection attacks.
- Telematics reporting data lead to a significantly increased opportunity for adversaries to track or predict the routes of ORS vehicles and their drivers.
- There are several practical methods that if used in combination can help to mitigate these attacks.

ACKNOWLEDGEMENTS

NNSA Office of Radiological Security
Katherine Holt, Director of International Radiological Security Program
katherine.holt@nnsa.doe.gov
+1 (202) 374-0412

REFERENCES

C Miller, C. V. (2014). *A Survey of Remote Automotive Attack Surfaces.*

Moore, M. R. (2018). *Radiological Transport Vehicle Cyber and Global Positioning System Vulnerability Analysis for the Office of Radiological Security Global Fleet.* Oak Ridge: Oak Ridge National Laboratory, ORNL/SPR-2018/11.