U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

NHTSA
www.nhtsa.gov

**DOT HS 812**

**September 2014**

# Characterization of Potential Security Threats in Modern Automobiles

## A Composite Modeling Approach

## DISCLAIMER



Suggested APA Format Citation:

McCarthy, C., Harnett, K., & Carter, A. (2014, September). *Characterization of potential security threats in modern automobiles: A composite modeling approach*. (Report No. DOT HS 812). Washington, DC: National Highway Traffic Safety Administration.

**Technical Report Documentation Page**

| 1. Report No.<br>DOT HS 812 | 2. Government Accession No. | 3. Recipient's Catalog No. |
|---|---|---|
| 4. Title and Subtitle<br>Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach | | 5. Report Date<br>September 2014<br>6. Performing Organization |
| 7. Authors<br>Charlie McCarthy, Kevin Harnett, Art Carter | | 8. Performing Organization |
| 9. Performing Organization Name and Address<br>Volpe National Transportation Systems Center<br>Security and Emergency Management Division<br>55 Broad Street<br>Cambridge, MA | | 10. Work Unit No. (TRAIS)<br>11. Contract or Grant No.<br>DTNH22-12-V-00085<br>DTFH61-12-V00021 |
| 12. Sponsoring Agency Name and Address<br>National Highway Traffic Safety Administration<br>1200 New Jersey Avenue SE.<br>Washington, DC 20590 | | 13. Type of Report and Period<br>Final Report<br>14. Sponsoring Agency Code |

15. Supplementary Notes

16. Abstract

The primary objective of the work detailed in this report is to describe a composite modeling approach for potential cybersecurity threats in modern vehicles. Threat models, threat descriptions, and examples of various types of conceivable threats to automotive systems are included, along with a matrix containing a condensed version of the various potential attacks.

This publication is part of a series of reports that describe our initial work under the goal of facilitating cybersecurity best practices in the automotive industry (Goals 1 and 2). The information presented herein increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines.

| 17. Key Words | 18. Distribution Statement |
|---|---|
| Cybersecurity, NIST, NHTSA, Guidelines, Risk Management, Baseline, Use Cases, Best Practices | Document is available to the public from the National Technical Information Service www.ntis.gov |

| 19. Security Classif. (of this report) | 20. Security Classif. (of this page) | 21. No. of Pages | 22 |
|---|---|---|---|
| Unclassified | | 46 | |

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

# Acknowledgements

The authors would like to thank the automotive industry original equipment manufacturers who participated in informational interviews conducted by the National Highway Traffic Safety Administration on the subject of automotive cyber security.

The authors would also like to thank the National Science Foundation, the Defense Advanced Research Project Agency, and the members of the SAE International Vehicle Electrical System Security Committee and Automotive Security Guidelines and Risk Development Task Force for their comments and suggestions pertaining to this report.

# Foreword

### NHTSA's Automotive Cybersecurity Research Program

Based on a systems engineering approach, the National Highway Traffic Safety Administration established five research goals to address cybersecurity issues associated with the secure operation of motor vehicles equipped with advanced electronic control systems. This program covers various safety-critical applications deployed on current generation vehicles, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity. These goals are:

1. Build a knowledge base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;
2. Facilitate the implementation of effective industry-based best practices and voluntary standards for cybersecurity and cybersecurity information sharing forums;
3. Foster the development of new system solutions for automotive cybersecurity;
4. Research the feasibility of developing minimum performance requirements for automotive cybersecurity; and
5. Gather foundational research data and facts to inform potential future Federal policy and regulatory decision activities.

### This report

The primary objective of the work detailed in this report is to describe a composite modeling approach for potential cybersecurity threats in modern vehicles. Threat models, threat descriptions, and examples of various types of conceivable threats to automotive systems are included, along with a matrix containing a condensed version of the various potential attacks.

This publication is part of a series of reports that describe our initial work under the goal of facilitating cybersecurity best practices in the automotive industry (Goals 1 and 2). The information presented herein increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines.

# Table of Contents

# Tables



# Figures

# List of Acronyms

| | |
|---|---|
| ABS | antilock brake system |
| ASF | application security frame |
| BCM | body control module |
| CAN | controller area network |
| CDMA | code division multiple access |
| COTS | commercial-off-the-shelf |
| CVE | common vulnerability environment |
| DoS | denial of service |
| DRM | Digital Rights Management |
| DSRC | dedicated short range communications |
| EBCM | Electronic Brake Control Module |
| ECM | engine control module |
| ECU | electronic control unit |
| EGR | exhaust gas recirculation |
| GPS | global positioning system |
| GSM | Global System for Mobile Communications |
| HVAC | heating, ventilation, and air conditioning |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| IDS | Intrusion Detection System |
| ISAC | Information Sharing and Analysis Centers |
| ITS | Intelligent Transportation Systems |
| LAN | local area network |
| LIN | local interconnect network |
| MAP-21 | Moving Ahead for Progress in the 21st Century Act |
| MOST | Media Oriented System Transport |
| NFC | Near Field Communications |
| OBD-II | on-board diagnostics |
| OEM | original equipment manufacturer |
| PC | personal computer |
| PT-ISAC | Public Transportation Information Sharing and Analysis Center |
| RF | radio frequency |
| SD | secure digital |
| SDM | sensing and diagnostics module |
| SME | subject matter experts |
| ST-ISAC | Surface Transportation Information Sharing and Analysis Center |
| UMTS | Universal Mobile Telecommunications Systems |
| USB | universal serial bus |
| US-CERT | United States Computer Emergency Readiness Team |
| V2I | vehicle-to-infrastructure |
| V2V | vehicle-to-vehicle |
| V2X | vehicle-to-vehicle or infrastructure |

# 1.0 Introduction

Modern day automobiles are complex machines which can contain over 60 embedded electronic control units, networks to support these units, and a host of external interfaces, both wired and wireless. Wired interfaces can include USBs, CDs, DVDs, and secure digital (SD) cards. Wireless interfaces can include short-range and long-range connectivity, such as via Bluetooth, Wi-Fi, radio frequency, Near Field Communications, Global System for Mobile Communications/Code Division Multiple Access, and Universal Mobile Telecommunications System. The wireless interfaces can support a host of features including remote tire pressure monitoring, telematics, and Smart key keyless entry/ignition start. vehicle-to-vehicle and vehicle-to-infrastructure communications (collectively referred to as V2X communications) also promise tremendous benefits for efficiency, comfort, and driving safety which may be on the near horizon. The continuing trend in vehicle architecture is a shift towards more open systems.

Driven by robust consumer demand for increased safety and convenience functions, the use of embedded systems and the code to support them will likely continue to grow. By using embedded systems, manufacturers can provide upgrades and premium functionality more readily and cost effectively. In a 2011 EE Times article [1], IBM Corporation's Meg Selfe, a vice president for complex and embedded systems at IBM Rational, remarked that the Chevrolet Volt uses an estimated 10 million lines of code running on about 100 ECUs. In comparison, she estimated that a typical 2009 model used six million lines of code, and a 2005 model used about 2.4 million lines of code.

To date, there are no known field experiences with exploited cyber-vulnerabilities in automobiles in the absence of a prolonged direct physical access to the vehicle. This is, in part, due to design, testing and quality assurance practices original equipment manufacturers and system designers employ. However, it is recognized that increasing interconnectedness with internal and external networks and growing system complexity could introduce new security vulnerabilities in cyber-physical systems that could potentially be exploited by various adversaries.

The safety and security of vehicle electronic systems is a continuing focus for NHTSA. The U.S. Department of Transportation's 2012 highway authorization act, Moving Ahead for Progress in the 21st Century Act (MAP-21), contains specific language in Section 31402 pertaining to electronic systems [2]:

> (a) IN GENERAL. — Not later than 2 years after the date of enactment of this Act, the Secretary shall complete an examination of the need for safety standards with regard to electronic systems in passenger motor vehicles. In conducting this examination, the Secretary shall—
>
> (1) consider the electronic components, the interaction of electronic components, the security needs for those electronic systems to prevent unauthorized access, and the effect of surrounding environments on the electronic systems; and
>
> (2) allow for public comment.
>
> (b) REPORT. — Upon completion of the examination under subsection (a), the Secretary shall submit a report on the highest priority areas for safety with regard to the electronic systems to the Committee

on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.

In road transportation scenarios related to the security of vehicle information or functions, stakeholders may be concerned primarily with the following four areas.

- **Privacy/Security** – unwanted or unauthorized acquisition of data pertaining to
  - Vehicle or driver activities (e.g., location of vehicle, navigation destination, etc.)
  - Vehicle or driver identity data
  - Vehicle or sub-system design and implementation (i.e., OEM/supplier proprietary data)
- **Unwanted or Unauthorized** commercial transactions
- **Operational** – interference with
  - On-board non-safety vehicle systems such as infotainment, and heating, ventilation, and air conditioning systems, etc.
  - V2X communications that may have non-safety impacts on the operational performance of vehicles
  - V2X communications that may have non-safety impacts on intelligent transportation systems (ITS)
- **Safety** – interference with on-board vehicle systems or V2X communications that may affect the safe operation of vehicles and ITS

A vehicle's cyber-controlled subsystems could be compromised in a number of ways, such as via deliberate cyber-attacks, owners of the system unintentionally changing default parameters in a way that reduces safeguards in place, through possible physical damage to network components, or via radio frequency interference.

### 1.0.1 Automotive Networks

In a vehicle, the exchange of data between the various ECUs can take place in one of two primary ways:

1. Data is transferred between ECUs over dedicated wires as in peer-to-peer communications; and
2. Data is transferred between ECUs via a network data bus.

There are multiple types of vehicle networks. Table 1 contains a partial listing of current automotive networks. There may be multiple networks within the same vehicle supporting different functions with varying levels of safety impact potential.

**Table 1: Sample Automotive Networks**

| Network Name | Physical Layer | Network Topology | Typical Usage |
|---|---|---|---|
| **CAN (Controller Area Network)** | Twisted pair, 9-pin D-Sub | Point to Point | Body systems, engine management, transmission, etc. |
| **LIN (Local Interconnect Network)** | Single wire | Single Master to Multiple Slave (up to 16 slaves) | Door locks, climate control, seat belts, sunroof, lighting, window lift, mirror control |
| **FlexRay** | Electrical, optical | Single and Dual Channel | Drive by wire, brake by wire, steer by wire, stability control, etc. |
| **MOST (Media Oriented Systems Transport)** | Optical | Ring (up to 64 MOST devices) | Infotainment data |
| **BYTEFLIGHT** | Optical | Master/Slave | Safety critical applications (e.g., air bags) |

For example, one of the more common automotive platform networks is the controller area network bus[1]. The CAN bus links individual ECUs to form an integrated system. Data transfer in the CAN bus works in the same manner as a telephone party line. An ECU sends data into the bus while other ECUs listen and if the data concerns them, the other ECUs act upon it.

A typical CAN bus consists of a controller, a transceiver, two data bus lines, and two data bus terminals. Except for the physical data bus lines, the components reside in the ECUs. The CAN bus components perform the following functions:

1. **CAN Controller** receives outgoing data from the processor in the ECU, processes the data, and sends it to the CAN transceiver. In addition, the controller receives incoming data from the CAN transceiver, and then checks it to see if the data message is for that ECU. If the message is for that ECU, the CAN controller processes it and sends it to the ECU processer. If the message is not for that ECU, the data is ignored.
2. **CAN Transceiver** acts as a transmitter and receiver, converts outgoing data from the CAN controller to electrical signals and sends them over the CAN bus lines. Also, the CAN transceiver receives incoming signals from the CAN bus lines, converts these electrical signals, and sends them to the CAN controller.

[1] While there may be several networks in the modern automobile, as identified in Table 1, the CAN bus has the most publicly available and current vulnerability information in the cybersecurity community.

3. **CAN Terminal** is a resistor that prevents data from being reflected back at the end of the lines.
4. **CAN Bus Lines** are physical wires that transmit the bi-directional signals from the CAN transceivers.

### 1.0.2 Electronic Control Units

The first ECUs (see Figure 1) were dedicated to engine management in response to meeting emission standards. Back in the 1980s, cars only had one "computer." Currently, there are between 70 and 100 ECUs in an automobile. An ECU can be interconnected to other ECUs via a digital bus network. There may be multiple bus networks in an automobile, split along component groups. Typically, critical ECUs such as the electronic brake control module are given a higher data rate bus than less critical ones such as HVAC.

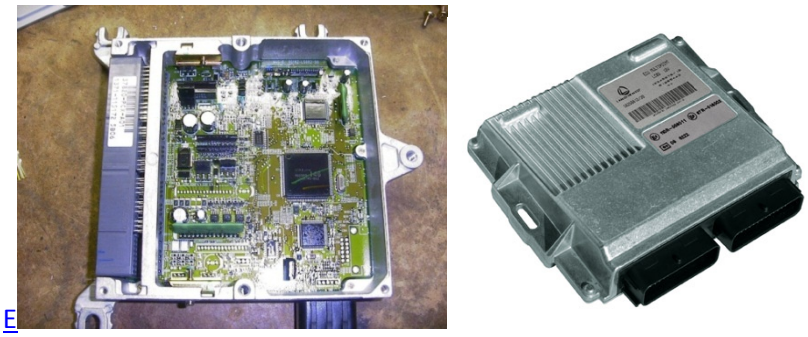

**Figure 1: Typical ECUs**

## 1.1 Objectives

This paper describes a modeling approach for characterizing potential threats for automotive control systems. Threat models, descriptions, and examples of various types of threats to automotive systems are included, along with a matrix containing a condensed version of the various sample attack possibilities.

The completed threat matrix can be found in Appendix B.

## 1.2 Methodology

Information for this modeling approach was provided through various groups, government entities, industry publications and periodicals, interviews with subject matter experts, SME presentations and studies, DOT-funded studies, and subject matter government reports. Appendix C provides a list of sources used in the development of this report.

### 1.2.1 Why Threat Modeling?

Threat modeling is a structured approach that allows cyber security threats to be classified. When integrated into the design process, threat modeling would likely reduce the lifecycle cost of providing security for an application.

An effective threat model:

- Identifies potential threats and the conditions that must be in place for a potential attack to make an impact;
- Provides information on how existing safeguards would affect the outcome of the attack;
- Provides information that would help target areas for mitigations; and
- Allows for categorization of attacks and provides a means to group threats to allow for development of mitigations that would address multiple threats.

### 1.2.2 Types of Threat Models

There are many different threat models in use today in various industries; however it is unclear whether these existing threat models can address all of the unique factors in the automotive cyber landscape. Therefore, a hybrid of various models is proposed.

A few of the many threat models in use are briefly described below.

**A. STRIDE [3]**

The Microsoft STRIDE model characterizes potential threats according to the types of exploit that are used. The STRIDE acronym is made up of the first letter of each of the threat categories, shown in Figure 2. In use, the STRIDE threats are considered against each component of the system, as well as the relationship between components from the attacker's point of view. Variants of the STRIDE model are currently used by at least one major OEM, according to the subject matter expert interviews. See Section 2.0.2 (Table 5) for a detailed description of the STRIDE model categories.

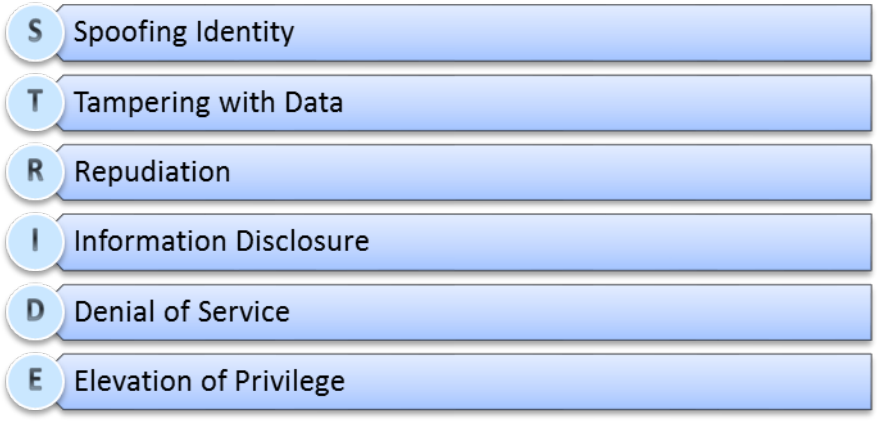


**Figure 2: STRIDE Threat Categories**

## B. Trike

Trike [4] is a threat modeling framework with similarities to the Microsoft threat modeling processes. However, Trike differs because it uses a risk-based approach with distinct implementation, threat, and risk models, instead of using the STRIDE aggregated threat model (attacks, threats, and weaknesses).

Trike's goals are:

- With assistance from the system stakeholders, to ensure that the risk this system entails to each asset is acceptable to all stakeholders;
- Communicate what has been done and its effects to the stakeholders; and
- Empower stakeholders to understand and reduce the risks to them and other stakeholders implied by their actions within their domains.

## C. Application Security Frame

The Microsoft ASF [5] methodology looks at the data network from a defender's point of view. The threat categories listed in Table 2 are designed to be system-administrator-centric.

**Table 2: ASF Threat Categories**

| | | |
|---|---|---|
| Input and Data Validation | Configuration Management | Cryptography |
| Authentication | Sensitive Data | Exception Management |
| Authorization | Session Management | Auditing and Logging |

# 2.0 Composite Threat Model

After closely analyzing STRIDE, Trike, and ASF from an automotive sector applicability standpoint, the common elements from various methods were selected to establish the composite threat modeling method described in this section. This method is summarized in Figure 3.

**Composite Threat Model Outline**

2.0.1 Identify critical applications/systems

- A. Application/system decomposition
  1. Create interconnection drawings
  2. Create high level data flow diagrams

2.0.2 Determination and analysis of threats

- A. Threat identification
- B. Threat analysis
  1. Drawing review
  2. Use case development
  3. Vehicle threat matrix development and population

**Figure 3: Composite Threat Model Outline**

## 2.0.1 Identify Critical Applications/Systems

A critical application/system (e.g., brake, powertrain) for a vehicle is viewed as a vehicle function that, if compromised maliciously, could result in a serious safety concern. This step identifies priority application/systems for analysis, which requires a working knowledge of the specific component/system and how it relates to other components/systems. It is essential to assess the interconnected network impacts, considering all possible data paths and potential attack vectors that could provide for entry into a critical system/component potentially through a noncritical system/component.

### A. Application/System Decomposition

Once a component/system has been identified as being critical (or that it is connected to a critical component/system), an interconnection and a data flow drawing of the component/system are created.

#### 1. Create Interconnection Drawing

It is essential to create a complete interconnection drawing which contains:

- *All relevant on-board components and systems*: Identify all components and systems that are physically connected to or communicate with the component/system being studied, with all connections.
- *External interface connections*: Identify external connections such as on-board diagnostics (OBD-II), Bluetooth, USB, etc.
- *Data entry/exit points*: Note any point whereby data can enter/exit the system/component.
- *Data types*: Identify the areas where there are separations of system and component data levels (i.e., critical versus non-critical) with special attention to those areas with data having differing levels of criticality handoffs (e.g., gateways).

**2. Create High Level Data Flow Drawing**

The purpose of the data flow drawing is to visually represent the data flows that support the functional relationships between the various systems/components, as well as the trust boundaries that exist between the various components.

## 2.0.2 Determination and Analysis of Threats

**A. Threat Identification**

Threat identification is a continuous process that includes monitoring the system's environment to determine if credible cyber threats exist. The automotive system developers and first tier suppliers are usually the best experts on their systems, and as such, it is essential for them to understand the landscape of cyber security threats and how they may impact safe operations. Cyber security threats are identified from multiple sources such as vulnerability databases, vendor and industry vulnerability notices, and security testing (by both vendors and OEMs), which often describe threats to a generic platform. It is important for the automotive system developers to analyze these threats and determine if they are applicable to their platforms and systems. Vulnerability data from intelligence agencies such as sector-specific Information Sharing and Analysis Centers, the U.S. Computer Emergency Readiness Team, the Industrial Control Systems Cyber Emergency Response Team, and MITRE's Common Vulnerability Environment can also assist in this analysis.

In other disciplines, such as safety, historical data are typically used to estimate the probability that a given threat may occur. Current data for "automotive" man-made and intentional malicious threats (cyber threats) are scarce and not sufficient to estimate occurrence and recurrence probabilities of these attacks with confidence, making the determination of a particular threat for any specific system fairly subjective at this time. It may be valuable to monitor and draw from intelligence data on similar components deployed in related but non-automotive environments when possible (e.g., aircraft, transit systems).

This process can play a key role in predicting component behavior and interactions within the system, which may integrate commercial-off-the-shelf (COTS) components and other propriety systems that may have been developed in isolation. The vast deployment of COTS components across multiple

industries serves as a very large repository of COTS interactions and may point to focus areas to assess cyber-vulnerabilities.

Techniques to identify threats should ideally include evidence of cyber activity across fleets, and related industries, through a trusted centralized repository or clearing house. Other industries have successfully established similar capabilities through the formation of sector-specific ISACs, e.g., the Public Transportation ISAC (PT-ISAC), the Surface Transportation ISAC (ST-ISAC), and the aviation/aircraft ISAC that is under development.

## B. Threat Analysis

### 1. Drawing Review

Once the interconnection and data flow drawings are completed, they are reviewed to provide context for development of the use cases. Examples of typical review questions are:

- What data paths are deemed critical to support the mission of the system?
- Are there any indirect data paths that an attacker could use to influence critical areas from non-critical areas?
- What are the gateways or components that handle differing levels of data criticality on the network?
- What are the physical and wireless entry points that connect the vehicle to external sources and networks?
- What are the confidentiality, integrity and availability data concerns?

### 2. Use Case Development

After creating and analyzing the interconnection and data flow drawings referenced above, use cases and potential attack scenarios can be developed. A use case or attack scenario describes a potential attack at a high level, so the amount of detail included in the use case should be kept to a minimum. The use case does not describe the minutiae of the attack, as the threat model is concerned only with the fundamentals of the attack. Typically, use case development requires input from multiple sources familiar with the system. Scenarios deemed too improbable on their own may later provide substance for other more likely types of attacks. Each use case includes a short descriptive title.

*(a) Use Case Elements*

When developing use cases the following elements are included.

- **Entry Points:** How an attacker may gain access to the vehicle systems
- **Access Methods:** The means that an attacker may use to access the entry points
- **Types:** The type of attack that may be launched
- **Outcomes:** The potential effects of the attack

Potential examples of use case elements for automobiles are listed in Table 3 through 6. Table 3 lists examples of entry points, both wired and wireless. Table 4 provides examples of access

methods. Table 5 provides an example of a type element in the use case. The types of attack in this example are borrowed from the STRIDE method. Table 6 lists examples of the outcomes element of the use case.

**Table 3: Use Case Elements – Potential Entry Points**

| Entry Point Type | Entry Point |
|---|---|
| **Wired** | OBD-II Port |
| | Network harness connectors |
| | Diagnostic Ports |
| | USB Port |
| | On-board Vehicle Networks (CAN, FlexRay, Ethernet, MOST, etc.) |
| | CD/DVD player |
| | Vehicle Charging Port |
| **Wireless – Short Range** | Radio Frequency (tire pressure monitor, key fob, etc.) |
| | Near Field Communications |
| | Wi-Fi |
| | Bluetooth |
| | Dedicated short range communications |
| **Wireless – Long Range** | GPS receiver |
| | GSM/CDMA |

**Table 4: Use Case Elements – Potential Access Methods**

| Access Method Type | Access Method |
|---|---|
| **Outside Networks** | Network-Call Center |
| | Network-Service Center |
| | Network-Home network |
| | Network-Cellular |
| **Component** | Component-Counterfeit |
| | Component-Tampered with or modified (OEM/Aftermarket) |
| **Portable** | Personal Computer |
| | OEM supplied-Smart key fob |
| | RF repeaters/transceivers |
| | Removable Media- e.g., CD or DVD disc |
| | Smart phone |
| | Smart music player- e.g., portable music device |
| | Custom ECU |

**Table 5: Use Case Elements - Types**

| Types (Borrowed From STRIDE Method) |
|---|
| **Spoofing Identity:** "Identity spoofing" is a key risk for applications that have many users but provide a single execution context at the application and database level. In particular, users should not be able to become any other user or assume the attributes of another user. |
| **Tampering with Data:** Users can potentially change data delivered to them, return it, and thereby potentially manipulate client-side validation, GET and POST results, cookies, HTTP headers, and so forth. The application should not send data to the user, such as interest rates or periods, which are obtainable only from within the application itself. The application should also carefully check data received from the user and validate that it is sane and applicable before storing or using it. |
| **Repudiation:** Users may dispute transactions if there is insufficient auditing or recordkeeping of their activity. For example, if a user denies initiating an action, and the activities were not tracked through the application, there may be insufficient basis for a resolution. Therefore, consider if the application requires non-repudiation controls, such as web access logs, audit trails at each tier, or the same user context from top to bottom. Preferably, the application should run with the user's privileges, not more, but this may not be possible with many off-the-shelf application frameworks. |
| **Information Disclosure:** Users are rightfully wary of submitting private details to a system. If it is possible for an attacker to publicly reveal user data at large, whether anonymously or as an authorized user, there will be an immediate loss of confidence and a substantial period of reputation loss. Therefore, applications must include strong controls to prevent user ID tampering and abuse, particularly if they use a single context to run the entire application. Also, consider if the user's web browser may leak information. Some web browsers may ignore the no caching directives in HTTP headers or handle them incorrectly. In a corresponding fashion, every secure application has a responsibility to minimize the amount of information stored by the web browser, just in case it leaks or leaves information behind, which can be used by an attacker to learn details about the application, the user, or to potentially become that user. Finally, in implementing persistent values, keep in mind that the use of hidden fields is insecure by nature. Such storage should not be relied on to secure sensitive information or to provide adequate personal privacy safeguards |
| **Denial of Service:** Application designers should be aware that their applications may be subject to a denial of service attack. Therefore, the use of expensive resources such as large files, complex calculations, heavy-duty searches, or long queries should be reserved for authenticated and authorized users, and not available to anonymous users. For applications that do not have this luxury, every facet of the application should be engineered to perform as little work as possible, to use fast and few database queries, to avoid exposing large files or unique links per user, in order to prevent simple denial of service attacks. |
| **Elevation of Privilege:** If an application provides distinct user and administrative roles, then it is vital to ensure that the user cannot elevate his/her role to a higher privilege one. In particular, simply not displaying privileged role links is insufficient. Instead, all actions should be gated through an authorization matrix, to ensure that only the permitted roles can access privileged functionality. |

**Table 6: Use Case Elements – Potential Outcomes**

| Outcomes | |
|---|---|
| Cause erratic behavior within normal operational parameters | Prevent normal data bus communications flow |
| Cause behavior outside of normal operational parameters that a driver can mitigate | Cause false or misleading information to be displayed to the driver |
| Cause behavior outside of normal operational parameters that a driver cannot mitigate | Cause driver distraction |
| Data breach in private information, e.g., passwords, address books | Theft of security data e.g., Digital Rights Management keys |

## 3. Vehicle Threat Matrix Development and Population

Once use cases have been developed, both the data contained within the use cases and data that supports the use cases are parsed into the vehicle threat matrix.

The vehicle threat matrix is used to consolidate threat data. It is constructed as a spreadsheet, allowing the matrix to be sorted by various categories as needed. In the matrix, categories of severity, sophistication level, and likelihood are indicated as high, medium, or low based on expert opinion. These categories allow for flexibility in their assignments while still maintaining the ability to sort the matrix data.

*(a)Threat Matrix Categories*

Table 7 contains the vehicle threat matrix categories and their descriptions. Category options for input are given where applicable.

**Table 7: Threat Matrix Categories**

| Matrix Category | Category Description | Category Options |
|---|---|---|
| **ID Number** | Identification number for the attack | |
| **Attacked Safety and Non-Safety Zone Groups /Attack Support Zone Groups** | Groups of various like categories of components and systems that are targeted by the attack or that are used to support the attack | • Communications:<br>  o Internal communications paths (e.g., CAN, FlexRay, IDb-1394, MOST)<br>• Vehicle Operations:<br>  o Powertrain - Engine control, hybrid drive systems, transmission, misc. power train sensors (e.g., torque convertor lockup)<br>  o Chassis and Safety - Brake control, steering, environmental sensors, air bag sensors, tire pressure sensors, misc. chassis sensors (e.g., steering angle)<br>  o Body Electronics - Instruments, door modules (e.g., remote locks, light control, seat control)<br>• Comfort Systems:<br>  o Climate control, air vent positions, remote start<br>• Infotainment:<br>  o Audio, display/video, navigation, embedded telephonic communications<br>• External interfaces:<br>  o GPS, diagnostic ports, USB, Bluetooth, key fob |
| **Attacked Zone Safety Related** | Whether or not the attacked zone contains safety related functions | • Yes<br>• No |
| **Component/System** | The component or system that is under attack | E.g., the electronic braking system as opposed to an electronic brake actuator |
| **Vulnerability[2] That Could Be Exploited** | Protocols/applications that could be used/corrupted in order to achieve the outcome of the attack | E.g., lack of firewalls, easy diagnostic access |

[2] NIST 800-30 defines vulnerability as "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or violation of the system's security policy."

| Matrix Category | Category Description | Category Options |
|---|---|---|
| **Attack Vector** | Entry point of the potential attack | E.g., OBD-II input, USB port, Bluetooth, GPS, audio system, etc. |
| **Access Method** | The transport mechanism that could be used to launch the attack | E.g., counterfeit component, portable device, call center network, RF repeater |
| **Attack Type** | Type of attack that could be used | • Spoofing identity<br>• Tampering with data<br>• Repudiation<br>• Information disclosure<br>• Denial of service<br>• Elevation of privilege |
| **Attack Name/Scenario** | A compressed narrative of the potential attack derived from the use cases | The narrative contains:<br>• Name of the attack (title)<br>• Who the attacker may be<br>• What the targeted component/system may be<br>• How the attacker may gain access to the component/system<br>• How the attack may be launched |
| **Resources Required** | Resources that may be needed to carry out the attack | E.g., hardware, software, access to vehicle (physical or remote), skill level |
| **Casualty Severity** | Projected outcome severity due to the potential attack | • High: High likelihood of severe injury or loss of life; loss of control of vehicle<br>• Medium: Potential to cause injury; experienced operator may be able to maintain control of vehicle<br>• Low: No injury; no loss of vehicle control during the attack; attack motive was for theft, nuisance, or publicity only |
| **Financial Severity** | The outcome severity in terms of direct or indirect financial loss to the owner, OEM, suppliers, or society | • High: Could cause major financial loss to vehicle, business or product reputation<br>• Medium: Potential to cause moderate financial loss to vehicle, business or product reputation<br>• Low: Minimal loss to vehicle, business or product reputation; attack motive was for nuisance or publicity only |

| Matrix Category | Category Description | Category Options |
|---|---|---|
| **Trip Phase** | The vehicle's movement category at the instance of the potential attack | One or more of the following may be used:<br>• Parked- not moving, engine shut off<br>• Idling- not moving, engine running<br>• Stop-and-go- i.e., heavy traffic<br>• City driving- typical city limits speed<br>• Urban driving- typical urban space speeds<br>• Highway driving- typical highway speeds<br>• Any- Not speed-dependent |
| **Loss of Privacy** | Whether or not items such as onboard address books, vehicle location, or passwords may have been compromised and shared with un-trusted parties | • Yes<br>• No |
| **Outcome** | Ramifications of a successful potential attack, assuming no mitigations were bypassed | |
| **Operator Override** | What an average operator may be able to do to override or avoid the ramifications of the potential attack | E.g., cycling the ignition; disabling functions via a switch; applying brakes |
| **Sophistication Level** | The design complexity of the potential attack | • High: Extremely complex code; may attack multiple components/systems; may use zero-day exploits; may have multiple triggers; hard to detect and remove; may be persistent (launching attack payload more than once), and may erase itself after attack is executed<br>• Medium: Moderately complex code; may contain remote trigger; may be persistent; may use zero-day exploits<br>• Low: Non-persistent; easy to detect; makes use of potential vulnerabilities |

| Matrix Category | Category Description | Category Options |
|---|---|---|
| **Difficulty of Implementation** | How difficult is it to implement the potential attack | • High: Extremely complex to implement; may require prolonged and advanced physical access to the vehicle; may need specialized tools and/or knowledge to launch.<br>• Medium: Moderately complex to implement; may require some physical access to vehicle; may need some and/or specialized knowledge to launch<br>• Low: Easy to implement; requires minimal/no physical access to vehicle; requires no specialized knowledge to launch |
| **Likelihood** | The likelihood of a potential attack to be carried out | • High: Well-known attack; very easy to perform; canned malware available for the attack<br>• Medium: Some knowledge of system needed; access to entry point more difficult; some custom code needed<br>• Low: Expert knowledge of component/system required; entry point difficult to access/unexpected; high level of custom coding involved |

*(b) Populating the Threat Matrix*

Below is one example of a use case that has been derived from research materials and input received from automotive SMEs on cybersecurity. Other use case examples can be found in Appendix A. It should be noted that these use case examples have not been reported in real world settings. Some have been studied in academic settings where experimenters had prolonged physical access to vehicles.

The use case below will be used to provide an example of the threat matrix population. Table 8 demonstrates how the threat matrix could be populated in this particular use case.

**Use Case Example: Brake Disconnect**

A person with physical access to the vehicle attaches a custom device [6] to the OBD-II port. The device has the capability to run a program that can monitor vehicle parameters over the CAN bus and execute the CAN device control service that can send a data packet normally used when building and testing the vehicle, to the electronic brake control module. This could diminish or

prevent the use of brakes when a programmed set of conditions takes place if there is linkage to the ECBM through the OBD-II data bus.

**Table 8: Threat Matrix Population Example**

| Matrix Category | Category Description | Option Chosen |
|---|---|---|
| **ID Number** | Identification number for the attack | 1 |
| **Attacked Safety and Non-Safety Zone Groups /Attack Support Zone Groups** | Groups of various like categories of components and systems that are targeted by the attack or that are used to support the attack | The EBCM has been identified as the component that could be attacked.<br><br>The attacker could use a device connected to the CAN bus, which falls under the external interface zone. The device connected to the CAN bus communicates with the EBCM, therefore the communications zone is also used. |
| **Attacked Zone Safety Related** | Whether or not the attacked zone contains safety related functions | The attack could occur against the Vehicle Operations group which may contain safety related items. |
| **Component/System** | The component or system that is under attack | The EBCM is the component that could be subject to an attack. |
| **Vulnerability That Could Be Exploited** | Protocols/applications that could be used/corrupted in order to achieve the outcome of the attack | In this category, subject matter knowledge combined with the interconnection and data flow drawings could highlight vulnerabilities that assist or allow the use case attack. |
| **Attack Vector** | Entry point of the potential attack | The attack vector could be the OBD-II port. In a complex attack attempt, the attack vector should describe the highest point of entry for the potential attack. |
| **Access Method** | The transport mechanism that could be used to launch the attack | A portable device (PC/microcomputer) may have been used to gain access to the platform's network. |
| **Attack Type** | Type of attack that could be used | Elevation of privileges |
| **Attack Name/Scenario** | A compressed narrative of the potential attack derived from the use cases | The attack scenario is the use case developed earlier. (If it's too lengthy it will be condensed down to the fundamentals of the attack). |
| **Resources Required** | Resources that may be needed to carry out the attack | Items such as hardware, software, access time, and prior knowledge are some of the items that can be used. |

| Matrix Category | Category Description | Option Chosen |
|---|---|---|
| **Casualty Severity** | Projected outcome severity due to the potential attack | There may be a degradation or loss of brake functionality; there could have been a loss of control which could have resulted in severe injury or loss of life. Therefore a severity level of high would be assigned. |
| **Financial Severity** | The outcome severity in terms of direct or indirect financial loss to the owner, OEM, suppliers, or society | There may be degradation or loss of brake functionality. Therefore a severity level of High would be assigned. |
| **Trip Phase** | The vehicle's movement category at the instance of the potential attack | "Highway speeds" would be indicated for the trip phase because the scenario may have triggered at high speed. |
| **Loss of Privacy** | Whether or not items such as onboard address books, vehicle location, or passwords may have been compromised and shared with un-trusted parties | "No" would be selected as there is no attempt during this attack to extract any data from either the passengers or vehicle platform. |
| **Outcome** | Ramifications of a successful potential attack, assuming no mitigations were bypassed | The braking capability of the vehicle may have been degraded or lost temporarily or for extended periods of time. |
| **Operator Override** | What an average operator may be able to do to override or avoid the ramifications of the potential attack | Potentially using emergency brakes; disengaging engine power; lowering of max gear setting |
| **Sophistication Level** | The design complexity of the potential attack | Significant knowledge of proprietary systems, coding and tools used would have been required implying "medium" complexity designation. |
| **Difficulty of Implementation** | How difficult is it to implement the potential attack | Brief direct access to the vehicle would have been needed in order to attach the microcomputer, which may or may not be detectable by the operator. A "low" designation is suggested. |
| **Likelihood** | The likelihood of a potential attack to be carried out | Like other field designations above, there is subjectivity in assessing likelihood of threats. This case could be seen as analogous to someone devising a mechanical tampering method that could also disable the brakes. |

Due to the number of categories, the threat matrix could become difficult to read when included in a report; therefore, a format specifically designed for reports is used. Figure 4 shows the completed threat

matrix for the example use case, with the working matrix layout. Figure 5 shows the same data, but in the matrix style for reports. Completed threat matrices for the other use cases (described in Appendix A) can be found in the report matrix format in Appendix B.

| ID # | Attacked Zone Group | Attacked Zone Safety Related | Attack Support Zone Groups | Component/ System | Vulnerability That Could Be Exploited | Attack Vector | Access Method | Attack Type | Attack Name/ Scenario | Resources Required | Casualty Severity | Financial Severity | Trip Phase | Loss of Privacy | Outcome | Operator Override | Sophistication Level | Difficulty of Implementation | Likelihood |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Vehicle Operations (Chassis and Safety) | Y | Communications, External Interface | Electronic Brake Control Module (EBCM) | EBCM Device control key and seed only 16 bits; Ability to access diagnostic areas | ODB-II Port | Portable Device | Elevation of Privileges | Brake disconnect: A person with physical access to the vehicle attaches a custom device to the OBD-II port. The device has the capability to run a program which can monitor vehicle parameters over the CAN bus and execute the CAN Device Control Service that can send a data packet normally used when building and testing the vehicle, to the Electronic Brake Control Module (EBCM). This could diminish or prevent the use of brakes when a programmed set of conditions takes place if there is linkage to the ECBM through the OBD-II data bus. | Access to OBD-II port, ability to run CAN Device Service, knowledge of EBCM packet information | High | High | Highway speed | No | Cause behavior outside of normal operating parameters. Brakes will not engage. Operator is unable to stop the car using service brakes. | Depending on conditions at the time of the attack, operator may be able to use emergency brakes to bring vehicle to a controlled halt. | Medium | Low | Medium |

**Figure 4: Threat Matrix Working Layout**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 1 | | **Attacked Zone Group** | Vehicle Operations (Chassis and Safety) |
| | | | **Attacked Zone Safety Related** | Y |
| **Vulnerability That Could Be Exploited** | EBCM device control key and seed only 16 bits; ability to access diagnostic areas | | **Attack Support Zones** | Communications, External Interface |
| | | | **Component/ System** | EBCM |
| | | | **Attack Vector** | ODB-II Port |
| | | | **Access Method** | Portable Device |
| | | | **Attack Type** | Elevation of privileges |
| | | | **Casualty Severity** | High |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Highway speed |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Low | | **Likelihood** | Medium |
| | | | **Operator Override** | Depending on conditions at the time of the attack, operator may be able to use emergency brakes to bring vehicle to a controlled halt. |
| **Attack Scenario** | Brake Disconnect:<br>A person with physical access to the vehicle attaches a custom device to the OBD-II port. The device has the capability to run a program which can monitor vehicle parameters over the CAN bus and execute the CAN device control service that can send a data packet normally used when building and testing the vehicle, to the EBCM. This could diminish or prevent the use of brakes when a programmed set of conditions takes place if there is linkage to the ECBM through the OBD-II data bus. | | | |
| **Resources Required** | Access to OBD-II port, ability to run CAN device service, knowledge of EBCM packet information | | | |
| **Outcome** | Cause behavior outside of normal operating parameters. Brakes will not engage. Operator is unable to stop the car using service brakes. | | | |

**Figure 5: Threat Matrix Report Layout**

# Appendix A: Use Case Examples

The use cases below have been derived from research materials and input received from automotive SMEs on cybersecurity. It should be noted that these use case examples have not been reported in real world settings. Some have been studied in academic settings where experimenters had prolonged physical access to vehicles.

**Brake Disconnect** [6]
A person with physical access to the vehicle attaches a custom device to the OBD-II port. The device has the capability to run a program which can monitor vehicle parameters over the CAN bus and execute the CAN device control service that can send a data packet normally used when building and testing the vehicle, to the EBCM. This could diminish or prevent the use of brakes when a programmed set of conditions takes place if there is linkage to the ECBM through the OBD-II data bus.

**Horn Activation**
A person with physical access to the vehicle installs a wireless interface to the USB port which can remotely send commands to the vehicle data bus such as to activate the vehicle's horn [6, 7]. This could happen via short range proximity wireless or long range wireless pathways.

**Engine Halt Air Bag**
An owner installs an after-market radio purchased from a third party, which may come with an on-board malware that can access a vehicle data bus (assuming there is a pathway) that could potentially mimic the air bag deployed message from the inflatable restraint sensing and diagnostic module to the ECM. The ECM reads the forged packet and shuts down the engine at highway speeds.

**Portable Device Injection**
The owner downloads music from an untrusted source and creates a CD. The downloaded file could contain specific malware that when played sets the dominant state node for the infotainment unit for that vehicle and then uses the infotainment unit to launch a denial-of-service type of attack against the BCM. As the attack takes place, the instrument cluster may freeze in its current state, and when the vehicle is turned off, it may not allow the vehicle to be restarted without communication to the BCM being reestablished first.

**Dealership Download**
The LAN at the service department gets compromised. When an automobile is connected to the dealership's network via the OBD-II port during the process of providing service, the attacker could install malware that could be exploited later on while using the service department's computers as a pass through.

**Cellular Attack**
An attacker calls the car's embedded cell number [8] and launches malicious code that defeats the analog to digital modem's software security challenge via a buffer overflow attack.[3] Once the software modem is compromised, the attacker could gain access to the telematics unit. The malicious code then could cause the telematics unit to connect to an IP address. Once a connection to the IP address may be established, the attacker could use the telematics unit as an entry point to download and run further malicious code, which could execute subsequent attacks that may provide automotive systems false sensor data which could result in erroneous action.

**Key Fob Cloning**
An attacker exploits vulnerabilities in the theft alarm system to make a clone of a key fob [9], which provides full access to the car.

**Long Distance Keyless Entry Repeater Version**
When the vehicle is parked, a team of attackers use loop antennas and wireless repeaters to relay the polling request from the driver's key fob [10] to the vehicle to get access. The same method could also be used to start the vehicle.

**Call Center Fleet Attack**
A hacker group gains control of servers at a telematics call center. The hackers then could issue engine disable commands to all cars under their control from the compromised call center.

**Car Rental or Lease**
A person with access to large number of vehicles that are typically operated by others, such as a rental car [6] employee, could potentially install malware via physical access to the vehicle. The malware could take form in any of the attack types described in this section.

**Malware Onboard**
An end-of-line programming station gets compromised with malware. The malware is downloaded into ECUs during the manufacturing process. The malware could be designed to execute under specific conditions and time periods. The malware could take form in any of the attack types described in this section.

[3] A buffer overflow attack is where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including a breach of system security.

# Appendix B: Completed Threat Matrices

**Brake Disconnect**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 1 | | **Attacked Zone Group** | Vehicle Operations (Chassis and Safety) |
| | | | **Attacked Zone Safety Related** | Y |
| **Vulnerability That Could Be Exploited** | EBCM Device control key and seed only 16 bits; Ability to access diagnostic areas | | **Attack Support Zones** | Communications, External Interface |
| | | | **Component/ System** | Electronic Brake Control Module |
| | | | **Attack Vector** | ODB-II Port |
| | | | **Access Method** | Portable Device |
| | | | **Attack Type** | Elevation of Privileges |
| | | | **Casualty Severity** | High |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Highway Speed |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Low | | **Likelihood** | Medium |
| | | | **Operator Override** | Depending on conditions at the time of the attack, operator may be able to use emergency brakes to bring vehicle to a controlled halt. |
| **Attack Scenario** | Brake Disconnect:<br>A person with physical access to the vehicle attaches a custom device to the OBD-II port. The device has the capability to run a program which can monitor vehicle parameters over the CAN bus and execute the CAN device control service that can send a data packet normally used when building and testing the vehicle, to the electronic brake control module. This could diminish or prevent the use of brakes when a programmed set of conditions takes place if there is linkage to the ECBM through the OBD-II data bus. | | | |
| **Resources Required** | Access to OBD-II port, ability to run CAN device service, knowledge of EBCM packet information | | | |
| **Outcome** | Cause behavior outside of normal operating parameters. Brakes will not engage. Operator is unable to stop the car using service brakes. | | | |

**Horn Activation**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 2 | | **Attacked Zone Group** | Vehicle Operations (Body Electronics) |
| | | | **Attacked Zone Safety Related** | N |
| **Vulnerability That Could Be Exploited** | Device control key not needed | | **Attack Support Zones** | Communications, External Interface |
| | | | **Component/ System** | Body Control Module |
| | | | **Attack Vector** | USB Port |
| | | | **Access Method** | RF transmitter |
| | | | **Attack Type** | Spoofing |
| | | | **Casualty Severity** | Low |
| | | | **Financial Severity** | Low |
| | | | **Trip Phase** | Any |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Medium | | **Likelihood** | Medium |
| | | | **Operator Override** | None |
| **Attack Scenario** | Horn Activation:<br>A person with physical access to the vehicle installs a wireless interface to the USB port which can remotely send commands to the vehicle data bus such as to activate the vehicle's horn. This could happen via short range proximity wireless or long range wireless pathways. | | | |
| **Resources Required** | Access to USB port, ability to run CAN device service, knowledge of BCM packet information | | | |
| **Outcome** | Cause driver distraction. Cause erratic behavior within normal parameters. Horn blows on command. | | | |

**Engine-Halt Airbag**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 3 | | **Attacked Zone Group** | Vehicle Operations (Engine Control) |
| | | | **Attacked Zone Safety Related** | Y |
| **Vulnerability That Could Be Exploited** | ECM Can be spoofed, ECM can be reached from non-critical area | | **Attack Support Zones** | Communications, Infotainment |
| | | | **Component/ System** | Engine Control Module (ECM) |
| | | | **Attack Vector** | Network Harness Connectors |
| | | | **Access Method** | Component Tampered With/Modified |
| | | | **Attack Type** | Spoofing |
| | | | **Casualty Severity** | Medium |
| | | | **Financial Severity** | Medium |
| | | | **Trip Phase** | City, Urban, Highway |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Low | | **Likelihood** | Low |
| | | | **Operator Override** | None |
| **Attack Scenario** | Engine-Halt Airbag:<br>An owner installs an after-market radio purchased from a third party, which may come with an on-board malware that can access a vehicle data bus (assuming there is a pathway) that could potentially mimic the airbag deployed message from the inflatable restraint sensing and diagnostic module to the ECM. The ECM reads the forged packet and shuts down the engine at highway speeds. | | | |
| **Resources Required** | Knowledge of CAN and SDM protocols and packet composition, ability to design and load malware into radio | | | |
| **Outcome** | Cause erratic behavior outside of normal parameters. Engine shuts off while at speed. Possible loss of power steering, and power assist for braking. | | | |

**Portable Device Injection**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 4 | | **Attacked Zone Group** | Vehicle Operations (Body Electronics) |
| | | | **Attacked Zone Safety Related** | N |
| **Vulnerability That Could Be Exploited** | CAN susceptible to DOS attacks, Node can be set to dominant state indefinitely | | **Attack Support Zones** | Communications, External Interfaces, Infotainment |
| | | | **Component/ System** | Body Control Module (instrument panel) |
| | | | **Attack Vector** | CD/DVD Player |
| | | | **Access Method** | Removable Media |
| | | | **Attack Type** | Denial of Service |
| | | | **Casualty Severity** | Low |
| | | | **Financial Severity** | Medium |
| | | | **Trip Phase** | Any |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Low | | **Likelihood** | Medium |
| | | | **Operator Override** | None |
| **Attack Scenario** | Portable Device Injection:<br>The owner downloads music from an untrusted source and creates a CD. The downloaded file could contain specific malware that when played sets the dominant state node for the infotainment unit for that vehicle and then uses the infotainment unit to launch a denial-of-service type of attack against the BCM. As the attack takes place, the instrument cluster may freeze in its current state, and when the vehicle is turned off, it may not allow the vehicle to be restarted without communication to the BCM being reestablished first. | | | |
| **Resources Required** | Knowledge of CAN and BCM protocols and packet composition, ability to design malware program | | | |
| **Outcome** | Cause erratic behavior outside of normal parameters. Prevents normal bus communications flow. Causes false or misleading information to be displayed. Instrument panel freezes. When car is turned off cannot be restarted unless communication to BCM is restored. | | | |

**Dealership Download**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 5 | | **Attacked Zone Group** | Vehicle Operations |
| | | | **Attacked Zone Safety Related** | N/A |
| **Vulnerability That Could Be Exploited** | No intrusion detection system (IDS), improper or no firewall configurations, multiple network links to internet, weak password strength, etc. | | **Attack Support Zones** | Communications, External Interfaces |
| | | | **Component/ System** | CAN Network/ECUs |
| | | | **Attack Vector** | Diagnostic Port |
| | | | **Access Method** | Network Service Center |
| | | | **Attack Type** | Tampering With Data |
| | | | **Casualty Severity** | Any (dependent on environment at time of the attack) |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Any (dependent on environment at time of the attack) |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Medium | | **Likelihood** | Medium |
| | | | **Operator Override** | Unknown |
| **Attack Scenario** | Dealership Download:<br>The LAN at the service department gets compromised. When an automobile is connected to the dealership's network via the OBD-II port during the process of providing service, the attacker could install malware that could be exploited later on while using the service department's computers as a pass through. | | | |
| **Resources Required** | Ability to gain control of service department network, ability to create malware for CAN environment | | | |
| **Outcome** | Multiple automobiles affected, service department's reputation destroyed. | | | |

**Cellular Attack**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 6 | | **Attacked Zone Group** | Vehicle Operations |
| | | | **Attacked Zone Safety Related** | N/A |
| **Vulnerability That Could Be Exploited** | Flaws in random implementation challenge, and authentication system, Possibility of playing modulated version of attack payload. Susceptible to buffer overflow | | **Attack Support Zones** | Communications, Infotainment |
| | | | **Component/ System** | Telematics |
| | | | **Attack Vector** | GSM/CDMA |
| | | | **Access Method** | Cellular Network |
| | | | **Attack Type** | Tampering With Data |
| | | | **Casualty Severity** | Any (dependent on the environment at time of the attack) |
| | | | **Financial Severity** | Any (dependent on the environment at time of the attack) |
| | | | **Trip Phase** | Any |
| | | | **Sophistication Level** | High |
| **Difficulty of Implementation** | High | | **Likelihood** | Low |
| | | | **Operator Override** | None |
| **Attack Scenario** | Cellular Attack:<br>An attacker calls the car's embedded cell number and launches malicious code that defeats the analog to digital modem's software security challenge via a buffer overflow attack. Once the software modem is compromised, the attacker could gain access to the telematics unit. The malicious code then could cause the telematics unit to connect to an IP address. Once a connection to the IP address may be established, the attacker could use the telematics unit as an entry point to download and run further malicious code, which could execute subsequent attacks that may provide automotive systems false sensor data which could result in erroneous action. | | | |
| **Resources Required** | Extensive knowledge of software modems, ability to reverse engineer modem protocol | | | |
| **Outcome** | Car’s brakes are applied for no apparent reason | | | |

**Key Fob Cloning**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 7 | | **Attacked Zone Group** | Vehicle Operations (Body Electronics) |
| | | | **Attacked Zone Safety Related** | N |
| **Vulnerability That Could Be Exploited** | Key fob flashing via OBD-II port | | **Attack Support Zones** | Communications, External Interfaces |
| | | | **Component/ System** | Key Fob |
| | | | **Attack Vector** | OBD-II Port |
| | | | **Access Method** | Custom ECU |
| | | | **Attack Type** | Spoofing |
| | | | **Casualty Severity** | Low |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Parked |
| | | | **Sophistication Level** | Low |
| **Difficulty of Implementation** | Low | | **Likelihood** | High |
| | | | **Operator Override** | None |
| **Attack Scenario** | Key Fob Cloning:<br>An attacker exploits vulnerabilities in the theft alarm system to make a clone of a key fob, which provides full access to the car. | | | |
| **Resources Required** | Knowledge of anti-theft alarm system, OBD key programmer hardware and blank/used key fobs obtained via internet | | | |
| **Outcome** | Automobile can be easily stolen. | | | |

**Long Distance Keyless Entry Repeater Version**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 8 | | **Attacked Zone Group** | Vehicle Operations (Body Electronics) |
| | | | **Attacked Zone Safety Related** | N |
| **Vulnerability That Could Be Exploited** | Key fob and car transmitting in open | | **Attack Support Zones** | Communications, External Interfaces |
| | | | **Component/ System** | Keyless Entry System |
| | | | **Attack Vector** | Radio Frequency |
| | | | **Access Method** | RF Repeater |
| | | | **Attack Type** | Spoofing |
| | | | **Casualty Severity** | Low |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Parked |
| | | | **Sophistication Level** | Low |
| **Difficulty of Implementation** | Low | | **Likelihood** | Medium |
| | | | **Operator Override** | Keep Key Fob in RF Shielded Area |
| **Attack Scenario** | Long-Distance Keyless Entry Repeater Version:<br>When the vehicle is parked, a team of attackers use loop antennas and wireless repeaters to relay the polling request from the driver's key fob to the vehicle to get access. The same method could also be used to start the vehicle. | | | |
| **Resources Required** | Knowledge of specific automobile/owner target, accomplice, wireless repeater set-up, two small loop antennas | | | |
| **Outcome** | Automobile can be easily stolen. | | | |

**Call Center Fleet Attack**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 9 | | **Attacked Zone Group** | Vehicle Operations (Power Train) |
| | | | **Attacked Zone Safety Related** | Y |
| **Vulnerability That Could Be Exploited** | Weak or non-existent IDS, firewalls incorrectly configured, etc. | | **Attack Support Zones** | Communications, External Interfaces |
| | | | **Component/ System** | Telematics |
| | | | **Attack Vector** | GSM/CDMA |
| | | | **Access Method** | Network Call Center |
| | | | **Attack Type** | Spoofing |
| | | | **Casualty Severity** | Medium |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Any |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | | | **Likelihood** | Low |
| | | | **Operator Override** | None |
| **Attack Scenario** | Call Center Fleet Attack:<br>A hacker group gains control of servers at a telematics call center. The hackers then could issue engine disable commands to all cars under their control from the compromised call center. | | | |
| **Resources Required** | Knowledge of firewalls, various network hacking techniques, and telematics command groups | | | |
| **Outcome** | Cause erratic behavior outside of normal operational parameters. Automobiles not running will be able to be started. Automobiles on the road will initiate a controlled shutdown. | | | |

**Car Rental or Lease**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 10 | | **Attacked Zone Group** | Vehicle Operations (Power Train) |
| | | | **Attacked Zone Safety Related** | Y |
| **Vulnerability That Could Be Exploited** | Ability to re-flash ECM without authentication | | **Attack Support Zones** | Communications, External Interfaces |
| | | | **Component/ System** | Engine Control Module |
| | | | **Attack Vector** | OBD-II port |
| | | | **Access Method** | PC |
| | | | **Attack Type** | Elevation of privileges |
| | | | **Casualty Severity** | Medium |
| | | | **Financial Severity** | High |
| | | | **Trip Phase** | Any |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | Medium | | **Likelihood** | Medium |
| | | | **Operator Override** | None |
| **Attack Scenario** | Car Rental or Lease:<br>A person with access to large number of vehicles that are typically operated by others (such as a rental car employee) could potentially install malware via physical access to the vehicle. The malware could take form in any of the attack types described in this section. | | | |
| **Resources Required** | Knowledge of CAN and ECU flashing procedures, ability to design and load malware into re-flashed ECM, access to fleet cars | | | |
| **Outcome** | Automobiles not running will not be able to be started. Automobiles on the road will shut down. Major loss of business for rental car facility. | | | |

**Malware Onboard**

| Threat Model Matrix | | | | |
|---|---|---|---|---|
| | | | | |
| **ID#** | 11 | | **Attacked Zone Group** | Vehicle Operations (Power Train) |
| | | | **Attacked Zone Safety Related** | Y |
| **Vulnerability That Could Be Exploited** | Poor IT security at ECU manufacturer, ability to spoof transmission control module | | **Attack Support Zones** | Communications |
| | | | **Component/ System** | Transmission Control Module |
| | | | **Attack Vector** | Network |
| | | | **Access Method** | Component Tampered With/Modified |
| | | | **Attack Type** | Tampering With Data |
| | | | **Casualty Severity** | Low |
| | | | **Financial Severity** | Medium |
| | | | **Trip Phase** | Idling |
| | | | **Sophistication Level** | Medium |
| **Difficulty of Implementation** | High | | **Likelihood** | Low |
| | | | **Operator Override** | Manual Solenoid Release (some cars) |
| **Attack Scenario** | Malware Onboard:<br>An end-of-line programming station gets compromised with malware. The malware is downloaded into ECUs during the manufacturing process. The malware could be designed to execute under specific conditions and time periods. The malware could take form in any of the attack types described in this section. | | | |
| **Resources Required** | Knowledge of CAN and ECU manufacturing procedures, ability to design and load malware, access to PC linked to manufacturing process | | | |
| **Outcome** | Automatic transmission will be locked in park. Possible OEM reputation damage. | | | |

# Appendix C: Works Cited


[1] Merritt, R. (2011, May 4)."IBM tells story behind Chevy Volt design. San Jose, CA: EE Times. Retrieved from www.eetimes.com/document.asp?doc_id=1259444

[2] Moving Ahead for Progress in the 21st Century Act (MAP-21). P.L. 112-141, 49 *U.S.C.* 30171. Sec. 30171.

[3] Microsoft Developer Networks. (2005). The STRIDE threat model. Retrieved from http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[4] Open Web Application Security Project . (2010, September 29). Threat risk modeling. Retrieved from www.owasp.org/index.php/Threat_Risk_Modeling

[5] Microsoft Developer Network. (2005). Cheat sheet: Web application security frame. Retrieved from http://msdn.microsoft.com/en-us/library/ff649461.aspx

[6] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., … & Savage, S. (2010). Experimental security analysis of a modern automobile. In *31st IEEE Symposium on Security and Privacy*, Oakland, CA, May 16-19, 2010.

[7] Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (2008). E-safety vehicle intrusion protected applications. Munich, Germany: Author. Retrieved from http://evita-project.org/

[8] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., … & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In D. Wagner (Chair), *SEC'11, Proceedings of the 20th USENIX Conference on Security*, USENIX Association, August 8-12, San Francisco, CA. . Available at www.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf

[9] Torchinsky, J. (2012, July 6). Watch hackers steal a BMW in three minutes. (Web page). Retrieved from http://jalopnik.com/5923802/watch-hackers-steal-a-bmw-in-three-minutes?tag=car-crime

[10] Francillon, A., Danev, B., & Capkun, S. Relay attacks on passive keyless entry and start systems in modern cars. Paper presented at *Network and Distributed System Security Symposium*, February 6-9, 2011, San Diego, CA. Available at www.internetsociety.org/sites/default/files/franc.pdf

DOT HS 812
September 2014

U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**


10930-090314-v1a