2022 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
CYBERSECURITY OF GROUND SYSTEMS TECHNICAL SESSION
AUGUST 16-18, 2022 - NOVI, MICHIGAN

ELECTRIC VEHICLE CHARGING CYBERSECURITY

Austin Dodson, Patrick Saenz

Southwest Research Institute, San Antonio, TX

ABSTRACT

Electric vehicles (EVs) are growing in popularity in both the defense and commercial sectors, with mandates and directives helping to inspire greater adoption. This increased popularity requires testing of an EV's connected systems to ensure security against cyberattacks. The research efforts presented in this paper show that the EV battery management system (BMS) and SAE J1772 charging standard are susceptible to cyberattacks. Spoofing attacks on the vehicle's J1772 charging interface can be used to limit or prevent charging of an EV's battery. Penetration testing of an EV's BMS shows how vulnerabilities can be exploited to successfully attack an EV through the Controller Area Network (CAN) bus on the vehicle. This paper also discusses the implications of these attacks from a defense standpoint with high-level protections also discussed.

1. INTRODUCTION

Electric vehicles (EVs) are growing in popularity in both the defense and commercial sectors with mandates and directives helping to inspire greater adoption. This increased popularity requires testing of an EV's connected systems to ensure security against cyberattacks.

To understand where cyberattacks are possible, a holistic view of an EV and its connected systems is required. Some of these interfaces will vary, but common across most EVs are the in-vehicle network, or Controller Area Network (CAN) bus and the EV's charging interface, which will also vary depending on physical location and manufacturer (e.g. China's GB/T charging interface, Tesla's proprietary charging interface).

The CAN bus is a serial data communication interface which uses two wires to generate a differential signal for communication. Devices on the network are called nodes and are connected to the communication lines directly. CAN messages are broadcast to all nodes on the network. To prevent collisions on the network, each node is assigned an arbitration identifier or arb ID which is the first part of a message broadcast. Each device receives this arb ID bit-by-bit, and device priority is determined by which device transmitted the lowest value arb ID.

All EVs maintain an external charging interface for use at charging stations. The charging interfaces are standardized, and the common interface for North America is SAE J1772. The charging interface (review Figure 1, shown as charger control system (CCS)) is responsible for supplying charging power to the battery pack. It also contains safety features that can trip a fail-safe relay if unsafe conditions are detected (e.g. supplying a charge without a proper connection to the EV). For correct operation, the CCS requires communication from the Battery Management System (BMS), usually over CAN.

The BMS controls the charging process by initiating and stopping charging. To begin charging, the BMS will first check the charge information and health of each cell (or group of cells) in the battery pack. If these initial checks pass, the BMS will send signals enabling the EV to charge, in which the charging equipment will begin providing charging power to the EV. On top of health checks, the BMS provides adjustable safety limits for the battery pack which can shut down charging and discharging if the battery or charger exceeds safe limits.

While charging systems have safety mechanisms to help mitigate risk, they are proven to be vulnerable to cyber-attacks. This research will expose various methods to attack an EV charging system using both spoofing attacks on the CAN bus and Man-in-the-Middle (MitM) attacks on the J1772 interface.

2. SPOOFING CCS & BMS FUNCTIONALITY

Spoofing attacks are characterized by an attacker sending data to appear as another trusted node on a network. While these attacks are much more common in traditional ethernet-based networks, these types of attacks are also possible on the CAN bus. In the context of an EV, an attacker can attempt to spoof the messages associated with the BMS to manipulate the EV charging process. For example, an attacker can attempt to stop and EV from charging by either triggering a safety mechanism, or by stopping communication between the BMS and the CCS.

In this research, a security assessment was performed to investigate spoofing attacks and their effects against a representative EV charging system. To begin, the research team created an access point on the CAN bus by attaching a new node directly on the network between the CCS and the BMS. Spoofing attacks were then injected into the CAN bus network and the effects were recorded. This was performed on a testbed designed to mimic an EV charging network as shown in Figure 1.

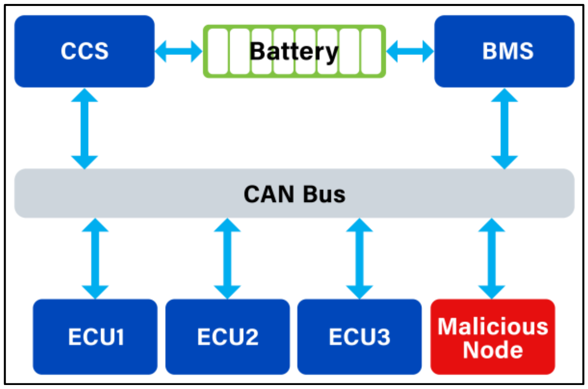

Figure 1. CAN Bus Testbed

In this security assessment, six (6) different attacks were designed to manipulate the charging and discharging of the EV onboard battery pack. These attacks and their effects are detailed in the following subsections.

2.1. Attack 1: Spoof CCS Current Parameter

For this attack, as shown in Figure 2, the attacking node spoofs messages to assume the identity of the BMS by using the “BMS to CCS” arb ID. This message stores information on the voltage and current to charge the battery pack. To execute this attack, the attacker node does not initially send any messages and allows the charger to normally charge the battery pack. After a user-specified number of correct messages, the hacker node starts to gradually increase the current by spoofing the “BMS to CCS” arb ID. If the BMS is protecting the battery pack effectively, the BMS should shut down the charge relay after crossing the current safety threshold. This would allow the attacking node to stop the charging process.

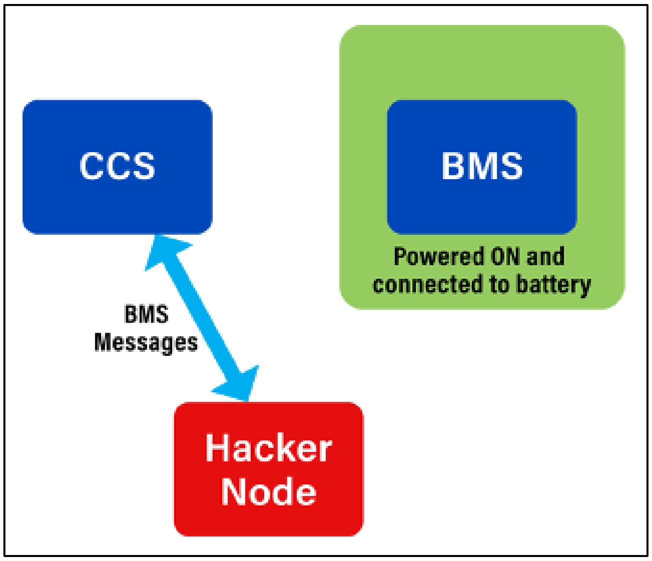

Figure 2. Spoof CCS Current Arb ID Setup

This attack was successful and triggered the BMS safety mechanism. Charging of the battery was halted and required a power cycle to reset the system.

2.2. Attack 2: Spoof CCS Voltage Parameter

For this attack, the same configuration as Attack 1 is used as shown in Figure 2. Also, like Attack 1, the attacking node spoofs messages to assume the identity of the BMS by using the "BMS to CCS" arb ID. This message stores information on the voltage and current to charge the battery pack. To execute this attack, the attacker node does not initially send any messages and allows the charger to normally charge the battery pack. After a user-specified number of correct messages, the hacker node starts to gradually increase the voltage by spoofing the "BMS to CCS" arb ID. If the BMS is protecting the battery pack effectively, the BMS should shut down the charge relay after crossing the voltage safety threshold. This would allow the attacking node to stop the charging process.

This attack was not successful as it did not increase the actual voltage used for charging the battery pack; thus, the BMS safety mechanism was not triggered. This attack did not stop the CCS from charging the battery correctly.

2.3. Attack 3: Man-in-the-Middle CCS Parameters

For this attack, as shown in Figure 3, the hacker node is between the communication from CCS to BMS, and spoofs messages to the BMS acting as the CCS by using the "CCS to BMS" parameter ID. For this configuration, the CCS is removed from the CAN bus by disconnecting it from the bus or powering it off. The purpose of this attack is to deny service to the battery pack without the BMS knowing that the CCS is not currently communicating/connected. If successful, this attack will cause the BMS to stop charging because of an error state (e.g. charging equipment on EV malfunction).

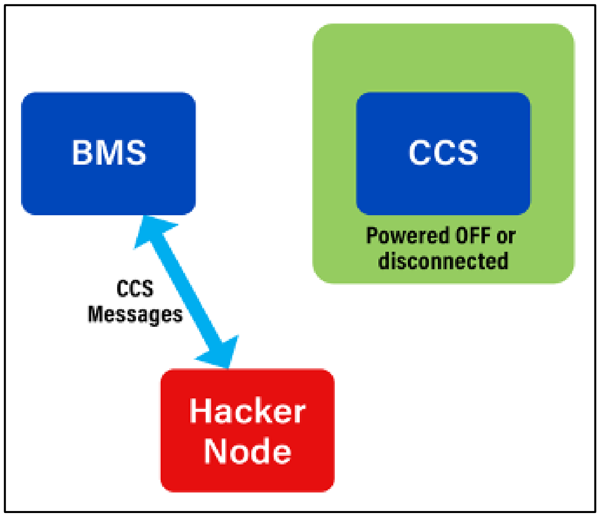

Figure 3. Attacks 3, 4, and 5 Configuration

This attack was successful as it was able to get past any error flagging in the BMS and prevented the system from charging.

2.4. Attack 4: Spoofing BMS Current Parameter

For this attack (configuration in Figure 3), the hacker node spoofs messages to assume the identity of the CCS by sending messages containing the "CCS to BMS" parameter ID. For this configuration, the CCS is removed from the CAN bus by disconnecting it from the bus or powering it off. Once the EV starts charging and a user-specified number of CAN messages with the "CCS to BMS" parameter ID have been seen, the attacker node starts sending messages to gradually increase the current. If successful, this attack will force the BMS to protect the battery pack by shutting down the charge relay after receiving false current readings from the CCS.

This attack did not trigger any BMS safety mechanisms, and the system was able to continue charging.

2.5. Attack 5: Spoofing BMS Voltage Parameter

For this attack (configuration in Figure 3), the hacker node spoofs messages to assume the identity of the CCS by sending messages containing the "CCS to BMS" parameter ID. For this configuration, the CCS is removed from the CAN bus by disconnecting it from the bus or powering it off. Once the EV starts charging and a user-specified number of CAN messages with the "CCS to BMS" parameter ID have been seen, the attacker node starts sending messages to gradually increase the voltage. If successful, this attack will force the BMS to protect the battery pack by shutting down the charge relay after receiving false voltage readings from the CCS.

This attack did not trigger any BMS safety mechanisms, and the system was able to continue charging.

2.6. Attack 6: Man-in-the-Middle CAN Network Flooding

For this attack, as shown in Figure 4, the hacker node spoofs messages to assume the identity of the CCS by sending messages containing the "CCS to BMS" parameter ID. Instead of attempting to set or increase the current values, the content of the messages are all 1s. The purpose of this is to cause a Denial of Service (DoS), in which the BMS is overwhelmed by improperly formatted messages on the CAN bus.

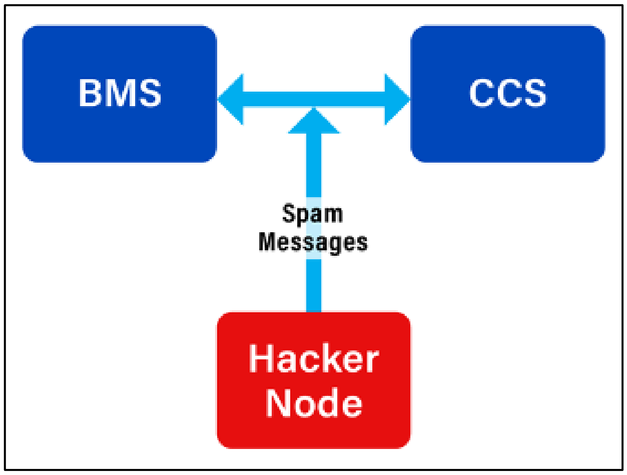

Figure 4. Man-in-the-Middle Flood Configuration

This attack required overwhelming the hardware due to the timing of the messages containing the "CCS to BMS" parameter ID. The CCS requires a communication packet from the BMS at a minimum of every five (5) seconds or charging is stopped. The CAN bus was successfully flooded with messages preventing communication for greater than five (5) second periods and the CCS was not able to begin charging.

2.7. Results

The results of these attacks show vulnerabilities exist in the BMS' and CCS' handling of messages on the CAN bus. These attacks can cause damage to the battery or lead to costly repairs to the system due to incorrect error reporting. One issue with these attacks is that they require access to the CAN bus, and therefore will often require a level of physical access to the interior of the EV (assuming no external-facing CAN bus connections exist). Access to the CAN bus is also possible through pairing these attacks with an exploit that provides remote access. For example, a telematics unit could have its wireless functionality compromised and provide access to the internal CAN bus.

3. J1772 CCS ATTACKS

This section details our research into vulnerabilities possible through access to only the EV's charging port. Multiple connectors for charging exist, each with their own protocols for communicating to the charger. For example, common connectors include Type 1 (Yazaki), Type 2 (Mennekes), Type 3 (Scame), CCS Combo 1 and 2, CHAdeMO, and Tesla. For this effort, the focus was on the Type 1 or SAE J1772 connection, a commonly used connector in North America. This connector uses a protocol that specifies the charge level of an EV by generating signals to send to the charger. If an attacker was able to intercept these signals from the EV and generate their own signals, they would then have control of the charging interface on the EV charging network. With this type of attack in mind, this research set out to create a MitM for the J1772 connector.

The MitM attack vector is regularly utilized to perform attacks on two-way communications such as Ethernet and CAN. The MitM attacks were executed by placing a malicious device between an external charger and an EV. This allowed for manipulation of the charging current which then limits charging, denies charging, or overcharges an EV.

These attacks were performed using a 2016 model commercial vehicle, a Level 2 charger, and a Raspberry Pi 4. Using this equipment and J1772 documentation, the signals between the EV charger and the vehicle were reverse engineered.

For J1772 there are two non-power signals:

1. **Control Pilot.** A Pulse Width Modulation (PWM) signal from the vehicle to the charger requesting a varying level of current.
2. **Proximity Detection.** Resistance circuit on vehicle that flags abrupt disconnects.

Following this analysis, the focus was on simulating the Control Pilot and Proximity Detection pins using commercial-off-the-shelf (COTS) hardware. The table of the PWM duty cycles used to set the charging current by manipulating the Control Pilot signal is shown in **Error! Reference source not found.** (per SAE J1772 standard [1]).

Table 1. Control Pilot PWM Relationship to Charging Current

PWM	SAE Continuous Amps	Short Term Peak
50%	30A	36A
40%	24A	30A
30%	18A	20A
25%	15A	-
16%	9.6A	-
10%	5.7A	-

By recreating these signals, a MitM platform capable of spoofing signals to the charger was developed to control the amount of charging provided to the vehicle. The following sections detail the attacks executed and their results.

Charge Limiting Attack – Charging provided by the charger is reduced by sending a 10% duty cycle PWM when the vehicle is requesting a much higher charge level. Success can be seen monitoring the current out from the charger which matches the 10% duty cycle (5.7 Amps). The charger display is shown in Figure 5.

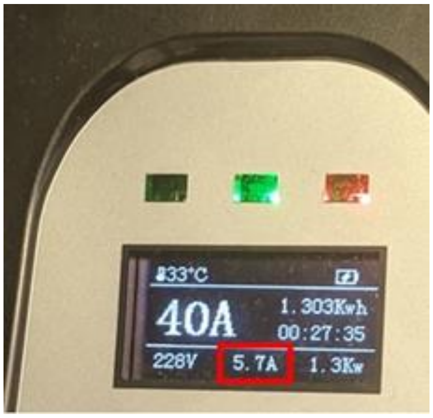

Figure 5. Successful Limit of Charge

Deny Charge Attack – Resistance between the Proximity Detection and ground pins are set to 2.74K Ohms representing a disconnect state to the charge. With this setting, the vehicle displays a warning “Not Able to Charge” indicating successful denial of charge.

Overcharge Attack – With a fully charged battery, a 50% PWM (30A) request from the charger is supplied briefly. The vehicle disconnects power and displays “Problem Detected with Charging Station”. For this test, the vehicle successfully protects the battery from overcharging.

4. IMPLICATIONS FOR DEFENSE

The results of this research demonstrate the need for security mechanisms in EV-related systems. This need becomes more important when these attacks could be applied to the military’s ground vehicles. Though a direct statement has not been made on the requirement of EVs in the military fleet, current research is looking to incorporate EV technology into existing platforms. For example, manufacturers like Oshkosh have begun to implement hybrid systems in the eJLTV [2], which uses both a diesel motor and electric generator to extend vehicle range and provide a remote power source.

Hybrids, while not fully electric and may not require the use of an external charging source, are still susceptible to these types of attacks. Instead of an external charger providing power, the motor will be connected to a generator containing a BMS, where the attacks discussed in this paper would still be applicable.

Further, while full EVs are not possible currently due to weight and battery technology constraints, it is possible that these will become a part of the military’s fleet. This is highlighted in the study *Powering the U.S. Army of the Future* performed by the National Academies of Science, Engineering and Medicine (NASEM), which states that full EV’s will not be possible in the foreseeable future.

5. CONCLUSION

This paper presents attacks on internal systems used for battery management and an EV charging interface. Attackers were able to manipulate the charging process at multiple levels, leading to interruptions or errors in the charging process. While these attacks were successful in affecting the charging of EVs, mitigations exists that would protect the vehicle from similar exploits. These mitigations include securing communication through Secure Onboard Communication (SecOC), separating busses through a secure gateway to limit lateral system movements, and monitoring and detecting attacks on-vehicle through the use of an intrusion detection system (IDS).

6. REFERENCES

[1] S. o. A. Engineers, "SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler," [Online]. Available: https://www.sae.org/standards/content/j1772_201710/.

[2] "Oshkosh Defense Hybrid Electric JLTV (eJLTV)," [Online]. Available: https://oshkoshdefense.com/vehicles/light-tactical-vehicles/ejltv/.