X-in-the-Middle: Attacking Fast Charging Piles and Electric Vehicles

Wu HuiYu & Li YuXiang Tencent Blade Team
About US

Wu HuiYu (@NickyWu_)
Senior security researcher at Tencent Blade Team. Mainly focusing on AIoT security research. Bug hunter, Winner of GeekPwn 2015 & 2020, and speaker of Black Hat USA, DEFCON, HITB, CanSecWest and POC.

Li YuXiang (@Xbalien29)
Senior security researcher at Tencent Blade Team. Focusing on mobile security and IoT security. Reported multiple vulnerabilities of Chrome & Android. Speaker of BlackHat USA, DEFCON 27, CanSecWest, HITB AMS 2018.
About Tencent Blade Team

• Founded by Tencent Security Platform Department in 2017
• Focusing on security research in the areas of AIoT and Cloud virtualization
• Reported 200+ vulnerabilities to vendors such as Google, Apple, Microsoft, Amazon
• More about us : https://blade.tencent.com
Agenda

Introduction to EV Charging
Attack Surface Analysis
What is "X-in-the-Middle" Attack
How to attack "Plug and Charge"
Introduction to EV Charging

• The rapid expansion of the electric vehicle market has promoted the construction of charging infrastructure.

• DC charging has higher charging power, and in order to confirm the charging voltage and current, the electric vehicle and the charging station will communicate after being connected.
# Introduction to EV Charging

<table>
<thead>
<tr>
<th>Connector</th>
<th>CHAdeMO</th>
<th>GB/T</th>
<th>US-COMBO CCS1</th>
<th>EUR-COMBO CCS2</th>
<th>Tesla</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inlet</td>
<td><img src="CHAdeMO_inlet.png" alt="Image" /></td>
<td><img src="GB_T_inlet.png" alt="Image" /></td>
<td><img src="US-COMBO_inlet.png" alt="Image" /></td>
<td><img src="EUR-COMBO_inlet.png" alt="Image" /></td>
<td><img src="Tesla_inlet.png" alt="Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>CAN</th>
<th>PLC</th>
<th>CAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2X Function</td>
<td>✓</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Max Power</td>
<td>400kW 1000x400</td>
<td>185kW 750x500</td>
<td>200kW 600x400</td>
</tr>
<tr>
<td>Market Power</td>
<td>150kW</td>
<td>125kW</td>
<td>150kW</td>
</tr>
<tr>
<td>Start @</td>
<td>2009</td>
<td>2013</td>
<td>2014</td>
</tr>
</tbody>
</table>
Introduction to EV Charging

• Electric vehicles infrastructure is making progress towards a more intelligent, more high-power direction.

• The construction of charging stations is accelerating all over the world, but there is little research on the security of electric vehicle infrastructure.
Attack Surface Analysis

- EV Charging piles are also IoT devices, which usually have built-in systems and operating interfaces, its attack surface involves hardware, systems, cloud services and communications.
- Our focus is on the security of the communication protocol between the electric vehicle and the charging pile.
Attack Surface Analysis

If we can implement a man-in-the-middle attack, we might be able to:

- Find Vulnerabilities in BMS and Charge controller through Fuzzing
- Analyze private protocols and try to bypass identity authentication mechanism
- Damage the EV by tampering with the charging voltage and current
what is "X-in-the-Middle" attack

1. Overview
2. Challenge & Solution
3. Quick Test on Tesla SuperCharger
Challenge

• It should be able to ensure that personal safety and vehicle safety are not threatened in the test.

• High compatibility, suitable for all electric vehicles with Chinese DC charging standard.

• CAN-BUS communication requires low latency, and it is necessary to ensure that no frame is dropped when performing a man-in-the-middle attack.
Challenge
Challenge

GB DC ADAPTER
Solution
Solution

• Open source solution for CAN-BUS Monitoring & Fuzzing & Tampering

1. Raspberry Pi 4B + 2-CH CAN HAT + Ubuntu for ARM
   https://github.com/eerimoq/cantools
   https://github.com/collin80/SavvyCAN
   https://github.com/CANToolz/CANToolz

2. CANSPY
   https://bitbucket.org/jcdemay/canspy

• More details and code will be released in the future.
Quick Test on Tesla SuperCharger
Quick Test on Tesla SuperCharger

• we found that some of the messages in the CAN-BUS communication between SuperCharger and Tesla Model3 use private protocols, and some messages conform to the GB/T 27930 standard.

• When testing with Model3, there is a high probability that it will not be able to charge successfully. The reason is still being analyzed.

• If you want to reverse the complete protocol, it may be a better choice to analyze the firmware of BMS or SuperCharger.
How to attack "Plug and Charge"

1. what's "Plug and Charge"
2. How to use XCharger attack "Plug and Charge"
3. Security Advise
4. Future Trends
What's "Plug and Charge"

- Plug and Charge is a new way of automating payment for EV charging. Users do not need to swipe their cards or scan codes, just connect the charging pile to the vehicle charging port to automatically complete identity authentication and payment.

- For electric vehicle companies that build their own charging piles, such as Tesla, private communication and authentication protocols can be used to ensure the security of "Plug and Charge".
What's "Plug and Charge"

Different implementations of "Plug and Charge"

A. Install a camera near the charging pile to verify the vehicle license plate for authentication.
B. Install an RFID tag at the position of the electric vehicle charging socket, and read the tag content for authentication when the charging gun is connected.
C. The SDK provided by the charging pile operator is built into the intelligent system of electric vehicles, and the authentication is automatically completed when the vehicle reaches the charging station and opens the charging cover.
D. The vehicle VIN is transmitted for authentication during the charging handshake process.
What's "Plug and Charge"

Considering compatibility and cost, some public charging station operators have chosen to use VIN to complete vehicle identity authentication on the basis of GB/T 27930 standard.

What's "Plug and Charge"

1. Handshake Initiation
2. Handshake Recognition
3. Parameter Configuration
4. Charging
5. Suspension of Charging
6. End of Charging

What's "Plug and Charge"
What's "Plug and Charge"

- We use cantools and the corresponding DBC file to successfully translate all messages during the charging process.
- The BMS of the electric vehicle transmits the vehicle's VIN to the charging pile for identity authentication in the BRM message during the handshake recognition.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1826F46</td>
<td>3</td>
<td>01 01 00</td>
<td>Message translation</td>
</tr>
<tr>
<td>1</td>
<td>18275F4</td>
<td>2</td>
<td>4C 1D</td>
<td>Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1</td>
</tr>
<tr>
<td>2</td>
<td>18275F4</td>
<td>3</td>
<td>01 01 00</td>
<td>Vehicle message BM: maximum allowable charging voltage for vehicle handshake: 750.0V</td>
</tr>
<tr>
<td>3</td>
<td>18275F4</td>
<td>2</td>
<td>4C 1D</td>
<td>Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1</td>
</tr>
<tr>
<td>4</td>
<td>18275F4</td>
<td>3</td>
<td>01 01 00</td>
<td>Vehicle message BM: maximum allowable charging voltage for vehicle handshake: 750.0V</td>
</tr>
<tr>
<td>5</td>
<td>18275F4</td>
<td>2</td>
<td>4C 1D</td>
<td>Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1</td>
</tr>
<tr>
<td>6</td>
<td>18275F4</td>
<td>3</td>
<td>01 01 00</td>
<td>Vehicle message BM: maximum allowable charging voltage for vehicle handshake: 750.0V</td>
</tr>
<tr>
<td>7</td>
<td>18275F4</td>
<td>2</td>
<td>4C 1D</td>
<td>Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1</td>
</tr>
</tbody>
</table>

What's "Plug and Charge"

1. BMS transmits the vehicle's VIN to the charging pile
2. The charging pile transmits the VIN to the server
3. The server returns the credentials of the user bound by VIN
4. Start charging and pay according to user's credential

Charging pile operator server

Bind the vehicle's VIN and enable the automatic payment

Charging APP user

DC Fast Charging Pile

Electric Vehicle
What's "Plug and Charge"

- Vehicle identification number (VIN) is a unique code, including a serial number, used by the automotive industry to identify individual vehicles.
- VIN is public plaintext information, with specific coding rules, and can also be obtained from the front windshield of the car.
How to use XCharger Attack "Plug and Charge"
How to use XCharger Attack "Plug and Charge"
Real World Attack

- We rented 5 electric cars of different models and tested multiple charging stations that support plug-and-charge. We verified that after obtaining the VIN on the windshield of the vehicle, the charging pile can be successfully attacked by XCharger to achieve free charging.
- All the vulnerabilities we found have been notified to the vendor and fixed.
Security Advise

• Charging pile operators can deploy a risk control system to collect all battery information (such as battery type, capacity, manufacturer, production date, battery pack serial number, number of charges) transmitted during the charging handshake process of vehicles that use the plug-and-charge function, and generate the corresponding electric vehicle fingerprint information;

• Since the attacker cannot know the detailed battery information of the target vehicle in advance, simply tampering with the VIN cannot pass the fingerprint information verification, and the risk control system can accurately detect the attack and block it;

• Advantages: low cost, no need for additional hardware modification;

• Disadvantages: Because part of the battery information (such as battery pack serial number, charging times) is an optional transmission item in GB/T27930, and part of the battery information of a specific model is public, So the risk control system may not be able to collect enough information to ensure safety.
Security Advise

• For the two-way authentication scheme, charging pile operators need to cooperate with electric vehicle manufacturers to ensure safety. This may require adding a public key transmission function to the vehicle's BMS firmware, or implementing a near-field communication function between the vehicle and the charging pile. Or use a specific private protocol for communication.

• Advantages: very secure, you can mitigate the risk of middle attack.

• Disadvantages: high cost, not compatible with all vehicles.
Future Trends

HPC: specs and roadmap

- **CHAdemo 1.2/2.0**
  - 0.9/1.0/1.1
  - 62.5kW (125A x 500V)
  - 200-400kW (400A x 1kV)

- **GB/T**
  - 187.5kW (250A x 750V)

- **New GB/T ChaoJi-1**
  - 900kW (600A x 1.5kV)

- **ChaoJi-2**
  - 3.0
  - 900kW (600A x 1.5kV)

- **ChaoJi** key points:
  - Control-pilot circuit harmonised with new GB/T and CCS (and IEC 61851-23-1)
  - Backward compatibility with CHAdemo, GB/T and (potentially) CCS
  - Simple, light and compact connector
  - Future proof covering currents up to 600A with liquid-cooling
  - V2G and PnC ready
  - Optional combo-style inlet integrating AC type-1, -2 and GB/T-AC

Harmonisation 2020/2021
Future Trends

ISO 15118
Thank You

blade@tencent.com