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 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 2019, HITB AMS 2018, XCON 2018, CSS 2019.

About Tencent Blade Team

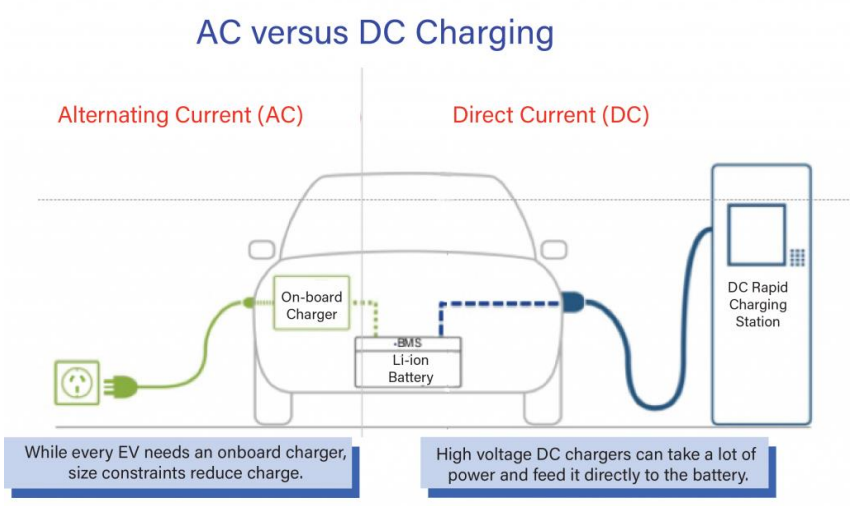
- Founded by Tencent Security Platform Department in 2017
- Focusing on security research in the areas of AIoT and Cloud virtualization
- Reported 200+ vulnerabilities to vendors such as Google, Apple, Microsoft, Amazon
- More about us : https://blade.tencent.com

Agenda

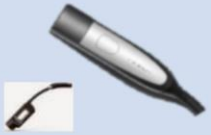
- Introduction to EV Charging
- Attack Surface Analysis
- What is "X-in-the-Middle" Attack
- How to attack "Plug and Charge"

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

	CHAdeMO	GB/T	US-COMBO CCS1	EUR-COMBO CCS2	Tesla
Connector					
Inlet					
IEC	✓	✓	✓	✓	
IEEE	IEEE		SAE		
EN	✓			✓	
JIS	✓	✓	✓	✓	
GB		✓			
Protocol	CAN		PLC		CAN
V2X Function	✓				?
Max Power	400kW 1000x400	185kW 750x250	200kW 600x400	350kW 900x400	?
Market Power	150kW	125kW	150kW	350kW	120kW
Start @	2009	2013	2014	2013	2012

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.

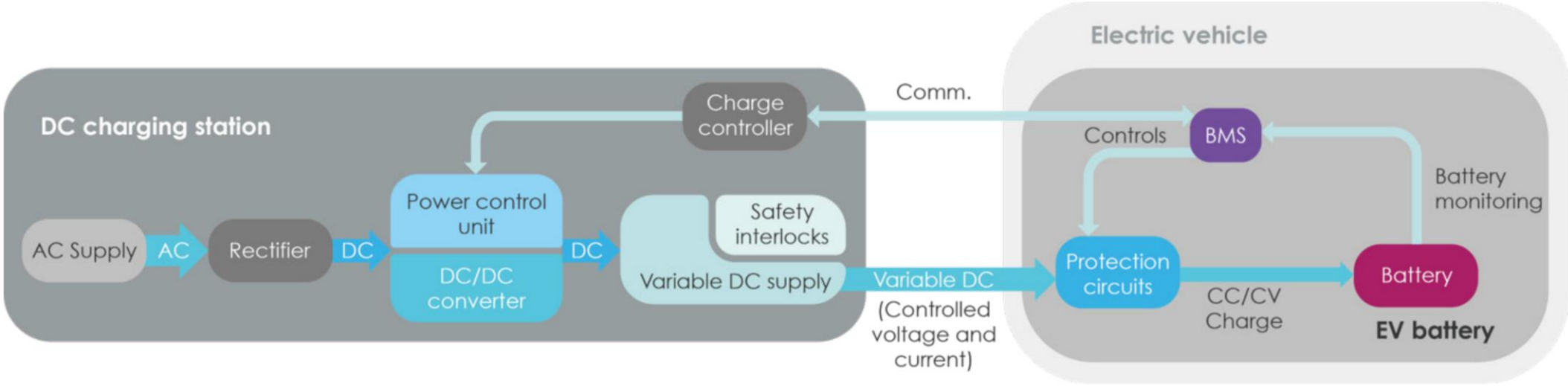
Attack Surface Analysis

- 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:

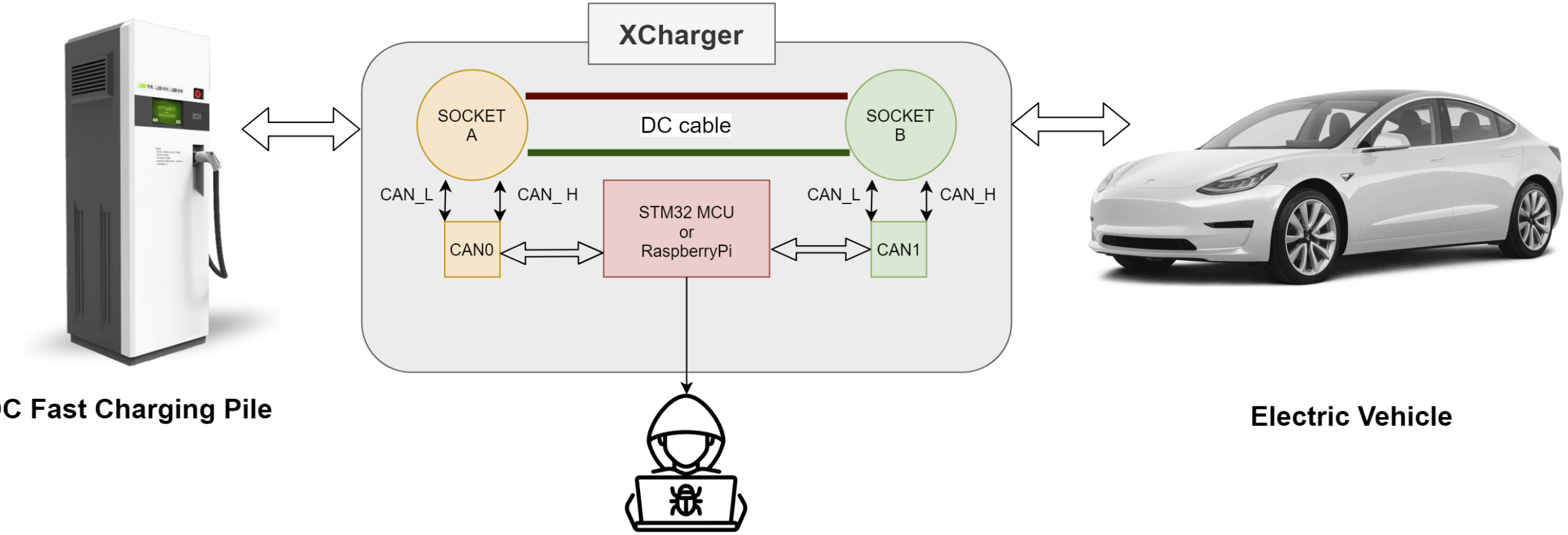
- Find Vulnerabilities in BMS and Charge controller through Fuzzing
- Analyze private protocols and try to bypass identity authentication mechanism
- Damage the EV by tampering with the charging voltage and current



what is "X-in-the-Middle" attack

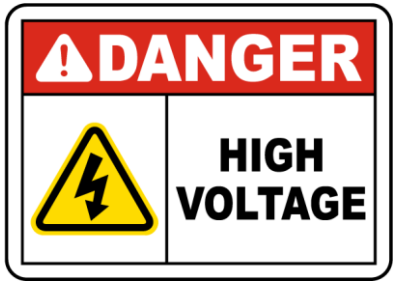
1. Overview
2. Challenge & Solution
3. Quick Test on Tesla SuperCharger

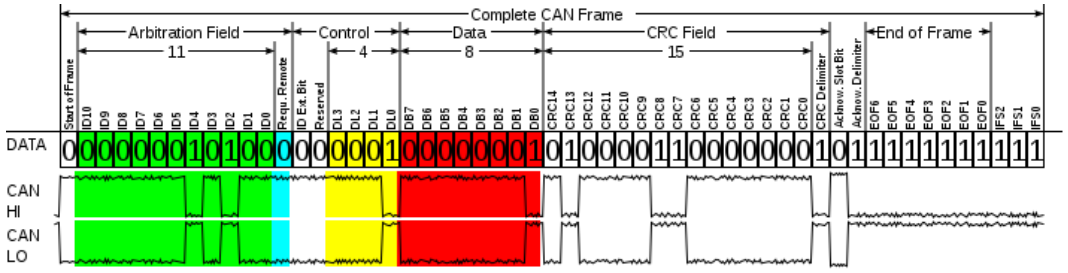
Overview


XCharger
SOCKET A
DC cable
SOCKET B
CAN_L
CAN_ H
CAN0
STM32 MCU or RaspberryPi
CAN_L
CAN_H
CAN1
DC Fast Charging Pile
Electric Vehicle

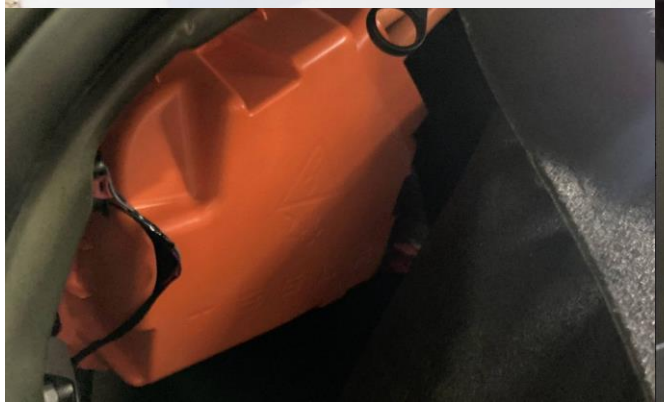
Challenge

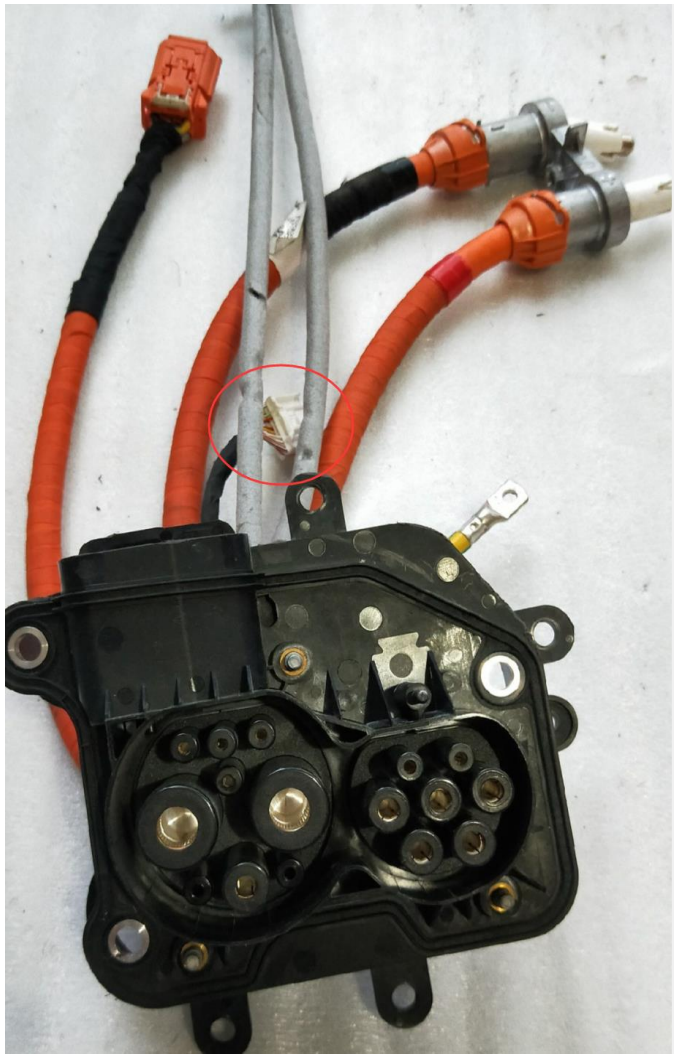
- It should be able to ensure that personal safety and vehicle safety are not threatened in the test.
- High compatibility, suitable for all electric vehicles with Chinese DC charging standard.
- CAN-BUS communication requires low latency, and it is necessary to ensure that no frame is dropped when performing a man-in-the-middle attack.





Challenge





Solution


Inlet A for Connector
Inlet B for EV
Charging Pile's CAN BUS
BMS's CAN BUS
CAN_H CAN_L
CAN_H CAN_L
USB
DWIN

Solution

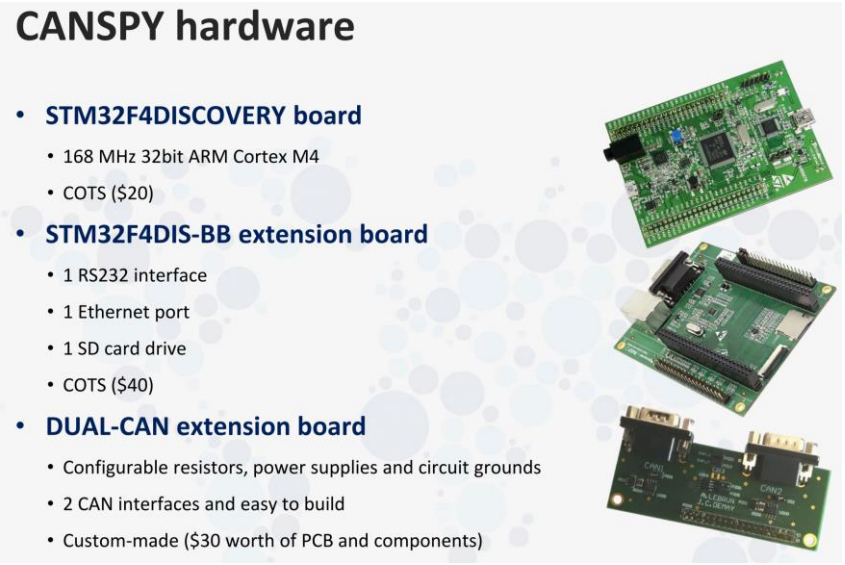
- Open source solution for CAN-BUS Monitoring & Fuzzing & Tampering
  1. Raspberry Pi 4B + 2-CH CAN HAT + Ubuntu for ARM

     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.



https://www.waveshare.net/wiki/2-CH_CAN_HAT

https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platorm-For-Auditing-CAN-Devices.pdf

Quick Test on Tesla SuperCharger

	A	B	C	D
1	FRAME SEQ	FRAME ID	DLC	DATA
2	15526	1C5456F4	8	04 02 00 00 00 00 00 00
3	15527	185556F4	8	00 00 08 00 3F 00 00 00
4	15528	185656F4	8	02 36 30 38 00 00 00 00
5	15529	1856F456	8	E1 FC 60 F0 FC FF FF FF
6	15530	1C5456F4	8	04 02 00 00 00 00 00 00
7	15531	185556F4	8	00 00 08 00 3F 00 00 00
8	15532	185656F4	8	00 4C 52 57 33 45 37 45
9	15533	1856F456	8	C1 F9 60 F0 FC FF FF FF
10	15534	1826F456	3	01 01 00
11	15535	1807F456	7	BD 12 00 00 00 00 00
12	15536	1854F456	8	00 00 90 80 C0 FF FF FF
13	15537	80	8	01 02 03 04 05 06 07 08
14	15538	1C5456F4	8	04 02 00 00 00 00 00 00
15	15539	185556F4	8	00 00 08 00 3F 00 00 00
16	15540	185656F4	8	01 41 34 4C 43 30 37 37
17	15541	1857F456	8	39 8A 00 00 FF FF FF FF
18	15542	1856F456	8	E1 FC 60 F0 FC FF FF FF
19	15543	1C5456F4	8	04 02 00 00 00 00 00 00
20	15544	185556F4	8	00 00 08 00 3F 00 00 00
21	15545	185656F4	8	02 36 30 38 00 00 00 00
22	15546	1856F456	8	E1 FC 60 F0 FC FF FF FF
23	15547	1C5456F4	8	04 02 00 00 00 00 00 00

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.

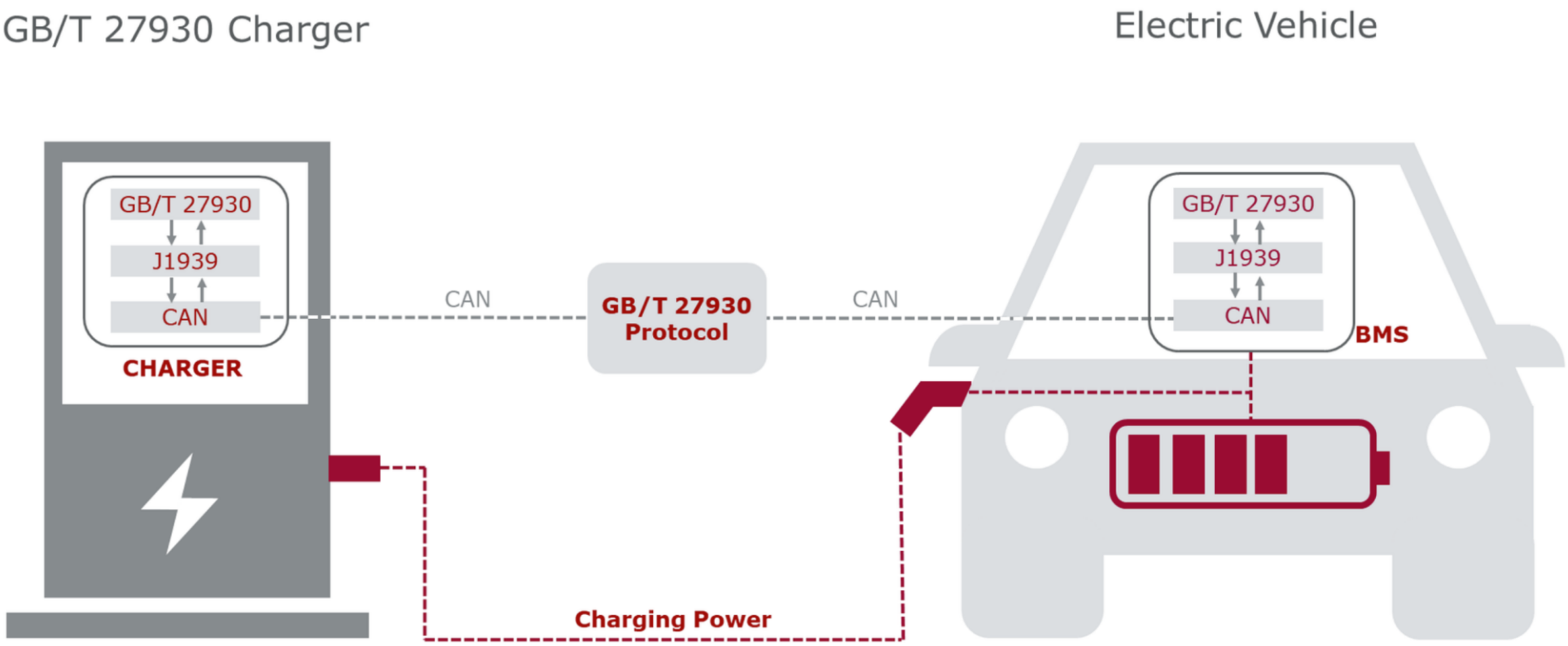
How to attack "Plug and Charge"

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

What's "Plug and Charge"

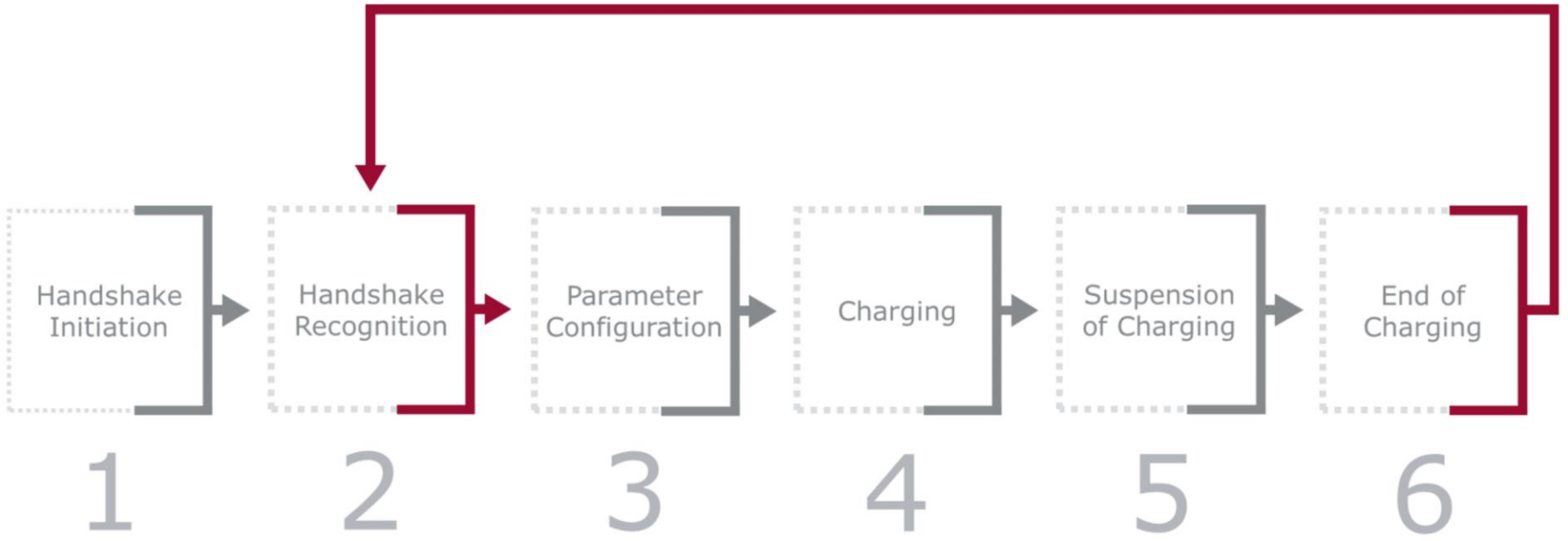
- Plug and Charge is a new way of automating payment for EV charging. Users do not need to swipe their cards or scan codes, just connect the charging pile to the vehicle charging port to automatically complete identity authentication and payment.
- For electric vehicle companies that build their own charging piles, such as Tesla, private communication and authentication protocols can be used to ensure the security of "Plug and Charge".
- 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. Operators do not realize that VIN is not a security identification in insecure CAN-BUS communication.

What's "Plug and Charge"



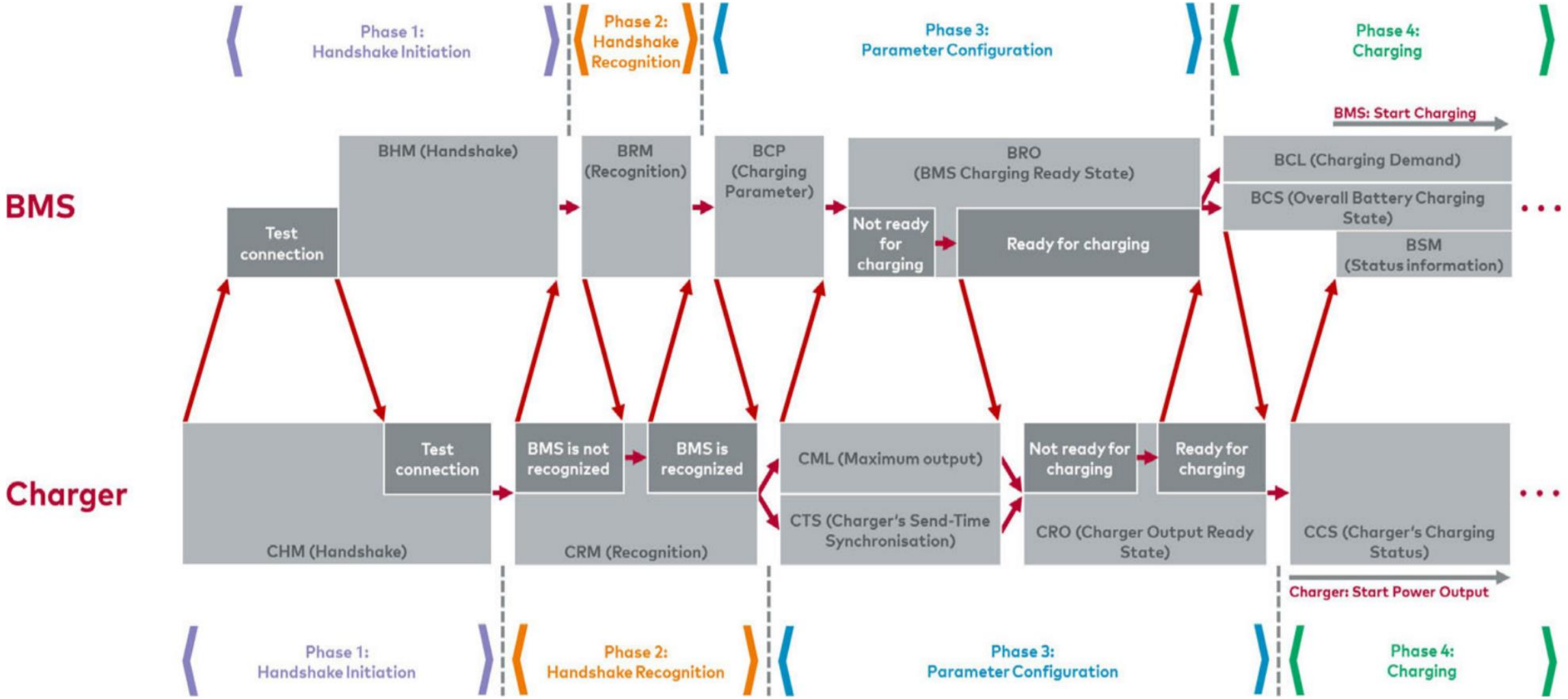
https://www.vector.com/int/en/know-how/technologies/protocols/gbt-27930/

What's "Plug and Charge"



https://www.vector.com/int/en/know-how/technologies/protocols/gbt-27930/

What's "Plug and Charge"



https://assets.vector.com/cms/content/know-how/_technical-articles/Emobility_GBT_27930_CAN_Newsletter_PressArticle_201911_EN.pdf

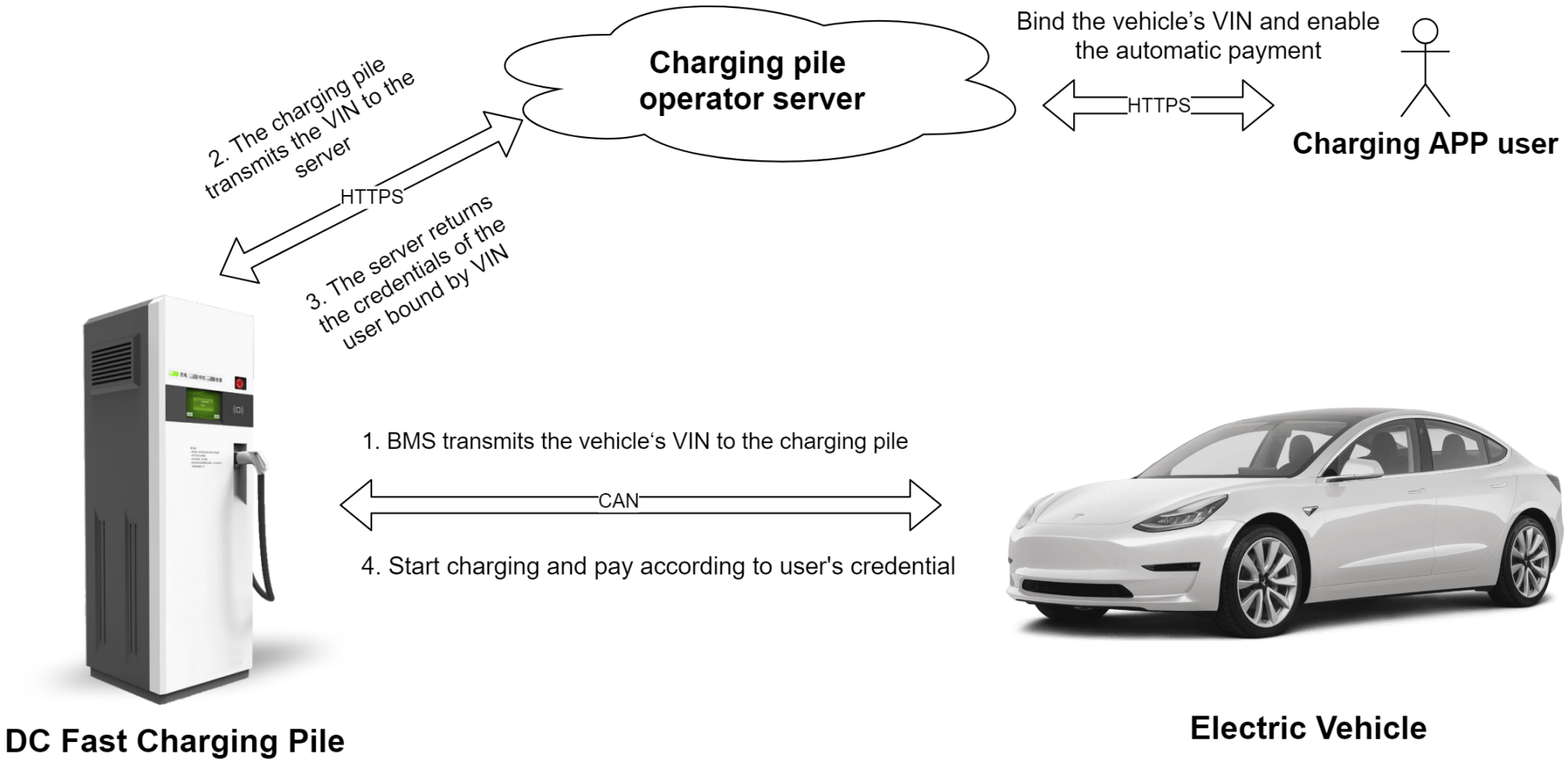
What's "Plug and Charge"

- 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.

A	B	C	D	E
FRAME SEQ	FRAME ID	DLC	DATA	Message translation
0	1826F456	3	01 01 00	Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1
1	182756F4	2	4C 1D	Vehicle message BHM: maximum allowable charging voltage for vehicle handshake: 750.0V
2	1826F456	3	01 01 00	Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1
3	182756F4	2	4C 1D	Vehicle message BHM: maximum allowable charging voltage for vehicle handshake: 750.0V
4	1826F456	3	01 01 00	Charger message CHM: Charger handshake Charger Communication Protocol version number: v1.1
5	182756F4	2	4C 1D	Vehicle message BHM: maximum allowable charging voltage for vehicle handshake: 750.0V
6	1801F456	8	00 01 00 00 00 00 00 00	Charger message CRM: charger identification result: BMS can not identify charger number: 00000001
7	1CEC56F4	8	10 31 00 07 FF 00 02 00	Vehicle message BRM:BMS and vehicle identification message multi-packet message: first message
8	1CECF456	8	11 07 01 FF FF 00 02 00	The charger is ready to receive multi-packet messages: vehicle message BRM:
9	1CEB56F4	8	01 01 01 00 01 90 01 AC	Parse according to the agreement: the message is: vehicle message BRM: package 1
10	1CEB56F4	8	02 0D XX XX XX XX XX 56	Parse according to the agreement: the message is: vehicle message BRM: package 2
11	1CEB56F4	8	03 34 12 1F 08 02 64 00	Parse according to the agreement: the message is: vehicle message BRM: package 3
12	1CEB56F4	8	04 00 00 00 74 61 6E 67	Parse according to the agreement: the message is: vehicle message BRM: package 4
13	1CEB56F4	8	05 6F 00 00 00 00 00 00	Parse according to the agreement: the message is: vehicle message BRM: package 5
14	1CEB56F4	8	06 00 00 00 00 00 00 00	Parse according to the agreement: the message is: vehicle message BRM: package 6
15	1CEB56F4	8	07 02 08 E0 07 FF FF FF	The last packet of the vehicle message BRM:BMS and the vehicle identification message. Protocol version: v1.1 lead-acid battery ···
16	1CECF456	8	13 31 00 07 FF 00 02 00	The charger receives and completes the multi-packet message: the vehicle message BRM: receives a total of 49 bytes of data

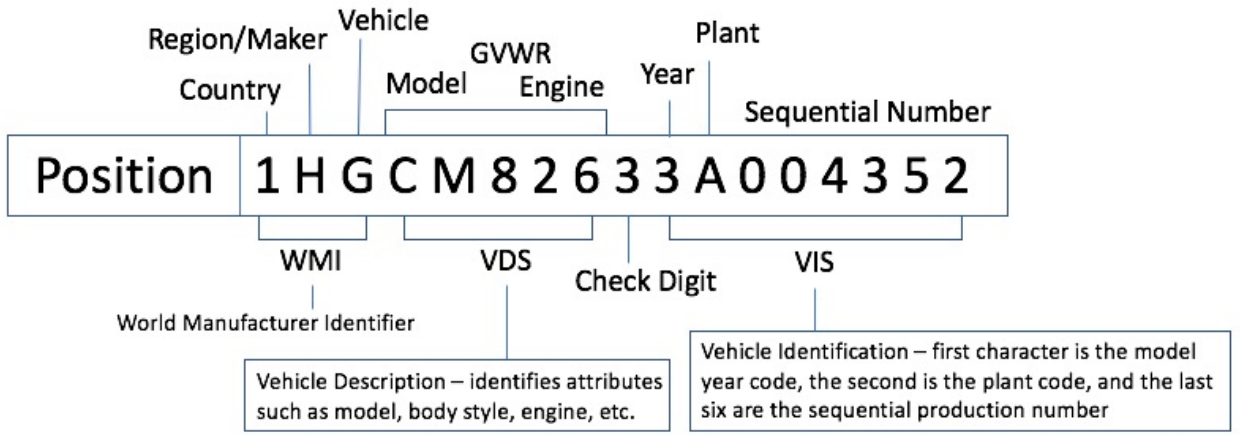
https://github.com/sebastianwilczek/CANoe-Configurations/blob/master/SmartCharging/GBT27930/Simulation/GBT_27930_2015.dbc

What's "Plug and Charge"



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.



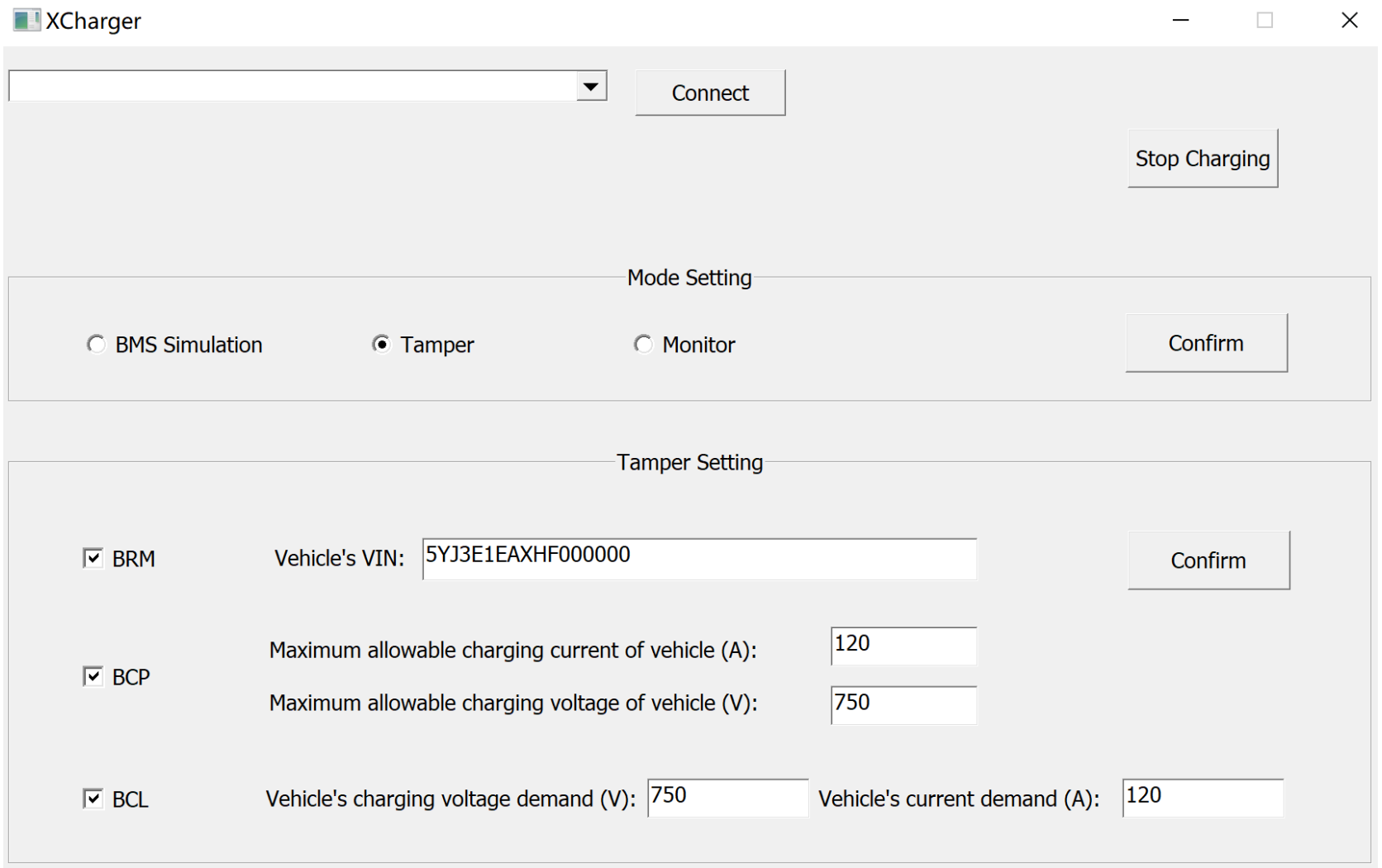
MODEL 3

Driver's side windshield

RH C pillar

Driver Side Lower B Pillar

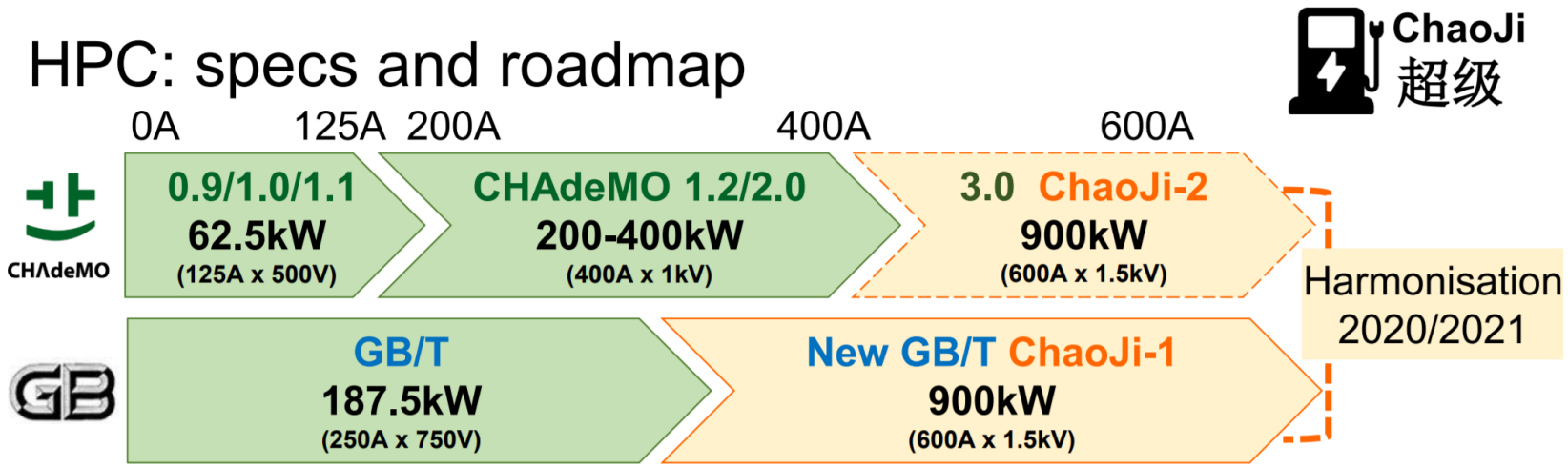
How to use XCharger Attack "Plug and Charge"



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.

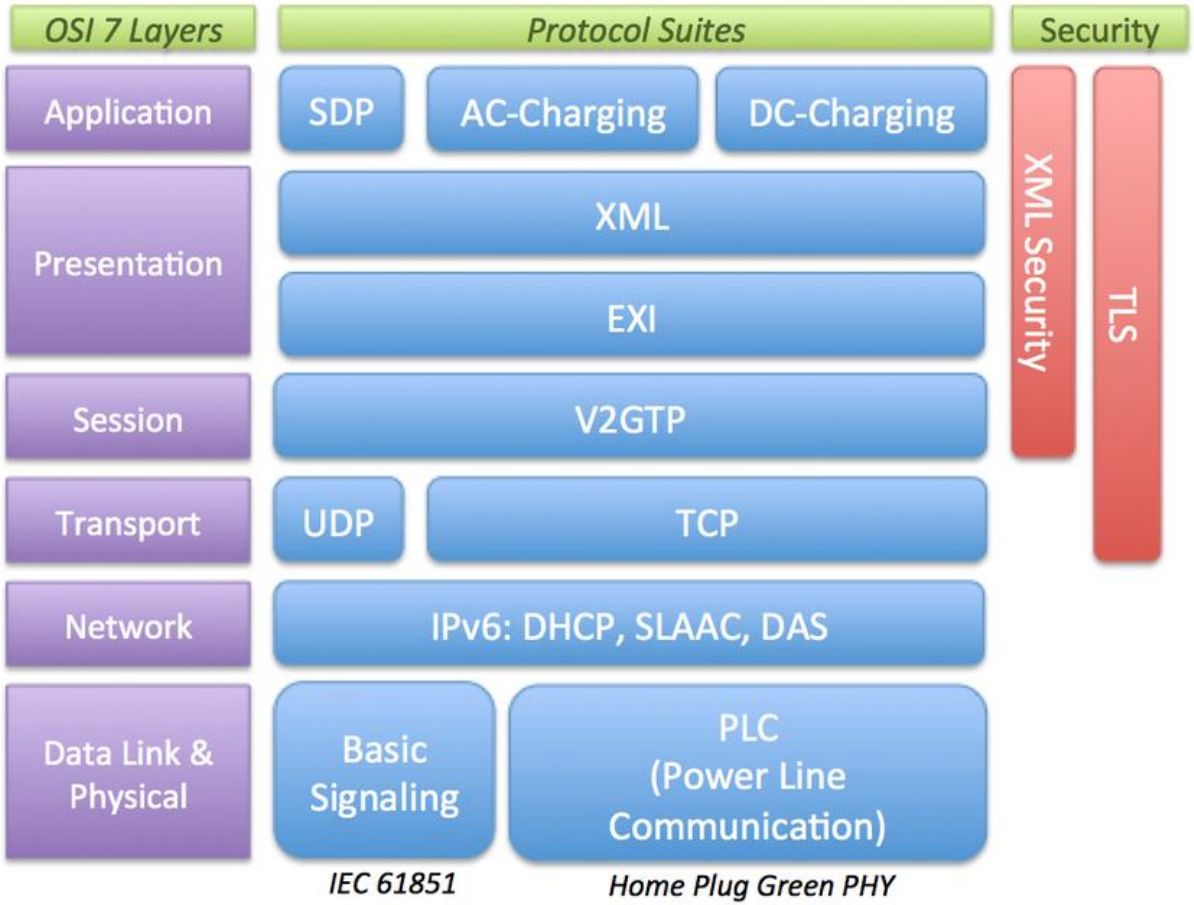
Future Trends



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

Future Trends



ISO 15118

Thank You

blade@tencent.com