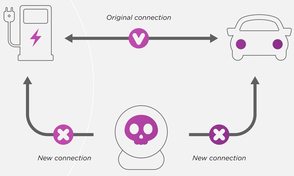
irdeto

GIVE US 2 MINUTES, AND WE'LL SHOW YOU HOW A CHARGING STATION CAN BE CYBER ATTACKED
(IN REAL LIFE)

Man-in-the-Middle (MitM) attacks let bad actors intercept and manipulate communication between an EV station and a driver or back-end, risking data theft and station control.



A REAL-LIFE EXAMPLE:
HOW DID THE MITM ATTACK HAPPEN?

The security researchers from Tencent's Blade Team executed a MitM attack on the communication between an EV and a charging point.

1 Analyze communication between the charging station and vehicle and test for software vulnerabilities randomly.

2 Use any freely available tool, like American Fuzzy Lop (AFL), to target the security of the communication protocol between the charging station and vehicle.

3 With the help of a fuzzing tool you can capture, modify, replay and fuzz the data exchanged during the communication process between the charging station and vehicle.

4 Due to compatibility and cost, many operators have chosen to use the Vehicle Identification Number (VIN) to complete vehicle identity authentication.

VIN is public plaintext information and can also be obtained from the front windshield of the car.

5 You can leverage the insight from the vulnerability scan to execute the exploit, breaching the charging station's security, for example, insert the VIN—either a spoofed or an intercepted legitimate one—as a form of pseudo-authentication to fool the system into granting access.

6 10110 01010 01100

Once access is gained, you can modify operational parameters. This could include changing the charging station's logic to misinterpret the VIN as a trigger for free charging, effectively disabling the payment mechanism or creating a backdoor for future exploitation.

WHO ARE AFFECTED?

- Charge point operators
- E-mobility service providers
- Payment companies

HOW CAN IT BE AVOIDED?

- Implement strong authentication mechanisms like cryptographic keys or tokens
- Use digital certificates from trusted authorities
- Employ secure communication protocols like TLS for data confidentiality, integrity and authenticity
- Regularly update security systems and implement monitoring and intrusion detection mechanisms
- Ensure compliance with industry standards and best practices

PREVENT THIS FROM HAPPENING TO YOU!

Contact us today!