Demo #24: Ransom Vehicle through Charging Pile

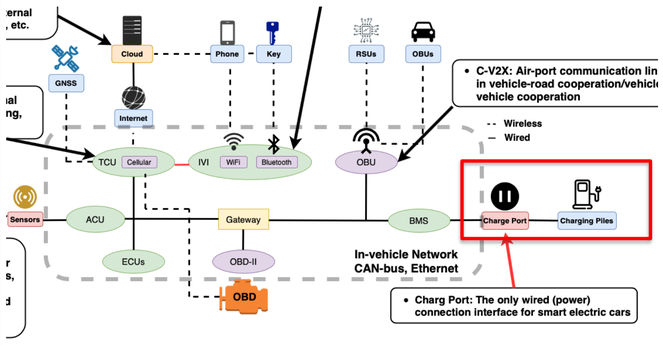
Shangru Song[1]*, Hetian Shi[1]*, Ruoyu Lun[3], Yunchao Guan[1],
Xiang Li[1], Jihu Zheng[1], Jianwei Zhuge[1,2]
[1]Tsinghua University, [2]Zhongguancun Laboratory, [3]State Laboratory of Science and Engineering Computing
* Indicates equal contribution

Abstract

✳ This work shows a new method of remote ransom attack on electric vehicles(EV) through charging piles **without approaching EV**.
✳ We also designed an extra **physical plugin** to expand the effect of this method.

Motivation

- From EV threats panorama, charging pile is the only wired link, providing unique physical basis of ransom attacks.
- Existing attacks mainly accomplish their purpose by exploiting vulnerabilities of vehicle itself [1]. The vulnerabilities of the charging pile will affect more brands of vehicles.

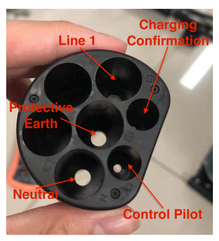


EV Threats Panorama

Attack Prerequisite

✦Initially, **message format** and **vulnerabilities** through **reverse MCU firmware**.
✦Charging connector is **locked** on the port during charging period.
✦ A safe charging process doesn't allow vehicles to disconnect connector while charging or **damage** the charging pile.
✦Experiments in China & public 3rd party Charging piles with GB/T AC Connector

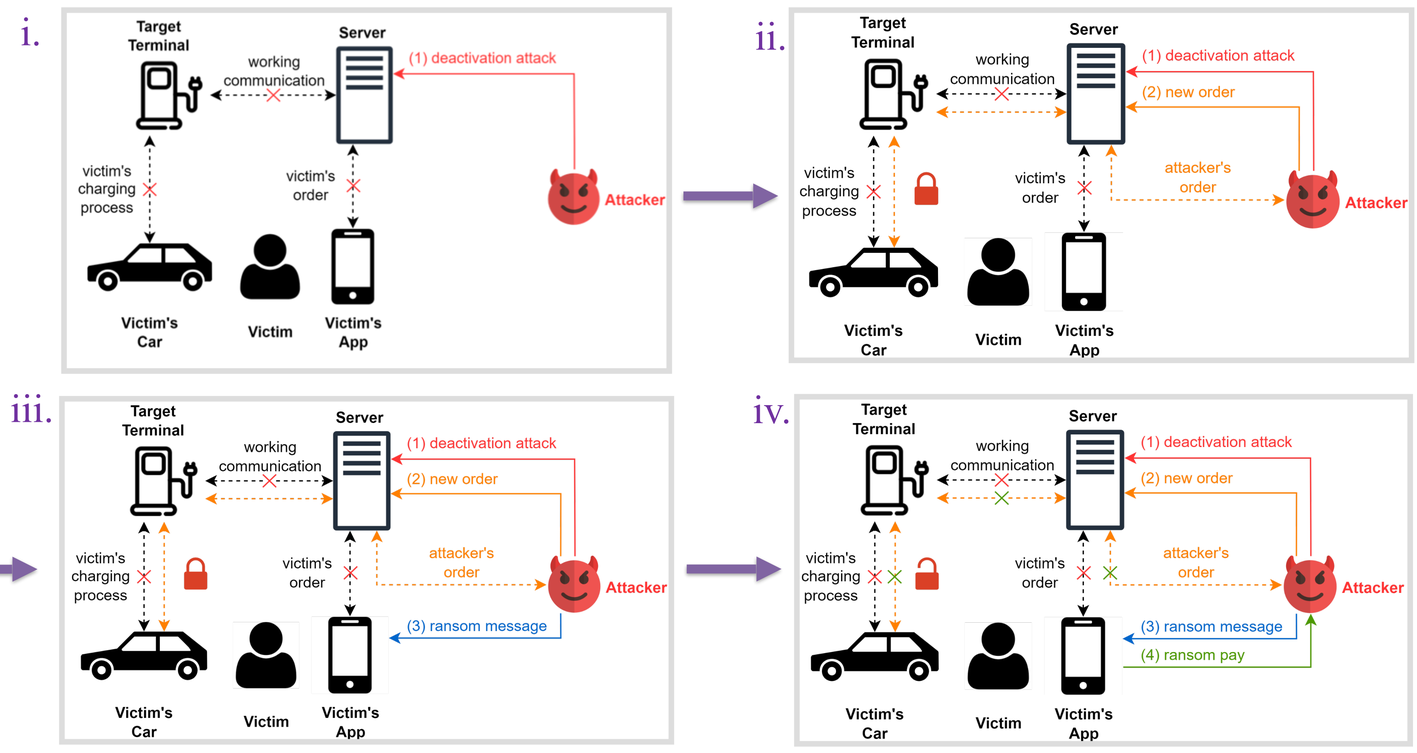
EV will pop out a **connector lock** during charging process



GB/T AC Connector ports functions

Regular CPRA Method

Here demonstrates the regular Charging Pile Ransom Attack process:
Firstly, EV owner starts an order to charge his car.
Then, the attack begins.
i. **Deactivation attack** ii. **spoof the charging process to attacker's order**
iii. **send ransom message** iv. **Ransom is paid & release the car**



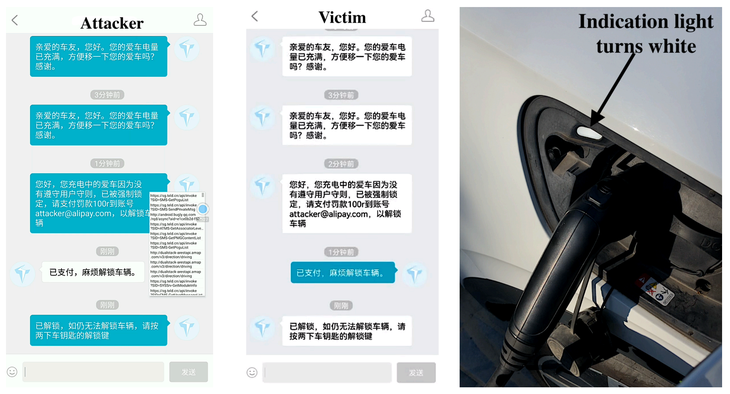
Attack Process of proposed CPRA Method

Experiments Results

	Ransom Successfully (EV models)
Regular	Volkswagen ID.4
With plugin	Tesla model S & ROEWE rx 5

Vulnerable Brands (Charging Pile)
TELD & Starcharge

Ransom paid and messages received, after pressing open switch twice on the key, indicator light turns white, car is free to go.



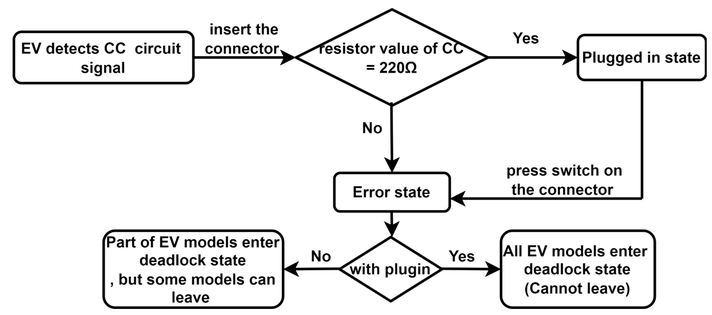
ransom message sent / received

Light turns white from green after ransom paid indicates successful attack.

Real-world Experiment Demo

Physical Plugin

✤ Some EV models detect Charging Confirmation(CC) signal.
✤ Spoof CC signal & fix the impedance of this path (220Ω resistor)



SFC of the physical plugin

Acknowledgements

This work was supported by NSFC under No. U1936121. The authors want to thank GeekPwn Organizing Committees and judges for their professional judgment for the free-charging demo and altruistic help for this work.

Detailed information are available:https://github.com/Moriartysherry/ransom

Reference:
[1] M. Wolf, R. Lambert, T. Enderle, and A. Schmidt, "Wanna drive? feasible attack paths and effective protection against ransomware in modern vehicles," in Proc. ESCAR Europe,2017.