Demo: Ransom Vehicle through Charging Pile

Shangru Song*§, Hetian Shi*§, Ruoyu Lun‡, Yunchao Guan*, Xiang Li*, Jihu Zheng*, Jianwei Zhuge*†✉
*Tsinghua University †Zhongguancun Laboratory ‡State Key Laboratory of Science and Engineering Computing

I. Introduction

Ransom attacks have attracted widespread attentions from researchers, however, there have been relatively few researches on vehicles, especially for electric vehicles(EVs). Such attacks mainly accomplish their purpose by exploiting vulnerabilities of vehicle itself, but often have a narrow attack surface[1].

In this demo with real EVs and public charging piles, we show a new approach, the Charging Pile Ransom Attack(CPRA), that can remotely ransom EVs through the charging connector between EVs and charging piles. Additionally, we design a physical plugin for charging connectors that can extend the EV models affected by the described ransom attack. In this case, the CPRA need a preparing step to locally install the plugin on the connector.

II. Attack Demonstration

Attack prerequisite. We assume attackers have obtained application layer protocol message format of charging pile and weak authentication vulnerabilities through reverse microcontroller unit firmware of equipment. Then attackers could pretend to be target charging pile to communicate with the server through network, deactivating the target charging pile. A safe charging process doesn't allow vehicles to disconnect the charging connector while charging, some vehicles' charging connector interfaces would be in the deadlocked state until their charging piles stop supplying power. Forced disconnection, for instance, cutting cable may cause electric shock risk, and damaging public charging pile may cause legal troubles.

Attack goal. The attack goal is make charging EVs unable to stop charging or leave charging pile terminal without approaching the target, until victims pay ransom to attackers.

Attack process. The CPRA process is shown in Figure 1. (1) Deactivation attack: attackers send fake telegrams to the server, changing the server side's status of the charging pile target terminal into offline, which in turn eliminates the victim's charging order on the App. Then attackers stop the attack. (2) After the charging pile recovers online state, attackers launch a new order to take over the charging process, and (3) concurrently send a ransom message to the victim anonymously through the communication channel on the App. (4) Until the ransom is payed, attackers will stop the charging process and let the vehicle go. Experiments verified that our approach, CPRA, is effective on Volkswagen ID.4 and a considerable part of public 3rd party charging piles in China, including TELD and Starcharge.

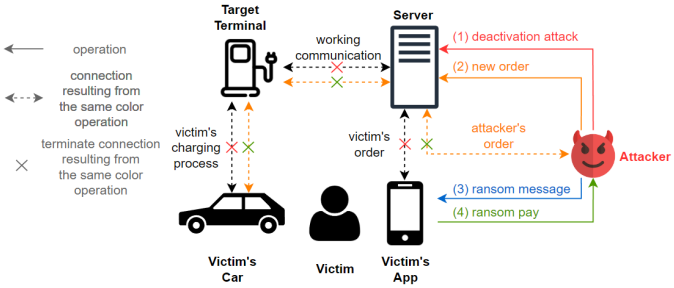
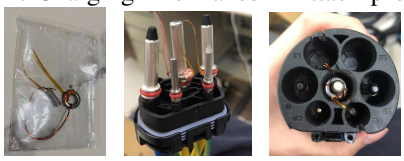


Fig. 1: Charging Pile Ransom Attack process



(a) plugin (b) inner view (c) outside view

Fig. 2: Different views of physical plugin on the connector

Expanding affected models. However, we find some EV models, such as ROEWE rx5 and Tesla model S, detect Charging Confirmation(CC) signal of the charging connector to control deadlocked state of the interface, specifically by detecting the circuit impedance of this path. When pressing the switch on the charging connector, the CC signal changes, and these EVs would exit deadlocked state. To make our CPRA effective on these models, we design a hidden physical plugin for the charging connector that can spoof the signal received by the interface. In another word, this physical plugin disables the switch on the charge connector by fixing the CC circuit impedance so that these EVs cannot unlock the deadlocked state. As shown in Figure 2, this plugin consists of a metal ring, a special cable and an insulating sleeve. The cable is designed with specific resistors(e.g. 220Ω for GB/T AC Connector) to hold the CC signal in place, without affecting regular functions of charging pile and is almost invisible from outside. Experiments verified this plugin is effective for formerly mentioned EV models.

Ethic Consideration. We have reported the vulnerabilities of public charging piles to make the described ransom attack feasible to the vendors, through GeekPwn competition organizers. All EVs tested are owned by the authors, thus our testing did not affect any normal users.

Demonstration. We provide videos to demonstrate (1) the process of CPRA and (2) the effect of the physical plugin on our YouTube channel, which can be accessed at https://github.com/Moriartysherry/ransom.

Acknowledge. Supported by NSFC under No.U1936121.

References

[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.

§Both are first authors.
✉Corresponding Author: zhugejw@tsinghua.edu.cn

Symposium on Vehicles Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23024
www.ndss-symposium.org