清華大學
Tsinghua University

Demo #24: Ransom Vehicle through Charging Pile

Shangru Song*, Hetian Shi*, Ruoyu Lun, Yunchao Guan, Xiang Li,
Jihu Zheng , Jianwei Zhuge
* Indicates equal contribution

02/27/2023

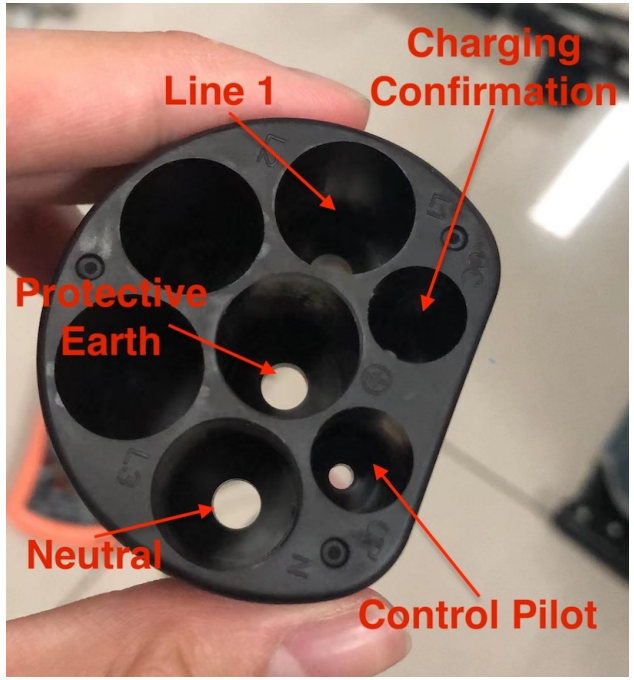
Charging connector

Charging connector composition

- **Line, earth, neutral wire**
- **Charging Confirmation (CC):** Confirm the connection state of the charging connector and the vehicle
- **Control Pilot (CP):** Transmitting control signals

Charging connector state classification while charging：

- Always deadlock state： ransom directly
- Exit deadlock state after pressing the switch： ransom after installing plugin



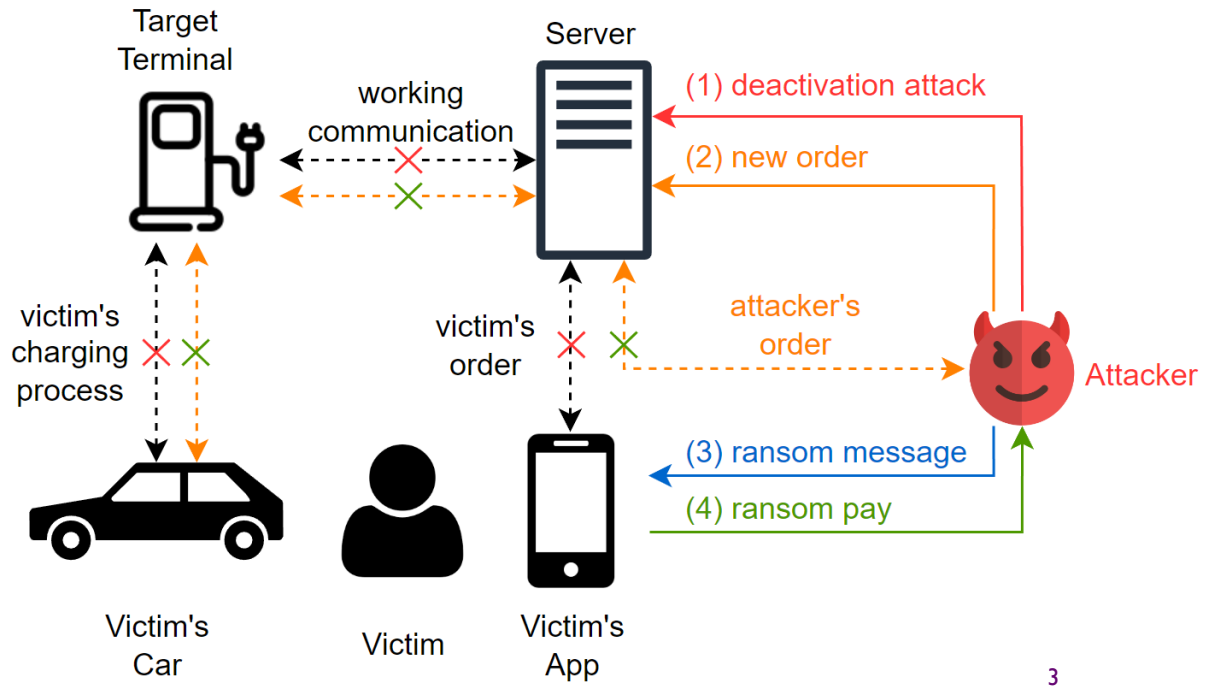
GB/T AC Charging Connector

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

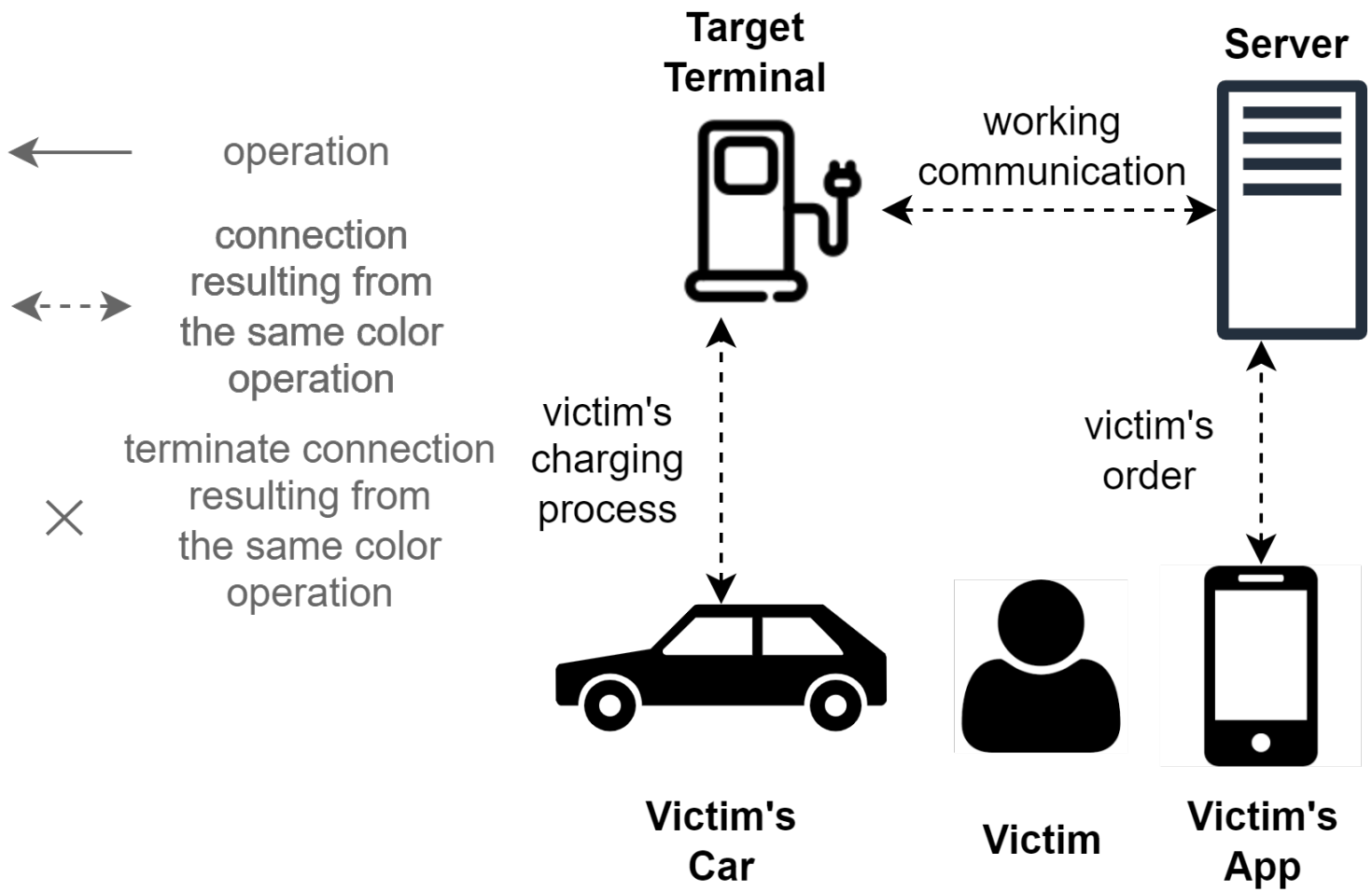
Remote ransom vehicle through charging pile

Prerequisite:

- Deactivation attacks can deactivate and take over the owner's control of the charging process
- Safe charging process doesn't allow vehicles to disconnect the charging connector while charging



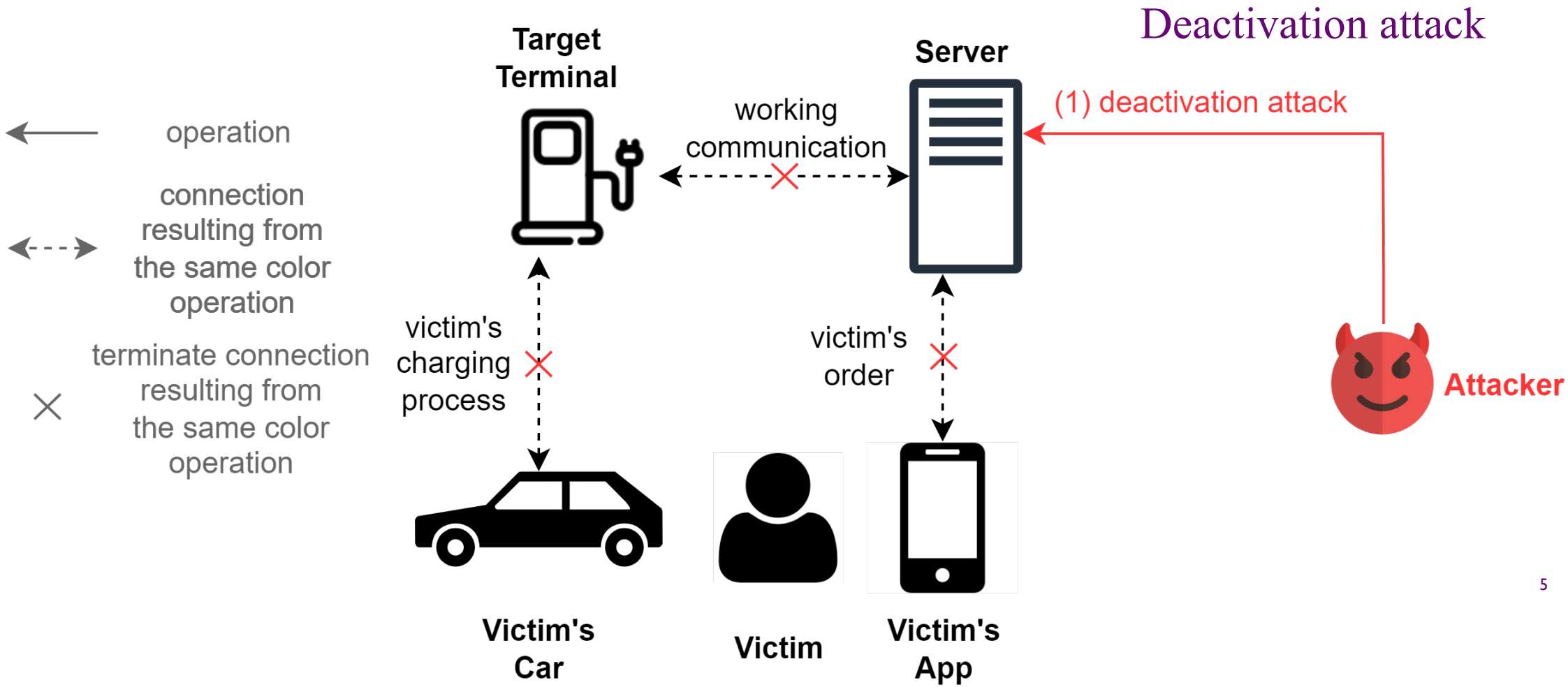
Remote ransom vehicle through charging pile



Regular charging process

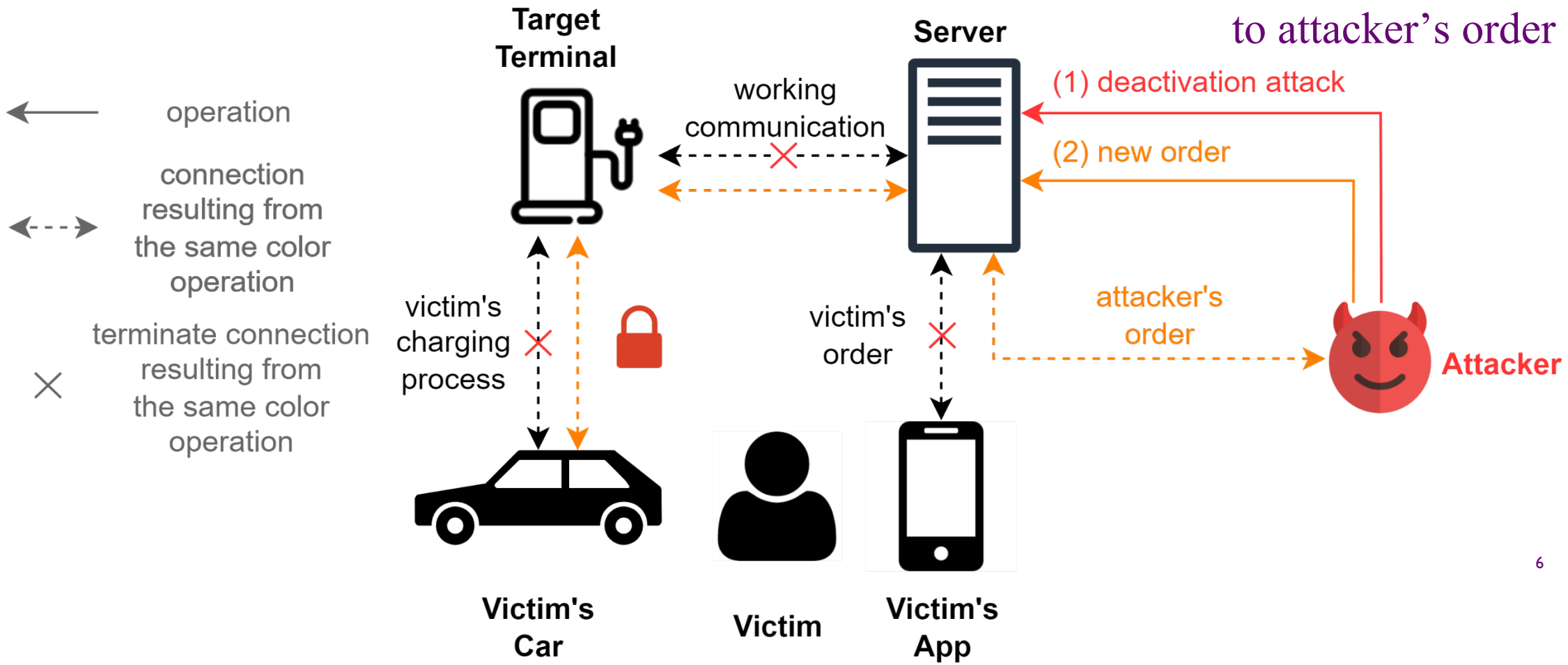
Attacker

Remote ransom vehicle through charging pile

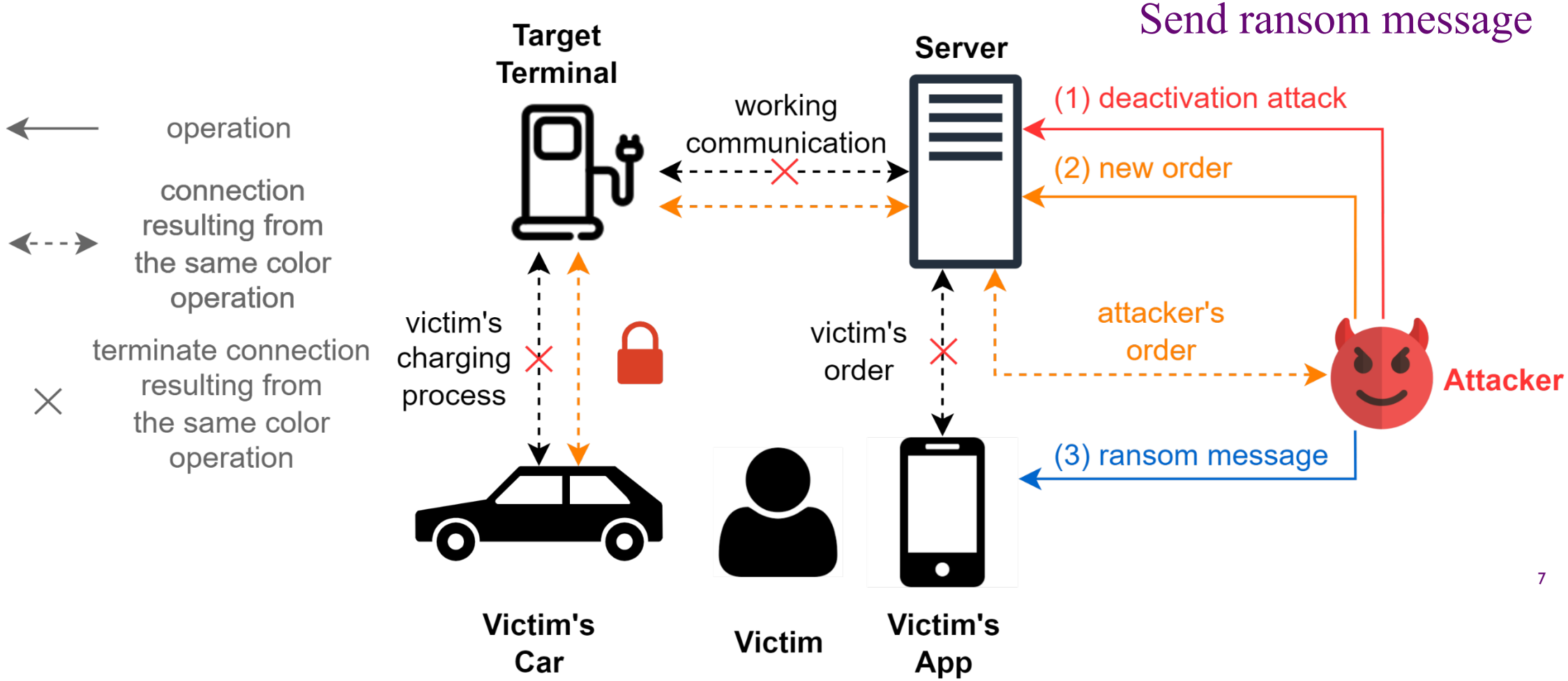


Remote ransom vehicle through charging pile

Spoof the charging process to attacker's order

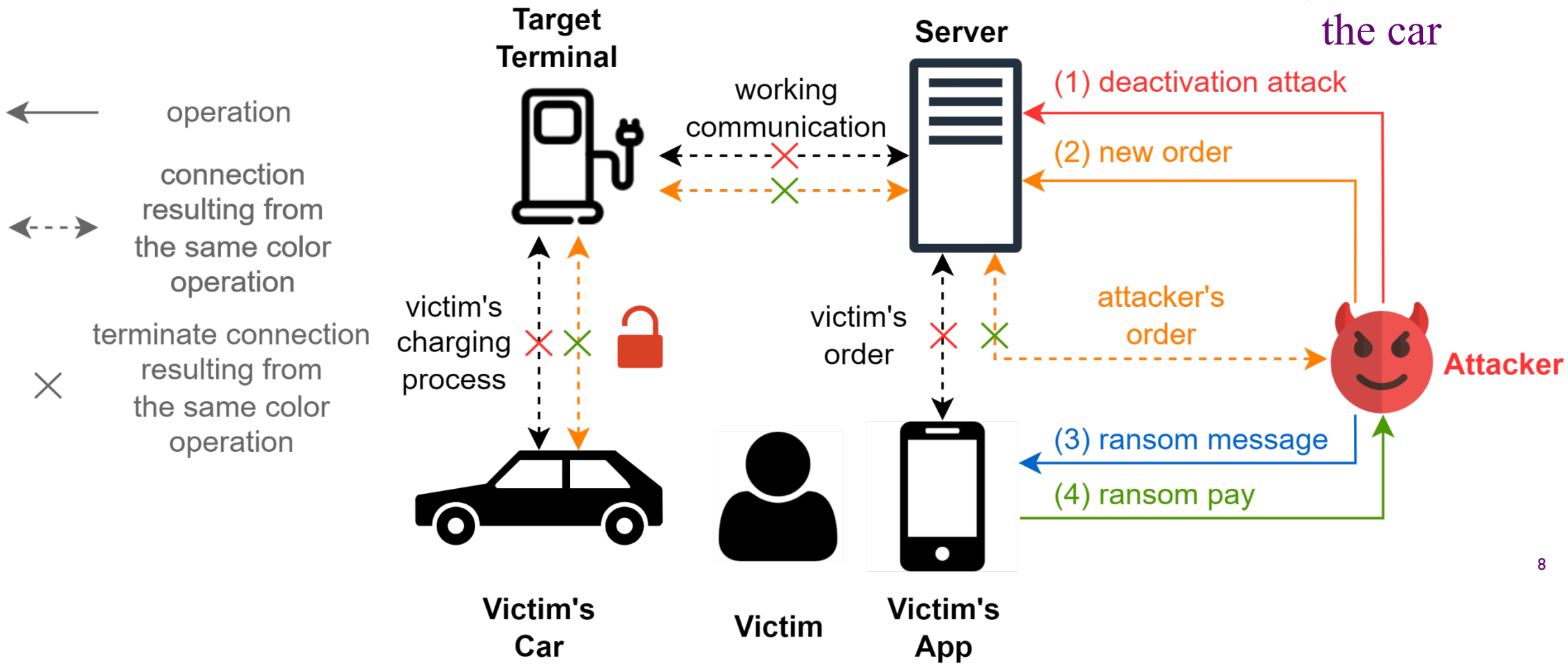


Remote ransom vehicle through charging pile



Remote ransom vehicle through charging pile

Ransom get paid & release the car



Problem Appeared

Some special EV Models, such as **Tesla model S** and **ROEWE rx5**

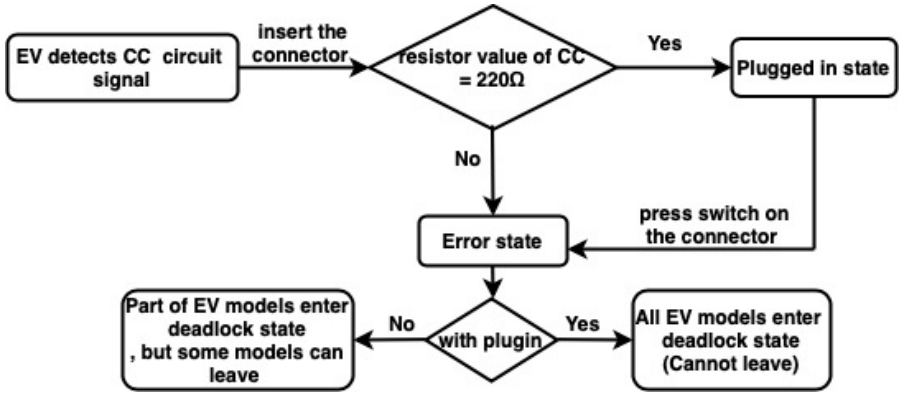
The **indicator light** color from green changes into white when pressing the switch on the charging connector. Victims can unplug the charging connect and escape.

We find： These EV models control the deadlocked state of the interface through detecting **CC signal's** changes.

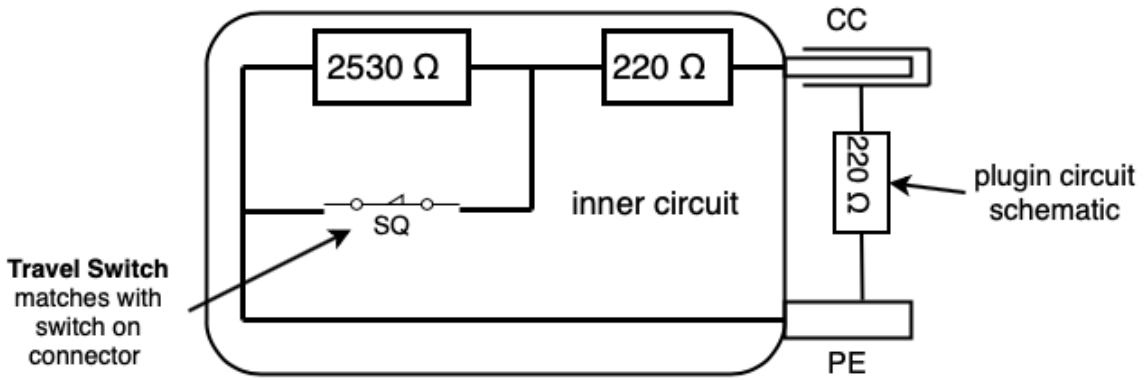
Principles

CC signal changes when pressing the switch on the charging connector

Here is a switch. After pressed, it will change the impedance value of CC circuit into 2750 Ω rather than 220 Ω



SFC of the physical plugin



CC circuit after installing plugin

Physical plugin for charging connectors

Challenge solved

- Small space in the connector interface makes it difficult to attach additional plugin
- Plugin needs to spoof the CC signal without affecting the regular charging function
- Plugin needs to be small and hidden
- Plugin needs to be easy to install and not damage the connector structure

The plugin design should be fit in this connector.

Physical plugin for charging connectors

inner view

outside view