TechXplore

Hacker finds way to unlock Tesla models, start cars

May 18 2022, by Margi Murphy

Tesla Inc. customers might love the carmakers' nifty keyless entry system, but one cybersecurity researcher has demonstrated how the same technology could allow thieves to drive off with certain models of the electric vehicles.

A hack effective on the Tesla Model 3 and Y cars would allow a thief to unlock a vehicle, start it and speed away, according to Sultan Qasim Khan, principal security consultant at the Manchester, UK-based security firm NCC Group. By redirecting communications between a car owner's mobile phone, or key fob, and the car, outsiders can fool the entry system into thinking the owner is located physically near the vehicle.

The hack, Khan said, isn't specific to Tesla, though he demonstrated the technique to Bloomberg News on one of its car models. Rather, it's the result of his tinkering with Tesla's keyless entry system, which relies on what's known as a Bluetooth Low Energy (BLE) protocol.

There's no evidence that thieves have used the hack to improperly access Tesla vehicles. The carmaker didn't respond to a request for comment. NCC provided details of its findings to its clients in a note on Sunday, an official there said.

Tesla in April acknowledged that "relay attacks are known limitation of the passive entry system," according to NCC Group.

Khan said he had disclosed the potential for attack to Tesla and that company officials didn't deem the issue a significant risk. To fix it, the carmaker would need to alter its hardware and change its keyless entry system, Khan said. The revelation comes after another security researcher, David Colombo, revealed a way of hijacking some functions on Tesla vehicles, such as opening and closing doors and controlling music volume.

BLE protocol was designed to conveniently link devices together over the internet, though it's also emerged as method that hackers exploit to unlock smart technologies including house locks, cars, phones and laptops, Khan said. NCC Group said it was able to conduct the attack on several other carmakers and technology companies' devices.

Kwikset Corp. Kevo smart locks that use keyless systems with iPhone or Android phones are impacted by the same issue, Khan said. Kwikset said that customers who use an iPhone to access the lock can switch on two-factor authentication in lock app. A spokesperson also added that the iPhone-operated locks have a 30-second timeout, helping protect against intrusion.

Kwikset will be updating its Android app in "summer," the company said.

"The security of Kwikset's products is of utmost importance and we partner with well-known security companies to evaluate our products and continue to work with them to ensure we are delivering the highest security possible for our consumers," a spokesperson said.

A representative at Bluetooth SIG, the collective of companies that manages the technology said: "The Bluetooth Special Interest Group (SIG) prioritizes security and the specifications include a collection of features that provide product developers the tools they need to secure communications between Bluetooth devices.

"The SIG also provides educational resources to the developer community to help them implement the appropriate level of security within their Bluetooth products, as well as a vulnerability response program that works with the security research community to address vulnerabilities identified within Bluetooth specifications in a responsible manner."

Khan has identified numerous vulnerabilities in NCC Group client products and is also the creator of Sniffle, the first open-source Bluetooth 5 sniffer. Sniffers can be used to track Bluetooth signals, helping identify devices. They are often used by government agencies that manage roadways to anonymously monitor drivers passing through urban areas.

A 2019 study by a British consumer group, Which, found that more than 200 car models were susceptible to keyless theft, using similar but slightly different attack methods such as spoofing wireless or radio signals.

In a demonstration to Bloomberg News, Khan conducted a so-called relay attack, in which a hacker uses two small hardware devices that forward communications. To unlock the car, Khan placed one relay device within roughly 15 yards of the Tesla owner's smartphone or key fob and a second, plugged into his laptop, near to the car. The technology utilized custom computer code that Khan had designed for Bluetooth development kits, which are sold online for less than $50.

The hardware needed, in addition to Khan's custom software, costs roughly $100 altogether and can be easily bought online. Once the relays are set up, the hack takes just "ten seconds," Khan said.

"An attacker could walk up to any home at night—if the owner's phone is at home—with a Bluetooth passive entry car parked outside and use this attack to unlock and start the car," he said.

"Once the device is in place near the fob or phone, the attacker can send commands from anywhere in the world," Khan added.

Citation: Hacker finds way to unlock Tesla models, start cars (2022, May 18) retrieved 27 April 2024 from https://techxplore.com/news/2022-05-hacker-tesla-cars.html