Tesla fixes security in Model S after Chinese hack

21 September 2016

Tesla Model S

Tesla said Wednesday that it had fixed a software vulnerability in its luxury electric Model S sedan after a Chinese security team hacked a car's systems and remotely controlled it.

The newest hacking case of remote manipulation of a car served to underscore the potential dangers of vehicles that are heavily connected via wireless technologies.

"Tesla has already deployed an over-the-air software update that addresses the potential security issues" of the hack, the company said in a statement.

Keen Security Lab, a unit of Chinese internet giant Tencent, announced on Monday that after a months-long effort it had discovered "multiple security vulnerabilities" in the Model S and had been able to remotely control a car in both parking and driving mode.

Keen posted a video showing its ability to manipulate an unmodified Tesla remotely.

Keen said that after the hack it informed Tesla Motors and the two companies were cooperating on the issue.

"Following the global industry practice on 'responsible disclosure' of product security vulnerabilities, we have reported the technical details of all the vulnerabilities discovered in the research to Tesla. The vulnerabilities have been confirmed by Tesla Product Security Team," it said.

Tesla downplayed the risk, saying the intrusion could only be carried out when the car's web browser is in use.

It "also required the car to be physically near to and connected to a malicious Wi-Fi hotspot," the company said.

"Our realistic estimate is that the risk to our customers was very low, but this did not stop us from responding quickly."

Tesla added that it would reward Keen under its "bug bounty program" which is intended to encourage outsiders to probe its systems for weaknesses.

Tesla shares were down 0.8 percent at $202.85 in trade Wednesday.

It was the second time in two years that cars of Tesla, the brash startup of inventor Elon Musk, were targeted by hackers.

In 2015, two Americans were able to break into a Model S through its media system , giving them the power to remotely start a car and stop it while it was in motion.

Musk, who is also behind the ambitious private space firm SpaceX, said that Tesla would upload a new version of its car software to cars late Wednesday.

He added in a tweet that the release was "a major

overhaul on almost every level" from the current software version.

Hacking risks

US auto and highway regulators are increasingly concerned about the vulnerability to hacking of cars whose advanced information systems are always connected to the internet and other wireless communications.

In 2015 two US researchers showed that they could commandeer from a distance a Jeep Cherokee. Working from laptop computers at home, they tinkered with the Cherokee's steering and brakes as well as the radio, windshield wipers and more.

A number of automakers, including General Motors and Fiat Chrysler, have launched programs to encourage "white hat" hackers to find vulnerabilities in their systems.

In Tesla's case, the company is offering hackers rewards of $100 to $10,000 to find and alert the company of bugs in its systems.

A particular new concern is the development of self-driving cars, which rely on a huge level of wireless connectivity.

On Monday the US government outlined new standards for developers of self-driving technology that included demonstrating their cars were secure from hacking and also protected user privacy.