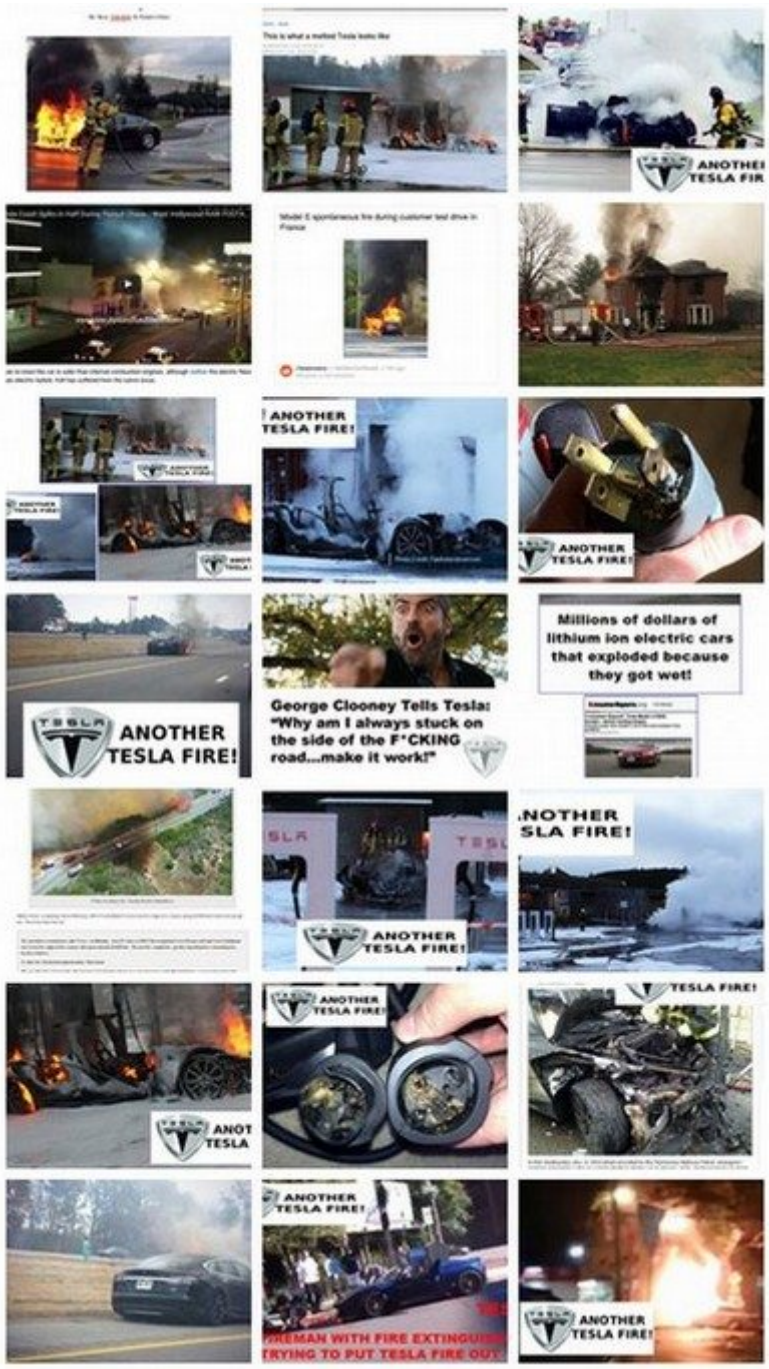
Tesla proven to be easily hacked and able to be taken over by other nations

A large number of Tesla’s have suddenly shot off cliffs, swerved into trees and buildings and otherwise killed the drivers and innocent bystanders with sudden movements. Is Tesla covering up constant take-overs of the Tesla cars by hackers?



Researchers hack Tesla Model S with remote attack

The researchers were able to remotely control the braking system, sunroof, door locks, trunk, side-view mirrors and more

Credit: Tesla

Lucian Constantin
IDG News Service

Tesla Motors is considered one of the most cybersecurity-conscious car manufacturers in the world—among other things, it has a bug bounty program. But that doesn't mean the software in its cars is free of security flaws.

Researchers from Chinese technology company Tencent found a series of vulnerabilities that, when combined, allowed them to remotely take over a Tesla Model S car and control its sunroof, central display, door locks and even the braking system. The attack allowed the researchers to access the car's controller area network (CAN) bus, which lets the vehicle's specialized computers communicate with each other.

"As far as we know, this is the first case of remote attack which compromises CAN Bus to achieve remote controls on Tesla cars," the researchers from Tencent's Keen Security Lab said in a blog post Monday. "We have verified the attack vector on multiple varieties of Tesla Model S. It is reasonable to assume that other Tesla models are affected."

The blog post is accompanied by a demonstration video in which the researchers show what they can achieve through their attack, which works either while the car is parked or being driven.

First, while the car was parked, the researchers used a laptop to remotely open its sunroof, activate the steering light, reposition the driver's seat, take over the dashboard and central display and unlock the car.

In a second demonstration, they turned on the windshield wipers while the car was being driven at low speed in a parking lot for demonstration purposes. They also showed that they can open the trunk and fold the side-view mirror when the driver is trying to change lanes. While these operations can be distracting to the driver in certain situations, causing a safety risk, the most dangerous thing they were able to do was to engage the car's braking from 12 miles away.

Such an attack, performed against a car being driven at high speed on a highway, could result in a serious rear-end collision.

The researchers reported all of the vulnerabilities through Tesla's bug bounty program, and the company is working on patches. Fortunately, Tesla cars can receive firmware updates remotely

and Tesla car owners are advised to make sure that their vehicles are always running the latest software version.

Car hacking has become a hot topic in recent years among security researchers, regulators and car manufacturers themselves. As cars become more interconnected, the ways in which they can be remotely hacked will only increase, so it's important that the computers handling critical safety features are isolated and protected.

Tesla did not immediately respond to a request for comment.

Related:

- Security
- Car Tech

Lucian Constantin Romania Correspondent

Follow

Lucian Constantin writes about information security, privacy, and data protection for the IDG News Service.

More by Lucian Constantin

Hackers control TESLA 12 miles away...

Brakes to wipers...