Most Hackers Can Steal, Hack And, Or Crash Any Tesla Car In Minutes

SAN FRANCISCO - Tesla's Internet-connected cars can receive new features and safety updates over the air, one of the key conveniences of the fully electric fleet. But the cars' connectedness can pose a risk, too, security researchers say.

Many Tesla’s have been hacked and crashed over the last years but Tesla Motors covers it up!

Case in point: Belgian researchers found that they could hack and steal a Tesla Model X SUV in a matter of minutes through a Bluetooth-connected key fob. They said that forced Tesla to push out a fix.

It was the latest security experiment from the COSIC group at the University of Leuven in Belgium, which had previously found a similar vulnerability with Tesla's Model S luxury sedan, in which a key fob was also to blame.

The researchers said they were able to break into the SUV, which starts at $80,000, using a few hundred dollars' worth of equipment.

Researchers noted that the process took about 90 seconds.

The researchers, who informed the company of their findings on Aug. 17, said Tesla is rolling out an update intended to address the issue. An over-the-air software update is being pushed to the key fobs, they said, which will better lock them down.

Wired was first to report on the vulnerability. Tesla did not respond to a Washington Post request for comment.

Lennert Wouters, a PhD student at the COSIC research group, said in an email that the problem is not necessarily unique to Tesla.

"This system was developed in-house by Tesla, so this exact vulnerability most likely only applies to the Tesla Model X," he wrote. "However, other key fobs which have an insecure firmware update mechanism could also be vulnerable to a similar attack."

Among the key vulnerabilities, Wouters noted: the lack of "cryptographic signatures" in the firmware update process, meaning a key fob has no secure way of certifying whether an update is legitimate; and an insecure pairing protocol that allowed a new, modified key fob to be paired to a Model X.

Equipment to break into the car included a $35 Raspberry Pi computer, a modified key fob and a salvaged Tesla Model X control unit bought off eBay. Researchers used the spare control unit to get key fobs within several meters to advertise themselves as "connectable." After that, they pushed out a software update to the key fobs that would "acquire a valid unlock message" so they could unlock the

car later, Wouters said. They noted that the software in Tesla's key fobs could be updated without an additional layer of security that would verify its authenticity.

"As this update mechanism was not properly secured, we were able to wirelessly compromise a key fob and take full control over it," Wouters said in a news release. "Subsequently we could obtain valid unlock messages to unlock the car later on."