Hackers Demonstrated How Anybody Can Unlock and Steal a Tesla Model S in Under 2 Seconds

BRANDON FRIEDERICH

Elon Musk's fleet of all-electric Teslas may be brimming with advanced technology—and some old-school Atari games—but the same can't be said about the vehicles' security systems.

Case in point: A team of researchers at Belgium's KU Leuven university have discovered a way to hack any Tesla Model S key fob and retrieve its cryptographic code in under two seconds using just $6oo worth of gadgets.

From there, they can simply unlock the car and drive off. Wired has further details on the preparation needed to perform the hack.

> The researchers found that once they gained two codes from any given key fob, they could simply try every possible cryptographic key until they found the one that unlocked the car.
>
> They then computed all the possible keys for any combination of code pairs to create a massive, 6-terabyte table of pre-computed keys.
>
> With that table and those two codes, the hackers say they can look up the correct cryptographic key to spoof any key fob in just 1.6 seconds.

In addition to a portable hard drive containing a table of all possible key codes, all the researchers needed was a Yard Stick One radio, a Proxmark radio and a little hacker know-how to boost the EV, as demonstrated in the video below:

Wired has further details on how the process works:

> First, they use the Proxmark radio to pick up the radio ID of a target Tesla's locking system, which the car broadcasts at all times. Then the hacker swipes that radio within about 3 feet of a victim's key fob, using the car's ID to spoof a "challenge" to the fob.
>
> They do this twice in rapid succession, tricking the key fob into answering with response codes that the researchers then record. They can then run that pair of codes through their hard drive's table to find the underlying secret key—which lets them spoof a radio signal that unlocks the car, then starts the engine.

The KU Leuven team says the Model S is hackable because its keyless entry system, which is built by manufacturer Pektron, uses weak encryption. KU Leuven researcher Tomer Ashur sure didn't sugar coat his analysis of the issue.

"It was a very foolish decision," Ashur told Wired. "Someone screwed up. Epically."

The researchers were paid a $10,000 "bug bounty" when they presented their findings to Tesla in August of 2017, but the fix didn't come until June of 2018.

"Based on the research presented by this group, we worked with our supplier to make our key fobs more secure by introducing more robust cryptography for Model S in June 2018," a Tesla spokesperson wrote to Wired. "A corresponding software update for all Model S vehicles allows customers with cars built prior to June to switch to the new key fobs if they wish."

For Model S owners who don't want to pay for the new fob, Tesla just rolled out an optional "Pin to Drive" feature requires an additional code to be entered that prevents hackers from operating the car.

But seriously, what's the price of a set of keys when you've already paid $75,000 for a luxury ride?

http://outline.com/7hCTpc