HACKERS CAN STEAL A TESLA MODEL S IN SECONDS BY CLONING ITS KEY FOB

The researchers also believe their attack might work against cars sold by McLaren and Karma, and motorcycles sold by Triumph, which use keyless entry systems made by the same manufacturer. ETHAN MILLER/GETTY IMAGES

TESLA HAS TAKEN plenty of innovative steps to protect the driving systems of its kitted-out cars against digital attacks. It's hired top-notch security engineers, pushed over-the-internet software updates, and added code integrity checks. But one team of academic hackers has now found that Tesla left its Model S cars open to a far more straightforward form of hacking: stealthily cloning the car's key fob in seconds, opening the car door, and driving away.

A team of researchers at the KU Leuven university in Belgium on Monday plan to present a paper at the Cryptographic Hardware and Embedded Systems conference in Amsterdam, revealing a technique for defeating the encryption used in the wireless key fobs of Tesla's Model S luxury sedans. With about $600 in radio and computing equipment, they can wirelessly read signals from a nearby Tesla owner's fob. Less than two seconds of computation yields the fob's cryptographic key, allowing them to steal the associated car without a trace. "Today it’s very easy for us to clone these key fobs in a matter of seconds," says Lennert Wouters, one of the KU Leuven researchers. "We can completely impersonate the key fob and open and drive the vehicle."

Just two weeks ago, Tesla rolled out new antitheft features for the Model S that include the ability to set a PIN code that someone must enter on the dashboard display to drive the car. Tesla also says that Model S units sold after June of this year aren't vulnerable to the attack, due to upgraded key fob encryption that it implemented in response to the KU Leuven research. But if owners of a Model S manufactured before then don't turn on that PIN—or don't pay to replace their key fob with the more strongly encrypted version—the researchers say they're still vulnerable to their key-cloning method.

Keys to the Kingdom

Like most automotive keyless entry systems, Tesla Model S key fobs send an encrypted code, based on a secret cryptographic key, to a car's radios to trigger it to unlock and disable its immobilizer, allowing the car's engine to start. After nine months of on-and-off reverse engineering work, the KU Leuven team discovered in the summer of 2017 that the Tesla Model S keyless entry system, built by a manufacturer called Pektron, used only a weak 40-bit cipher to encrypt those key fob codes.

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 their proof-of-concept attack, which they show in the video below, the researchers demonstrate their keyless-entry-system hacking technique with a hardware kit comprising just a Yard Stick One radio, a Proxmark radio, a Raspberry Pi minicomputer, their pre-computed table of keys on a portable hard drive, and some batteries.

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.

That whole attack chain, the researchers say, is possible thanks to the Pektron key fob system's relatively weak encryption. "It was a very foolish decision," says KU Leuven researcher Tomer Ashur. "Someone screwed up. Epically."

The KU Leuven researchers say they told Tesla about their findings in August 2017. Tesla acknowledged their research, thanked them, and paid them a $10,000 "bug bounty" for their work, the researchers say, but it didn't fix the encryption issue until its June encryption upgrade and more recent PIN code addition.

In a statement to WIRED, Tesla said those fixes were rolled out as quickly as possible given the time needed to confirm the researchers' work, test a fix, and integrate it into their manufacturing processes. "Due to the growing number of methods that can be used to steal many kinds of cars with passive entry systems, not just Teslas, we've rolled out a number of security enhancements to help our customers decrease the likelihood of unauthorized use of their vehicles," a Tesla spokesperson wrote to WIRED. "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 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." The company also noted that you can trace a Tesla on your phone, which should make it relatively easy to locate a stolen vehicle.

The researchers believe their attack might also work against cars sold by McLaren and Karma and motorcycles sold by Triumph, which also use Pektron's key fob system. But they weren't able to get their hands on those vehicles to test them. Neither Karma nor Triumph responded to WIRED's request for comment, nor did Pektron itself. McLaren says it's still investigating the issue but is alerting its customers to the potential theft risk and offering them free "signal-blocking pouches" that block radio communications to their key fobs when they're not in use. "While this potential method has not been proven to affect our cars and is considered to be a low risk, plus we have no knowledge of any McLaren vehicle being stolen by this or the previously reported ‘relay attack’ method, nevertheless we take the security of our vehicles and the concerns of our customers extremely seriously," a McLaren spokesperson writes.

If those other manufacturers are indeed affected, beyond putting keys in those "signal-blocking pouches"—Faraday bags that block radio communications—just how all of them might definitively fix the problem is far from clear. The researchers say that the companies would likely have to replace every vulnerable key fob, as well as push out a software update to affected vehicles. Unlike Tesla, whose cars receive over-the-air updates, that might not be possible for other manufacturers' vehicles.

Warning Sign

Despite the questions surrounding how to prevent the attack, KU Leuven's Ashur argues that revealing the vulnerability is necessary to pressure Tesla and other carmakers to protect their customers from theft. Now that Tesla has added a PIN feature, it also serves as a warning that Tesla owners should turn on that feature to protect against a surprisingly easy method of grand theft auto. Aside from the PIN, Tesla also allows Model S owners to disable passive entry for its key fobs, meaning drivers would have to push a button on the fob to unlock the car. That would also stymie the KU Leuven attack.

"This attack is out there, and we’re not the only people in the world capable of coming up with it," Ashur says.

meone screwed up.
cally."

ASHUR, KU LEUVEN

For years, hackers have demonstrated that it's possible to perform so-called relay attacks against keyless entry systems, spoofing a car's radio signals to elicit a response from its key fob and then replaying that signal in real time to the car's locking system. In some cases, hackers have pulled off those attacks by amplifying the key's radio signal, or by bridging the distance between the car and the victim's key fob by holding one radio device close to each. Those relay attacks have been used to pull off very real car thefts, though it's never been clear how many, given the lack of evidence left behind. Relay attack thefts are no doubt part of Tesla's motivation for adding its PIN precaution, regardless of the KU Leuven research.

But even those relay attacks still only allow a car thief to spoof a victim's key once. Even if they manage to drive the car away, they're unable to unlock or start it again. The KU Leuven attack, by contrast, allows a thief to permanently clone the victim's key, so that they can unlock and drive the car in perpetuity. "Basically, we can do everything a relay attack can do and more," says Wouters.

With that dangerous key-cloning method now in the open, anyone who owns a vulnerable Model S would be wise to turn on Tesla's newly added PIN feature or disable passive entry. Punching four numbers into the car's dash or a button on its key fob before starting it up may be an annoyance, but it beats returning to a empty parking spot.