HACKERS CAN STEAL OR CRASH ANY TESLA CAR

The company is rolling out a patch for the vulnerabilities, which allowed one researcher to break into a car in 90 seconds and drive away.

The technique takes advantage of a collection of security issues—both major and minor— has always prided itself on its so-called over-the-air updates, pushing out new code automatically to fix bugs and add features. But one security researcher has shown how vulnerabilities in the Tesla Model X's keyless entry system allow a different sort of update: A hacker could rewrite the firmware of a key fob via Bluetooth connection, lift an unlock code from the fob, and use it to steal a Model X in just a matter of minutes.

Lennert Wouters, a security researcher at Belgian university KU Leuven, today revealed a collection of security vulnerabilities he found in both Tesla Model X cars and their keyless entry fobs. He discovered that those combined vulnerabilities could be exploited by any car thief who manages to read a car's vehicle identification number—usually visible on a car's dashboard through the windshield—and also come within roughly 15 feet of the victim's key fob. The hardware kit necessary to pull off the heist cost Wouters around $300, fits inside a backpack, and is controlled from the thief's phone. In just 90 seconds, the hardware can extract a radio code that unlocks the owner's Model X. Once the car thief is inside, a second, distinct vulnerability Wouters found would allow the thief to pair their own key fob with the victim's vehicle after a minute's work and drive the car away.

"Basically a combination of two vulnerabilities allows a hacker to steal a Model X in a few minutes time," says Wouters, who plans to present his findings at the Real World Crypto conference in January. "When you combine them, you get a much more powerful attack."

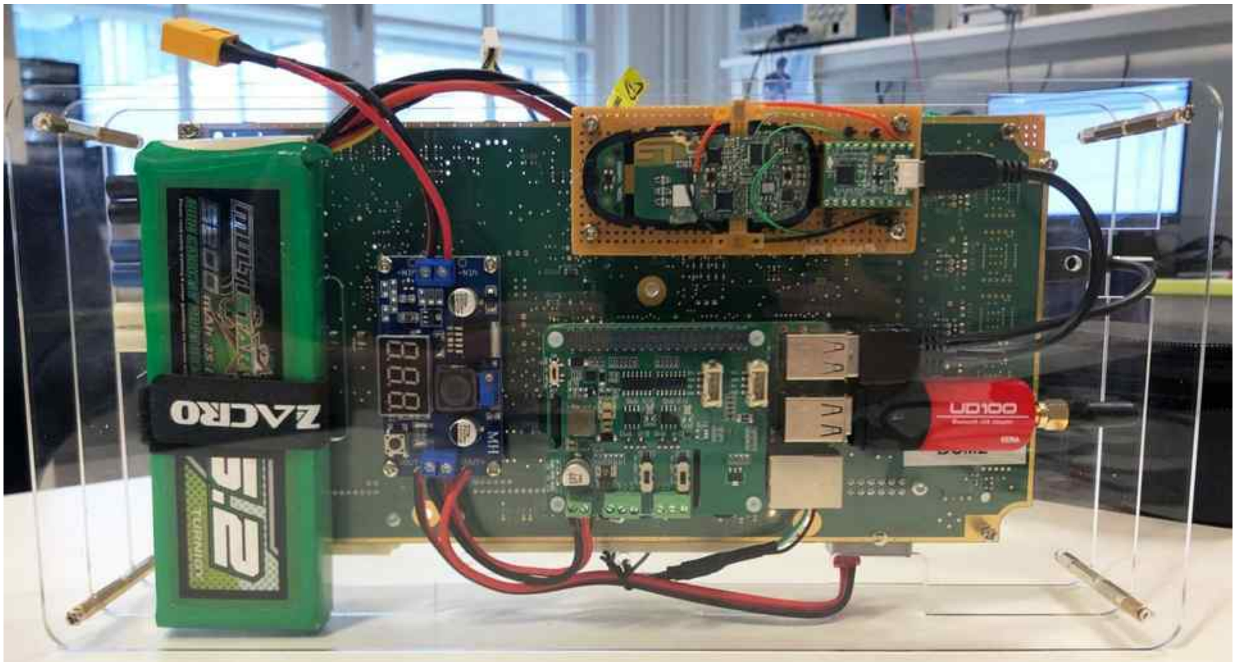
Wouters says he warned Tesla about his Model X keyless entry hacking technique in August. He says the company has told him it plans to start rolling out a software update to its key fobs this week—and possibly components of its cars too—to prevent at least one step in his two-part attack. WIRED also reached out to Tesla to learn more about its software fix, but the company didn't respond. (Tesla dissolved its press relations team in October.) Tesla told Wouters that the patch may take close to a month to roll out across all of its vulnerable vehicles, so Model X owners should be sure to install any updates Tesla makes available to them over the coming weeks to prevent the hack. In the meantime, the Belgian researcher says he's been careful not to publish any of the code or reveal technical details that would enable car thieves to pull off his tricks.

Wouters' technique takes advantage of a collection of security issues he discovered in the Model X's keyless entry system—both major and minor—that together add up to a method to fully unlock, start, and steal a vehicle. First, the Model X key fobs lack what's known as "code signing" for their firmware updates. Tesla designed its Model X key fobs to receive over-the-air firmware updates via Bluetooth by wirelessly connecting to the computer inside a Model X, but without confirming that the new firmware code has an unforgeable cryptographic signature from Tesla. Wouters found that he could use his own computer with a Bluetooth radio to connect to a target Model X's keyfob, rewrite the firmware, and use it to query the secure enclave chip inside the fob that generates an unlock code for the vehicle. He could then send that code back to his own computer via Bluetooth. The whole process took 90 seconds.

At first, Wouters found that establishing the Bluetooth connection wasn't so easy. The Model X key fob's Bluetooth radio only "wakes up" for a few seconds when the fob's battery is removed and then put back in. But Wouters discovered that the computer inside the Model X responsible for the keyless entry system, a component known as the body control module (BCM), can also perform that Bluetooth wake-up command. By buying his own Model X BCM on eBay—where they go for $50 to $100—Wouters could spoof the low-frequency radio signal sent to the key fob. (While that initial wake-up command has to be sent from close radio range—about 15 meters—the rest of the firmware update trick can be carried out from hundreds of feet away if the victim is outdoors.)

Wouters also found that the BCM derived the unique code it uses to prove its identity to the key fob from the last five digits of the car's VIN number. A thief would be able to read those digits from the target car's windshield, and could then use it to create a code for their bootleg BCM. "You end up with a BCM that thinks it belongs to the target vehicle," Wouters says. "I can then force that BCM to instruct key fobs that have the same identifier as that car to wake up, basically."

Even all that clever hacking, however, only got Wouters as far as unlocking the car. To unlock and drive it, he had to go one step further. Once inside the Model X, Wouters found that he could plug his own computer into a port that's accessible via a small panel under the display. He says this can be done in seconds, without tools, by pulling off a small storage container on the dash. That port lets the computer send commands to the car's network of internal components, known as a CAN bus, which includes the BCM. He could then instruct the Model X's actual BCM to pair with his own key fob, essentially telling the car his spoofed key is valid. Though each Model X key fob contains a unique cryptographic certificate that should have prevented the car from pairing with a rogue key, Wouters found the BCM didn't actually check that certificate. That allowed him—with just a minute of fiddling under the dash—to register his own key to the vehicle and drive it away.



Wouters' custom-made Tesla Model X hacking tool, built for around $300, includes a Model X body control module, a disassembled key fob, a Raspberry Pi minicomputer, and a battery.COURTESY OF Wouters notes that the two most serious vulnerabilities he found—the lack of validation for both key fob firmware updates and pairing new key fobs with a car—point to an apparent disconnect between the security design of the Model X's keyless entry system and how it was implemented. "The system has everything it needs to be secure," Wouters says. "And then there are a few small mistakes that allow me to circumvent all of the security measures."

To demonstrate his technique, Wouters assembled a breadbox-sized device that includes a Raspberry Pi minicomputer, a secondhand Model X BCM, a key fob, a power converter, and a battery. The whole kit, which can send and receive all the necessary radio commands from inside a backpack, cost him less than $300. And Wouters designed it so that he could stealthily control it, inputting the car's VIN number, retrieving an unlock code, and pairing a new key all from a simple command prompt on his smartphone, as shown in the video above.

Wouters says there's no evidence his technique has been used for real-world grand theft auto. But thieves have actively targeted Tesla's keyless entry systems to steal vehicles in recent years, using relay attacks that amplify the signal from a key fob to unlock and start a car, even when the key fob is inside the victim's home and the car is parked in their driveway.

Wouters' method, while far more complex, could easily have been put into practice if he hadn't warned Tesla, says Flavio Garcia, a researcher at the University of Birmingham who has focused on the security of cars' keyless entry systems. "I think it's a realistic scenario," says Garcia. "This weaves together a number of vulnerabilities to build an end-to-end, practical attack on a vehicle."

The Model X hacking technique isn't Wouters' first time exposing vulnerabilities in Tesla's keyless entry systems: He's twice before found cryptographic vulnerabilities in Tesla Model S keyless entry systems that would have similarly allowed radio-based car theft. Even so, he argues that there's nothing particularly unique about Tesla's approach to keyless entry security. Comparable systems are likely just as vulnerable. "They're cool cars, so they're interesting to work on," Wouters says. "But I think if I spent as much time looking at other brands, I would probably find similar issues."

More unique for Tesla, Wouters points out, is that unlike many other automakers it has the ability to push out OTA software patches rather than requiring that drivers bring their key fobs to a dealer to be updated or replaced. And that's the upside of treating cars like personal computers: Even when that update mechanism turned out to be a hackable vulnerability, it also offers Tesla owners a lifeline to fix the problem.