Bypassing ECU safeguards

Security researchers have found new ways to bypass safeguards of a Jeep Cherokee's CAN-connected ECUs.

A Jeep Cherokee did end up in a ditch during the tests, when the wheel was turned remotely at 50 km/h (Photo: The NRMA/Flickr)

For the third time in a row, automotive cyber security researchers Charlie Miller and Chris Valasek presented a car hack at the Black Hat security conference. Two years ago, they analyzed the schematics of 24 different car makes and models. They were looking for possible vulnerabilities that car hackers might be able to explore. Last year, they demonstrated that they can in fact hack a Jeep Cherokee without ever touching the car. This year, they went back to an approach that required a physical connection to the Jeep Cherokee and its CAN network – but only because the researchers gave Chrysler the chance to fix the security flaw they discovered last year. In this year's demonstration, the hackers showed what could have happened without last year's security patch.

Like last year, Miller and Valasek showed Wired reporter Andy Greenberg their results days before the conference. This time they wanted to circumvent safeguards deep in the vehicle's network, not only achieve wireless access. According to Greenberg, "CAN network components are designed to resist certain dangerous digital signals: The diagnostic mode that Miller and Valasek used to disable the Jeep's brakes, for instance, wouldn't work at any speed above five miles per hour."

So the researches looked for ways to bypass these safeguards – and they found them. "Instead of merely compromising one of the ECUs on a target car's CAN network and using it to spoof messages to the car's steering or brakes, they also attacked the ECU that sends legitimate commands to those components, which would otherwise contradict their malicious commands and prevent their attack. By putting that second ECU into "bootrom" mode—the first step in updating the ECU's firmware that a mechanic might use to fix a bug—they were able to paralyze that innocent ECU and send malicious commands to the target component without interference."

This gave the hackers the power to activate the brake at any speed, disable the steering, and turn the wheel themselves. Another attack enabled them to alter the settings of the cruise control, accelerating the Jeep. This, however, can be countered by the driver – if the driver notices that it is happening and reacts in time.

While Miller and Valasek still needed access to the car to hack it, it has been demonstrated that wireless hacks are completely possible. And after a wireless hack, this is the kind of attack hackers are able to pull off. Only this year, researchers showed that as early as 2010 they managed to get access to a car via a playing a song spiked with malicious code.

In articles on car hacking, the CAN network itself is often considered insecure, because it is old and not made for the challenges of the connected car. In reality, it is not the CAN network itself that is insecure – it is secure, if the access to it is secured. Yesterday, Miller and Valasek held their talk on "Advanced CAN injection techniques for vehicle networks" at the Black Hat conference. In the abstract to their talk, the hackers themselves say that "there are often many limitations on what actions the vehicle can be forced to perform when injecting CAN messages. […] In this talk, we discuss how physical, safety critical systems react to injected CAN messages and how these systems are often resilient to this type of manipulation. We will outline new methods of CAN message injection which can bypass many of these restrictions and demonstrate the results on the braking, steering, and acceleration systems of an automobile. We end by suggesting ways these systems could be made even more robust in future vehicles."

One easy fix to the "bootrom" mode the researchers misused for their hack would be a physical switch that the mechanic has to flip to put the car in the potentially dangerous mode. Additionally, the CAN network should be monitored for this kind of ECU-silencing hacks. Several companies already offer solutions to automotive security threats, among them Tower Sec, Symantec, and Argus.

Meanwhile another threat was published this week: At the Usenix Workshop on Offensive Technologies conference, a group of University of Michigan researchers plan to present the findings of a set of tests on industrial vehicles. Connecting a laptop to the vehicles via on-board diagnostic ports, they found that they could simply look up most commands using J1939. That allowed them to replicate those signals on the vehicles' networks without the reverse engineering other car hackers have had to do to replay commands inside consumer vehicles, which lack the standardization of industrial trucks. The researchers claim that the entire truck-hacking project only took them two month.

ae