Computer scientists work to prevent hackers from remotely controlling cars

November 21 2016

One of these has now been closed by computer scientists at the Center for IT Security and Privacy (CISPA) and the German Research Center for Artificial Intelligence (DFKI)—with the help of software that manufacturers can retrofit into any car. In order to remotely brake a car traveling at more than 100 kilometer per hour, it was enough for the American security researcher Stephen Checkoway to use the music player software installed in the car together with a smartphone connected to it. "If the software were not connected to the internal network, the so-called CAN bus, of that mid-range sedan, then Checkoway would have had to work harder," explains Stefan Nuernberger, who leads the Smart Systems Lab at the German Research Center for Artificial Intelligence (DFKI).

The CAN bus was developed in 1983 by the auto industry in order to avoid having to install meter-long cable trees in cars. The advantage of a bus structure lies in that only a single transmission line is used, which interconnects all of the devices and allows them to communicate with each other. The CAN bus connects not only sensors—for example, for the speed controls—but also actuators such as servo motors. Steering devices, such as a parking assistant, also send their commands through the bus. "From the perspective of IT security, however, this harbors a crucial downside: As soon as one of the devices on the bus is controlled by an attacker, it can masquerade as a different device to the others, and forge messages," explains Nuernberger.

Therefore, Nuernberger is working together with Christian Rossow,

professor of IT security at Saarland University, to ensure that components like the emergency braking assistant on the CAN bus need not doubt the authenticity of the sender, nor the veracity of the information sent. The software they developed for that purpose, "vatiCAN", accomplishes this, since only a valid sender can attach the required authentication codes to its messages.

That makes the following security check possible: the emergency braking assistant sends, as before, its command to the brakes. After that, it calculates, with the help of a secret key, an authentication code that is only valid for a single data packet and is also sent to the brakes. Meanwhile, the brakes have themselves calculated the authentication code, and compare theirs with the one sent over the CAN bus. If the codes are identical, the brakes can be sure that the message was not manipulated, and carry out the order. "The brakes know indirectly that the message could only have come from the braking assistant, because the assistant could not have calculated the correct code otherwise," says Nuernberger.

The researchers combat other attacks, for example recording and re-sending of messages (replay attacks), by adding a timestamp to the message. If it isn't current, then something is wrong with the message. "With the additional calculations, the transfer of the message takes only two more milliseconds," reports Nuernberger, who has tested vatiCAN on a VW Passat. This is also acceptable for control procedures where immediate response is required. "When data packets are delayed by two milliseconds, then at a speed of 130 kilometer per hour, the braking distance is seven centimeter longer," according to Nuernberger. The researchers have already presented their method at an international conference in Santa Barbara, California. Their software can be freely used and is available for download on the Internet.

Provided by Saarland University

Citation: Computer scientists work to prevent hackers from remotely controlling cars (2016, November 21) retrieved 3 May 2024 from https://phys.org/news/2016-11-scientists-hackers-remotely-cars.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.