# Scientists prevent hacker attacks on cars

September 20 2017


Dr. Stefan Nürnberger. Credit: Stephanie Bremerich (CISPA)

Today, many cars are offering a digital gateway which hackers can misuse. Scientists at the Competence Center for IT Security at Saarland University and the German Research Center for Artificial Intelligence have therefore developed a technology that can prevent such attacks. With the freely available software 'vatiCAN,' car manufacturers can

retrofit their programs. The new technology is presented at the International Motor Exhibition in Frankfurt am Main.

In a luxury vehicle today, a few dozen computers are built in, each of which has far more computing power than an Apollo rocket. These computers make it easier for mechanics to diagnose faults, or warn the driver of a dangerous lane change. "The computers, however, only follow predetermined control commands, without thinking about them like a human being. If an intruder confuses the command hierarchy, suddenly uncontrolled commands can interfere with the devices in the car and abruptly make it slow down or swerve," says Stefan Nürnberger, leader of the research group for Automotive Security at German Research Center for Artificial Intelligence (DFKI) in Saarbrücken. Only a few years ago such scenarios were virtually impossible, because criminals would have needed to gain physical access to the vehicle in order to manipulate it.

"Today, more and more vehicles have a permanent Internet connection. This makes it possible, for example, to incorporate current traffic jam information into route planning, or activate the auxiliary heating remotely. But if such internet-capable control devices have security holes, attackers can send commands to thousands of vehicles," the computer science PhD student warns. Together with Christian Rossow, professor of IT security at Saarland University, Nürnberger is working to make sure that components such as an emergency braking assistant always check the authenticity of the commands sent to them. The "vatiCAN" software developed for this purpose ensures that only a genuine sender can attach the necessary authentication codes to these messages.

"These codes are continually renegotiated between the control device of the vehicle and therefore cannot be known to an attacker from the outside. Each control device that uses our software can thus distinguish

real messages from forged ones," explains Nürnberger. For their security solution, it was important to the researchers that it could easily be retrofitted by car manufacturers. "The language used by the control devices in a car is not changed by 'vatiCAN.' This allows the software to be integrated into existing vehicles in order to protect them against attacks," says the Saarbrücken researcher. Since it would be a Sisyphean task to adapt each language and protocol for each brand and model, the participation of manufacturers is requested: they would have the information needed to easily integrate the anti-hacking software.

## Further technical details:

The vatiCAN solution also prevents attacks such as the recording of authenticated messages by inserting a timestamp into each message. If it isn't current, the message was recorded and could turn out to be dangerous. "With these additional calculations, transferring the message takes only two more milliseconds," explains Nürnberger, who has tested vatiCAN on a VW Passat. This is still acceptable for control procedures where an immediate response is required: "If data packets are delayed by two milliseconds, the braking distance is extended by only seven centimeters at a speed of 130 kilometers per hour," says Nürnberger.

The researchers have already presented their method at an international conference in Santa Barbara, California. The software can be downloaded from the Internet and used free of charge.

**More information:** www.automotive-security.net/vatican

Provided by Saarland University