Außer Rand und Band – Forscher hacken Auto

Einmal gehackt, gehorchte das Auto dem Team um Steven Savage von der Universität des US-Bundesstaates Kalifornien in San Diego (UCSD) und Tadayoshi Kohno von der Universität des US-Bundesstaates Washington in Seattle aufs Wort. Auf einem stillgelegten Flugplatz reagierte der Wagen unter anderem gar nicht mehr auf die Bremse oder leitete ohne Zutun des Fahrers eine Vollbremsung ein.

Details beschreiben die Wissenschaftler in einem Aufsatz, den sie an diesem Mittwoch auf einer Fachtagung in Kalifornien präsentieren. Den Zugriff auf die Electronic Control Units verschafften sich die Forscher über den Port der so genannten On-Board-Diagnose, ein Fahrzeugdiagnosesystem.

Über ein selbst geschriebenes Programm gelang es ihnen dann, die Kommunikation der ECUs untereinander abzuhören und sie zu manipulieren. Das Spionageprogramm lief auf einem Laptop im Auto, auf das die Forscher drahtlos zugriffen. Auch deshalb ist ein Angriff unwahrscheinlich – schließlich müsste ein Hacker einen Computer in dem Auto unterbringen, das er manipulieren möchte. Wenn Autos aber in Zukunft mit internetfähigen ECUs ausgestattet werden, steigt die Gefahr entsprechend.

“Unsere Arbeit ist ein entscheidendes Stück in dem Puzzle und bietet die erste Studie, die auf der Basis von Experimenten die echten Sicherheitsrisiken eines modernen Autos aufzeigt”, schreibt das Wissenschaftler-Team, zum Abschluss seines Aufsatzes.