

IAA 2017: Wissenschaftler der Saar-Uni verhindern Hackerangriffe auf Autos

11.09.2017, 12:00 | Wissenschaft, Forschung, Bildung

Pressemitteilung von: *Universität des Saarlandes*

Presseagentur: *Universität des Saarlandes*



Dr. Stefan Nürnberger führt an seinem Demonstrator die Funktionsweise der Software VatiCAN vor. (Foto: Stephanie Bremerich (CISPA))

Über Mobilfunk sind heute viele Autos permanent mit dem Internet verbunden. Für Hacker bietet sich damit ein digitales Einfallstor, das zu verheerenden Szenarien führen kann. Angreifer könnten zum Beispiel über eine Sicherheitslücke in tausend baugleiche Fahrzeuge eindringen und bei allen zeitgleich auf die Bremse treten. Wissenschaftler des Kompetenzzentrums für IT-Sicherheit der Universität des Saarlandes (CISPA) haben daher eine Technik entwickelt, die solche Angriffe erkennen kann und direkt unschädlich macht. Mit der frei verfügbaren Software „vatiCAN“ können Autohersteller ihre Programme nachrüsten.

In einem Oberklassefahrzeug sind heute einige Dutzend Computer verbaut, von denen jeder einzelne die Rechenleistung einer Apollo-Rakete weit übersteigt. Diese Computer erleichtern der Werkstatt zum Beispiel die Fehlerdiagnose oder warnen den Fahrer vor einem folgenschweren Spurwechsel. „Die Rechner befolgen aber nur vorgegebene Steuerungsbefehle, ohne wie ein Mensch darüber nachzudenken. Wenn nun ein Fremder die Kommandohierarchie durcheinander bringt, können plötzlich unkontrollierte Steuerbefehle auf die Geräte im Auto einprasseln und das Fahrzeug abrupt abbremsen oder zum Schleudern bringen“, sagt Stefan Nürnberger, Leiter der Forschungsgruppe für Automotive Security am Kompetenzzentrum für IT-Sicherheit CISPA in Saarbrücken. Noch vor wenigen Jahren seien solche Szenarien so gut wie unmöglich gewesen, da sich Kriminelle erst physisch Zugang zum Fahrzeug verschaffen mussten, um dieses zu manipulieren.

„Heute haben immer mehr Fahrzeuge eine permanente Internetverbindung. Sie erlaubt es zum Beispiel, aktuelle Stauinformationen in die Routenplanung einzubeziehen oder die Standheizung aus der Ferne zu aktivieren. Enthalten solche internetfähigen Steuergeräte aber Sicherheitslücken, können Angreifer ihre Befehle an tausende Fahrzeuge schicken“, warnt der promovierte Informatiker. Zusammen mit Christian Rossow, Professor für IT-Sicherheit an der Universität des Saarlandes, arbeitet Nürnberger daran, dass Komponenten wie etwa ein Notbremsassistent jederzeit die Echtheit der an sie gerichteten Befehle überprüfen können. Die dafür entwickelte Software „vatiCAN“ sorgt dafür, dass

nur der echte Sender die notwendigen Authentifizierungs-codes an Nachrichten anhängen kann.

„Diese Codes werden zwischen den Steuergeräten des Fahrzeugs ständig neu ausgehandelt und können so einem Angreifer von außen nicht bekannt sein. Diejenigen Steuergeräte, die unsere Software verwenden, können so echte von gefälschten Nachrichten unterscheiden“, erläutert Nürnberger das Prinzip. Bei ihrer Sicherheitslösung war den Forschern wichtig, dass diese von den Autoherstellern einfach nachgerüstet werden kann. „Die Sprache, die Steuergeräte in einem Auto sprechen, wird durch ‚vatiCAN‘ nicht verändert. So lässt sich die Software nachträglich in bereits existierende Fahrzeuge integrieren, um sie gegen Angriffe zu schützen“, sagt der Saarbrücker Forscher. Da es eine Sisyphusaufgabe wäre, jede Sprache und jedes Protokoll für jede Marke und jedes Modell anzupassen, seien hier die Hersteller gefragt. Sie besäßen die notwendigen Informationen, um die Anti-Hack-Software leicht zu integrieren.

Auf der Internationalen Automobilausstellung (IAA) vom 14. bis 24. September in Frankfurt am Main simulieren die Saarbrücker Forscher an einem echten Fahrzeug einen Hackerangriff und zeigen, wie sich dieser mit Hilfe der Software abwenden lässt (Saarland-Stand, Halle 4.0, Stand A26).

Weiterführende technische Details:

Die vatiCAN Lösung verhindert darüber hinaus Angriffe, wie beispielsweise das Mitschneiden von authentifizierten Nachrichten, indem in jede Nachricht ein Zeitstempel einfließt. Ist er nicht aktuell, war die Nachricht aufgezeichnet und könnte gefährlich werden. „Durch diese zusätzlichen Berechnungen benötigt das Übertragen der Nachricht nur zwei Millisekunden mehr“, erklärt Nürnberger, der vatiCAN an einem VW Passat getestet hat. Dies sei auch für Steuervorgänge akzeptabel, bei denen es auf die unmittelbare Reaktion ankomme: „Verzögern sich Datenpakete um zwei Millisekunden, verlängert das bei einer Geschwindigkeit von 130 Kilometer pro Stunde den Bremsweg um gerade mal sieben Zentimeter“, so Nürnberger.

Ihr Verfahren haben die Forscher bereits auf einer internationalen Konferenz in Santa Barbara in Kalifornien vorgestellt. Die Software kann im Internet kostenlos heruntergeladen und verwendet werden.

www.automotive-security.net/vatican

Fragen beantwortet:

Dr. Stefan Nürnberger

Kompetenzzentrum für IT-Sicherheit (CISPA) der Universität des Saarlandes

Telefon: 0681 85775-4823

E-Mail: stefan.nuernberger@cispa.saarland

Hinweis für Hörfunk-Journalisten: Sie können Telefoninterviews in Studioqualität mit Wissenschaftlern der Universität des Saarlandes führen, über Rundfunk-Codec (IP-Verbindung mit Direktanwahl oder über ARD-Sternpunkt 106813020001). Interviewwünsche bitte an die Pressestelle (0681/302-3610).

Quelle: idw

Portrait

-

News-ID: 967921 • Views: 399 (Stand: 05.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/967921/IAA-2017-Wissenschaftler-der-Saar-Uni-verhindern-Hackerangriffe-auf-Autos.html>