idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Universität Luxemburg - Université du Luxembourg
Thomas Klein

23.11.2017
http://idw-online.de/de/news685212

Forschungsergebnisse, Kooperationen
Informationstechnik, Verkehr / Transport
überregional

Intel und Universität Luxemburg kooperieren, um selbstfahrende Autos sicherer zu machen

Mit der wachsenden Komplexität autonomer Fahrzeuge wird es immer schwieriger, sie vor Hackern zu schützen. Deshalb haben die Intel Corporation und das Interdisciplinary Centre for Security, Reliability and Trust (SnT) der Universität Luxemburg ein Partnerschaftsrahmenabkommen unterzeichnet. Die Zusammenarbeit soll solche Fahrzeuge sicherer machen, indem sie Angriffe automatisch neutralisieren und sich sogar selbst reparieren, bevor ein Angreifer die Möglichkeit hat, essenzielle Funktionen zu beeinträchtigen.

Das Abkommen wurde nach der bereits bestehenden Zusammenarbeit von SnT mit dem Intel Collaborative Research Institute for Collaborative Autonomous & Resilient Systems (ICRI-CARS) geschlossen. Die Arbeit wird von Wissenschaftlern der Critical and Extreme Security and Dependability Research Group (CritiX) des SnT durchgeführt. Die Forschung konzentriert sich insbesondere auf die Lösung von Problemen, die sich auf die IT-Sicherheit auswirken, die sich zum Beispiel aus der Notwendigkeit ergeben, dass selbstfahrende Autos miteinander „kollaborieren" müssen.

Es gibt bereits leistungsfähige Bordcomputer, die verschiedene Fahrfunktionen übernehmen können, wie z. B. das Einparken und Halten der Spur. Bei der Entwicklung hin zu komplett autonomen Autos müssen solche Fahrzeuge stärker zusammenarbeiten: Um ein sicheres Fahrverhalten zu gewährleisten, müssen die Autos Informationen über ihre Umgebung teilen, angefangen bei Baustellen und den Wetterverhältnissen bis hin zu Fußgängern, die die Fahrbahn betreten.

Leider machen komplexe Software und umfassende Konnektivität, die für ein solch kollaboratives autonomes Fahren notwendig sind, diese Systeme anfälliger für Angriffe. Hacker könnten beispielsweise Sensorgeräte oder die Kommunikation zwischen den Fahrzeugen beeinflussen, um die Kontrolle über mehrere Autos zu übernehmen und einen Rettungsweg zu blockieren oder um die Kontrolle über Polizei- oder Militärfahrzeuge zu übernehmen. Fahrkontrollsysteme könnten unter Umständen sogar gehackt werden, um Unfälle zu verursachen.

Mit den derzeit verfügbaren Methoden würde dies verhindert, indem sichergestellt wird, dass die Software der Systeme keine Fehler und Schwachstellen aufweist, die von Hackern ausgenutzt werden, aber das ist nicht mehr möglich: „In der Realität können wir nur versuchen, 15.000 Codezeilen in einer Software zu verifizieren – das entspricht 13 Experten, die ein Jahr lang rund um die Uhr arbeiten", so der Forscher Dr.-Ing. Marcus Völp. „Allein Windows 10 hat rund 50 Millionen Codezeilen, um ein Beispiel zu nennen. Wir müssen deshalb akzeptieren, dass Angreifer Schwachstellen finden und Autos hacken werden, was bedeutet, dass wir Systeme mit der Fähigkeit benötigen, in Echtzeit zu reagieren und sich wiederherzustellen, während sie angegriffen werden."

Die neuen Methoden, die derzeitig von CritiX entwickelt werden, sehen vor, dass jedes in einem Auto verwendete System – z. B. die für die Kraftstoffeinspritzung und Luftkalibrierung verantwortliche Motorsteuerung – aus mehreren unabhängigen Softwarekomponenten besteht und nicht nur aus einer. Dann müsste über ein Drittel dieser

Komponenten kompromittiert werden, damit ein Hacker das System manipulieren kann. Außerdem ist beim Ansatz von CritiX jede Komponente mit einem Labyrinth vergleichbar und um dieses zu kompromittieren, muss ein Hacker den Weg ins Zentrum dieses Labyrinths finden. Während dieses Prozesses werden sich jedoch sämtliche vorher kompromittierten Komponenten selbst heilen und wiederherstellen, sodass sich ein Hacker ständig mit einem Spektrum neuer Labyrinthe konfrontiert sähe.

„Das stellt nicht nur eine theoretische Herausforderung dar, sondern auch eine praktische“, so der Prof. Dr. Paulo Esteves-Veríssimo, Leiter von CritiX und FNR PEARL Chair. „Eines der größten Probleme in diesem Fall besteht darin, sicherzustellen, dass die Erneuerung in Echtzeit durchgeführt werden kann, ohne dass es zu einer Überhitzung kritischer Systeme kommt.“ Das Team muss ebenso garantieren, dass die verbleibenden Komponenten weiterhin funktionieren und sicher sind, während sich einzelne Komponenten erneuern.

Die Arbeit des Teams im Bereich des autonomen Fahrens hat bereits Früchte getragen – 2016 identifizierte das Paper der Gruppe "Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems" deutliche Lücken zwischen den ergriffenen Sicherheitsmaßnahmen zum Schutz der Passagiere und jenen
gegen absichtliche Manipulationen. Bei seinem derzeitigen Projekt entwickelt das Team die Methoden, Protokolle und Lösungen, die notwendig sind, um diese Lücke zu schließen, und arbeitet an der automatischen Widerstandsfähigkeit gegen Angriffe.

URL zur Pressemitteilung:
https://wwwen.uni.lu/university/news/latest_news/intel_joins_forces_with_snt_in_securing_autonomous_cars

Von links nach rechts: Dr. Marcus Völp, Dr. David Kozhaya, Prof. Paulo Esteves-Veríssimo