Angriff auf die Bordelektronik

TU-Forscher sorgen für Schutz vor Car Hacking

Wissenschaftler im Sonderforschungsbereich »CROSSING« arbeiten daran, moderne Autos mit ihrer umfangreichen elektronischen Ausstattung vor Hackerangriffen zu schützen.

Bild: Gregor Rynkowski

Forscht für sichere Autos: Professor Ahmad-Reza Sadeghi

Egal ob auf der Autobahn oder in der Innenstadt – für jeden Autofahrer ist es das Horrorszenario: Ein plötzliches Stauende, ein Kind rennt auf die Straße – und beim Tritt aufs Pedal versagen die Bremsen, das Auto kracht mit voller Wucht in das Hindernis. Neben technischen Defekten kommt in modernen Autos eine neue Ursache dafür infrage: Hacker haben das System des Autos angegriffen und die technisch funktionsfähigen Bremsen elektronisch deaktiviert.

Doch wie können Autos »gehackt« werden? Moderne Fahrzeuge verfügen über eine große Anzahl von Steuergeräten, auch Microcontroller genannt, die Nutzern mehr Komfort und Sicherheit bieten sollen: Sie steuern Bremsen, Reifendruck, Klimaanlage – sogar das Lenkrad kann durch den automatischen Einpark-Assistenten bewegt werden. Bekommt ein Hacker Zugriff darauf, kann er diese Funktionen von außerhalb steuern.

Im Sonderforschungsbereich CROSSING beschäftigt sich das Team um Professor Ahmad-Reza Sadeghi und Dr. Lucas Davi mit dem Sicherstellen der Vertrauenswürdigkeit (engl. »Attestation«) der Microcontroller sowie der aus ihnen gebildeten Netzwerke. »Das Problem ist, dass immer mehr intelligente Komponenten in Autos verbaut werden, und damit auch immer mehr Software«, erklärt Davi. Aus Erfahrung wisse man, dass Software immer zu einem kleinen Prozentsatz Fehler enthalte – die daraus entstehenden Lücken nutzen die Angreifer für ihre »Hacks« aus.

EINSATZ VON MICROCONTROLLERN STEIGT

Der Einsatz von Microcontrollern nimmt nicht nur in Autos ständig zu: »Im Internet der Dinge kommunizieren Tausende von Sensoren miteinander, Fitness-Tracker messen damit sensible persönliche Daten, auch in Flugzeugen und kritischen Infrastrukturen kommen diese winzigen Steuergeräte zum Einsatz«, zeigt Sadeghi weitere Anwendungsszenarien auf. Umso wichtiger sei es, dass Angreifer keinen Zugriff darauf bekommen.

Um das zu verhindern, forschen die Wissenschaftler daran, wie die Vertrauenswürdigkeit von Microcontrollern sichergestellt werden kann – also wie man erkennen kann, ob die kleinen Komponenten gehackt wurden, um dann entsprechende Gegenmaßnahmen einzuleiten. Sie setzen dabei auf »Attestation«, wörtlich übersetzt ist das eine »Beglaubigung«, dass die Komponente sicher und vertrauenswürdig ist. »Attestation überprüft die Zustandsintegrität eines Gerätes, also beispielsweise, ob Software oder sogar Hardware verändert wurde«, erklärt Sadeghi.

Ziel der Forscher ist es, Attestierungsprotokolle für Verbünde von Steuergeräten zu entwickeln, da sich die heutigen Verfahren auf einzelne, isolierte Geräte beschränken. Dies sei aber nicht mehr zeitgemäß, führt Sadeghi aus, denn in modernen Autos seien die Steuergeräte miteinander und oft auch mit dem Internet vernetzt. Bekommt ein Angreifer Zugriff auf eines davon, kann er oft auch andere Komponenten im System unter seine Kontrolle bringen – er hackt sich quasi vom Multimediasystem oder der Klimaanlagenautomatik ins intelligente Türschloss oder in die Bremssteuerung.

SICHERHEIT WÄHREND DES BETRIEBS

Außerdem sollen die Attestierungsverfahren dynamischer werden: »Heutige, also statische Attestation kann nur gewisse Konfigurationen messen, also überprüfen, ob eine Software auf dem Gerät richtig geladen wurde«, wichtig sei aber auch zu validieren, wie die Software sich während des Betriebs, zur sogenannten Laufzeit (engl. »Runtime«) verhält, so Davi. Denn hier nutzen Angreifer besonders oft Schwachstellen aus.

Die CROSSING-Forscher haben bereits gemeinsam mit dem Prozessorhersteller Intel eine Sicherheitsarchitektur für eingebettete Geräte entwickelt, die viele dieser Anforderungen erfüllt. TyTAN stellt einen sogenannten Trust Anchor (dt. »Vertrauensanker«) zur Verfügung, »quasi einen Microcontroller auf dem Microcontroller, der eine zusätzliche Kontroll- und Vertrauensinstanz ist. Er härtet die Komponente gegen Angriffe ab«, erklärt Davi. Im Moment proben die Wissenschaftler den Ernstfall noch mit einem Modellauto. In Zusammenarbeit mit Industriepartnern wie Intel und BMW sollen die Lösungen aber bald in die Praxis überführt werden.

SONDERFORSCHUNGSBEREICH CROSSING

Mehr als 65 Wissenschaftlerinnen und Wissenschaftler aus den Forschungsbereichen Kryptografie, Quantenphysik, Systemsicherheit und Softwaretechnik an der TU Darmstadt arbeiten in CROSSING zusammen und betreiben sowohl Grundlagen- als auch anwendungsorientierte Forschung. Das Ziel von CROSSING ist es, kryptografiebasierte Sicherheitslösungen zu entwickeln, um auch in Zukunft sichere und vertrauenswürdige Rechenumgebungen zu schaffen. Neben hohen Ansprüchen an die Effizienz und Sicherheit der entwickelten Lösungen spielt auch die »Usability« – also die Benutzbarkeit – eine große Rolle: Softwareentwickler, Administratoren und sogar Endanwender sollen in der Lage sein, die Lösungen zu verwenden, auch wenn sie keine Kryptografieexperten sind.

CROSSING wird seit Oktober 2014 als Sonderforschungsbereich der Deutschen Forschungsgemeinschaft (DFG) mit acht Millionen Euro gefördert. Das Programm ist auf bis zu zwölf Jahre ausgelegt.