OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

FORSCHUNGSBERICHT 2016, OTH REGENSBURG

AUTOREN MIT EINRICHTUNG

Nils Weiß, OTH Regensburg

Matthias Segerer, OTH Regensburg

Prof. Dr. Rudolf Hackenberg, OTH Regensburg

TITEL

CARSEC - Sicherheitsuntersuchung an vernetzten Fahrzeugen

ABSTRACT

Autos und Computer. Die Verschmelzung dieser beiden Welten hat bereits vor Jahrzehnten begonnen. Verkaufsargumente wie exklusive Ausstattung oder hohe Motorleistung werden zunehmend von Themen aus der Computerwelt verdrängt. Automobilhersteller wetteifern um die besten Connected Diensten, Smartphone-Apps und Cloud-Anbindungen. Nicht zuletzt hat der Abgasskandal gezeigt, welche Auswirkungen moderne Software auf das Herzstück des Autos haben kann.
Durch die fortschreitende Vernetzung von Fahrzeugen mit dem Internet ergeben sich komplett neuartige Gefahren und Bedrohungen für die IT- Sicherheit. In einem initialen Forschungsprojekt unter Leitung von Prof. Dr. Hackenberg wurde ein vernetztes Fahrzeug auf Angriffsflächen und mögliche Schwachstellen hin untersucht. Durch die Betrachtung des Gesamtsystems aus Fahrzeug, Smartphone, Webservern, Werkstatttestern und vielen weiteren Komponenten konnte eine Risikoanalyse für verschiede Angriffsszenarien erstellt werden. Diese Forschungsarbeit legt den Grundstein für weitere Forschungsprojekte, zum Thema IT-Security im vernetzen Fahrzeug, an der OTH Regensburg.

BERICHT

Neue Gefahren durch neue Features.

Die Automatisierung immer komplexer werdender Aufgaben wie Spurhalte- oder Notbremsassistenten erfordert fahrzeugintern eine immer bessere Vernetzung vormals eigenständiger Systeme. Diese Kommunikation erfolgt über sogenannte Boardnetze[1], welchen jedoch in vielen vorangegangenen Studien bereits Schwachstellen nachgewiesen werden konnten[2]. Mit dem Trend zur Vernetzung der Fahrzeuge mit externen Geräten oder dem Internet vor allem im Bereich des Infotainments, eröffnen sich gleichzeitig immer mehr Möglichkeiten diese Schwachstellen auch über externe Kanäle ausnutzen zu können. Dadurch könnten Angriffe auf die Computersysteme eines vernetzten Fahrzeugs den Komfort, das Eigentum aber auch die Sicherheit der Passagiere sowie wirtschaftliche Interessen der Fahrzeughersteller gefährdet werden. Datendiebstahl, Blockierung von Komfortdiensten im Fahrzeug aber auch wesentlich tiefgreifendere Bedrohungen wie die Übernahme und Fernsteuerung eines Fahrzeugs sind dabei denkbar. Dabei können Angriffe sowohl an der Außenhaut des Fahrzeugs, als auch entfernt und damit wesentlich anonymer über das Internet erfolgen, wodurch viele Angriffsszenarien auch als hochskalierbar betrachtet werden müssen. Dies wiederum stellt in vielerlei Hinsicht auch eine Gefährdung der wirtschaftlichen Interessen der Fahrzeughersteller im Allgemeinen dar, nicht zuletzt da auch Erpressungsversuche sowie die unberechtigte Funktionalitätserweiterung durch Neukalibration der Fahrzeuge nicht ausgeschlossen werden können.[3]

Praktische Sicherheitsuntersuchungen – Hacken im Namen der Wissenschaft.

Grau ist alle Theorie. Dies gilt gerade für Sicherheitsuntersuchungen. Um Bedrohungen und Sicherheitslücken realistisch einschätzen zu können, damit daraus abstrahierte Sicherheitsmodelle für strategische Entscheidungen erstellt werden können, ist die genaue Kenntnis eines Systems unerlässlich. Im Rahmen dieses Forschungsprojekts wurden alle sicherheitsrelevanten Komponenten wie externe Schnittstellen, Bootloader oder Bussysteme eines Fahrzeugs praktisch untersucht, um so Kenntnisse über die Angreifbarkeit eines

Teilsystems im Fahrzeug zu erlangen. Für einen kompletten Angriff, müssen in einem Fahrzeug grundsätzlich immer mehrere Komponenten angegriffen werden. Mit jeder zusätzlichen Komponente steigt jedoch die Komplexität eines Angriffs exponentiell an, wo durch ein vollständiger Angriff eines Fahrzeugs im Rahmen einer Sicherheitsuntersuchung in der Regel zu kostenintensiv und somit zu unwirtschaftlich wäre. Durch das gezielte Untersuchen einzelner Komponenten wird somit viel Aufwand gespart. Grundsätzlich hängt die Sicherheit eines Fahrzeugs von dem schwächsten Glied der Kette ab. Dieses gilt es zu identifizieren und zu bewerten. Betrachtete externe Schnittstellen waren in diesem Projekt beispielsweise GSM, Bluetooth, WLAN, Smartphone Apps, interne Webbrowser und die OBD-2 Schnittstelle[4]. Im Fahrzeug wurden Bussysteme wie CAN, FlexRay und Ethernet untersucht. Damit die mögliche Infektion eines Fahrzeugs abgeschätzt werden konnte, mussten im dritten Schritt noch Bootloader und Update-Mechanismen einzelner Steuergeräte betrachtet werden. Durch die Resultate der praktischen Untersuchung lassen sich realistische Abschätzungen für die Bedrohungen von einzelnen Komponenten erstellen, die dann, modelliert zu einem abstrahierten Sicherheitsmodell, ein Maß für die Bedrohung des gesamten Fahrzeugs angeben.

[BILD 1]

Theoretisch Analyse – Von der Praxis zum Sicherheitsmodel.

Die Sicherheit einer Komponente wurde in dieser Untersuchung (in Anlehnung an ISO 18045:2008) unter anderem dadurch abgeschätzt, wieviel Zeit das Aufspüren einer Schwachstelle sowie die eigentliche Durchführung des Angriffs am Objekt benötigen würde. Auch die spezifischen Systemkenntnisse und generell nötiges Fachwissen um eine Schwachstelle aufzuspüren und ausnutzen zu können wurden ebenso berücksichtigt wie das für die Angriffe notwendige Spezialequipment (Hard- oder Software). Um zudem auch den Abhängigkeiten der einzelnen potentiellen Angriffsvektoren untereinander sowie verschiedenen bewusst oder unbewusst handelnden Tätern Rechnung zu tragen, erfolgte die Bedrohungsmodellierung als Graph.

[BILD 2]

Ausblick

In Zusammenarbeit mit Industriepartnern wird das Forschungsprojekt “CARSEC” an der OTH Regensburg weitergeführt. Im Fokus der nächsten Jahre stehen weitere praktische Untersuchungen, die Entwicklung automatisierter Sicherheitstests für Fahrzeuge sowie die Verbesserung allgemeiner Bedrohungsmodelle um Risiken besser kategorisieren zu können. Hierzu müssen weitere Angriffsvektoren identifiziert und untersucht werden. Durch den Ausbau von Kompetenzen im Bereich Webtechnologien und Penetration-Testing wird ein weiterer Themenschwerpunkt durch die Forschungsgruppe „CARSEC“ abgedeckt werden. Gegen Ende des Forschungsprojektes sollen aus den gewonnenen Erkenntnissen ganzheitliche Lösungsansätze für die Industrie entwickelt werden.

WEITERE INFORMATIONEN

LITERATUR

[1] Zimmermann, Prof. Dr.-Ing. W. ; Schmidgall, Dr. R.: *Bussysteme in der Fahrzeugtechnik*. 5. Springer Vieweg, 2014

[2] Evenchick, Eric: *An Introduction to the CANard Toolkit*. Black Hat Conference Asia, 2015

[3] Szijj, András; Buttyán, Levente ; Szalay, Zsolt: *Hacking cars in the style of Stuxnet*. http://www.hit.bme.hu/ buttyan/publications/carhacking-Hacktivity- 2015.pdf, Oktober 2015

OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

[4] Miller, Dr. C. ; Valasek, Chris: *A Survey of Remote Automotive Attack Surfaces*. DEF CON 22 Hacking Conference. Las Vegas, NV: DEF CON, August 2014

KONTAKTKASTEN

Projektleitung:
Prof. Dr. Rudolf Hackenberg +49 941 943 1264
Laboratory for Safe and Secure Systems (LaS^3)
Rudolf.Hackenberg@oth-regensburg.de

Projektmitarbeiter:
1 Doktorand und 2 Forschungs-Master-Studierende

BILD-, GRAFIKUNTERSCHRIFTEN, TABELLENÜBERSCHRIFTEN (INSG. MAX. 2)

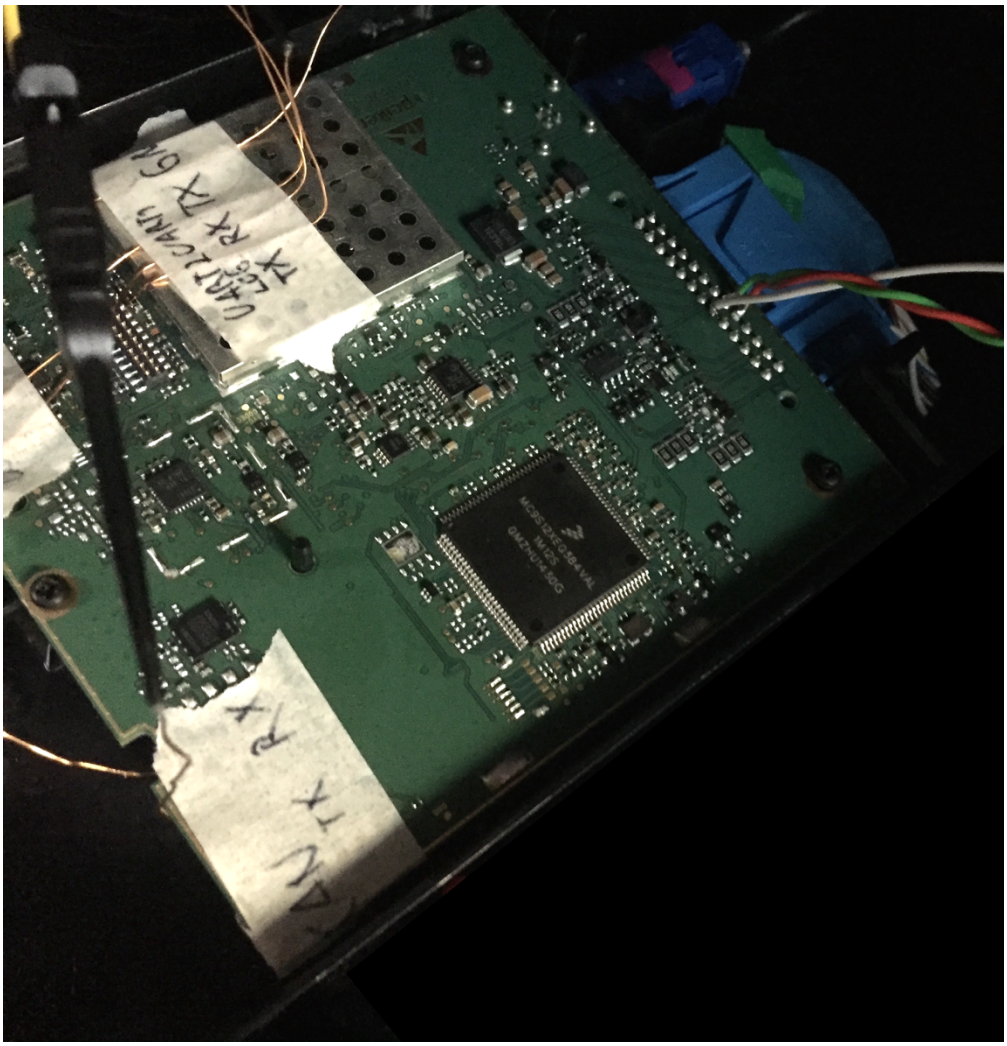

Bild 1: Steuergerät während einer Sicherheitsuntersuchung

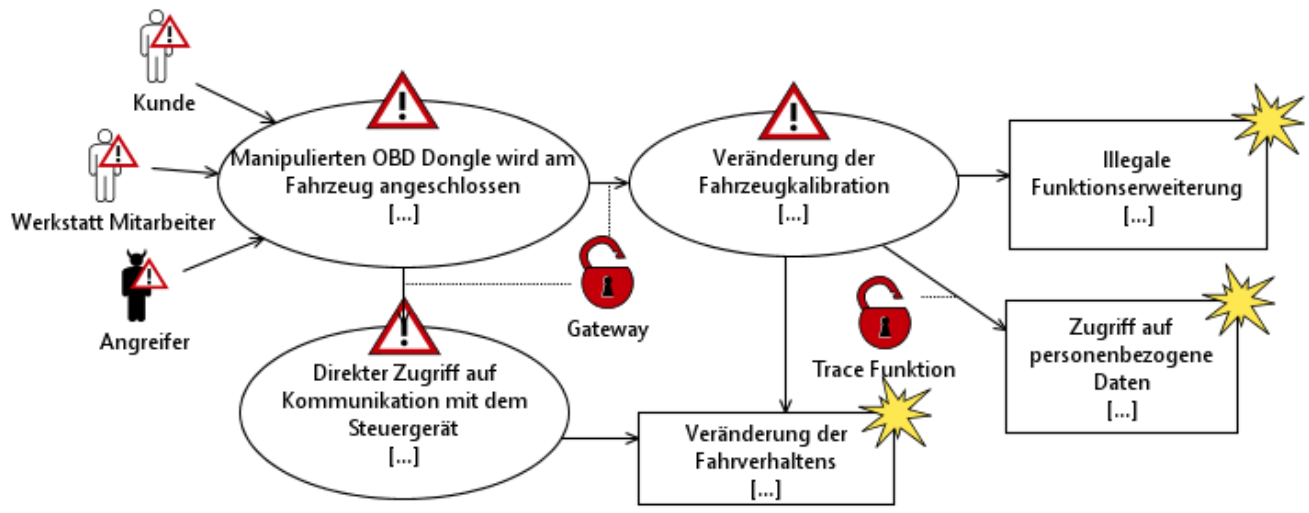

Bild 2: Ausschnitt aus dem Bedrohungsmodell in der CORAS UML Notation

Anzahl der verwendeten Zeichen für Abstract, Bericht, Zusammenfassung, Literatur und Kontaktkasten