

Achtung: Malware voraus

Eine Analyse zukünftiger Gefahren für Fahrzeugsicherheitssysteme





Achtung: Malware voraus

INHALT

Einführung	3
In Fahrzeugen integrierte Geräte	4
Hackerangriffe auf Autos	6
Infotainment- und Netzwerksysteme	8
Neue Verkehrsregeln	9
Beitragende	10



Einführung

Der Komfort, den wir tagtäglich genießen, basiert auf modernsten Technologien. Computer-Chips spielen in allen Bereichen unseres täglichen Lebens eine wichtige Rolle. Sie sorgen dafür, dass wir jederzeit und überall auf verschiedenste Informationen zugreifen können. Dank Internetprotokollen können einstmals „stumme“ Geräte auf noch nie dagewesene Weise mit uns und miteinander kommunizieren.

Ericsson rechnet für das Jahr 2020 mit 50 Milliarden internetfähigen Geräten – ein gewaltiger Sprung im Vergleich zu 1 Milliarde im Jahr 2010. Dabei handelt es sich jedoch nicht nur um die Geräte, die wir bewusst jeden Tag einsetzen. Vielmehr wird der größte Teil von ihnen eingebettet sein, z. B. in spezialisierten Geräten wie Kassenterminals, Check-In-Kiosk-Systemen in Flughäfen, medizinischen Geräten, Zugangskartenlesern, Produktionsmaschinen, programmierbaren Logik-Controllern, Industrieleitsystemen sowie unzähligen anderen Geräten, die neuerdings Internetanschluss erhalten. Die bisherigen Erfahrungen zeigen dabei aber, dass die meisten Hersteller die Sicherheit vernachlässigen, obwohl in diesen Geräten von Anfang an Sicherheits- und Verwaltungsfunktionen implementiert sein müssten.

Ursprünglich verlief der Informationsfluss der eingebetteten Geräte vor allem in eine Richtung. Daten wurden zur reinen Diagnose vom Gerät gesendet, was fast immer nur im Notfall geschah. Eine reguläre Datenübertragung war nicht vorgesehen. Zudem hatten diese Geräte nur geringen Einfluss auf unser Leben. Heute werden sie jedoch mit Richtlinien und Tasks „gefüttert“ – und sie geben ihre Daten an eine zentrale Konsole zurück. Ohne eingebettete Geräte ist der Komfort bei Fahrzeugelektronik, Haushaltsgeräten, Wasser- und Energieversorgung sowie ähnlichen Systemen nicht denkbar. Durch dieses Phänomen hat das Bedrohungspotenzial für diese Geräte rapide zugenommen. Aus diesem Grund sind Sicherheitstechnologien wie Whitelists und Konfigurationskontrollen in Kombination mit weltweiten Bedrohungsanalysen anhand der Daten von Millionen Knoten nicht mehr nur eine Option, sondern eine Notwendigkeit. Diese Lösungen stellen den ersten Schritt zum umfassenden Schutz eingebetteter Systeme dar.

Wenn eingebettete Geräte Netzwerkzugang erhalten, müssen Sicherheitsadministratoren wissen, ob diese Systeme angemessen geschützt sind. Dabei wollen sie die Richtlinien für diese Geräte über dieselbe Konsole steuern, mit der sie auch alle anderen Computer kontrollieren.

Wir bei McAfee engagieren uns für den Schutz eingebetteter Geräte – unabhängig davon, ob es sich dabei um PCs handelt. Daher arbeiten wir mit Wind River und Experten verschiedener Bereiche zusammen, um die Sicherheit eingebetteter Systeme zu analysieren und branchenspezifische Empfehlungen für den Schutz dieser Geräte sowie von Kunden und der breiten Öffentlichkeit zu entwickeln. Dieser Bericht konzentriert sich auf eingebettete Systeme in Fahrzeugen und stellt den Beginn einer Reihe über die Sicherheit eingebetteter Geräte dar. Wir hoffen, dass diese Informationen für Sie nützlich sind.

Stuart McClure
*Senior Vice President
und General Manager
McAfee*



In Fahrzeugen integrierte Geräte

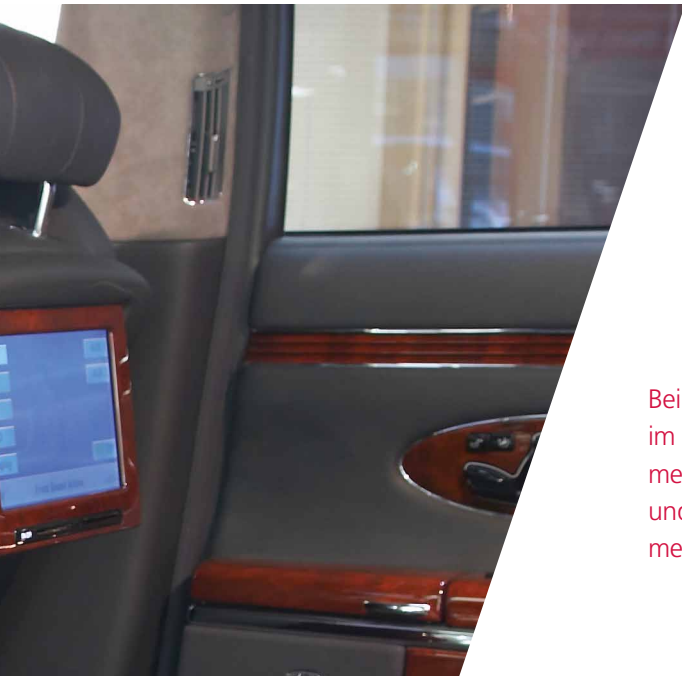
Die Automobilindustrie stattet ihre Modelle mit immer mehr Funktionen aus, die für mehr Komfort sorgen und das Autofahren individueller machen sollen. Die Kunden von heute möchten selbst in ihren Autos dauerhaft mit dem Internet verbunden sein. Aus diesem Grund verbessern die Fahrzeugbauer die Anschlussmöglichkeiten für personalisierte Geräte wie Smartphones und Tablets.

Moderne Autos können per Fernsteuerung über das Mobilgerät gestartet werden. Dazu wird eine Verbindung zwischen dem Fahrzeug und dem Mobilfunkbetreiber oder Internet hergestellt, über die der Schlüsselinhaber eine entsprechende Anforderung sendet. Das ist nur ein Beispiel dafür, wie viel Computertechnik inzwischen im Motorraum und hinter dem Armaturenbrett steckt. Mit zunehmender Beliebtheit dieser persönlichen Systeme mit Internetanschluss steigt jedoch auch die Bedeutung der Absicherung.

Komfort wurde bisher durch Funktionen wie separate Klimaregelung für Fahrer und Beifahrer, beheizte Sitze oder das Vorhandensein ausreichender Getränkehalter definiert. Heute zählen neben gutem

Design auch spezielle eingebettete Technologien dazu. Personalisierte Systeme wie Bluetooth, GPS-Navigation, Fahrzeug-Infotainment und Online-Hilfe gehören mittlerweile bei vielen Fahrzeugmodellen zur Grundausstattung. Bei Fahrzeugwerbung steht Elektronik im Vordergrund, und der Trend zu immer mehr eingebetteten Mikrocontrollern und Kommunikationsfunktionen ist nicht mehr aufzuhalten.

Diese eingebetteten Geräte werden in fast allen Fahrzeug-Subsystemen eingesetzt, darunter Airbags, Radio, elektronische Sitzverstellung, ABS, ESP, Tempomat, Kommunikationssysteme und fahrzeuginterne Kommunikation.



Bei Fahrzeugwerbung steht Elektronik im Vordergrund, und der Trend zu immer mehr eingebetteten Mikrocontrollern und Kommunikationsfunktionen ist nicht mehr aufzuhalten.



Viele Autobauer bieten mobilfunkbasierte Kommunikation an, z. B. OnStar von GM, SYNC von Ford, Assist von BMW, Enform von Lexus, Safety Connect von Toyota und mbrace von Mercedes. Einige Fahrzeughersteller integrieren außerdem Wi-Fi-Hotspots in ihre Fahrzeuge und ermöglichen damit Internetzugriff für die Geräte der Insassen.

Interessant dabei: Viele dieser eingebetteten Systeme können auch untereinander kommunizieren und bieten dadurch noch mehr Anpassungsmöglichkeiten. Einige Beispiele:

- Durch Entsperrten des Fahrzeugs mit einem bestimmten Remote-Schlüssel werden automatisch der Sitz und die Spiegel an den jeweiligen Fahrer angepasst.
- Mit zunehmender Geschwindigkeit wird automatisch die Lautstärke des Audiosystems erhöht, um die Tonqualität für die Fahrzeuginsassen gleichbleibend zu halten.
- Je nach Fahrer kann eine Höchstgeschwindigkeit festgelegt werden, um Geschwindigkeitsüberschreitungen zu verhindern.

Autohersteller führen gegenwärtig mutige Experimente durch, beispielsweise von Google per Autopilot gesteuerte Fahrzeuge sowie intelligente Straßen, die Daten zu Verkehrsbedingungen und Fahrzeuggeschwindigkeiten weitergeben. Solche Versuche zeigen, welche Möglichkeiten sich durch die koordinierte und vernetzte Kommunikation verschiedenster Fahrzeugsysteme ergeben.

Die große Sorge besteht allerdings darin, dass sich zwar die Technologien weiterentwickelt haben, jedoch wenig für die Sicherheit dieser Systeme getan wurde. Die ersten Zentralverriegelungssysteme mit Fernbedienung verfügten über keinerlei Sicherheitsfunktionen und konnten ganz einfach kompromittiert werden, da eine gewöhnliche universell einsetzbare Fernbedienung für Heimergeräte das Schlüsselsignal aufzeichnen und zu einem späteren Zeitpunkt wiedergeben konnte. Bereits in den frühen 1980er Jahren war Fahrzeugsicherheit ein Problem. Damals erreichten Autodiebstähle Rekordwerte, da die Zündung ganz einfach durch Kurzschließen der Elektronik gestartet werden konnte. In den späten 1980er Jahren wurden Verschlüsselungsmechanismen eingeführt, die solche Angriffe verhinderten.



Hackerangriffe auf Autos

Je mehr Fahrzeuge mit digitalen Technologien ausgestattet werden, desto stärker wächst die Bedrohung durch böswillige Manipulationen der Soft- und Hardware. Es gibt viele Beispiele für wissenschaftlich motivierte Angriffe, die das Gefahrenpotenzial und den Umfang möglicher Kompromittierungen der Verbraucher verdeutlichen.

Im vergangenen Jahr zeigten Forscher der University of California in San Diego sowie der University of Washington, dass wichtige Fahrzeugsicherheitskomponenten gehackt werden können, wenn der Angreifer physischen Zugang zu den elektronischen Komponenten im Fahrgastraum erhält. Für den Einsatz der „CarShark“ genannten Proof-of-Concept-Software waren lediglich selbst geschriebener Code sowie ein Standardcomputeranschluss erforderlich. Die Wissenschaftler hatten Möglichkeiten gefunden, ein modernes Auto mit einem Laptop zu hacken. Das gleiche Forschungsteam erweiterte vor kurzem den Versuch auf Fernangriffe per Bluetooth. Dies zeigt, dass eingebettete Systeme in Autos und elektronische Geräte wie Mobiltelefone sowie GPS- und Bluetooth-Funktionen besser abgesichert werden müssen.

Eine weitere Angriffsmethode stellten Forscher der University of South Carolina und der Rutgers University vor. Moderne Fahrzeuge sind in den USA standardmäßig mit Reifendruck-Überwachungssystemen ausgestattet. RFID-Tags (Radio Frequency Identification) in den Reifen liefern über Nahdistanz-

kommunikation Sensordaten an das Fahrzeug. Die Forscher zeigten, dass Fahrzeuge mithilfe von reichweitengesteigerten Lesegeräte bis zu einer Entfernung von etwa 40 Metern anhand der RFID-Tags überwacht und die Privatsphäre der Fahrzeuginsassen kompromittiert werden können. Bislang ist noch keine aktive Ausnutzung bekannt. Gleichzeitig ist offen, ob und in welchem Ausmaß die Privatsphäre der Insassen bei einer solchen Überwachung gefährdet ist. Daher darf dieses Problem nicht auf die leichte Schulter genommen werden.

Der nächste Schritt besteht darin, den CarShark-Angriff mit den Schwachstellen der Bluetooth-Implementierung in Autos zu kombinieren. Sobald der Angreifer die Bluetooth-PIN kennt, kann er den CarShark-Angriff starten. In einem solchen Fall können auch andere drahtlose webbasierte Fahrzeugsperresysteme das Auto aus der Ferne lahmlegen. Solche Sperrsysteme sollen eigentlich Autodiebstahl verhindern, können jedoch für böswillige Zwecke missbraucht werden und die Fahrzeuge nichtsahrender Benutzer blockieren.¹

¹ <http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html>



„Die große aber unvermeidbare Herausforderung besteht darin, Fahrzeugsysteme sicherer als vergleichbare Internetdienste zu machen. Die Fahrzeughersteller werden die Entwicklungszyklen der Fahrzeugsicherheitssysteme an die der allgemeinen IT-Sicherheit anpassen müssen.“

– Winfried Stephan, Senior Consultant
T-Systems ICT Security Consulting and Engineering

Vor einiger Zeit wurden in Texas (USA) 100 Fahrzeuge mithilfe eines Fernsperrsystems blockiert.² Das vom Autohändler installierte System war von einem verärgerten ehemaligen Mitarbeiter manipuliert worden, der die Autos aus der Ferne gesperrt und die Hupen ausgelöst hatte.

Sicherheitsbedenken betreffen ebenso werksseitig in Autos eingebettete Systeme wie Lösungen von Drittanbietern. Im April dieses Jahres wurde bekannt, dass ein Anbieter von GPS-Navigationssystemen das Fahrverhalten seiner Benutzer aufzeichnete und diese Daten an die niederländische Polizei verkaufte, die daraufhin an Stellen mit häufiger Geschwindigkeitsüberschreitung Radarkameras installierte.³

Neue Tools wie Viper Smart Security nutzen das Internet, damit Fahrzeughalter den Standort ihres Fahrzeugs überwachen können. Zudem besitzen sie eine Facebook-Funktion, mit der Aktivitäten des Autos sofort gemeldet werden. Diese Informationen können leicht dazu genutzt werden, den Aufenthaltsort sowie typische Tagesabläufe des Fahrzeugführers zu ermitteln. Die Sicherheitsprobleme beziehen sich hierbei nicht auf das Fahrzeug. Vielmehr wird durch die Kombination von Überwachung und Social-Media-Techniken die Privatsphäre des Kunden in Frage gestellt. Die über Facebook-Aktualisierungen erfassten Daten könnten verkauft oder für andere böswillige Aktionen gegen den Fahrzeugführer genutzt werden.

Sicherheitstests und „gutwillige“ Hacker zeigen potenzielle Bedrohungsvektoren und Ausnutzungsmöglichkeiten auf. Ein im Auftrag einer US Gemeindeverwaltung tätiger Sicherheitsexperte stellte fest, dass mehrere IP-Adressen, die von der städtischen Polizeibehörde verwendet wurden, direkt mit einem Linux-Gerät an Board der Streifenwagen verbunden waren. Mithilfe von FTP- und Telnet-Befehlen konnte er auf die Audio- und Videodaten des digitalen Videorekorders zugreifen, der die Daten der im Streifenwagen installierten Kamera aufzeichnet und überträgt. Auf diese Weise konnte er nicht nur Live-Übertragungen aus beiden im Fahrzeug montierten Kameras erfassen, sondern hätte auch die Festplatte des Videorekorders manipulieren können.

Mit den Standardkennwörtern, die fest im FTP-Server des Videorekorders eingestellt waren und im online frei verfügbaren Support-Handbuch genannt werden, konnte er problemlos Dateien hoch- und herunterladen sowie löschen, die über Monate hinweg gespeichert worden waren.⁴ Dies hätte durch einfache Sicherheitsmaßnahmen verhindert werden können. Der erste Fehler bestand darin, dass das für das Eindringen in das Aufzeichnungssystem erforderliche Wissen verfügbar war. Aber erst dadurch, dass keine einmaligen starken Kennwörter festgelegt wurden, konnten wertvolle Beweisdaten manipuliert und gelöscht werden.

² http://www.pcworld.com/article/191856/employee_wreaks_havoc_on_100_cars_wirelessly.html

³ <http://www.npr.org/blogs/thetwo-way/2011/04/28/135809709/dutch-police-used-tomtoms-gps-data-to-target-speeders?sc=17&f=1019>

⁴ http://www.theregister.co.uk/2011/05/03/cop_car_hacking

„Fahrzeuge aller Preissegmente sind mit verschiedenen elektronischen Systemen ausgestattet, die in naher Zukunft über erheblich höhere Rechenleistung sowie verbesserte Schnittstellen verfügen werden. Jede Schnittstelle ist dabei eine weitere Motivation sowie ein Mittel für Angreifer, auf das Fahrzeug zuzugreifen. Wir müssen beim Schutz der Schnittstellen in Autos eingebetteter Systeme mit neuen Herausforderungen rechnen. Die Fahrzeughersteller müssen daher den Konflikt lösen, der sich durch die Implementierung von Sicherheitsmaßnahmen einerseits und die Kundenakzeptanz andererseits ergibt. Ich rechne damit, dass das Thema Sicherheit in zwei Autogenerationen eine völlig neue Rolle spielen wird.“

– Prof. Dr. Stefan Goß, Professor für Fahrzeugtechnik,
Ostfalia Hochschule für angewandte Wissenschaften



Infotainment- und Netzwerksysteme

Das Infotainment-System ist für Angreifer besonders interessant, da es häufig sehr eng mit dem persönlichen Leben und den Daten des Fahrzeugführers verbunden ist. Der Zugriff auf die richtigen Daten zum richtigen Zeitpunkt kann viel Geld einbringen. Im Gegensatz zu den anderen eingebetteten Fahrzeugsystemen, die meist mit proprietärer oder spezialisierter Software ausgestattet sind, verwenden eingebettete Geräte von Infotainment-Systemen häufig Standard-Software.

App Stores, Internetzugriff oder drahtlos verbundene persönliche Geräte ermöglichen den unabsichtlichen Download von Malware auf das Infotainment-System des Fahrzeugs. Weltweit eingesetzte Software-Plattformen für Fahrzeug-Infotainment-Systeme sowie Standards wie GENIVI⁵ vereinheitlichen die Architekturen und gewährleisten dadurch bessere Kompatibilität und Integration. Gleichzeitig wächst bei allgemein befolgten Software-Standards der Bedarf nach Schutz vor Angriffen und Manipulation. Schon bei der Entwicklung von Infotainment-Systemen und Mobilfunknetzwerken muss die Sicherheit berücksichtigt und implementiert werden.

Der zunehmende Einsatz eingebetteter Systeme und der immer umfangreichere Code, mit denen die Anforderungen der Verbraucher an diese Systeme erfüllt werden, zwingt die Hersteller zur Entwicklung eines Modells, das die schnelle Aktualisierung und Bereitstellung von Premium-Funktionen ermöglicht.

Laut Frost and Sullivan werden zum Betrieb von Autos in naher Zukunft 200 bis 300 Millionen Zeilen Software-Code erforderlich sein. Die zunehmende Funktionsvielfalt und Verknüpfung mit anderen eingebetteten Systemen sowie die Mobil- oder Internetverbindungen können sich als Einfallstor für ausnutzbare Sicherheitslücken erweisen.

Ein Artikel der *San Jose Mercury News* vom Juni 2011 befasste sich mit den zahlreichen Bereichen, mit denen Autohersteller Elektronik zur Steigerung von Komfort und Sicherheit sowie als Wettbewerbsvorteil einsetzen. Neben Luxuswagen von Premium-Herstellern wie BMW und dem Elektroauto Tesla werden zunehmend auch preiswerte Autos wie die von Ford mit Internetfunktionen ausgestattet, um den Fahrer zu informieren, zu unterhalten und zu schützen.

⁵ <http://www.genivi.org/>



„Sicherheit wird schon bald zur Schlüsseltechnologie für fast alle Innovationen in Autos. Die meisten Verbraucher würden böswillige Software eher auf ihrem Laptop als im Bremssystem ihres Autos akzeptieren. Daher stellt die Integration starker Sicherheitslösungen einen Wettbewerbsvorteil für den Hersteller dar.“

– Prof. Dr.-Ing. Christof Paar, Ruhr-Universität Bochum und University of Massachusetts in Amherst (USA)

Fragen von Verbrauchern

- Welche Systeme sind mit dem Internet oder Mobilfunknetz verbunden, und wie sind sie gesichert?
- Sind Navigationssysteme, GPS sowie wichtige Elektroniksysteme des Autos miteinander verbunden?
- Wie ist das Bluetooth-System abgesichert?
- Wie viele Daten werden an die GPS-Komponente übertragen, und werden sie irgendwo gespeichert?
- Besitzt das System Diagnosemöglichkeiten, um Manipulationen aufzudecken?
- Gibt es einen lokalen Speicher, der Informationen aus meinen „intelligenten“ Geräten speichert oder abrufft?
- Kann ich beim Weiterverkauf des Autos die integrierten Infotainment- und Kommunikationssysteme auf die Werkseinstellungen zurücksetzen, um sicherzustellen, dass meine persönlichen Einstellungen und Daten nicht mehr abrufbar sind?
- Welche Gewährleistung übernehmen der Hersteller oder der Mobilfunkanbieter, falls die gesicherte Kommunikation kompromittiert wurde?

Neue Verkehrsregeln

Die Zukunft ist näher als wir annehmen möchten. Im Juni 2011 wies der US-Bundesstaat Nevada die zuständigen Mitarbeiter des Kraftfahrzeugamts an, Straßenverkehrsregeln für autonome (selbstfahrende) Fahrzeuge auszuarbeiten.⁶ Stellen Sie sich vor, Sie steigen in einer Großstadt in ein Taxi, bei dem kein Fahrer am Lenkrad sitzt, sondern ein Computer. Dies könnte der erste Schritt zu autonomen Fahrzeugen auf öffentlichen Straßen werden.

Die Zeiten, in denen bewegliche Teile ausschließlich mechanisch waren, sind längst vorbei. Wir sind im Zeitalter von Computer-Chips und Systemen angekommen, die modernen Fahrzeugen höhere Effizienz verleihen. Abseits der reinen Motorleistung bietet die wachsende Anzahl eingebetteter Systeme und integrierter Kommunikationstechnologien in modernen Autos den Komfort und die Anpassungsmöglichkeiten, die von Autokäufern gewünscht werden. Doch werden diese Systeme in 10 Jahren immer noch das Vertrauen der Verbraucher genießen oder als Einfallstor für Malware und die Kompromittierung der Privatsphäre dienen?

⁶ http://www.computerworld.com/s/article/9217967/Nevada_paves_way_to_getting_robotic_cars_on_the_road

Beitragende

Stuart McClure, Senior Vice President und General Manager, McAfee

Stuart McClure betreut die McAfee-Produktlinie des Geschäftsbereichs Risk and Compliance und ist dabei für Vertrieb, Entwicklung, Produkt-Management, Produkt-Marketing, Strategie, Qualitätssicherung und Kunden-Support verantwortlich. Bevor er zu McAfee kam, war McClure Executive Director of Security Services bei Kaiser Permanente, einer Organisation im Gesundheitswesen mit einem Betriebsertrag von 34 Milliarden US-Dollar. Anschließend war er als Senior Vice President of Global Threats and Research bei McAfee tätig und leitete in dieser Funktion ein Eliteteam im Bereich globale Sicherheitsbedrohung. Er war Gründer, President und Chief Technology Officer von Foundstone, Inc. (jetzt McAfee Foundstone).

McClure ist aufgrund seiner umfassenden und tiefgehenden Sicherheitskenntnisse weithin anerkannt und gilt heute als einer der branchenweit führenden Experten im Bereich Informationssicherheit. Er war Co-Autor des Buchs *Hacking Exposed: Network Security Secrets & Solutions* (Das Anti-Hacker-Buch: Sicherheit und Lösungen bei Netzwerken), das in über 30 Sprachen übersetzt wurde und als eines der maßgeblichen Bücher zum Thema Computersicherheit gilt. McClure ist ein vielfach publizierter und weithin anerkannter Visionär im Sicherheitsbereich, war über 22 Jahre auf der Technologie- und Führungsebene tätig und verfügt über tiefgehende Erfahrung im technischen und betrieblichen sowie im Finanzbereich.

André Weimerskirch, Dr.-Ing., Chief Executive Officer und President, ESCRYP T Inc.

André Weimerskirch, Dr.-Ing., ist Chief Executive Officer (CEO) und President des in den USA ansässigen Unternehmens ESCRYP T Inc. und dort für die internationalen Aktivitäten des Unternehmens zuständig. Von 2004 bis 2007 hatte er die Position des Chief Technology Officer (CTO) bei der ESCRYP T GmbH inne. Er studierte an der Technischen Universität Darmstadt Wirtschaftsinformatik und Mathematik und erwarb später am Worcester Polytechnic Institute (USA) den Master of Science in Informatik. Anschließend erhielt er an der Ruhr-Universität Bochum einen Dokortitel für angewandte Datensicherheit. Seither befasst sich Weimerskirch mit zahlreichen Industrieprojekten, die sich auf die USA und Europa beziehen und ihren Schwerpunkt im Bereich Datensicherheit und Datenschutz in eingebetteten Systemen haben. Er veröffentlichte zahlreiche Artikel in wissenschaftlichen und brancheninternen Workshops und beteiligte sich an der Entwicklung mehrerer Industriestandards für automobiler Datensicherheit. Er ist einer der wichtigsten Akteure in den USA und Europa bei der Definition von Sicherheits- und Datenschutztechniken für Kommunikation zwischen Fahrzeugen.



Dr. Marko Wolf, ESCRYP T GmbH, Deutschland

Dr. Marko Wolf ist leitender Sicherheitsingenieur bei der ESCRYP T GmbH, wo er sich vorwiegend auf eingebettete sowie Fahrzeugsicherheit konzentriert. Er studierte Elektrotechnik und Informationstechnik an der Ruhr-Universität Bochum sowie an der Purdue University (USA). Nach Erhalt des Master of Science im Jahr 2003 begann er seine Doktorarbeit zum Thema vertrauenswürdige Computing und Fahrzeug-IT-Sicherheit, die er im Jahr 2008 mit der ersten umfassenden Arbeit zu Fahrzeug-IT-Sicherheit abschloss. Er ist Herausgeber/Autor der Bücher *Embedded Security in Cars* (Eingebettete Sicherheit in Autos, Springer, 2006) und *Security Engineering for Vehicular IT Systems* (Sicherheitstechnologien für Fahrzeug-IT-Systeme, Vieweg+Teubner, 2009), fungiert als Programmleiter der internationalen Workshop-Reihe „Embedded Security in Cars (ESCAR)“ (Eingebettete Sicherheit in Autos) und hat über 30 Artikel zum Thema IT-Sicherheit veröffentlicht.

Prof. Dr.-Ing. Christof Paar, Ruhr-Universität Bochum und University of Massachusetts in Amherst (USA)

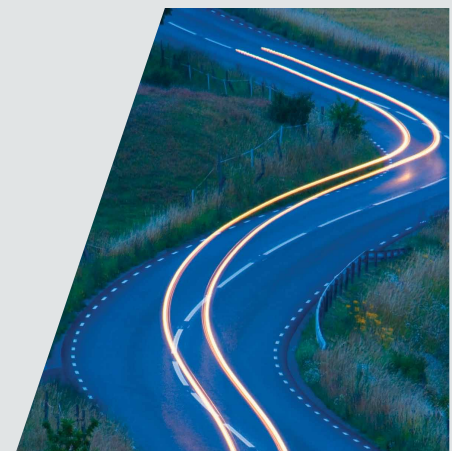
Christof Paar leitet den Lehrstuhl Eingebettete Sicherheit an der Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität Bochum und ist Assistenzprofessor an der University of Massachusetts in Amherst (USA). Er ist einer der international führenden Experten für industrielle IT-Sicherheit. Von 1994 bis 2001 leitete Paar den Bereich für Kryptografie und Informationssicherheit am Worcester Polytechnic Institute (USA). Er war Mitgründer der Konferenz für Kryptografische Hardware und eingebettete Systeme (Cryptographic Hardware and Embedded Systems, CHES), die als weltweit führende Veranstaltung für angewandte IT-Sicherheit gilt. Paar verfügt über umfangreiche Erfahrung in der Forschung und Entwicklung in europäischen und US-amerikanischen Unternehmen. Er ist Aufsichtsrats- und Verwaltungsratsmitglied in verschiedenen Sicherheitsunternehmen und hat bereits mehrere Technologie-Startups begleitet. Paar veröffentlichte bisher mehr als 150 referierte Veröffentlichungen zu angewandter IT-Sicherheit und hält mehrere Patente.

Winfried Stephan, Senior Consultant T-Systems ICT Security Consulting and Engineering

Winfried Stephan ist seit 15 Jahren bei T-Systems ICT Security Consulting and Engineering im Bereich Sicherheitsanalysen und Beratung tätig. Er beschäftigt sich seit 37 Jahren mit Kryptografie-Anwendungen. In seiner Zeit bei T-Systems arbeitete er an Projekten zur Entwicklung und Implementierung eines Sperrsystems sowie anderer Automobildienste.

Prof. Dr. Stefan Goß, Ostfalia Hochschule für angewandte Wissenschaften

Prof. Dr. Stefan Goß ist seit 25 Jahren im Bereich der Kfz-Elektronik tätig. Er fungierte von 2002 bis 2007 als weltweiter Leiter für die Entwicklung von Telematik und Geräteausstattung bei Volkswagen und anschließend von 2007 bis 2011 als weltweiter Leiter für die Entwicklung von On-Board-Diagnose-Tools, bevor er im Jahr 2011 die Stelle als Professor für Fahrzeugtechnik an der Ostfalia Hochschule für angewandte Wissenschaften übernahm.



Informationen zu McAfee

McAfee ist ein hundertprozentiges Tochterunternehmen der Intel Corporation (NASDAQ: INTC) und der weltweit größte auf IT-Sicherheit spezialisierte Anbieter. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer, ITK-Netze und Mobilgeräte auf der ganzen Welt vor Angriffen schützen und es den Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von der einzigartigen Global Threat Intelligence-Technologie entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. McAfee ist stets auf der Suche nach neuen Möglichkeiten, seine Kunden zu schützen.

<http://www.mcafee.com/de>



McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

McAfee und das McAfee-Logo sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind alleiniges Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2011 McAfee, Inc. 31607rpt_malware-ahead_0811