MEHR IT-SICHERHEIT AUF UNSEREN STRASSEN

Über die Absicherung unserer digitalen Fahrzeugzukunft gegen Hacker und Viren

Essay zur Dissertation „Security Engineering for Vehicular IT Systems“von Marko Wolf
am Lehrstuhl für Embedded Security an der Ruhr-Universität Bochum

Zusammenfassung

Die Wandlung von Fahrzeugen zu softwarebasierten, digital vernetzten Informationssystemen ist bereits im vollen Gange. So enthält heute bereits ein Kompaktwagen ein Vielfaches der Rechenleistung einer Apollo-Mondlandefähre einschließlich erster Schnittstellen zur Kommunikation mit der Außenwelt.

Die digital vernetzte Fahrzeugzukunft birgt aber auch ein enormes Gefahrenpotenzial. Obwohl die heutige Fahrzeugelektronik gegen technische Fehler oder Ausfälle gewappnet ist, bedenkt sie jedoch kaum Personen oder Schadprogramme, welche versuchen sie gezielt zu manipulieren. Das Spektrum böswilliger Eingriffe reicht dabei von einfachen Tachomanipulationen über manipulierte Verkehrsleitsysteme bis hin zum Angriff auf fahrrelevante Anwendungen.

Die zuverlässige Absicherung von Fahrzeugen gegen Hacker und Viren ist nicht nur unabdingbar für die Sicherheit aller Verkehrsteilnehmer, sondern auch zwingende Voraussetzung für viele verkehrstechnische, behördliche und geschäftliche Fahrzeuganwendungen.

Zombies in Texas!

Eine einfache Manipulation an den ungesicherten Steuerungen zweier elektronischer Verkehrstafeln reichte aus, dass diese vor gefährlichen Zombies, anstatt vor einer nahenden Baustelle warnten (vgl. Abbildung 1). Die in der Folge durchaus „spürbaren Verkehrsbehinderungen“ in einer kleinen Ausfallstraße Anfang dieses Jahres in Austin, Texas (USA) zeigen doch eindrucksvoll wie schnell unsere digital vernetzte Fahrzeugzukunft auch missbraucht oder gar zur Gefahr werden kann [5].

Die digitale Revolution

Trotzdem, die Automobilindustrie steht kurz vor einer ihrer größten technologischen Umbrüche seit der Erfindung des Automobils vor über 150 Jahren: das digitale, vernetzte Fahrzeug. Waren Autos, Lastkraftwagen oder Motorräder bisher weitgehend isolierte, rein elektromechanische Systeme, ist deren Evolution hin zu softwarebasierten, digital miteinander vernetzten, interaktiven Informationssystemen bereits im vollen Gange.

Abb. 1: „Gehacktes“ elektronisches Verkehrszeichen in Austin, Texas im Januar 2009. (AP/Chris Nakashima-Brown)

Die Wandlung von mechanischen Steuerungen aus stählernen Zahnrädern und Gelenken in digitale Softwareprogramme aus Bits und Bytes ermöglichen hochintelligente und hochkomplexe Funktionen, welche mit den bisherigen, elektromechanischen Steuerungen kaum realisierbar sind. Gleichzeitig sind softwarebasierte Fahrzeugfunktionen oftmals auch noch deutlich leichter, flexibler, wartungsärmer und kostengünstiger. So ist es nicht ungewöhnlich das bereits heute etwa 90% aller Innovationen im Fahrzeug ausschließlich auf neuen Softwarefunktionen beruhen [1].

Die digitale drahtlose Vernetzung von Fahrzeugen mit der sie umgebenden Verkehrsinfrastruktur und mit anderen Fahrzeugen wiederum macht aus stummen passiven „Dateneinbahnstraßen“ hochintelligente, interaktive Kommunikationsknoten. Über Funk können sich Fahrzeuge so gegenseitig vor Gefahren warnen oder intelligente Verkehrssteuerungen mit präzisen, hochaktuellen Informationen versorgen, um beispielsweise eine der größten Ressourcenverschwendungen unserer Zeit, den alltäglichen Stau, gar nicht erst entstehen zu lassen. Noch progressivere Konzepte reichen von vollautomatischen Vorfahrtsregelungen bis hin zum Autopiloten im Fahrzeug, bei dem der Fahrer sich nach der Eingabe seines Ziels nur noch entspannt zurücklehnen braucht.

Die Kehrseite der Medaille

Die zunehmende digitale Informationstechnik (IT) und interaktive Vernetzung von Fahrzeugen birgt gleichzeitig aber auch ein enormes Gefahrenpotenzial. Obwohl heute praktisch alle Fahrzeuganwendungen gegen mögliche (zufällige) technische Fehler oder Ausfälle vorbereitet sind (z.B. mittels Prüfsummen oder mehrfacher Redundanz), berücksichtigt die heutige Fahrzeugelektronik jedoch fast nie einen gezielt vorgehenden menschliche Angreifer (z.B. einen Computer-Hacker) oder entsprechende Schadprogramme (z.B. Viren, Würmer oder Trojaner), welche eine bestimmte Fahrzeug-Funktionalität zwar syntaktisch korrekt, jedoch in böswilliger Absicht benutzen. Die Schäden durch solche unautorisierten Eingriffe an unzureichend geschützten Fahrzeug-Elektroniksystemen durch Diebstahl, Tachometermanipulationen oder illegales Chiptuning sind für Hersteller und Kunden, und damit letztlich auch für die Gesellschaft schon heute beträchtlich [4]. Im Vergleich zum Schadenspotenzial von böswilligen Manipulationen an ungeschützten Fahrzeug-IT-Systemen und der Fahrzeug-Kommunikation in der Zukunft sind diese Risiken jedoch fast schon vernachlässigbar.

Angriffe auf Personalcomputer (PC) oder Internetserver, welche schon heute ähnlich komplex aufgebaut sind und über ähnlich ungeschützte Netzwerke miteinander kommunizieren wie zukünftige Fahrzeug-IT-Systeme, können bereits erhebliche Schäden verursachen. Nichtsdestotrotz bleibt in diesen Fällen das durchaus immense Schadenpotenzial in der Regel „nur“ auf Produktivitätsverluste, entgangene Umsätze oder zerstörte Daten begrenzt. Im Vergleich dazu können allerdings schon kleinste Manipulationen an dem IT-System eines Fahrzeugs, welches zwei Tonnen Stahl bei 120 km/h in Echtzeit steuert, Leib und Leben von Fahrzeuginsassen und anderen Verkehrsteilnehmern in größte Gefahr bringen. Insbesondere, da der Benutzer eines solchen IT-Systems (d.h. der Fahrer), im Vergleich zum Benutzer eines angegriffenen PCs, in der Regel weder genügend Zeit, noch ausreichende Alternativen hat, um im Falle eines erfolgreichen Angriffs überhaupt noch adäquat reagieren zu können. Dabei reicht, insbesondere bei fahrrelevanten Automobilanwendungen, oft schon ein einziger erfolgreicher Angriff aus, um die Reputation eines Herstellers nachhaltig zu schädigen (Stichwort: Elchtest), selbst dann, wenn die tatsächliche Gefährdung insgesamt nur marginal bleibt [6]. Neben gezielten Angriffen auf die Integrität eines Fahrzeugs, kann ein manipuliertes Fahrzeug wiederum böswillig benutzt werden, um andere Verkehrsteilnehmer negativ zu beeinträchtigen oder zu schädigen. Dabei reicht das Schadenpotenzial im Falle der interaktiven Fahrzeugkommunikation von gefälschten Warnmeldungen über manipulierte Vorfahrtsregelungen bis hin zu gezielten Verkehrsumleitungen mit denen sich der Verkehr ganzer Städte ins Chaos stürzen ließe.

Dass es dagegen bisher nur wenige wirksame Schutzmaßnahmen gibt, ist nicht nur durch den eingangs bereits erwähnten rasanten Wandel in der Fahrzeugelektronik bedingt. Fahrzeuge sind neben den Angriffen durch Außenstehende und ihre zusätzlichen externen Schnittstellen, insbesondere auch noch den Angriffen ihrer legitimen Benutzer ausgesetzt. Das bedeutet, dass ähnlich wie beim Bezahlfernsehen oder bei Spielkonsolen, aber anders als beispielsweise bei einem Bankserver, sich das Angriffsziel selbst vollständig in der Hand des Angreifers befindet.

Die Intentionen für Manipulationen am eigenen Fahrzeug können dabei ganz unterschiedlich sein. Ein Fahrer könnte beispielsweise versuchen bestehende Restriktionen zu umgehen, sei es um bestimmte Fahreinträge nachträglich zu manipulieren (z.B. im digitalen Fahrtenschreiber) oder die IT-Systeme seines Fahrzeuges missbräuchlich gegen andere zu verwenden (z.B. um gefälschte Funknachrichten zu versenden). Angriffe durch den eigenen Benutzer sind durch den zusätzlichen umfangreichen direkten physischen Zugriff auf alle im Fahrzeug verbauten IT-Systeme besonders mächtig.

Schlüsseltechnologie IT-Sicherheit

Heutige Fahrzeug-IT-Systeme benötigen demnach dringend verlässliche Schutzmaßnahmen, nicht nur um die eigene Betriebs- und Fahrsicherheit zu gewährleisten, sondern um darüber hinaus auch die verschiedensten Gesetzesanforderungen zur Produkthaftung zu erfüllen oder die umfangreichen Investitionen der Fahrzeughersteller und Zulieferer zuverlässig gegen mögliche Produktfälscher zu schützen. Hinzu kommen die vielen IT-Sicherheitsanforderungen von Fahrern und Insassen (z.B. im Bereich des Datenschutzes), welche im Zuge verschiedenster neu aufkommender, automobiler Geschäftsmodelle und behördlicher Anwendungen (z.B. elektronisches Nummernschild) notwendig werden.

Wie ein ähnliches Debakel, wie heute schon aus der Welt der Internet-PCs bekannt, in der digital vernetzten Fahrzeugzukunft vermieden werden kann, ist zentraler Gegenstand dieser Dissertation. Dazu versucht die Arbeit die beiden bisher unabhängig voneinander existierenden Themengebieten der Fahrzeug-Informationstechnik und der Informationssicherheit sinnvoll miteinander zu verknüpfen. Diese interdisziplinare Arbeit ist damit die weltweit erste, welche die beiden Themen so

miteinander verbindet und dabei einen umfassenden, detaillierten Einblick in das sich rasant entwickelnde Gebiet der automobilen IT-Sicherheit gibt, um die Vertrauenswürdigkeit und Zuverlässigkeit von automobilen IT-Anwendungen heute und in Zukunft sicher gewährleisten zu können.

Und die Anzahl potenziell gefährdeter Fahrzeuganwendungen ist dabei ungeahnt groß. Auch wenn aktuell vor allem noch die Themen Tachomanipulation, Diebstahlschutz oder der Schutz vor unerlaubter Nachahmung und Fälschungen die IT-Sicherheitsproblematik im Fahrzeugbereich dominieren, haben viele, deutliche kritischere Fahrzeuganwendungen die Schreibtische der Forschungsabteilungen bereits in Richtung Serienfertigung verlassen. Neue Anwendungen wie das elektronische Nummernschild, das Nachladen von Fahrzeugsoftware oder eben die interaktive Fahrzeugkommunikation sind ohne ausreichende Schutzmaßnahmen kaum zuverlässig realisierbar.

Automobile Angreifer und Angriffe

Um mögliche Bedrohungen schon beim Entwurf einer Fahrzeug-Anwendung zu erkennen, können Vorgehensweisen und Methoden, welche sich beispielsweise in der Systemsicherheit bereits etabliert haben, sinnvoll auch für die Automobilwelt adaptiert werden. Dabei werden zunächst mögliche Angreifer und Angriffsmethoden sowie ihre möglichen Intentionen für Eingriffe in ein Fahrzeug identifiziert und klassifiziert. Die Angreifer können hierfür unter anderem nach ihren Fähigkeiten, technischen und finanziellen Möglichkeiten oder ihrem Zugriffsmöglichkeiten auf das Angriffsziel (von logisch bis physikalisch) unterschieden werden. So lassen sich mögliche Sicherheitsrisiken von Beginn an entdecken und geeignet abschätzen.

Der augenscheinlichste Angreifer ist vielleicht der externe Angreifer (Klasse E), wie zum Beispiel ein Fahrzeugdieb, welcher etwa versucht ein Fahrzeug über das Abhören und spätere erneute Senden der Funkschlüsselnachricht zu entwenden. Der externe Angreifer kann in der Regel nur für kurze Zeit, leicht zugängliche Angriffspunkte im Außenbereich eines Fahrzeugs für Angriffe benutzen, dabei aber durchaus über umfangreiches Expertenwissen und technisch ausgefeilte Hilfsmittel verfügen. Ein weiterer wichtiger Angreifer ist, wie eingangs bereits kurz erwähnt, der legitime Benutzer des Fahrzeugs selbst (Klasse I-1). Dieser könnte versuchen wichtige Datenaufzeichnungen wie den digitalen Fahrtenschreiber oder kritische Fahrzeugfunktionen wie die Motorsteuerung gezielt zu manipulieren, um damit mögliche Gesetzesverstöße zu vertuschen oder technische Beschränkungen (z.B. die Höchstgeschwindigkeit oder die Abgassteuerung) zu umgehen. Ein Fahrzeugnutzer verfügt dafür in der Regel aber nur über ein begrenztes Know-how und begrenzte technische Ressourcen, hat dafür aber vollen Zugriff auf das Angriffsziel. Vor allem aber verfügt er, im Vergleich zum Beispiel zu einem Hackerangriff auf einen Bankserver, über praktisch unbegrenzte Zeit und nahezu unbegrenzte Versuche ohne eine Entdeckung oder aktive Gegenmaßnahmen fürchten zu müssen. Kommt er selbst nicht weiter, beauftragt der Fahrzeugbesitzer vielleicht zusätzlich einen fähigen Mechaniker (Klasse I-2), welcher bei gleichem Zugriffsumfang noch über weitaus umfangreichere Erfahrung und mächtige technische Gerätschaften verfügen kann. Für Angriffe, welche beispielsweise durch den Verkauf von gefälschten Komponenten ganz besonders große Gewinne versprechen, sind wiederum hoch professionelle Angreifer (Klasse I-3) etwa aus dem Bereich der organisierten Kriminalität durchaus bereit sehr große finanzielle Mittel zu investieren, um aktuelles Forschungswissen mit High-Tech-Werkzeugen zu kombinieren, um sich finanziell besonders lohnende Angriffe erfolgreich durchzuführen. Hierbei handelt es sich vor allem um Angriffe, deren Ergebnisse sich anschließend für weitere Manipulationen leicht wiederverwenden lassen, wie das Ausspionieren eines weltweit einheitlichen Verschlüsselungssystem (Stichwort: Premiere-Bezahlfernsehen) oder die Angriffe eines Herstellers auf eine Konkurrenzprodukt, um sich vergleichsweise kostengünstig, wertvolles Knowhow seines Konkurrenten zu beschaffen.

Das Spektrum der Angriffsmethoden ist dabei im Fahrzeugbereich besonders weit gefächert. Zunächst können auch Angreifer auf ein Fahrzeug, wie der Hacker in einem Computernetzwerk, versuchen allein mittels logischer Angriffe einen Sicherheitsmechanismus im Fahrzeug zu umgehen. Logische Angriffe basieren vor allem auf konzeptionellen Schwächen oder so genannten Brute-Force-Angriffen, welche systematisch alle möglichen Kombinationen ausprobieren beispielsweise um eine geheime PIN-Kennzahl zu ermitteln. Durch den Einsatz von standardisierten und durch die internationale wissenschaftliche Gemeinde geprüften Algorithmen, Parametern und Protokollen sollten logische Angriffe, welche auf den konzeptionellen Schwächen einer Sicherheitslösung beruhen, selten das schwächste Glied für einen erfolgreichen Angriff darstellen.

Weitaus erfolgreicher als logische Angriffe sind oftmals Softwareangriffe, welche Sicherheitslücken in der Implementierung oder einfach vorhandene Softwarefunktionalität gezielt missbrauchen, um einen erfolgreichen Angriff durchzuführen. Da schon heutige Fahrzeuge bisweilen Software im Umfang eines herkömmlichen PC-Betriebssystems

enthalten, ist die Wahrscheinlichkeit von kritischen Sicherheitslücken in Automobil-Software ähnlich hoch einzuschätzen, wie es in der heutigen PC-Welt der Fall ist. Daher gehören Softwareangriffe im Fahrzeugbereich momentan zu den Angriffen mit dem höchsten Angriffspotenzial.

Dahingegen sind Angriffe auf die Kommunikation von Fahrzeugen mit anderen Fahrzeugen oder der Verkehrsinfrastruktur aufgrund der bisher noch seltenen Verwendung von interaktiven Kommunikationsanwendungen heute noch vergleichsweise unkritisch. Dabei ist es ohne zusätzliche Schutzmaßnahmen besonders leicht Funknachrichten abzuhören, zu verändern oder zu fälschen, da dies schon mit einfachsten Gerätschaften und ohne Zugriff auf ein Fahrzeug möglich ist, wie die erfolgreichen Angriffe auf den digitalen TMC-Dienst (traffic message channel) jüngst eindrucksvoll gezeigt haben.

Die letzte, hier exemplarisch vorgestellte und gleichzeitig technisch mächtigste Angriffsmethode sind die physikalischen Angriffe, welche im Unterschied zu den meisten Angriffen aus der Computerwelt, nur deshalb möglich sind, weil viele Angreifer im Automobilbereich sowohl logisch als auch physikalisch vollständig über ihr Angriffsziel verfügen können. Die Bandbreite physikalischer Angriffe ist hierbei riesig und reicht vom einfachen Auslesen und Überschreiben von Speicherbausteinen bis hin zu Angriffen, welche das Steuergerät eines Fahrzeugs bis auf Transistorebene untersuchen und manipulieren können (z.B. um eine geheime Information zu extrahieren).

Werkzeugkasten IT-Sicherheit

Natürlich ist man auch im Automobilbereich Angreifern und Angriffen nicht schutzlos ausgeliefert. Viele Sicherheitslösungen, welche aus der Netzwerk- und Systemsicherheit bekannt sind, lassen sich auch für den Einsatz im Fahrzeug adaptieren. Dabei können sich eine Reihe von charakteristischen Schwierigkeiten, aber auch einige Vorteile im Vergleich zu ihrer herkömmlichen Einsatzumgebung ergeben. Was die Realisierung von IT-Sicherheitslösungen im Fahrzeug technisch und strategisch besonders schwierig macht sind unter anderem die:

- vergleichsweise begrenzte Rechenleistung und kleine Speicher
- physikalisch anspruchsvolle Umgebung (z.B. Temperatur, Feuchtigkeit)
- begrenzte Möglichkeit nachträglicher Korrekturen (z.B. keine Security-Updates)
- heterogene und verteilte Systemarchitektur
- langen Produktlebenszyklen und umfangreichen Haftungsübernahmen
- Zusatzkosten mit schwer (dem Kunden) vermarktbaren Nutzen
- hohen Anforderungen an Interoperabilität und Kompatibilität
- begrenzte Bereitschaft der Nutzer für zusätzlichen Bedienungsaufwand

Nichtsdestotrotz impliziert die Umsetzung von IT-Sicherheitslösungen in Fahrzeugen, im Vergleich beispielsweise zur Realisierung einer IT-Sicherheitslösung zur Absicherung eines Internet-Banking-Servers, auch einige charakteristische Vorteile wie zum Beispiel:

- periodische, vorhersehbare und unvorhersehbare Inspektionen (z.B. durch den TÜV oder die Polizei)
- kein statisches, das heißt kein örtlich fixiertes Angriffsziel
- stetige, umfangreiche Standardisierung, Evaluierung und Zertifizierung (z.B. gesetzliche Zulassungsprüfung)

Sind mögliche Angriffsziele, Angreifer und Angriffsmethoden und damit mögliche Gefährdungen frühzeitig bekannt, können schon beim Entwurf eines Fahrzeug-IT-Systems geeignete Schutzmaßnahmen berücksichtigt werden. Um zu zeigen, dass man die verschiedenen Angriffe und Angreifer auch im Fahrzeugbereich effektiv abwehren kann, werden nachfolgend einige Sicherheitstechnologien und Schutzmechanismen kurz exemplarisch vorgestellt.

Kryptographie – Wissenschaft der Geheimschriften

Einer der wichtigsten Bausteine aus dem Werkzeugkasten der IT-Sicherheit ist die Kryptographie, also die Wissenschaft der Verschlüsselung von Informationen gegen unberechtigtes Auslesen, Verändern oder Fälschen. Dabei werden vor allem zwei wichtige Verfahren zur Verschlüsselung unterschieden, die symmetrische Kryptographie und die asymmetrische Kryptographie. Die symmetrische Kryptographie oder die klassische Kryptographie beruht auf verschieden Algorithmen unterschiedlichster Mächtigkeit, die jedoch eines stets gemeinsam haben: Sender und Empfänger einer geheimen Nachricht teilen sich das gleiche Geheimnis um diese zu ver- und zu entschlüsseln. Das lässt sich vielleicht am besten anhand eines verschlossen Kästchens

vorstellen, welches die zu schützenden Nachrichten enthält und nur der Sender und der Empfänger über den passenden Schlüssel verfügen um das Kästchen zu öffnen oder zu schließen. Wer nicht über den passenden Schlüssel verfügt, kann so die Nachrichten im Kästchen weder lesen noch verfälschen. Voraussetzung für das Kästchenbeispiel und somit auch für die symmetrische Kryptographie ist, dass Sender und Empfänger sich vorher über einen passenden Schlüssel einigen müssen bzw. diesen schon vorher sicher austauschen müssen, beispielsweise indem sie sich vorher persönlich treffen. Wie aber kann man jemanden eine geheime Nachricht senden, ohne dass man denjenigen vorher getroffen hat und man auch über keinen sicheren Kanal (z.B. einen vertrauenswürdigen Kurier) verfügt, um dem Empfänger den gemeinsamen Schlüssel sicher zukommen zu lassen?

Diese fundamentale Problematik der Kryptographie blieb über Jahrtausende - die Anfänge der klassischen Kryptographie liegen im Ägypten des Altertums - ungelöst und konnte erst in den 1970er Jahren durch die beiden Kryptographen Whitfield Diffie und Martin Hellman gelöst werden [3]. In der von Diffie und Hellmann begründeten asymmetrischen Kryptographie werden anstatt eines gemeinsamen Geheimschlüssels, zwei jeweils verschiedene, aber mathematisch miteinander verknüpfte Schlüssel jeweils zum Ver- und Entschlüsseln verwendet. Während der so genannte öffentliche Schlüssel (public key) eines Empfängers von jedem beliebigen Sender zum Verschlüsseln einer Nachricht an diesen benutzt werden kann, besitzt ausschließlich der Empfänger den zugehörigen geheimen so genannten privaten Schlüssel (private key) zum Entschlüsseln der Nachrichten. Um die asymmetrische Kryptographie anhand des vorherigen Kästchenbeispiels noch einmal zu veranschaulichen, kann man sich vorstellen, dass der künftige Empfänger jedem der ihm eine geheime Nachricht überbringen möchte, ihm zuvor ein offenes Kästchen mit einem offenen Vorhängeschloss zur Verfügung stellt. Der Sender deponiert seine geheime Nachricht dann in das so vorbereitete Kästchen und schiebt das Schloss (ohne Schlüssel) zu, welches anschließend nur noch durch den Empfänger mit seinem geheim gehaltenen Schlüssel wieder geöffnet werden kann. Asymmetrische Verfahren überwinden somit nicht nur den sicheren Austausch von geheimen symmetrischen Schlüsseln, sondern können auch für eine Reihe anderer wichtiger kryptographischer Mechanismen verwendet werden. Bei der sogenannten digitalen Signatur werden beispielsweise der geheime private Schlüssel zum digitalen Unterschreiben einer Information und der öffentliche Schlüssel zum Überprüfen der erzeugten digitalen Unterschrift verwendet. Da im Unterschied zur symmetrischen Kryptographie ausschließlich der Besitzer des zugehörigen geheimen privaten Schlüssels in der Lage ist eine Information zu unterschreiben, kann so die Authentizität einer Information sicher gestellt werden. Zur Prüfung einer digitalen Unterschrift kann wiederum jeder den passenden öffentlichen Schlüssel des Unterschreibers verwenden. Leider ist auch hier keine Medaille ohne Kehrseite. Der große Nachteil asymmetrischer kryptographischer Verfahren ist ihre enorme mathematische Komplexität. So ist in der Regel ein um mehrere Größenordnungen höherer Rechenaufwand notwendig, um die gleiche Information statt mit einem symmetrischen Verfahren, asymmetrisch zu ver- oder zu entschlüsseln. Üblicherweise hilft man sich aber auch hier mit einem kleinem Kniff, der sogenannten Hybrid-Encryption. Hierfür wird ein aufwändiges und langsames asymmetrisches Verfahren ausschließlich dafür eingesetzt, den Absender einer Nachricht zunächst zu authentifizieren um mit ihm anschließend einen gemeinsamen symmetrischen Schlüssel auszutauschen. Der gesamte nachfolgende Nachrichtenaustausch wird dann ausschließlich mit Hilfe eines deutlich effizienteren und schnelleren symmetrischen Verfahrens durchgeführt.

Die wichtigsten durch wissenschaftliche Gemeinde über Jahrzehnte geprüften und standardisierten Verfahren der symmetrischen Kryptographie sind der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES). Die beiden wichtigsten Vertreter der asymmetrischen Kryptographie sind der Rivest-Shamir-Adleman-Algorithmus (RSA) und die Elliptic Curve Cryptography (ECC).

Kommunikationssicherheit

Auf den vorgenannten kryptographischen Algorithmen basierende Protokolle und Schemata werden im Fahrzeug unter anderem zur Absicherung der Steuergeräte-Software, zur Verschlüsselung von Fahrzeug-Speichern und zur Absicherung der Kommunikation innerhalb (z.B. zwischen verschiedenen Steuergeräten) und außerhalb des Fahrzeugs verwendet. Während mittels asymmetrischer Kryptographie-Verfahren vor allem die Echtheit eines Absenders geprüft wird (Stichwort: digitale Signatur) und symmetrische Schlüssel sicher ausgetauscht werden, sind symmetrische Kryptographie-Verfahren hauptsächlich zum effizienten Schutz der eigentlichen Fahrzeugkommunikation im Einsatz. Die symmetrischen Verfahren sichern so den Nachrichtenaustausch im und außerhalb des Fahrzeugs effizient gegen unerlaubtes Abhören, gegen Manipulation und vor Fälschungen und können auch in eher leistungsschwachen Steuergeräten ef-

fizient realisiert werden. Trotzdem müssen für alle kryptographischen Verfahren die unterschiedlichen Kommunikationssysteme individuell angepasst werden, Vertrauensgruppen gebildet und Prozesse zur Schlüsseleinbringung oder Schlüsselerneuerung definiert werden. Zentrale Bausteine für die Kommunikationssicherheit im Fahrzeug sind außerdem die kryptographischen Protokolle, welche ebenfalls in der Dissertation detailliert behandelt werden, um das Überprüfen neu hinzugefügter Fahrzeuge oder Fahrzeug-Steuergeräte sowie das sichere Entfernen zuverlässig und effizient zu realisieren.

Software-Sicherheit

Die Absicherung von Fahrzeuganwendungen gegen Softwareangriffe beginnt genau wie die Absicherung der Fahrzeugkommunikation schon während der Entwicklung beim Softwarehersteller und umfasst dort unter anderem den Softwareentwurf, die Implementierung und das Software-Testen. Glücklicherweise gibt es bereits aus dem Bereich der Software-Safety (d.h. der Absicherung von Software gegen zufällige Fehler ohne gezielte Angriffe) erprobte Techniken, Prozesse und Werkzeuge, welche relativ leicht auch zur Entdeckung von IT-Sicherheitslücken adaptiert und parametrisiert werden können. Mit Hilfe standardisierter Kodier-Richtlinien, Code-Scanner, rollenbasierter Prüfverfahren oder Testangriffen können viele mögliche Einfallstore und potenzielle Schwächen bereits vor der Auslieferung der Software entdeckt und behoben werden.

Abschließend kann jede Software noch mit Hilfe einer digitalen Signatur gegen nachträgliche unautorisierte Änderungen oder Manipulationen geschützt werden. Dabei wird mittels eines geheimen Signaturschlüssels (Stichwort: asymmetrische Kryptographie), über den allein der Software- oder Fahrzeughersteller verfügt, der freigegebenen Software ein kryptographischer Prüfcode angefügt, welcher die Integrität der Software nachweisbar macht. Vor dem Einspielen einer digital signierten Software in ein Fahrzeugsteuergerät (dem so genannten Flashen) kann dann mittels des zugehörigen öffentlichen Prüfschlüssels die Unversehrtheit der Software im Fahrzeug geprüft und bei eventuellen Manipulationen durch das Fahrzeug abgebrochen werden.

Eine solche Integritätsprüfung der Fahrzeugsoftware sollte nicht nur während jeder Softwareaktualisierung durchgeführt werden, sondern kann zusätzlich beispielsweise auch bei jedem Fahrzeugstart die Unversehrtheit aller vorhandenen Software prüfen und den Fahrer oder Anwendungen vor möglichen Manipulationen warnen. Um eine Software auch zur Laufzeit gegen verschiedene Angriffe zu schützen, können ebenfalls viele bekannte Verfahren aus der PC-Welt entsprechend angepasst auch im Fahrzeug eingesetzt werden. Die Palette möglicher Softwareschutzmaßnahmen reicht hierbei von Lösungen zur Ressourcen-Virtualisierung (z.B. Xen-Virtualisierung) über feingranulare Zugriffsteuerungen bis hin zu komplexen kryptographischen Verfahren zur unlösbaren Verknüpfung von Informationen beispielsweise mit genau einer Fahrzeugkomponente in einer ganz bestimmten Konfiguration. Insbesondere das letztere Verfahren, welches beispielsweise zum Schutz von Software und Daten, die für die Fahrsicherheit oder die Produkthaftung besonders wichtig sind, wird in Dissertation ausführlich behandelt.

Hardware-Sicherheit

Alle Schutzmaßnahmen welche in Software umgesetzt worden sind, müssen sich wiederum darauf verlassen können, dass ihre zugrunde liegende Hardware wie vorgesehen funktioniert. Diese Annahme ist beispielsweise für einen Bankserver, welcher in einer geschützten Umgebung (z.B. einem abgeschlossenen Raum mit Zutrittsbeschränkung) aufgestellt ist, sicher relativ leicht zutreffend. Bei Fahrzeugen, wo auch der legitime Benutzer als Angreifer nicht ausgeschlossen werden kann, kann sich gerade eine Softwareschutzfunktion nicht automatisch auf die Korrektheit ihrer ausführenden Hardware verlassen. So könnte ein Angreifer, welcher auch physikalisch über sein Angriffsziel verfügt, ganze Speicherbausteine austauschen, interne Übertragungsleitungen oder gar den Prozessor selbst während dieser mit geheimen Informationen arbeitet gezielt abhören und so viele rein softwarebasierte Sicherheitslösungen leicht überwinden. Deshalb werden alle elementaren Sicherheitsfunktionen wie das Ver- und Entschlüsseln von Daten, das Prüfen von digitalen Signaturen oder das Speichern wichtiger geheimer Schlüssel ausschließlich in besonders geschützten Hardwarebausteinen, den so genannten Kryptochips zusätzlich abgesichert ausgeführt. Natürlich kann auch ein Kryptochip keine hundertprozentige Sicherheit garantieren, jedoch ist der Aufwand einen Kryptochip „zu brechen“ im Vergleich zu einem Softwareangriff typischerweise um mehrere Größenordnung höher und lohnt sich so nur, wenn sich das Ergebnis im großen Stil wieder verwenden lässt. Die einfachste Maßnahme zum Schutz von Hardware sind spezielle Versieglungen (z.B. Speziallacke oder offizielle Siegel), welche einen erfolgreichen Angriff zwar nicht verhindern, diesen aber etwa bei regel- und unregelmäßig Kontrollen deutlich sichtbar machen können (tamper-evidence). Zusätzliche passive Schutz-

maßnahmen versuchen einen Hardwareangriff wiederum so schwer wie möglich zu machen (tamper-resistance) indem sie Kryptochips mit besonderen „Hardwareschutzschilder“ beispielsweise aus Spezialstahl oder Keramik ausstatten. Eine der mächtigsten Techniken Hardwareangriffe erfolgreich zu verhindern, sind aktive Schutzmaßnahmen (tamper-response), welche mittels einer Vielzahl verschiedenster Sensoren (z.B. Druck oder Licht) zunächst in der Lage sind einen Angriff zu erkennen und um anschließend darauf aktiv von Selbstabschaltung bis hin zur Selbstzerstörung reagieren zu können.

Organisatorische Sicherheit

Alle oben aufgeführten rein technischen Schutzmaßnahmen sind allerdings wertlos, wenn nicht gleichzeitig auch alle mit einer Schutzmaßnahme verbundenen organisatorischen Prozesse und Strukturen über den gesamten Lebenszyklus eines Fahrzeugs von der Entwicklung, über Herstellung und Betrieb bis zur Verschrottung wirksam abgesichert werden können. Nur so kann verhindert werden, dass eine technisch an sich perfekte Sicherheitslösung beispielsweise durch „soziale Manipulationen“ (social hacking) oder schlicht durch Unachtsamkeit kompromittiert werden kann. Soziale Manipulationen, welche auf typisch menschlichem Verhalten und typisch menschlichen Eigenschaften beruhen, sind beispielsweise fingierte Telefonanrufe oder E-Mails mit vorgetäuschten Identitäten und erfundenen Szenarien, welche um Passwörter oder die Zusendung geheimer Informationen bitten, falsche Handwerker oder Servicekräfte, welche sich in Büros schmuggeln um kritische Daten zu stehlen, bis hin zum gezielten Durchsuchen von Abfallbehältern nach verwertbaren Informationen (dumpster diving).

Neben den finanziellen Verlusten durch aufwändige kostenintensive Nachbesserungen, den Verlust von Betriebsgeheimnissen oder empfindlichen Vertragsstrafen, folgt oft noch ein nachhaltiger Imageschaden und Vertrauensverlust für den Hersteller, sobald eine solche Datenpanne öffentlich bekannt wird [2].

Dabei ist die Durchsetzung von organisatorischer Sicherheit ist im Automobilbereich oft besonders schwierig, da sie nur schwer über die vielen involvierten Personen und Prozesse von Entwicklung, über Produktion, Betrieb und Wartung eines Fahrzeugs hinweg, durchgängig realisierbar ist. Zentrale Komponenten zur organisatorischen Sicherheit sind daher die zuverlässige Identifikation kritischer Informationen und strenge, klar verständliche Sicherheitsrichtlinien (einschließlich Notfallplänen) zum Umgang und zur Weitergabe dieser Informationen, zu Zugriffs- und Zugangsbeschränkungen und zur Geheimhaltung die unter allen Umständen von allen Mitarbeitern über alle Abteilungen hinweg eingehalten müssen. Die Wirksamkeit der Sicherheitsrichtlinien sollte (einschließlich Testangriffen) regelmäßig geprüft und stets den sich ändernden Randbedingungen (z.B. neues Produkt oder neuer Mitarbeiter) angepasst werden, um mögliche Lücken so früh wie möglich zu erkennen und wieder zu schließen.

Fazit

Heute ist die dringende Notwendigkeit von IT-Sicherheit überall in der Automobilbranche akzeptiert und fast alle Automobilhersteller und Zulieferer haben bereits begonnen entsprechende dezidierte IT-Sicherheits-Gruppen neu in ihren Forschungs- und Entwicklungsabteilungen einzurichten. Nichtsdestotrotz ist die automobile IT-Sicherheit noch ein sehr junges Forschungsfeld in dem viele Herausforderungen noch zu meistern sind, von denen aber letztlich alle, also Automobilhersteller, Automobilzulieferer, Verkehrsinfrastrukturbetrieber und natürlich auch alle Automobilnutzer, wie folgt profitieren können:

- Schutz gegen unautorisierte Manipulationen durch externe und interne Angreifer
- Erhöhung der Fahr- und Betriebssicherheit sowie der Zuverlässigkeit von Fahrzeugen
- Sicherstellung der Vertrauenswürdigkeit und Vertraulichkeit im Umgang mit Fahrzeugdaten
- Schutz vor unberechtigten Forderungen im Rahmen der Produkthaftung und Gewährleistung
- Schutz vor Produktfälschungen und Sicherung von gewerblichen Schutz- und Urheberrechten
- Schutz vor unberechtigten Eingriffen an Anwendungen, Daten und Geschäftsmodellen von Herstellern, Zulieferern, Gesetzgeber, Behörden und Drittanbietern

Leider gibt es im Bereich der IT-Sicherheit keine einfachen Standardlösungen, mit denen eine beliebige Fahrzeugkomponente „sicher“ gemacht werden kann. Es können auch nur selten bereits bestehende Sicherheitslösungen für andere Gegebenheiten direkt weiter verwendet werden. Stattdessen sind fast immer wieder sorgfältig individuell angepasste Sicherheitslösungen notwendig, um den besonderen Herausforderungen eines automobilen Lebenszyklus und den auf vielen damit verbundenen praktischen und technischen Einschränkungen

gerecht werden zu können. So erfordert die wirksame Realisierung von IT-Sicherheit für Fahrzeuge eben nicht nur hocheffiziente technische Mechanismen, sondern stets auch eine Vielzahl organisatorischer Maßnahmen, welche eine Sicherheitslösung über den gesamten Lebenszyklus eines Fahrzeugs zuverlässig absichern. Hierbei kann wiederum oft schon eine einzige winzige technische oder organisatorische Schwachstelle ausreichen, um die ganze Sicherheitslösung wertlos zu machen. Das ist ein ganz entscheidender Unterschied im Vergleich zur Umsetzung von anderen technischen Systemen, wo eine einzelne suboptimale Komponente in der Regel nicht gleich das gesamte System wertlos macht. Letztlich bleibt die IT-Sicherheit im Automobil aber vor allem ein außerordentlich interdisziplinäres Gebiet, in dem typischerweise eher theoretisch orientierte Kryptographie- und Sicherheitsexperten mit bisher vor allem praktisch orientierten Ingenieuren zusammentreffen werden. Dies erfordert von beiden Seiten ein stetiges Bemühen um ein gemeinsames Verständnis und eine gemeinsame Sprache zu entwickeln. Die vorliegende Arbeit kann in diesem Sinne auch als erster Brücke gesehen werden, welche versucht IT-Sicherheitsexperten und Automobilingenieure in diesem neuen fachübergreifenden Gebiet erfolgreich miteinander zu verbinden.

Literatur

[1] Manfred Broy. Challenges in Automotive Software Engineering. In *ICSE '06: Proceedings of the 28th International Conference on Software Engineering*, pages 33–42. ACM Press, 2006.

[2] K. Campbell. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3):431–448, 2003.

[3] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

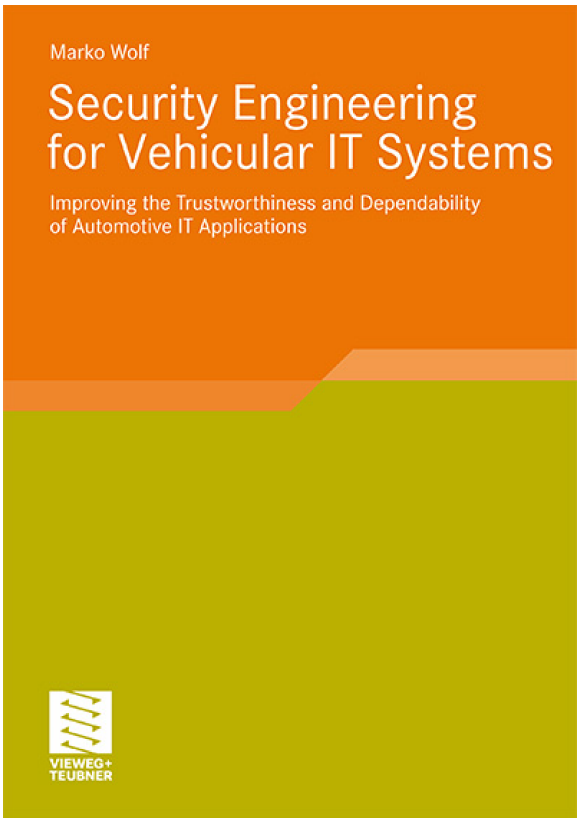
[4] Anne Hahn. Die Tacho-Betrüger. ADAC motorwelt, April 2005.

[5] Annalee Newitz. Hackers Warn Texas of Coming Zombie War. io9.com – Gawker Media Network, January 29, 2009.

[6] Heike Puchan. The Mercedes-Benz A-class Crisis. *Corporate Communications: An International Journal*, 6(1):42–46, 2001.

Veröffentlichung

Die Dissertation wurde im April 2009 mit einem Vorwort von Prof. Dr.-Ing. Christof Paar (Lehrstuhl für Embedded Security, Ruhr-Universität Bochum) im Vieweg+Teubner-Verlag veröffentlicht.



Titel: Security Engineering for Vehicular IT Systems: Improving the Trustworthiness and Dependability of Automotive IT Applications

Autor(en): Wolf, Marko

Taschenbuch: 228 Seiten mit 38 Abbildungen und 21 Tabellen (20,6 x 14,7 x 1,3 cm)

Verlag: Vieweg+Teubner, 1. Auflage, 16. April 2009

Sprache: Englisch

ISBN: 978-3-8348-0795-3

Preis: 49,90 Euro