Elektroautos und IT Security: Sicherheit für alternative Transportsysteme

Christof Paar[1,3] · Jan Pelzl[3] · Andy Rupp[2] · Kai Schramm[1] · André Weimerskirch[1]

[1]escrypt Inc. – Embedded Security, Ann Arbor, MI 48108, USA
{cpaar, kschramm, aweimerskirch}@escrypt.com

[2]University of Massachusetts, Amherst, MA 01030, USA
rupp@ecs.umass.edu

[3]escrypt GmbH – Embedded Security, 44801 Bochum, Deutschland
jpelzl@escrypt.com

Zusammenfassung

Die Nachfrage nach emissionsfreien Fahrzeugen wird aus wirtschaftlichen, ökologischen und politischen Gründen stark ansteigen. Nach der breitflächigen Einführung elektrischer Fahrzeuge werden verschiedene Parteien mit gegenläufigen Interessen, beispielsweise Fahrzeugbesitzer, Energieanbieter und Betreiber von Stromtankstellen, interagieren, wodurch Anreize zu unehrlichem Handeln geschaffen werden. Um Missbrauch zu verhindern werden neue Sicherheitsmechanismen aus den Bereichen Netzsicherheit und eingebettete Sicherheit benötigt. Beispielsweise müssen die Absicherung des Zahlungsverkehrs, die betrugssichere Strommessung sowie der Datenschutz gewährleistet werden. Zusätzlich muss die Infrastruktur abgesichert sein. Dieser Beitrag untersucht zum ersten Mal Bedrohungen in zukünftigen „grünen" intelligenten Verkehrssystemen und analysiert die Vorteile, die IT-Sicherheit in diesem Kontext bietet.

1 Einleitung

Aller Voraussicht nach wird die Verbreitung von Elektrofahrzeugen in Zukunft stark zunehmen. Da ein großer Teil der Treibhausgase in Industrieländern durch PKWs und LKWs verursacht wird, ist die Verringerung von Fahrzeugemissionen ein wichtiger Schritt zur Bekämpfung der globalen Erwärmung. Ein weiteres Problem ist, das Benzinfahrzeuge einen großen Teil der verfügbaren Ölressourcen verbrauchen, was westliche Industrieländer von politisch instabilen Regionen abhängig macht. Ein viel versprechender Ansatz zur umfassenden Senkung des Ölverbrauchs ist die Einführung von Elektrofahrzeuge. Momentan

wird in Europa und in den USA intensiv an entsprechenden Systemen gearbeitet, siehe z.B. [SJMN08, Daim08].

Die Einführung von emissionsfreien Fahrzeugen kommt mit großen technischen Herausforderungen. Insbesondere die Themen Batterietechnologien (Kapazität und Ladezeit) sowie Infrastruktur (Ladestationen, Energienetze) sind wichtige Basisanforderungen. Fortschritte in diesen Gebieten während der letzten Jahre haben zu zahlreichen Feldversuchen und vor kurzem sogar zu kommerziellen Elektrofahrzeugen geführt. Beispielsweise bietet TESLA Motors Fahrzeuge in Israel und verschiedenen US-Bundesstaaten an [TESL].

Während die Herausforderungen bezüglich Batterietechnologie bekannt (wenn auch nicht notwendigerweise umfassend gelöst) sind, werden sich durch den breitflächigen Einsatz von Elektrofahrzeuge auch gänzlich neue technische Probleme stellen. Diese neuen Herausforderungen treten auf, wenn Energieversorger, Betreiber der Infrastruktur, Mittelsmänner, Endverbraucher und Regulierungsbehörden interagieren. Beispielsweise sind zuverlässige und sichere Zahlungssysteme erforderlich, elektrische Energie muss manipulationssicher gemessen werden, und die Verletzungen der Privatsphäre (z.B. Erstellung von Bewegungsprofilen) muss verhindert werden. Zudem ist die Absicherung der Infrastruktur gegen Angriffe von außen zu leisten. Solche Probleme treten weder in Labor- noch in Feldversuchen auf, sondern erst wenn Parteien mit gegenläufigen Interessen in dem System aktiv sind. In solchen Situationen kann unehrliches und schädigendes Verhalten von Teilnehmern auftreten. Um das Funktionieren von zukünftigen Elektrofahrzeugsystemen zu gewährleisten, müssen Methoden der modernen Netzwerksicherung und der eingebetteten Sicherheit herangezogen werden. Während einigen Bedrohungen mit Hilfe etablierter IT-Sicherheitslösungen begegnet werden kann, müssen auch eine Reihe neuer Ansätze entwickelt werden, die die besondere Situation von Elektrofahrzeugsystemen berücksichtigen. Es sollte an dieser Stelle angemerkt werden, dass IT-Sicherheit innerhalb von Fahrzeugen sowie für Car-to-Car und Car-to-Infrastructure Kommunikation im Laufe der letzten Jahre intensiv untersucht worden ist [LePW05, RaPH06]. Alle führenden Fahrzeughersteller besitzen inzwischen Sicherheitsabteilungen, die Embedded Security Lösungen wie beispielsweise sicheres Softwareupdate, Schutz vor Chiptuning und sichere Telematik erarbeiten. Die Absicherung zukünftiger Systeme von Elektrofahrzeugen stellt ein neues wichtiges Problem dar.

Dieser Beitrag analysiert die Security-Aspekte der nächsten Generation elektrischer Transportfahrzeugsysteme und diskutiert Lösungsmöglichkeiten. Es ist wichtig zu betonen, dass Sicherheit früh im Systementwurf berücksichtigt werden muss. Zahlreiche Beispiele haben gezeigt, dass die spätere Einführung von Sicherheitsfunktionen in bereits vorhandenen Systemen in der Regel eine sehr schwierige Aufgabe ist, die oft gar nicht oder nur sehr unbefriedigend gelöst werden kann. Das prominenteste Beispiel sind die zahlreichen fehlgeschlagenen Versuche, das Internet durch Sicherheitsprotokolle wie IPsec und DNSSEC großflächig abzudecken. Zurzeit sind uns keine Arbeiten bekannt, die das zukünftige Thema von IT-Sicherheit in elektrischen Verkehrssystemen behandeln.

2 Herausforderungen

Im Nachfolgenden werden Anforderungen an die Sicherheit zukünftiger elektrischer Transportsysteme beschrieben und Lösungen skizziert.

2.1 Sichere Zahlungssysteme und Datenschutz

Elektrische Fahrzeuge müssen aufgeladen oder ihre leeren Batterien durch aufgeladene ersetzt werden. Dies kann an speziellen Ladestationen, die mit heutigen Tankstellen vergleichbar sind, geschehen. Alternativ können die Batterien zu Hause, am Arbeitsplatz oder an einem öffentlichen Ort (z.B. Parkhaus) geladen werden, wie es zum Beispiel von Coulomb Technologies [Coul] vorgeschlagen wird. Ebenso sind Wechselstationen für Fahrzeugbatterien denkbar, wie es von Better Place [Bett] propagiert wird, möglich. Eine essentielle Voraussetzung für derartige E-Car-Infrastrukturen sind zuverlässige und sichere Zahlungssysteme, die sowohl den Endverbraucher als auch den Anbieter schützen.

Ähnlich wie bei der Bezahlung im öffentlichen und individuellen Personenverkehr, gibt es triftige Gründe für den Einsatz elektronischer Zahlungssysteme im Gegensatz zu Bargeld-basierten Systemen. Die wichtigsten Vorteile sind deutlich verringerte Kosten, erhöhte Kundenzufriedenheit, verbesserte Dienstleistungen für den Kunden, effizientere betriebliche Prozesse und die Möglichkeit einer flexibleren und dynamischeren Preisgestaltung. Ein Ansatz für die Umsetzung eines solchen Zahlungssystems bestünde in der Nutzung von existierenden Kreditkartensystemen, wie sie heute von Tankstellen genutzt werden. Obwohl diese Systeme verbreitet sind, weisen sie für Elektrofahrzeugsysteme eine Reihe von Schwachstellen auf. Es gibt, gerade in Deutschland, noch viele Personen, die eine Nutzung von Kreditkarten ablehnen (z.B. aus Datenschutzgründen) oder keine Kreditkarte besitzen. Dieser Personenkreis kann natürlich nicht von der Nutzung von Elektrofahrzeugen ausgeschlossen werden. Darüber hinaus weisen Kreditkartensysteme einen Mangel an Verfahren zum Datenschutz auf.

Eine andere Alternative sind verkehrsspezifische Zahlungssysteme, wie sie im Bereich des öffentlichen Nahverkehrs Anwendung finden. Die CharlieCard [MBTA] der Massachusetts Bay Transportation Authority (MBTA) oder der E-ZPass [EZPa] in den USA sind Beispiele für weit verbreitete Systeme. Bedauerlicherweise können diese Systeme gleichzeitig als Paradebeispiele für die ernsthaften Sicherheitsmängel in heutigen elektronischen Zahlungssystemen herangezogen werden. Ein großes Problem ist dabei der Einsatz proprietärer Verschlüsselungsalgorithmen, die häufig fehlerhaft sind, wie es das Beispiel der CharlieCard in Boston oder der Oyster-Card in London [NESP08, GaHG08] gezeigt hat. Weitere Sicherheitsanalysen, wie zum Beispiel ein Kursprojekt dreier Studenten des Massachusetts Institute of Technologie (MIT), das Schwachstellen des MBTA-Systems aufdeckte [RyAC08], lassen auch den Schluss zu, dass heutige derartige Zahlungssysteme noch nicht ausgereift sind. Neben Sicherheitsmängeln werden auch regelmäßig Datenschutzprobleme solcher Systeme aufgedeckt. Ein besonderes Problem besteht darin, die Vertraulichkeit des Aufenthaltsortes und der Bewegungen von Benutzern innerhalb des Transportsystems („location privacy“) zu schützen. In der Vergangenheit wurden beispielsweise Aufzeichnungen des E-ZPass-Systems von Anwälten benutzt, um in Scheidungsverfahren zu beweisen, dass die Ehemänner ihrer Mandantinnen sich zu bestimmten Zeitpunkten nicht an denen von ihnen angegebenen Orten befunden haben

[Hage07]. Diese Beispiele zeigen, dass (i) heutige Systeme kaum Datenschutz gewährleisten und (ii) diese Schwachstellen in fragwürdiger Weise ausgenutzt werden können. Datenschutz ist eine besonders komplexe Thematik, da hier kryptographische und technische sowie politische und soziale Fragestellungen auftreten. Angemessene Sicherheits- und Datenschutzmechanismen sind jedoch eine notwendige Voraussetzung für den weitflächigen Einsatz und die Akzeptanz elektronischer Bezahlsysteme. Eine Studie über Teilnehmer automatischer Mautsysteme hat jüngst gezeigt, dass vor allem ein höheres Maß an Sicherheit und Datenschutz gewünscht wird [Rile08].

Fahrzeuge sind eng an ihre Nutzer gebunden, so dass eine Feststellung des Fahrzeugstandorts weitreichende Informationen über den Fahrzeugnutzer preisgibt und die Erstellung von Profilen erlaubt. Solche Profile können Informationen über Fahr- sowie Benutzerverhalten enthalten. Beispielsweise könnte festgestellt werden, dass ein Fahrer jeden Dienstagabend im Rotlichtviertel seine Fahrzeugbatterien auflädt, während seine Frau ihr Fahrzeug jeden Dienstagabend an der Volkshochschule auftankt. Die Gefährdung der Privatsphäre sollte daher besonders betrachtet werden. Die potentiellen Angreifer können wie folgt klassifiziert werden: (1) Einzelpersonen, (2) Unternehmen und (3) Regierungen und Behörden. Einzelne Personen haben ggf. das Interesse, Informationen über andere Teilnehmer zu erhalten. Zudem könnten sie das System aus Neugierde oder wegen der Herausforderung angreifen. Unternehmen könnten aus wirtschaftlichen Gründen Interesse daran haben, Benutzerprofile zu erstellen. In der Regel beachten Unternehmen rechtliche Vorgaben, wobei das Ausnutzen rechtliche Lücken jedoch nicht auszuschließen ist. Der Gesetzgeber hat hier die Möglichkeit, Vorgaben zu schaffen. Als dritte Partei können Behörden Interesse daran haben, den Datenschutz zum Beispiel für die Strafverfolgung zu verletzen („Big Brother“ Problematik). Daher ist es notwendig, den rechtlichen Rahmen für Unternehmen und Behörden exakt zu bestimmen, und technische Lösungen anzubieten, die Angriffe auf den Datenschutz verhindern.

Allgemein kann gesagt werden, dass der Schutz des Endnutzers bei dem Design und der Umsetzung kommerzieller Systeme häufig vernachlässigt wird, wohingegen oft ein deutlich größerer Aufwand zum Schutz der Interessen des Systemanbieters betrieben wird. Daher ist es besonders wichtig, dass Mechanismen zum Schutz des Endnutzers vor der breitflächigen Einführung von Elektroautos entwickelt und getestet werden. Für den Datenschutz müssen insbesondere die folgenden beiden Aspekte berücksichtigt werden: (1) Technologische Verfahren müssen im Fahrzeug umgesetzt und durch die Infrastruktur unterstützt werden, und (2) die Gesetzgebung und die Systemanbieter müssen klare Richtlinien zum Schutz der Privatsphäre der Fahrzeugnutzer schaffen. Technische Maßnahmen schützen tendenziell vor Angriffen von Einzelpersonen, wohingegen rechtliche Vorgaben gegen Missbrauch von Unternehmen und Behörden schützen.

Aufgrund der beschriebenen Sicherheits- und Datenschutzprobleme ist eine 1-zu-1 Übernahme vorhandener Zahlungssysteme für zukünftige alternative Transportsysteme nicht geeignet. Daher scheint es sinnvoll zu sein, neue Systeme zu entwickeln, die umfassende Möglichkeiten zum einfachen und effizienten Bezahlen für intelligente Transportsysteme ermöglichen. So genannte multi-modale Systeme, die für das Aufladen von Elektroautos, die Nutzung von öffentlichen Verkehrssystemen, Parkgebühren, Straßenmaut, Benzin (für Hybridfahrzeuge) und ggf. auch für Kleineinkäufe geeignet sind, sind besonders attraktiv. Um

die Akzeptanz zu erhöhen, sollte ein neues Bezahlsystem eine Vielfalt an Schnittstellen wie kontaktlose und kontaktbehaftete Smartkarten und NFC Telefone unterstützen.

Die beschriebenen Herausforderungen können mit Methoden der modernen Kryptographie überwunden werden können. In der Literatur finden sich zahlreiche Arbeiten, die Zahlungssysteme – vorwiegend für Anwendungen im e-Commerce – mit starken Sicherheit- und Datenschutzeigenschaften beschreiben. Die Basis für kryptografische Protokolle dieser Art hat Chaum 1982 in seiner grundlegenden Arbeit [Chau82] gelegt, indem er das Konzept der „blind signature“ einführte. Diese kann z.B. mit Hilfe der Algorithmen RSA, ECDSA oder DSS realisiert werden [FIPSa].

In den letzten 20 Jahren wurden zahlreiche e-Cash Protokolle entwickelt. Ein wichtiges Ergebnisse ist, dass es sichere offline Zahlungssysteme gibt (d.h. Systeme, die keine permanente Verbindung zu Servern der Bank zum Durchführen einer Transaktion benötigen), die die Anonymität der Benutzer im Normalfall wahrt. Sobald ein Benutzer jedoch versucht, das System zu unterwandern, kann die Identität des Benutzers enthüllt werden. Ein guter Überblick zu e-Cash Systemen ist in [AJSW97, SaSc03] zu finden. Es ist wahrscheinlich, dass einige bisherige Ansätze für die hier vorliegende Anwendung übernommen werden können, wohingegen andere Komponenten neu entwickelt werden müssen, um den besonderen Anforderungen zu genügen.

2.2 Sichere Energiemessung

Wie das Benzin für konventionelle Fahrzeuge, wird die elektrische Energie für Elektrofahrzeuge einen großen wirtschaftlichen Wert darstellen. Das genaue und zuverlässige Messen elektrischer Energie ist ein etabliertes Thema, für das es zahlreiche Lösungen gibt. Allerdings wird künftig die Absicherung der Messergebnisse gegen bösartige Manipulation eine bedeutende Rolle für elektrische Transportsysteme spielen. Da elektrische Energie im Gegensatz zu Benzin nicht sichtbar ist und ein kaum messbares physikalisches Gewicht hat, es ist schwierig, die tatsächliche Menge der gelieferten elektrischen Energie manipulationssicher nachzuweisen. Diese Anforderung wird noch dringlicher werden, wenn spezielle Preisstrukturen für den Strom für Autobatterien eingeführt werden wird. Sowohl Preise, die niedriger als die Haushaltsstrompreise sind (als Anreiz für grüne Autos), als auch höhere Preise (als Ausgleich für Ausfälle bei der der Benzinsteuer) sind zukünftig denkbar.

Es ist interessant, das Angreifermodell in diesem Kontext zu diskutieren. Zunächst ist festzustellen, dass für nahezu alle involvierten Parteien ein Anreiz zum unehrlichen Verhalten existiert. Der Besitzer hat einen Anreiz, weniger Energie als er tatsächlich erhalten hat, zu melden. Der Energieversorger hat möglicherweise das umgekehrte Interesse, nämlich mehr Energie in Rechnung zu stellen, als tatsächlich zur Verfügung gestellt wurde. Durch die zunehmende Liberalisierung und dem Aufsplittern des Energiemarktes wird die Wahrscheinlichkeit von widerrechtlichem Verhalten der Versorger größer. Betreiber von Stromtankstellen könnten potentiell beide vorgenannten Parteien durch inkorrekte Messungen betrügen. Es wird vermutlich noch weitere Parteien zwischen Energieversorger und Ladestationen geben. Ein weiterer Teilnehmer, der betroffen sein könnte, ist die Regierung, sobald spezielle Steuern auf den Verbrauch von Autostrom erhoben werden. Es ist nicht unwahrscheinlich, dass dies in Zukunft der Fall sein wird, um den Ausfall von Benzinsteuern aufzufangen. Schon heute gibt es in den USA Schäden aufgrund unbezahlter Benzinsteuern, die zumindest zum Teil durch organisiertes Verbrechen verursacht werden.

Wir werden nun Methoden zur manipulationssicheren Energiemessung diskutieren. Diese Aufgabe stellt eine besondere Herausforderung dar, da die Ladestationen vollkommen durch den Eingreifer kontrolliert werden, beispielsweise den Betreiber der Stationen oder den Autobesitzer selber, wenn dieser zu Hause auflädt. Um starken Schutz gegen Manipulation zu gewährleisten, sind drei Komponenten nötig, die auf eingebetteten Sicherheitstechnologien basieren. Zunächst sollten die Energiemessdaten innerhalb der Aufladestation digital signiert werden. Durch digitale Signaturen wird sichergestellt, dass die Daten später nicht manipuliert werden können, solange ein Angreifer keinen Zugang zu dem privaten kryptographischen Signaturschlüssel hat. Signaturalgorithmen sind sehr rechenintensiv. Da in einer Ladestation aber nur im Minutenbereich Signaturen erstellt werden müssen, sollten auch kleine eingebettete CPUs über genügend Rechenressourcen verfügen. Mögliche Signaturalgorithmen sind ECDSA, RSA oder DSS [12], wobei elliptische Kurven (ECDSA) aufgrund ihrer niedrigen Komplexität und kurzen Bitlängen besonders interessant sind.

Die zweite Komponente ist die enge Verbindung des in Software oder Hardware realisierten Signaturmoduls mit der Energiemessschaltung. Wenn dies nicht der Fall ist, könnten die Werte der analogen Messung auf dem Weg zum Signaturmodul manipuliert werden. Selbst wenn beide ICs auf der gleichen Platine innerhalb der „Zapfsäule“ platziert sind, sind Manipulationen der Daten möglich. Diese so genannten Modchip-Angriffe werden regelmäßig gegen Pay-TV oder Videospiel-Konsolen wie zum Beispiel Xbox durchgeführt [XbLi]. Um solche Angriffe zu verhindern, muss das Messmodul entweder in einem einzigen IC mit der Signatureinheit integriert werden, oder beiden Module müssen in einem manipulationssicheren („tamper resistant“) Gehäuse realisiert werden. Ähnliche Fragestellungen werden im Zusammenhang von Trusted Computing und anderen eingebetteten Sicherheitssystemen diskutiert. Die dritte Sicherheitskomponente gewährleistet, dass die Messdaten abhörsicher übertragen werden. Obwohl nicht für jede Anwendung erforderlich, wird es oft erforderlich sein, dass die Daten nicht nur durch eine digitale Signatur gegen Veränderungen gesichert sind, sondern auch verschlüsselt, z.B. während der Übertragung zum Versorgungsunternehmen. Insbesondere wenn die Messdaten mit Zahlungsinformationen verknüpft werden, ist die Verschlüsselung eine zwingende Notwendigkeit. Um einen abhörsicheren Kommunikationskanal zu erreichen, können symmetrische Algorithmen wie der Advanced Encryption Standard (AES) eingesetzt werden [FIPSb].

Sowohl die digitale Signatur wie auch die symmetrische Verschlüsselung basieren auf kryptographischen Schlüsseln, die auslesesicher innerhalb der Messstation gespeichert werden müssen. Es existieren eine Reihe Methoden für die sichere Schlüsselspeicherung in eingebetteten Geräten, z.B. auf Smart Cards oder im Bankenwesen. Einer der anspruchsvollen Aspekte des Systems ist die Schlüsselverwaltung. Augrund der verteilten Natur erscheint eine Public-Key-Infrastruktur (PKI) ein viel versprechender Ansatz. Mit Hilfe einer PKI können die öffentlichen Schlüssel zur Prüfung digitaler Signaturen sowie zur Erzeugung von symmetrischen Sitzungsschlüsseln global bereitgestellt werden.

Es muss sichergestellt werden, dass die beschriebenen Sicherheitsmaßnahmen in den Ladestationen auch tatsächlich umgesetzt werden. Im Falle von konventionellen Zapfsäulen müssen diese geeicht und zugelassen werden, wodurch die Manipulationssicherheit der Treibstoffmessung gewährleistet wird. Für Stromladestationen bietet sich an, dass Evaluierungen nach dem Common Criteria Standard gefordert werden [CoCr]. Hier wird es

wichtig sein, das sogenannte Security Target korrekt zu definieren. Abschließend sollte erwähnt werden, dass Lösungen zur digitalen Absicherung der Strommessungen im Haushalt existieren, z.B. das SELMA Projekt [SELM].

2.3 Grüne Fahrzeuge und kritische Infrastrukturen

Elektrofahrzeuge werden auf eine Infrastruktur für das Aufladen und den Austausch der Batterien angewiesen sein. Diese wird aus vernetzten intelligenten Aufladestationen, dezentralen und zentralen Stromkraftwerken (wobei konventionelle und „grüne“ Alternativenergien möglich sind) und möglicherweise auch Stationen zum Batteriewechsel bestehen. Es kann davon ausgegangen werden, dass aus Gründen der intelligenten Energieverteilung, für Bezahlsysteme oder auch für die Verkehrslenkung diese Infrastruktur auch stark digital vernetzt sein wird. Hierdurch wird allerdings das ganze System auch gegen Angriffe von außen oder innen verwundbar. Insbesondere externe Parteien wie Terroristen, ausländische Regierungen oder Hacker ohne politische Motivation zählen zu den möglichen Angreifern.

Die Fragestellung der Absicherung von umfassenden Systemen mit wichtiger Bedeutung für das staatliche Gemeinwesen wird als Schutz kritischer Infrastrukturen (KRITIS) bezeichnet. Das Thema KRITIS wird insbesondere seit dem 11. September 2001 intensive diskutiert. Eine gute Einführung ist in [Lewi06] zu finden. In Deutschland gehören beispielsweise die Sektoren Transport und Verkehr, Energie und Finanzwesen zu den kritischen Infrastrukturen. Im Falle von elektrischen Verkehrssystemen ergeben sich neue Gefahren. Zum einen besteht hier eine enge Kopplung zwischen den beiden (getrennten) Infrastrukturen Energie einerseits und Transport und Verkehr andererseits. Zum anderen hängen von dem Transportsektor nicht nur der Privatverkehr sondern auch die Logistik ab, die wiederum für viele andere Bereiche kritisch ist. Aus Sicht der kritischen Infrastruktur ist es neben dem privaten Transportsektor ebenfalls wichtig, dass die für ein Land notwendige Logistik nicht zusammenbricht. Daher sollte die Nichtverwundbarkeit gegen systemweite Angriffe bei dem Entwurf der Infrastruktur für Elektrofahrzeuge berücksichtigt werden.

3 Zusammenfassung und Ausblick

Intelligente Elektrofahrzeuge versprechen eine Vielfalt von Vorteilen für die Gesellschaft und den Einzelnen. Momentan laufen eine Reihe Feldversuche, und die großflächige kommerzielle Einführung in naher Zukunft erscheint wahrscheinlich. Das Verhalten der Teilnehmer, die zum Teil gegenläufige Interessen verfolgen, wurde bisher nicht berücksichtigt. Um gezielten Missbrauch zu verhindern, müssen Methoden der modernen IT-Sicherheit und der eingebetteten Sicherheit in elektrische Fahrzeugsysteme integriert werden. Die benötigten Mechanismen reichen von kryptographischen Modulen für Aufladestationen und Batterien über Protokolle für sichere Zahlungssysteme bis hin zu einer Betrachtung des Versorgungsnetzwerkes als kritische Infrastruktur. Dieser Beitrag ist ein erster Schritt in diese Richtung.

Wir empfehlen eine detaillierte Analyse der Schwachstellen und die Entwicklung von Sicherheitslösungen, die die kommerziellen und technischen Rahmenbedingungen in Betracht ziehen. Da das Nachrüsten von Sicherheitsmechanismen in der Regel mit erheblichen

Schwierigkeiten verbunden ist, muss eine Betrachtung der Security-Aspekte in einem frühen Stadium erfolgen.

Literatur

[AJSW97] N. Asokan, Phillipe A. Janson, Michael Steiner, and Michael Waidner. The state of the art in electronic payment systems. Computer, 30(9):28-35, 1997.

[Bett] Better Place, Inc. http://www.betterplace.com.

[Chau82] David Chaum, Blind Signatures for Untraceable Payments, In Advances in Cryptology – CRYPTO 1982, 199-203.

[CoCr] The Common Criteria, http://www.commoncriteriaportal.org/thecc.html

[Coul] Coulomb Technologies, Inc. http://www.coulombtech.com.

[Daim08] Daimler Announcement. E-Mobility Berlin: Daimler and RWE Embarking on the Age of Electro-Mobility. September 2008, http://www.daimler.com/dccom/0-5-7153-1-1125767-1-0-0-0-0-0-9293-7145-0-0-0-0-0-0-0.html.

[EZPa] E-ZPass Interagency Group (IAG), E-ZPass, http://www.ezpass.com/

[FIPSa] FIPS-186-2, Digital Signature Standard

[FIPSb] FIPS 197, Advanced Encryption Standard

[GaHG08] Gerhard Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the Mifare Classic. Proceedings of CARDIS ’08: Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications, 267–282, Springer-Verlag, 2008.

[Hage07] Christina Hager (WBZ-TV.com). Divorce Lawyers Using Fast Lane to Track Cheaters. http://msl1.mit.edu/furdlog/docs/2007-08-10_wbz_fastlane_tracking.pdf.

[LePW05] Kerstin Lemke, Christof Paar, Marko Wolf. Embedded Security in Cars: Securing Current and Future Automotive IT Applications. Springer-Verlag, 2005.

[Lewi06] Ted Lewis. Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Wiley&Sons, 2006.

[MBTA] Massachusetts Bay Transportation Authority, CharlieCards & Tickets, http://www.mbta.com/fares_and_passes/charlie/

[NESP08] Karsten Nohl, David Evans, Starbug, and Henryk Plotz. Reverse-Engineering a Cryptographic RFID Tag. Proceedings of the 17th USENIX Security Symposium, 185–194, 2008.

[RaPH06] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing Vehicular Communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006.

[Rile08] Patrick F. Riley. The Tolls of Privacy: An Underestimated Roadblock for Electronic Toll Collection Usage, 24(6):521-528, 2008. [TESL] TESLA Motors. http://www.teslamotors.com.

[RyAC08] Russell Ryan, Zach Anderson, and Alessandro Chiesa. Anatomy of a subway hack. Angenommener Beitrag auf der DEFCON, der durch Gerichtsbeschluß verhinder wurde, 2008, http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf

[SaSc03] Ahmad-Reza Sadeghi and Markus Schneider. Electronic payment systems, Digital Rights Management, volume 2770 of Lecture Notes in Computer Science, pages 113-137, Springer, 2003.

[SELM] SELMA – Sicherer ELektronischer Messdaten-Austausch, http://www.selma-project.de/index.html

[SJMN08] San Jose Mercury News. Bay Area Mayors endorse $ 1 Billion Plan for Electric Cars. November 2008, http://www.mercurynews.com/business/ci_11032113.

[XbLi] The Hidden Boot Code of the Xbox, Xbox Linux, http://www.xbox-linux.org/wiki/The_Hidden_Boot_Code_of_the_Xbox.