

Pressemitteilung (Langfassung)

IT-Sicherheit meets Elektromobilität

Mit dem Projekt SecMobil zum weltweiten Vorreiter in dem Bereich IT-Sicherheit für Elektromobilität

Elektromobilität ist in aller Munde und viele Politiker bekennen Farbe zu dem elektrischen fahrbaren Untersatz der Zukunft. Technische Entwicklungen zur Elektromobilität werden in vielen deutschen Unternehmen mit Hochdruck vorangetrieben. Das „Secure eMobility“-Konsortium (bestehend aus Automobilhersteller, Zulieferer und Forschungseinrichtungen) hat erkannt, dass bei den heutigen Entwicklungen und Feldversuchen im Bereich der Elektromobilität der Aspekt der IT-Sicherheit nicht ausreichend behandelt wird. Mit der Unterstützung des Bundesministeriums für Wirtschaft und Technologie (BMWi) wird das „Secure eMobility“-Konsortium entsprechende IT-Sicherheitstechnologie für Elektromobilität entwickeln und die deutsche Vorreiterrolle sichern.

Wenn Bundeskanzlerin Angela Merkel von Elektromobilität spricht, fallen immer wieder Worte wie „Leitmarkt“ und „Leitanbieter“ [1]. Deutschland -weltweit führend im Bereich Automotive - rüstet sich für die Elektromobilität und will auch in diesem Bereich seine Führungsrolle behaupten. Die nationale Plattform Elektromobilität wird hierzu entsprechende Rahmenbedingungen schaffen [2]. Frau Merkel ist überzeugt, dass Deutschland auch in dem Bereich der Elektromobilität an die herausragenden Fähigkeiten der deutschen Automobilhersteller anknüpfen kann. Merkel: "Es gibt hierzu bereits eine Reihe von Modellversuchen, und die müssen zügig weiterentwickelt werden." [1].

Elektrifizierung von Automobilen wird zu weitgehenden Veränderungen in der gesamten automobilen Wertschöpfungskette führen. Schon heute stellt sich die Fahrzeug- und Zulieferindustrie darauf ein, aber der Wandel wird auch Auswirkungen auf andere Industriebranchen wie die Energie- und Informations- und Kommunikations- (IKT)-Branche haben. Elektrofahrzeuge werden über entsprechende Schnittstellen in das Stromversorgungs-System eingebunden und damit Teil eines intelligenten Verkehrssystems. Diese zukünftigen Automobile werden z.B. gekennzeichnet sein durch stärkere Kommunikation untereinander.

Auf dem Weg zur Elektromobilität werden oft zwei große Herausforderungen genannt: Batterieherstellung und Schaffung einer Infrastruktur zum Laden der Batterien. Allerdings sind offene Standards, Modularität und Datensicherheit (IT-Sicherheit) weitere unabdingbare Voraussetzungen für das erfolgreiche Einführen und Betreiben von der Elektromobilität.

Warum IT-Sicherheit für Elektromobilität?

IT-Sicherheit ist eine Querschnittstechnologie, die in allen Komponenten eines Systems vorhanden sein muss. In der Elektromobilität bedeutet dies, dass weder eine alleinige Absicherung des Fahrzeugs noch der Serversysteme ausreicht. Hingegen müssen alle Komponenten von Smart Car, Smart Grid und Smart Traffic bezüglich der Sicherheit holistisch betrachtet, standardisiert und (unternehmens-) übergreifend umgesetzt werden.

Durch die Einbindung in die bestehenden Energienetze werden Elektrofahrzeuge in viel stärkerem Ausmaß als konventionelle Fahrzeuge mit ihrer Umwelt kommunizieren, wodurch auch zusätzliche Dienste und somit auch weitere Probleme in Bezug auf IT-Sicherheit zu erwarten sind. Es wird eine völlig neue Fahrzeugarchitektur basierend auf Informations- und Kommunikationstechnologie (IKT) möglich bzw. erforderlich werden. Mit der Einführung von IKT im Elektromobilbereich ist allerdings eine inhärente Erhöhung des Missbrauchspotentials verbunden, welche von Schäden individueller Akteure bis hin zu kompletten Systemausfällen reichen kann.

Des Weiteren besteht eine starke Abhängigkeit zu der Infrastruktur (Smart Grid), welche gegen neuartige Angriffe geschützt werden muss, damit eine zuverlässige Energieverteilung und Abrechnung jederzeit funktioniert. Im Gespräch mit Prof. Dr. Christof Paar von der Ruhr-Universität Bochum sagte dieser: „Erst unlängst haben die Fälle des Stuxnet-Virus, welcher zu der Zerstörung von Hochgeschwindigkeitszentrifugen durch Schadsoftware führte, oder der Playstation-Angriff, durch welchen mehrere 10 Millionen Kunden- und Kreditkarteninformationen kompromittiert wurden, gezeigt, welchen erhebliche finanzielle und politische Schaden nicht optimal abgesicherte IKT-Systeme haben können.“ Weiter berichtete der Wissenschaftler: „Im Jahr 2010 haben Wissenschaftler in den USA demonstriert, welche dramatischen Folgen IT-Angriffe gegen die Bordelektronik im Fahrbetrieb haben können, wie z.B. Vollbremsung.“ Im Kontext der Elektromobilität ist der Umstand hervorzuheben, dass ein Teil der Angriffe keine PC-Systeme sondern vernetzte eingebettete Systeme zum Ziel hatten, die auch in der Elektromobilität eine zentrale und durch die Einbindung in Energieinfrastrukturen sogar noch eine größere Rolle spielen.

Der Geschäftsführer der Firma ESCRYPT GmbH – Embedded Security Dr. Thomas Wollinger, machte Hoffnung, dass entsprechende Bedrohungen durch entsprechende Entwicklungen abgeschwächt werden können: „Während einigen Bedrohungen mit Hilfe etablierter IT-Sicherheitstechnologien begegnet werden kann, müssen für die Elektromobilität als Ganzes jedoch umfangreiche, übergreifende und standardisierte Lösungen auf System-, Domain- und Modulebene entwickelt werden“. Aus diesem Grunde hat die ESCRYPT GmbH in Bochum im Zusammenspiel mit einigen Partnern den Förderantrag Secure eMobility (SecMobil) gestellt. Herr Dr. Jan Pelzl (Geschäftsführer der ESCRYPT GmbH – Embedded Security) fügte ergänzend dazu: „Ein wesentlicher Aspekt der Vertrauenswürdigkeit von IT-Systemen ist die Verfolgung eines ganzheitlichen Ansatzes. Für einen Angreifer reicht eine einzige Schwachstelle, um sein Ziel zu erreichen und das System zu kompromittieren.“

Das Bundesministerium für Wirtschaft und Technologie (BMWi) will mit dem Technologiewettbewerb "IKT für Elektromobilität II" ausgewählte Forschungs- und Entwicklungsaktivitäten (FuE-Aktivitäten) sowie Piloterprobungen zur beschleunigten Entwicklung und breitenwirksamen Nutzung ganzheitlicher, auf Informations- und Kommunikationstechnologien gestützter Konzepte der Elektromobilität fördern.

Das SecMobil-Konsortium, wird sich im „IKT für Elektromobilität II“ Programm übergreifend um die Konzeption und Umsetzung sowie die juristische Betrachtung der IT-Sicherheit kümmern. Das Konsortium besteht aus ESCRYPT GmbH – Embedded Security, Daimler AG, Elmos AG, smartlab Innovationsgesellschaft mbH, Ruhr-Universität Bochum und FH Gelsenkirchen. Die Konsortialführung wird die ESCRYPT GmbH – Embedded Security übernehmen.

Gesamtziel des Projektes SecMobil

Aufgrund der starken Abhängigkeit der Elektromobilität von IKT-Systemen kommt der modernen IT-Sicherheit eine langfristige Bedeutung als Querschnittstechnologie zu. Alle Akteure werden in der nächsten Evolutionsphase der Elektromobilität großes Interesse an vertrauenswürdigen Lösungen haben. Gleichzeitig ist das Thema der Datensicherheit in der Elektromobilität bisher kaum behandelt worden. Thomas Wollinger betonte: „Die Ausgangssituation hierfür ist besonders gut, da Deutschland sowohl über eine sehr hohe Kompetenz in der Fahrzeug- und Energietechnologie, als auch im Bereich IT-Sicherheit verfügt.“

Wichtig ist bei einer Betrachtung der wirtschaftlichen Aspekte auch, dass die IT-Sicherheit eng mit Geschäftsmodellen verknüpft ist und juristisch untersucht wird. Von daher eröffnet das vorliegende Projekt nicht nur die Möglichkeit kritische Sicherheitstechnologien zu pilotieren, sondern auch neue Geschäftsmodelle zu entwickeln, welche durch die zugrundeliegende IT-Sicherheit nachhaltig stabilisiert werden. Das Marktpotential der durch IT-Sicherheit nachhaltig gestützten Elektromobilität eröffnet sich durch die folgenden in dem Projekt zu entwickelnden Technologien:

- Technologien zur vertrauenswürdigen kostengünstigen Stromerfassung (im Elektromobilitätsbereich, aber auch in Haushalts- und Industrieanwendungen)
- Security-Basistechnologien im Fahrzeug, um Zusatzdienste wie bspw. Funktionsfreischaltung, Application Store, Identifikation mit dem neuen Personalausweis und Software-Updates und damit neue Geschäftsmodelle zu ermöglichen.
- Security-Basistechnologien für die Infrastruktur und für Dienste (PKI, ID-Management, usw.) um z.B. Identitätsmanagement und Abrechnungsvorgänge zwischen den verschiedenen Domänen (Smart Car, Smart Grid, Smart Traffic) zu pilotieren.

Projektlaufzeit: 1.1.2012 – 31.08.2014

Kontakt: Konsortialführer ESCRYPT GmbH –Embedded Security, info@secmobil.com, +49 234 43870219

[1] <http://www.bundesregierung.de/Content/DE/Artikel/2011/05/2011-05-14-podcast.html>

[2] http://www.bmu.de/verkehr/elektromobilitaet/nationale_plattform_elektromobilitaet/doc/45970.php