SECURING GREEN CARS:
IT SECURITY IN NEXT-GENERATION ELECTRIC VEHICLE SYSTEMS

Christof Paar[1,2,a], Andy Rupp[2], Kai Schramm[1], André Weimerskirch[1],
and Wayne Burleson[2]

[1]escrypt Inc – Embedded Security, Ann Arbor, MI 48108, USA

[2]ECE Department, University of Massachusetts at Amherst, Amherst, MA 01003, USA

{kschramm, aweimerskirch}@escrypt.com, {cpaar, rupp, burleson}@ecs.umass.edu

ABSTRACT

Due to economic, environmental and political reasons, there is an increasing demand for zero-emission vehicles. With the wide-scale deployment of electric car systems, a variety of parties with conflicting interests will be interacting, and there will be incentives for dishonest behavior. As a consequence, new technical challenges which are related to IT security and embedded security arise in the context of electric vehicle systems. For instance, payment and metering needs to be secured, privacy needs to be preserved, and the infrastructure needs to be protected. This work investigates for the first time the security threats that must be addressed in intelligent transportation systems, discusses possible solutions, and presents the benefits that IT security provides in this context

Keywords: Embedded security, electric vehicles, secure payment, secure metering, privacy, critical infrastructure

INTRODUCTION

It is likely that we are at the beginning of a massive deployment of electric vehicles. Since cars and trucks are responsible for a significant amount of the greenhouse gas emission in industrialized nations, the reduction of vehicle emission is a crucial part to curb global warming. Moreover, traditional gasoline-based cars and trucks consume a considerable part of the available oil resources, and make the USA and Europe dependent on political unstable regions. One key approach to a dramatic reduction in oil consumption is the introduction of electric vehicles. The USA is currently preparing large steps in this direction, as are several European countries, e.g., see (8)(9).

The large-scale introduction of emission-free vehicles comes with technological and economic challenges. In particular, battery technology (e.g., battery capacity and charge time) and the infrastructure (e.g., charge stations and grid), are essential prerequisites for a massive deployment. However, many core technologies have sufficiently advanced, so that by now numerous field trials are being conducted and, most recently, even commercial offerings of purely electric vehicles took place. For instance, TESLA Motors offers approved vehicles for standard use in Israel, Hawaii, and other parts of the US (1).

Whereas challenges such as battery technology are well known (if not necessarily completely solved), the wide-scale deployment of electric vehicles will come with a variety of new

[a] The author is on leave from the Horst Görtz Institute for IT Security at the University of Bochum, Germany

technical problems. These new challenges occur if the stake holder energy providers, infrastructure providers, end-users, and governments interact in real-world systems. For instance, both reliable and secure payment systems, secure metering, as well as privacy protection to avoid tracking and tracing will be required. Furthermore, protection of the infrastructure against malicious manipulation is required. These problems are almost never visible during field trials, as they tend to be performed by highly motivated and cooperative participants. However, once electric car systems are deployed in the real world, a variety of parties with conflicting interests are interacting. This can lead to dishonest selfish behavior, and might even include purely malicious objectives. In order to assure smooth operation of large-scale electric vehicle systems, methods of modern network security and embedded security need to be applied. While some threats can be countered with existing IT security solutions, addressing other threats needs adoption to the specific requirements of electric vehicle systems. It is worth mentioning that IT security within cars or for V2X communication has become much better understood over the course of the last few years (2)(10), and all major OEMs have by now dedicated security groups addressing problems such as secure software update, chip tuning or secure telematics. We believe that protecting electric vehicle systems is an equally important issue and should be addressed as soon as possible.

This work presents and analyzes security-specific aspects of future electric transport systems, and suggests solutions. Even though all threats can be addressed with modern security technologies, it is important to stress that security must be considered at an early stage of the system design. Introducing security functions as a late add-on to a system is a painfully difficult task which often fails, as numerous examples have shown time and again. Evidence for this is, e.g., given by the failed (large-scale) deployment of secured variants of Internet protocols like IPSec and DNSSEC. We are not aware of any previous work that deals with this emerging topic.

CHALLENGES

In the following we present challenges in future electric transport systems and sketch solutions.

Secure Payment and Privacy

Drivers of electric vehicles will need to charge or replace their batteries. It is expected that there are a wide variety of ways of doing this, ranging from charging stations akin to conventional gas station, charging at home, at work or at other third party locations (as proposed by Coulomb Technologies (6)), to battery replacement stations (as, e.g., propagated by Better Place (7)). A crucial element of all these approaches is a payment system which works reliably and secure, and which protects both the end-user as well as the provider.

Similar to revenue collection in the case of public transport there are good reasons to prefer electronic payment systems as opposed to sticking to cash-based payment: some fairly obvious advantages are significantly reduced revenue collection costs and a reduce of losses, enhanced customer satisfaction, improved services and operational efficiency as well as more flexible pricing strategies. One solution is to use systems based on credit cards, similar to the way we currently pay at gas stations or stores. These systems, even though widely spread, are not without problems. For instance, the transaction needs to be protected such that credit card information is not revealed to third parties. However, this would exclude users who are either not willing to use a credit card for their transportation needs, e.g., for privacy reasons, and those who cannot obtain one.

Another approach would be to adopt the kind of payment systems already established in the field of public and private transportation. For instance, Integrated Transportation Payment Systems (ITPS) like the Massachusetts Bay Transportation Authority (MBTA) CharlieCard (17) or the E-ZPass (18) show the potential of electronic payment systems as a reasonable, fair, and efficient method for revenue collection purposes. Unfortunately, at the same time they are also examples demonstrating serious shortcomings of today's ITPS. Existing systems seem to lack sufficient mechanisms protecting their security and especially the privacy of their users: one problem that this kind of systems seem to share with many other commercial systems implementing security functions is the deployment of cryptographically weak proprietary primitives, e.g., as demonstrated for the Charlie Card or Oyster Card in (3)(4). Moreover, work like the provisional vulnerability analysis of the MBTA system, done by three MIT students as a class project (19), suggests that this is by far not the only security problem. In addition to security issues, concerns about location privacy of ITPS users have also been raised, i.e., related to the non-traceability of users within the transportation system. For instance, the fact that E-ZPass and Fast Lane toll plaza records have been used by lawyers to prove their client's cheating husbands were not where they claimed to be at a certain date and time (20) shows (i) that this system does not protect location privacy and (ii) this might be exploited in a questionable way. Privacy is an especially challenging problem in this context since it spans cryptographic theory, engineering, policy and sociology. However, in order to enable a large-scale deployment and broad acceptance of an ITPS, adequate security and privacy mechanisms are an essential requirement. Indeed, current FasTrak users in the Bay Area rank “more secure technology to prevent security and privacy issues” in the top three recommendations of a recent study (21).

Since vehicles are closely coupled with their owners, tracking vehicles allows tracking vehicle owners and generating profiles. Such profiles might include information about driving behavior but also advanced information such as user behavior which is not directly related to driving behavior but is derived from the vehicle’s location. For instance, an owner might charge his battery each Tuesday evening in a red-light district while his wife charges her vehicle’s batteries every Tuesday evening at a community college. Such tracking endangers the privacy of drivers and, at least equally important, might be perceived in such a way. Potential attackers can be categorized as follows: (1) a (small) set of individuals, (2) commercial companies, and (3) government institutions. Individuals will attack the system to obtain privacy sensitive information in order to track other individuals. Individuals will also attack the system because of curiosity or because they consider a successful attack to be a challenge. Commercial companies will generate user profiles to finally increase their revenue. Commercial companies will typically respect legal restrictions but they will also exploit legal loopholes. Government institutions will have extensive power and they might even be able to define the legal environment. Therefore it is important to define a legal framework to account for companies and government institutions, and define technical solutions that account for individual attackers.

We like to note that the incorporation of privacy mechanisms into a commercial system, as a protection for the end-user, is more likely to be neglected in comparison to security mechanisms protecting the system from dishonest users or attackers. This is often due to the lesser degree of incentive for companies. It is important to design privacy preserving mechanisms before mass market deployment though. Such privacy preserving mechanisms need to incorporate two major aspects: (1) mechanisms need to be implemented in the software of vehicles and the back-end such that the vehicle-tracking is avoided to a certain level, and (2) legislation, law enforcement and providers need to define a privacy policy for infrastructure management that preserves privacy for vehicle drivers. As already described, the technical approach accounts for individual attackers whereas the legal approach accounts for companies and government institutions.

In the face of the above security and privacy issues it might not be advisable to adopt and extend existing ITPS for paying at e-car battery recharge or exchange stations. However, it would be nevertheless highly desirable to have a system designed not only for this single purpose but which allows for payments across various modes of transportation. That means such a *multi-modal* integrated payment system should be usable to pay for recharging e-cars as well as trains, buses, subways, parking, highway tolls, fuel, and even for small-scale commerce, e.g., buying a newspaper at a train station kiosk. This feature would greatly increase the acceptance and thus the deployment of a system and has already been demanded by several public and private sector entities. For the same reason, such a system should support multiple types of user devices for payment like contactless smart cards, NFC phones, etc. On the other side, it must also be noted that incorporating security and privacy into a payment system offering such advanced features constitutes an even more challenging task.

Nevertheless, we believe that all these hurdles can be overcome with methods of modern cryptography and embedded security. In fact, there is a wealth of cryptographic literature proposing payment schemes (mainly targeting e-commerce applications) featuring strong security and privacy properties we can build on. The foundation for this type of cryptographic protocol was laid by Chaum in 1982 in his seminal paper (22) where he introduced the concept of so-called *blind signatures* – which can, e.g., be realized using the RSA, DSA or ECDSA signature schemes (12) – being an essential technique for anonymous digital payments.

Since then e-cash protocols has been extensively studied. As a somewhat surprising finding, it is possible to construct secure off-line payment systems (i.e., systems that do not require a permanent connection to a bank server for authorizing each transaction) that protect the anonymity of honest users but is nevertheless able to disclose their identities as soon as they try to cheat the system. For excellent high-level overviews and taxonomy of e-cash systems we refer to (23)(24). We expect that while some of the required cryptographic components for an integrated e-car recharging payment system can be taken off-the-shelf, others need to be adapted or even newly developed to suffice the special needs of this application domain.

Secure Metering

As in gasoline-based vehicles, the “fuel” in form of electric energy will have a major economic value in electric car systems. The issue of accurately and reliably measuring electric energy is a well studied and understood area. However, in the future the protection of measurement data against malicious manipulations will become a crucial component for large-scale electric transportation systems. As electricity is neither visible nor has any physical weight like a full gas tank (nor does it have any odor), it is harder to actually verify the amount of electric energy delivered. The situation is becoming even more pressing if special electricity rates are introduced for charging car batteries. Both, rates lower than standard household rates in order to create an incentive for “green” cars, or a rate higher than household electricity in order to make up for lost gasoline taxes are imaginable in the future.

It is instructive to look at the attacker model in this scenario. First, we note that there is an inherent incentive for almost all parties involved to behave dishonestly. The owner has an incentive to report less energy than was actually delivered into the batteries. The energy provider might potentially be interested in the opposite, i.e., to charge for more energy than delivered. Especially in light of increasing deregulation and fragmentation of the energy market, it will become more likely that energy providers behave dishonestly. Finally, the owner of a charging station could potentially cheat both of the aforementioned parties through incorrect metering. In addition, there are potentially middle men, i.e., organizations that mediate between the energy producers and the charging stations. Another party potentially negatively affected is the government, which might loose revenue due to incorrectly reported e-car electricity. We note that today there is already fraud related to unpaid gasoline taxes, at least in part due to the involvement of organized crime in the gasoline distribution system. Secure metering is thus also of great relevance for state and federal governments.

We discuss now the technical measures for assuring that energy metering can not be manipulated. This is an especially challenging task since the charging stations can be under complete physical control of the attacker, e.g., a station owner or the car owner in case of charging at home. In order to provide strong manipulation protection, three components are required, which are based on embedded security technologies. First, the metering data which records the electric energy delivered should be signed using a digital signature within the charging station. A digital signature assures that the data can not be manipulated later unless an attacker has access to the private cryptographic signature key. Applicable signature algorithms include DSA, RSA or ECDSA, as specified in the US Federal Information Processing (FIPS) Standard (12). These algorithms are computationally demanding, but given that a signature has to be derived only every few second, even inexpensive embedded CPUs provide sufficient computational resources. The second crucial component is that the software or hardware module which computes the digital signature is closely linked to the actual metering device. Otherwise, a potential attack could be that the data from the analog metering IC is manipulated as it is being sent to the digital signature module. Even if both ICs are placed on the same circuit board within the “pump”, attacks are possible by manipulating bus data. Such “modchip” attacks are common against pay-TV or video game consoles such as the Xbox (13). In order to prevent the attack, the metering circuit has to be either in the same IC as the digital signature algorithm, or both modules have to be placed in tamper-resistant housing which detects manipulations. Interestingly, such an approach shows similarities to anti-counterfeiting technologies in which products or spare parts are equipped with electronic tags (e.g., RFID tags) which authenticate the part and are physically connected to the target in a tamper-resistance manner. The third security component assures that the data is hidden during transmission. Even though not absolutely necessary, in most scenarios it will be highly desirable that the metered data is not only protected with a digital signature against alterations, but also encrypted as it is being transmitted, e.g., to the charging station display or to the utility company. In order to establish such a confidential communication channel, symmetric algorithms like the Advanced Encryption Standard (AES) can be used, which is also a federal standard (14). If payment information are to be transmitted too, e.g., credit card numbers, encryption will be a crucial requirement.

Both the digital signature and the symmetric encryption rely on cryptographic keys which must be stored securely within the metering station. There are established methods for achieving secure key storage, e.g., in the financial industry. One of the more challenging aspects of the system will be the key management. Given the distributed nature of the system, using a public-key infrastructure (PKI) seems like a promising approach. A PKI allows to exchange the public keys needed for digital signatures and to compute the symmetric session keys.

It should not be overlooked that one has to assure that the discussed security measures are correctly implemented in a charging station. In the case of conventional gasoline stations, the pumps are certified such that the amount of delivered gasoline cannot be easily manipulated. A somewhat comparable process exists for digital security systems. In particular, the Common Criteria for Information Technology Security Evaluation, commonly referred to as Common Criteria, is an international standard for certifying digital security systems (11). It is typically applied to devices such as banking or pay-TV smart cards, ATM machines or computer network encryption equipment. Roughly speaking, the standard assures users that a specified security goal is actually achieved in a given product or device. Finally we note that there have been proposals for providing secure metering for household electricity, e.g., the SELMA consortium project (15).

Critical Infrastructure and Physical Safety

Electric vehicles will rely on an infrastructure for charging or replacing batteries. This grid will consist of networked and intelligent charging stations, energy generation units (from conventional power plants to networks of decentralized wind or solar energy plants), and possibly also stations for swapping batteries. The power grid and charging station will most likely be closely linked through information networks – e.g., for reasons of load balancing, payments or traffic management – and a single hacking attack can thus potentially have a very large impact. In addition to the impact on private transportation, from a national infrastructure perspective, it is particularly critical that the logistic chain is not affected. This close link between a network and transportation infrastructure is unique to electrical transport systems and should be studied closely. Security mechanisms which protect this infrastructure against malicious attacks must be implemented. We note that a wealth of expertise exists in the area of critical infrastructure protection (5), a field that received increased attention after the 9/11 terrorist attacks.

Unlike the attacks discussed earlier in this article, it is likely that adversaries who target the critical infrastructure are not necessarily insiders involved in the system (drivers, energy providers, charging stations). Rather, external parties such as terrorist groups, foreign governments or hackers without a political agenda will have an interest in this. The recent discussions about cybersecurity threats further stress this point. In the USA, the Obama administration just recently decided to review the status of the nation’s cybersecurity to examine how federal agencies’ protection critical assets (16). Even though the main focus is on protecting digital data, securing the future network that provides transportation energy will also be a critical component.

In order to obtain a broader perspective, one should be reminded that critical infrastructures are defined as complex and highly interdependent systems, networks, and assets that provide the services essential for a modern society. They are currently organized into the 17 critical infrastructure sectors, including banking and finance, drinking water, emergency services, energy, healthcare, telecommunications, and transportation systems. Clearly, future networks of charging stations will be part of the transportation infrastructure and must be protected against malicious cyberattacks. The preparation for Y2K, fall-out from post-9/11 events, and the 2003 blackout of the Northeast have all served as reminders of just how fragile these systems have and can become. A collapse of the electronically controlled power grid due to a cyberattack would be disastrous, because it would impact the transportation and power infrastructures simultaneously. In the USA the Department of Defense is responsible for supporting national critical infrastructure protection. We believe that it is crucial that the power grid for e-car systems will be included in the ensemble of critical assets. The protection of the transportation energy grid is an emerging issue that should be discussed by research groups, industry and government agencies alike.

Another type of attack aims at the manipulation of charging stations in order to physically harm drivers or damage the vehicle. For instance, overcharging batteries might destroy. Therefore, it is necessary to protect the network that connects the charging stations against hackers as well as the individual stations against manipulation. Moreover, battery manufacturers will have to investigate countermeasures which prohibit the overcharging of batteries. Methods such as physical and electrical tamper-proving and tamper-resistance are possible solutions for preventing such attacks. Also, previous work for safe operation done in the context of electrical metering devices used in solar collectors and wind generators must be considered and, if applicable, integrated in the charging system. In all these scenarios it is crucial to address both insider and outsider attacks.

CONCLUSIONS

Intelligent transportation systems and electric vehicles promise a variety of benefits for society and individuals. First field tests and commercial products suggest that mass market deployment will follow soon. So far no consideration has been given to the dishonest behavior of parties with conflicting interests in such systems. In order to prevent malicious actions by insiders and outsiders, method of IT security need to be introduced to electric transportation systems. Such methods range from cryptographic mechanisms in charging stations and batteries to secure and privacy-preserving payment systems to a critical infrastructure interpretation of the electric car charging network. This work is a first step towards addressing the corresponding problems and to start a discussion.

Security threats need to be analyzed in detail and customized security solutions need to be designed. Mass deployment of intelligent electric transportation systems without including security measures from the very beginning bears major risks. There are many examples where security was an afterthought which resulted in inherently insecure systems, the best example being the Internet.

REFERENCES

(1) TESLA Motors. http://www.teslamotors.com.

(2) Kerstin Lemke, Christof Paar, Marko Wolf. *Embedded Security in Cars: Securing Current and Future Automotive IT Applications*. Springer-Verlag, 2005.

(3) Karsten Nohl, David Evans, Starbug, and Henryk Plotz. *Reverse-Engineering a Cryptographic RFID Tag*. In Proceedings of the 17th USENIX Security Symposium, pages 185–194, 2008.

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

(5) Ted Lewis. *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation*. Wiley&Sons, 2006.

(6) Coulomb Technologies, Inc. http://www.coulombtech.com.

(7) Better Place, Inc. http://www.betterplace.com.

(8) San Jose Mercury News. *Bay Area Mayors endorse $ 1 Billion Plan for Electric Cars*. November 2008, http://www.mercurynews.com/business/ci_11032113.

(9) 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.

(10) Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. *Securing Vehicular Communications*. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006.

(11) The Common Criteria, http://www.commoncriteriaportal.org/thecc.html

(12) FIPS-186-2, Digital Signature Standard

(13) The Hidden Boot Code of the Xbox, Xbox Linux, http://www.xbox-linux.org/wiki/The_Hidden_Boot_Code_of_the_Xbox.

(14) FIPS 197, Advanced Encryption Standard

(15) SELMA – Sicherer ELektronischer Messdaten-Austausch (Secure Electronic Exchange of Messurement Data), http://www.selma-project.de/index.html

(16) Obama orders review of cyber security, Feb. 9th 2009, http://news.yahoo.com/s/ap/20090210/ap_on_go_pr_wh/obama_cyber_security

(17) Massachusetts Bay Transportation Authority, CharlieCards & Tickets, http://www.mbta.com/fares_and_passes/charlie/

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

(19) Russell Ryan, Zach Anderson, and Alessandro Chiesa. Anatomy of a subway hack. Presentation at DEFCON (prevented by restraining order), 2008, http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf

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

(21) Patrick F. Riley. The Tolls of Privacy: An Underestimated Roadblock for Electronic Toll Collection Usage, 24(6):521-528, 2008.

(22) David Chaum, Blind Signatures for Untraceable Payments, In *Advances in Cryptology CRYPTO 1982*, pages 199-203.

(23) 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.

(24) 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.