Security Concerns of a Plug-In Vehicle

Hina Chaudhry and Theodore Bohn
Center for Transportation Research, Energy Systems Division
Argonne National Laboratory
Email: hchaudhry@anl.gov, tbohn@anl.gov

***Abstract*-Electric vehicles, no doubt, will bring in many benefits to the economy and to the stakeholders concerned; however these will come at certain costs. Modern vehicles already have several intelligent electronic components, also known as electronic control units (ECU), which control several functionalities of the car and on top of that, with the introduction of the electric vehicles and in particular plug-in electric vehicles, a vehicle is no longer a vehicle, it is more of a network connected device. This paper therefore looks specifically at some of the security concerns that will emerge from plug-in electric vehicles charging and communicating to the utility and their potential impacts on the power grid as a whole.**

***Index Terms* – Attacker, authentication, authorization, communication, firmware, in-Vehicle network, PEV, security**

I. INTRODUCTION

With the current impetus on using clean energy, to cut our dependence on fossil fuels, there has been an increase in efforts in academia, industry, government agencies and national labs to make electric vehicle a viable transport option for everyone and which can be easily integrated into every day's life. There are other advantages of electric vehicles apart from it using the clean energy or in other words plain electricity. Electric vehicles in comparison to their gasoline brethren are effective in controlling pollution, going forward in couple of years, they will be cost effective with gasoline prices increasing every day, and will be a major resource of distributed energy. With their capability of transmitting electricity back to the grid, they will be the means of balancing the load at times of peak demand. At home they can power up the appliances when the tariff rates are high and charge back when the rates are low.

But all this has its own price. The electric vehicles will require a charging infrastructure in place which will connect them to the power grid indirectly; they will require the communication infrastructure in place which will send the necessary details to the utilities for authenticating, authorizing and correctly billing the electric vehicle owner; they will [1]require software and IT services to process and storing the information transmitted by the vehicle during commissioning, enrolling into a utility program, charging and billing. Underlying all these process, there is a big concern of how all this can secured properly. With a vehicle, the safety becomes the priority and thus it requires more than ordinary, safe controls in place. Already a modern vehicle comes with many electronic components also known as ECUs that make several controller area network (CAN), and with electric vehicle there will be an increase in these controls. Thus there is a greater need to secure both inside and outside vehicular communications. Further, with wireless technology being introduced for firmware updates [1] and remote diagnostics, [2], the security concerns are greater than never before. And these concerns will multiply more with electric vehicles coming into the picture.

The rest of the paper is organized in the following manner. Section II gives an overview of the security vulnerabilities that were found in previous surveys and studies. Section III provides a brief overview of the proposed plug-in electric vehicle infrastructure and the main entities involved. Section IV looks at a common scenario of a charging session of a plug-in electric vehicle and describes some of the main security concerns and their potential impacts. This is followed by Section V which provides some possible recommendations and finally the conclusion.

II. RELATED WORK

There have been surveys and studies in the past which documented the security issues that are inherent in the current in-vehicle networks. In their paper Wolf et al. [3] describes about attacks on automotive hardware and software, and explains about some of the security objectives, along with technical and non-technical constraints. A concept of security module along with some protection mechanisms is also presented in the paper.

Automotive security analysis of different vehicle systems like antitheft system, vehicular ad hoc network, ECU flashing, and integration of various business services is given by Brooks et al [4] in their paper. Different stakeholders and assets are identified. Further they used the CERT taxonomy [5] to analyze the attacks.

A similar analysis is given by Jenkins and Mahmud [6], where they looked at the security problems and attacks on the inter vehicle and in vehicle communications, along with software and hardware attacks.

Theodore Bohn is a principal engineer with Center for Transportation Research, Energy Systems Division of Argonne National Laboratory, USA.
Hina Chaudhry is a research aide at Center for Transportation Research, Energy Systems Division of Argonne National Laboratory, USA. She is also pursuing her PhD at Purdue University, USA.

978-1-4577-2159-5/12/$31.00 ©2011 IEEE

Vulnerabilities in embedded systems and how security can be introduced in their design is explained by Kocher et al. [7] in their paper.

Sniffing/replay attacks on CAN buses are discussed and described by [8] by Hoppe and Dittmann. They further take some practical examples in their paper [9] to showcase the security threats to CAN networks and provides some short term countermeasures.

More such studies and surveys are documented by Kleberger et. al [10] , where they emphasis on some areas that require immediate concerns. These areas are problems in In-Vehicle Networks, misuse and poor implementation of CAN protocol, and information leakage. They also propose architectural security features which address the issue of confidentiality, integrity, authentication, communication and timing in the in-vehicle network.

III. BACKGROUND

With the arrival of the plug-in electric vehicle, there is no doubt that there will be an increase in the communication requirements both from the vehicle and the utility providing the electricity. Before looking further into the various security issues that an electric vehicle might face, it is important to look at the various components and the entities that constitute the plug-in electric vehicle infrastructure. It is also important to remember that standards that will overlook these communications and the equipment that will be part of this infrastructure are being currently formulated and developed by the respective organizations like Society of Automotive Engineers (SAE), International Electrotechnical Commission (IEC) among others. Below is the diagram [11] that gives an overview of the utility/consumer/plug-in electric vehicle network. In the following paragraphs, a brief description of some of the major parts is given.

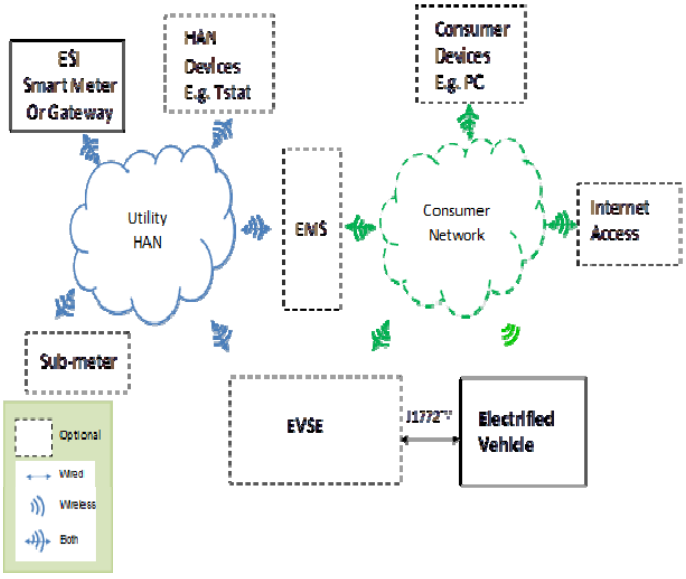

Figure 1. Overview of Utility/Consumer/Electric Vehicle Network

A. Plug-In Electric Vehicle (PEV)

Any class of vehicle whether it is Battery Electric Vehicle [11](BEV), Plug-in Hybrid Electric Vehicle (PHEV), Plug-in Electric Vehicle (PEV), etc., which can be plugged in to receive power from the electrical grid where this power is then used to apply traction to the vehicle wheels.

B. Energy Services Interfaces (ESI)

Energy services interface [11] provides security and often coordinate functions that enable secure interactions between relevant home area network devices and the utility. It permits applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and the integration with the building management systems. It also provides auditing/logging functions that record transactions to and from home area networking devices.

C. Energy Service Communication Interface (ESCI)

The ESCI is the communication device [11] between the vehicle and the utility ESCI. It should exist at the customer premise and be capable of securely communicating between the utility and the PEV to facilitate the exchange of demand side management information. The interface should report all charging session information like PEV id, interval kWhr consumption and the energy usage to the utility. The ESCI will also be capable of passing energy information, including price signals, schedules, event messages, configuration from the utility to the PEV.

D. Electric Vehicle Supply Equipment (EVSE)

The vehicle connects to the grid using an EVSE as described in the standard J1772 [12]. This document identifies the utility criteria using both a 1) Cordset EVSE (120 V AC to vehicle) 2) Premise mounted version EVSE (240V AC to vehicle) and a 3) Premise EVSE with an off board charger and delivers DC energy to the vehicle. Relevant messages are passed between the EVSE and the PEV for the proper charging of the PEV.

E. End User Measurement Device (EUMD)

A EUMD is the device [11] that measures and communicates energy usage information payload to Energy Service Communication Interface (ESCI). A EUMD will be located inside an Electric Vehicle Supply Equipment (EVSE) and would supply charging session information like PEV id, premise id, interval kWhr consumption to ESCI. A EUMD receives configuration information from the utility.

F. Energy Management System (EMS)

The energy management system [11] is the gateway to the utility and also to consumer appliances if applicable and any other networks.

G. Energy Portal (ES)

An energy portal [11] is any charging point for a PEV. At a minimum, the energy portal is a 120V, 15A outlet but can also be a 240 V EVSE outlet connected to the premise circuit.

H. Home Area Network (HAN)

A HAN is a network contained [11] within a user's home that connects a person's digital devices from multiple computers and their peripheral devices to telephones, VCRs, televisions, video games, other smart appliances and digital devices that are wired into the network.

I. ZigBee

ZigBee is a communication protocol [13] based on IEEE 802.15.4 protocol, and is a low-power, low complexity and low cost technology. It is widely used in building automatic control, industry automation, monitoring, among others. ZigBee is also an accepted technology for the communication between various entities involved during the PEV charging.

J. Controller Area Network (CAN)

Controller Area Network (CAN) [14] is a serial communications bus designed to provide simple, efficient and robust communications for in-vehicle networks.

K. Utility Programs

In order to encourage people to purchase a PEV [11], the utilities are developing customer rates/programs which could provide customers with PEV tariff that provides a low rate for off peak charging and a higher rate for on-peak charging. Some of these programs are [11]:

- Time-of-Use (TOU) Rates/Tariffs/Programs (Load Shifting)
- Direct Load Control Programs (Demand Response)
- Real Time Pricing (Demand Response/Load Shifting)
- Critical Peak Pricing (Load Shifting)
- Optimized Energy Transfer Programs (Regulation Services/Demand Response)

IV. SECURITY CONCERNS

As the plug-in electric vehicles will have the capabilities to connect and communicate to various electronic devices, equipment and interfaces through wired and wireless networks, there is a great potential for cyber attackers to gain access to the vehicle and inflict damages upon it. A modern vehicle already has an in-vehicle network consisting of several electronic control units (ECUs) which control the functioning of several systems like automatic brake systems, collision warning systems, etc., but with the emergence of electric vehicles on the road and the corresponding infrastructure in place, everything will be connected to each other like never before. Although there are several scenarios and use cases to look at, but probably looking at one of the most common scenarios will help us understand the security concerns much better. The scenario is when a PEV owner connects the vehicle to an energy portal for charging the vehicle. This portal can be at 1) his premise location like home, at 2) another person home, but inside the utility's service territory 3) another person home, but outside the utility's service territory 4) public location like curbside, workplace, business, multi-family dwelling. Here are the following steps [11] when the customer connects the PEV at his premise location.

TABLE I.
CUSTOMER CONNECTS PEV TO ENERGY PORTAL AT HIS PREMISE LOCATION

Step	Actor	Description of the Step
1	Customer	Customer connects PEV to energy portal at his premise location.
1a	Customer	Customer connects EVSE cordset to energy portal at his premise location.
1b	EVSE	Customer connects premise mounted EVSE to PEV.
2	PEV/ESCI	PEV and ESCI perform PEV binding.
3	PEV	PEV provides indicator to customer that the binding has been successful.
4	PEV	PEV sends energy request and schedule (according to enrolled PEV program).
5	Utility	Utility compares request with available energy and confirms or adjusts for message back to PEV. Utility sends energy available (amount & rate) and schedule.
6	PEV	PEV prepares for charging.
7	PEV	PEV begins charging based on customer selected preferences.
8	EUMD	Records charging information (PEV id, Premise id, energy usage and time stamp for each metering interval) and energy supplied to PEV for each charging session.
9	EUMD	It communicates to the ESI using the ESCI, the energy supplied to the PEV for each charging session.
10	ESCI	ESCI communicates to Utility, the energy supplied to the PEV for each charging session
11	Utility	Utility records each PEV charging session for bill generation and reporting to customer account associated with this premise and PEV id.

Based on the above scenario it can be seen that there are several ways in which an attack can be launched. The following paragraphs provide further details about the same.

A. Data

The data that will be transmitted over the networks during the charging session mainly consists of the consumer information like PEV id, Premise id, utility id, customer id, energy program that the customer is enrolled into (TOU, CPP, RTP, etc.), energy request, energy usage, and energy available (from utility).

Security Concerns:

- How the data in transit is going to be protected against being sniffed and later used in replay attacks by the hacker/attacker? Will the data be encrypted to ensure its confidentiality and integrity while in transit?
- How the data at rest will be secured? What secure policies should be applied on the databases to avoid attacks like SQL injections, etc.?

Possible Impacts:

- Unauthorized access to customer information, unauthorized modification of the customer information or customer's energy profile in which he is enrolled in.
- Sniffed data like PEV id, customer id can be later used by an attacker to impersonate a genuine customer for authentication and authorization purposes.

- Manipulation of the amount of energy requested by the customer, which in turn can turn fatal (fire, vehicle damage, etc.) if the energy delivered is much more than it was requested.

B. Communication Network

ZigBee protocol especially its smart energy profile is being considered to be used for the communication requirements between a PEV and the utility. It is currently used [13] for the home energy management, home and building automation, retail services, health care and for many more services.

Security Concerns:

- ZigBee protocol has been shown to have some weaknesses and have been exploited by the researchers for the proof of concept. Will these weaknesses be addressed before it is fully deployed for the communications between the several entities within the PEV infrastructure?

Potential Impacts:

- Sniffed data like PEV id, customer id can be later used by an attacker to impersonate a genuine customer
- Manipulation of the amount of energy requested by the customer, which in turn can turn fatal (fire, vehicle damage, etc.) if the energy delivered is much more than it was requested or what the vehicle can accept.

C. Infrastructure

Plug-in electric vehicles will be one of the major resources of distributed energy or DERs in future. They will be built with the capability of plugging back the electricity back to the grid whenever there is a peak demand of power and the vehicle owner enrolled in on one of the utility demand response programs. They can also be used to power the home appliances whenever the tariff rates are high, mostly during the weekdays. The security concerns in this type of scenario can be as follows:

Security Concerns:

- How can it be verified that every appliance, device including PEV on the network is not infected with malicious software?

Potential Impacts:

- An already infected or compromised PEV can infect the ESCI and other smart appliances with malwares or it can be vice versa.
- Possibility of infecting the substations/transformers with virus, malicious codes, spyware, etc. through infected ESCI/EMS and causing breakdowns, blackouts and perhaps catastrophic failures.

D. Firmware and Software

Electronics and software have become a major part of a modern vehicle providing convenience to the vehicle owner. Modern vehicles [10], [15] now contain an in vehicle network which comprises of nearly 50 to 70 electronic control units or ECUs to control the functionality of various systems. On each of these ECUs, a specific and independent firmware is run. During the course of time [10],[17] improved versions of firmware with added functionalities are introduced and to integrate them into the existing ECUs, a vehicle owner can take his vehicle to a service station where a wired connection to the vehicle is established and new firmware is flashed to the ROM of the particular ECU. With the developments in the wireless technology, these same functions will be carried over the air. Firmware updates over the air (FOTA) no doubt [1], will provide a vehicle owner minimal inconvenience, mass updates in case of fleet owners with little efforts and faster updates, as soon as they are released. This is the existing scenario right now, but with electric vehicles there will be requirements for more electronic controls and components to be updated and communicate and transfer the various details necessary for the maintenance. Standards and design of these power electronics systems are still being considered and worked upon by various bodies but it remains to be seen how security will be addressed. Some security concerns here are as follows.

Security Concerns:

- How can be it assured that the received firmware and software updates are coming from the trusted and authorized source and not from untrusted source?
- How it can be assured that the vehicle mechanics or the vehicle owner themselves will not tamper with the in-vehicle network? They might have the capability to install spyware and other rogue software in the vehicle.

Potential Impacts:

- An attacker can mount [10], [16], attacks on the wireless communication links and can eavesdrop, intercept, modify or inject arbitrary firmware messages on the communication link. By modifying the firmware, the attacker can change the functionality or may be even disable the functionality of the firmware.
- After successful intrusion[10],[16], an attacker can gain access to the onboard diagnostic system and send malicious diagnostic request for example triggering the airbag, causing injury to the driver and the vehicle to crash.
- An attacker can use the in-vehicle network to send and execute the malicious scripts, codes to the ESCI, EVSE, EUMD or energy portal, hence compromising them.
- These compromised systems (EUMD, EVSE, ESCI, energy portal, EMS etc.) can further compromise and infect other plug-in electric vehicles once they charge from the same energy portal, use the same EVSE and EUMD. This type of scenario can be seen when the charging station is at a public place like at work, multi-home dwellings, curbside, shopping malls, etc.
- Possibility of infecting the substations/transformers with virus, malicious codes, spyware, etc. and causing breakdowns, blackouts and perhaps catastrophic failures.

- Possibility of unauthorized access to the databases storing valuable information on consumers. Modification to the data like changing the customer charging profile, rates and tariffs, billing information, etc.

V. POSSIBLE SOLUTIONS

It is true that there are concerns and questions regarding the security of the overall plug-in vehicle infrastructure and hence concerted efforts are required to mitigate the threats and risks involved. In this section, we have looked at some of the possible solutions and mitigations in order to achieve adequate level of security, thereby increasing the cost of attacking for the attacker.

Fortunately some research has been done in the past that shows that the firmware/software updates can be done securely using the FOTA or firmware over the air method. In their paper, Nilsson and Larson [17] proposed a protocol that can provide data integrity, data authentication and data confidentiality. The proposed protocol works by creating a hash chain of the firmware, and by signing the first packet by a trusted source, thus authenticating the whole chain. Moreover, the packets are themselves encrypted using the symmetric keys. In their yet another paper [16], they discussed of taking a defense-in depth approach for securing the vehicle. They looked at prevention, detection, deflection, countermeasures and recovery and suggested authentication to prevent unauthorized access, intrusion detection systems (IDS) and logging mechanisms for detection, use of honeypots for information retrieval, intrusion prevention system (IPS) as a countermeasure and the necessity of traceability to perform recovery.

Use of honeypots in the in-vehicle networks is also proposed by Verendel et al. [15] in their paper as a means of learning about the attacker's preferences, techniques and the weaknesses in the existing systems and thereby improving the security of the vehicle overall.

Oguma et al. [18] in their paper proposed an attestation based security architecture for in-vehicle communication. They make use of a key predistribution system (KPS) based on public key cryptography, consisting of a center (vehicle manufacturer) and multiple players (ECUs). The center delivers a key generation algorithm to each player and a shared key is generated between any two players during their communication. The key security requirements fulfilled by this proposed architecture are the authentication of the software configuration, authenticated and encrypted communication and the flexibility of replacement (in the event of ECU being replaced).

The above mentioned security solutions can not only be applied to the in-vehicle networks, but also to the external network of a vehicle especially for plug-in vehicle. No doubt there will be requirements for added functionalities, most importantly, the ability to establish safe and secure communication to various disparate and heterogeneous networks, properly authenticating and authorizing the genuine owner before the charging process begins, providing the correct billing information and safeguarding against fraudulent activities by owners and the attackers alike. The databases storing the details of the consumers, their vehicles and their charging profiles should be secured by adopting adequate security policies. The data inputs from the users should properly be sanitized before storing it into the database. Issues regarding the privacy of users can be raised in future and hence proper safeguards and policies should be taken into account. Integration of intrusion detection systems (IDS), intrusion prevention systems (IPS) and other unified threat management systems into energy management systems (EMS), ESCI, EUMD, is possible and should be considered to harden the security perimeter.

VI. CONCLUSION

In this paper, we have tried to look at some of the vulnerabilities that the infrastructure for plug-in electric vehicle will bring along with it. These are by no means an exhaustive list of the potential vulnerabilities that might present themselves in the future. Although considerable research has been done showcasing various security vulnerabilities and shortcomings in the in-vehicle networks, there is little research on the security of plug-in electric vehicles, more so, as this is a new area, where standards are still being processed and developed. One of the challenges that the security practitioners face today is that of creating security solutions that can account to the high safety requirements, using very limited hardware, software, and power resources.

REFERENCES

[1] M. Shavit, A. Gryc, and R. Miucic, "Firmware Update over the Air (FOTA) for Automotive Industry," in *Asia Pacific Automotive Engineering Conference*, Hollywood, CA, USA, August 2007.

[2] S.You, M.Krage, and L.Jalics, "Overview of Remote Diagnosis and Maintenance for Automotive Systems," SAE International, Detroit, Michigan, Technical Paper Series SP-1922, April 11, 2005.

[3] A.Weimerskirch, T.Wollinger M.Wolf, "State of the Art: Embedding Security in Vehicles," *EURASIP Journal on Embedded Systems,Volume 2007, Article ID 7470*, p. 16.

[4] R.R. Brooks, S. Sander, Juan Deng, and J. Taiber, "Automobile security concerns ," *Vehicular Technology Magazine, IEEE* , vol. 4, no. 2, pp. 52-64, 2009.

[5] J.D.Howard and T.A.Longstaff, "A Common Language for Computer Security Incidents," Sandia National Laboratory, SAND98-8667, 1998.

[6] M. Jenkins and S. M. Mahmud, "Security needs for the future intelligent vehicles," in *SAE World Congress*, Detroit,MI, 2006.

[7] P. Kocher, R. Lee, G. McGraw, and A. Raghunathan, "Security as a New Dimension in Embedded System Design," in *41st annual Design Automation Conference*, New York,NY,USA, 2004, pp. 753-760.

[8] T. Hoppe and J. Dittmann, "Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy," in *2nd Workshop on Embedded Systems Security (WESS)*, Salzburg, Austria, 2007.

[9] J.Dittmann T.Hoppe and S.Kiltz, "Security Threats to Automotive CAN Networks --- Practical Examples and Selected Short-Term Countermeasures," in *SAFECOMP '08 Proceedings of the 27th international conference on Computer Safety, Reliability, and Security* , 2008, pp. 1-14.

[10] P. Kleberger, T. Olovsson, and E. Jonsson, "Security Aspects of the In-Vehicle Network in the Connected Car," in *IEEE Intelligent Vehicles Symposium (IV)*, Baden-Baden, Germany, June 5-9, 2011, pp. 1-6.

[11] Hybrid Committee, "Use Cases for Communication Between Plug-in Vehicles and the Utility Grid," SaE International, Detroit, Michigan, Standard J2836/1, Jan, 2010.

[12] Hybrid Committee, "SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler," SAE International, Detroit,Michigan, Standard J1772, Jan, 2010.

[13] (2011, July) ZigBee Smart Energy Overview. [Online]. http://www.zigbee.org/Standards/ZigBeeSmartEnergy/Overview.aspx

[14] R. I. Davis, A.Burns, R.J. Bril, and J. J. Lukkien, "Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised," *Real-Time Systems;Springer Science Business Media*, vol. 35, pp. 39–272, 2007.

[15] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, "An Approach to using Honeypots in In-Vehicle Networks," in *68th IEEE Vehicular Technology Conference (VTC)*, 2008, pp. 1-5.

[16] D. K. Nilsson and U. E. Larson, "A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure," *Journal of Networks*, vol. 4, no. 7, pp. 552–564, Sep 2009.

[17] D.K.Nilsson and U.E.Larson, "Secure Firmware Updates over the Air in Intelligent Vehicles ," in *ICC Workshops '08. IEEE International Conference on Communications Workshops, 2008.* , Beijing, 23 May 2008, pp. 380-384.

[18] H. Oguma et al., "New Attestation-Based Security Architecture for In-Vehicle Communication," in *IEEE Global Telecommunications Conference (GLOBECOM)*, New Orleans, LA, 2008, pp. 1-6.