BIOGRAPHICAL SKETCH

Marbin Pazos-Revilla received the B.Sc. degree in Information Technology from Barry University, Miami, FL., in 2004, and M.Sc. degree in Computer Science in 2011, from Tennessee Technological University. Marbin has worked in Tennessee Technological University since 2005 as a Technology Specialist for the College of Engineering where he has contributed to advancing Engineering Education with the use of technologies like MoLE-SI (Mobile Learning Environment and Systems Infrastructure). He has published and presented works in areas of Privacy-Preserving Secure Electric Vehicles Dynamic Charging and Charging Coordination, Internet of Things, and Engineering Education, and was the recipient of the "Best Paper Award in the 2016 Annual Conference of the North American Fuzzy Information Processing Society (NAFIPS)", in 2016. Marbin is currently working towards finishing his Ph.D. degree from Tennessee Tech University, with focus areas on Secure Authentication in Electric Vehicles and Internet of Things Security.

EDUCATION

PhD – Tennessee Tech University
Expected graduation December 2018

MS – Tennessee Tech University, 2011

BS – Barry University, 2004

College of Engineering

TENNESSEE TECH

The Department of

Electrical & Computer Engineering

Announces the Dissertation Defense

of

Marbin Pazos-Revilla

In Partial Fulfillment of the Requirements

For the degree of

Doctorate of Philosophy

November 19, 2018

Held in

208 Brown Hall at 4:00 p.m.
115 West 10th Street
Tennessee Tech University

FIELD OF STUDY

Secure Authentication in Electric Vehicles and IoT Security

DISSERTATION TOPIC

SECURE PHYSICAL-LAYER-ASSISTED AUTHENTICATION AND CHARGING COORDINATION FOR ELECTRIC VEHICLES AND HOME BATTERIES

EXAMINING COMMITTEE

Dr. Mohamed Mahmoud, Committee Chair
Associate Professor, Electrical & Computer Engineering

Dr. Ghadir Radman
Professor, Electrical & Computer Engineering

Dr. Syed Hasan
Associate Professor, Electrical & Computer Engineering

Dr. Ambreen Siraj
Professor, Computer Science

Dr. Motoya Machida
Associate Professor, Mathematics

ABSTRACT

Electric Vehicles (EVs) are becoming increasingly prevalent in today's society as a mean to reduce dependency on fossil fuels, fuel costs, and environmental pollution. Moreover, home batteries are currently used to charge from the power grid when the electricity prices are low and power homes when the prices are high. Energy storage units (ESUs), including EVs and home batteries, can also promote the power generation from renewable energy resources by storing the excess power generated. However, communications are needed to manage the ESUs, which can cause several security and privacy issues. In this thesis, we propose several schemes to address several challenges. The first scheme proposes an efficient anonymous authentication scheme for dynamic charging system. In dynamic charging systems, EVs can charge while in motion from charging elements, called charging pads, installed on roads using wireless energy transfer. The proposed scheme uses lightweight cryptosystems coupled with a physical-layer technique to create an efficient hierarchical authentication scheme that can preserve the location privacy of drivers. The second problem we address is secure and privacy-preserving charging coordination of ESUs. The uncoordinated charging of ESUs can create a peak load that cannot be handled by the power distribution system. The best way to avoid this problem is by charging coordination (or scheduling). The idea is that each ESU should send State of Charge (SoC) and Time to Complete Charge (TCC) to a charging coordinator that should run an algorithm to compute the charging schedules. However, SoC and TCC can reveal private information on the location of the EV owner and activities. In the proposed scheme, charging priorities are computed based on the SoC and TCC values, and a subset of the ESUs are selected to charge in one time slot, and the unselected ESUs can request charging in the next time slot. The objective is to maximize the number of charging requests that are served before they are expired. In this thesis, we propose two charging coordination schemes; centralized and distributed. The centralized scheme can be used when there is a robust communication infrastructure that connects the ESUs to the utility, while the decentralized scheme is useful when such an infrastructure is not available or costly. We secure the schemes against collusion attacks that aim to obtain/identify the SoC and TCC of the certain ESUs. In addition, if an ESU does not charge in one time slot, it needs to send a new request in the next time slot, and by linking these requests, some information can be revealed such as whether an EV is at home. In this thesis, we first study and analyze this attack, and then propose two solutions based on noise addition and submitting multiple request instead of only one. We have extensively evaluated the performance of our schemes using simulations and practical implementation. We have also analyzed the security and the privacy provided by our schemes. Our results confirm that the proposed schemes are efficient and secure, and can preserve users' privacy.