Assessment of RFID Implementation for Security in Electric Vehicle Charging Stations

Ephan Wong Khi Tung
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University
Kuala Lumpur, Malaysia
tp055488@mail.apu.edu.my

Julia Juremi
Forensics & Cybersecurity Research Centre (FSEC)
Asia Pacific University
Kuala Lumpur, Malaysia
julia.juremi@staffemail.apu.edu.my

Abstract - Electric vehicle charging stations, also known as EVCS, are infrastructure facilities that provide electric power to charge electric vehicles (EVs). These stations play a crucial role in supporting the widespread adoption of EVs by providing a convenient and accessible means of charging their batteries. There are different types of electric vehicle charging stations, categorized based on the charging speed and power they provide. the example of secure charging stations ae crucial for the successful transition to electric mobility is that protection of user data, preventing unauthorized access, safeguarding the power grid, and also ensuring availability and reliability. Secure charging stations play a critical role in ensuring the smooth and secure operation of the electric mobility ecosystem, protecting user data, preventing unauthorized access, and safeguarding the power grid. electric vehicle charging stations and their management systems are essential components of the EV charging infrastructure. They enable EV owners to conveniently charge their vehicles and contribute to the growth of sustainable transportation.

Keywords – Electric Vehicle (EV), Electric vehicle charging stations (EVCS), protect, hacking, data

I. Introduction

There are now more public power charging stations and more electric vehicles (EVs), which has changed the way sustainable transportation works. But this rise also makes it more likely that there will be security holes that need to be fixed. Cybersecurity risks are very dangerous because public charging stations depend on digital systems and are linked to other systems. Cybercriminals could use the weak spots in these networks to launch hacks that stop payment processes or get to customer data without permission. Physical flaws, like messing with the charge equipment, could also put the safety and purity of the charging process at risk. As electric vehicles (EVs) become more popular, it is important to protect the public power charging facilities to make sure that electric transport is safe and strong (Johnson, J. et al, 2021).

Electric vehicle charging station, or EVCS, are pieces of infrastructure that provide electricity to charge electric vehicles (Acharya, S., Dvorkin, Y., Pandzic, H., & Karri, R., 2020). These sites are very important for encouraging a lot of people to buy electric vehicles because they make charging their batteries easy and available. There are different kinds of charging points for electric vehicles based on how fast they charge and how much power they give. For example, secure charging stations are important for the smooth shift to electric transport because they protect user data, stop unauthorised access, protect the power grid, and make sure that the stations are always available and reliable. Secure charging stations are an important part of keeping the electric mobility environment running smoothly and safely. They protect user data, stop people from getting in without permission, and keep the power grid safe. EV charging points and the systems that control them are important parts of the infrastructure for charging EVs. They make it easy for people who own electric vehicles to charge them and help the growth of green transportation.

II. Problem Statement

Secure charging stations are indispensable for maintaining the integrity and efficiency of the electric mobility ecosystem. They serve as vital guardians, preserving the confidentiality and integrity of user data, thwarting unauthorized access attempts, and fortifying the resilience of the power grid (Sarieddine, K., Sayed, M. A., Jafarigiv, D., Atallah, R., Debbabi, M., & Assi, C., 2023). Within the expansive landscape of electric vehicle (EV) charging infrastructure, these stations and their associated management systems stand as foundational pillars, orchestrating the seamless flow of energy to EVs while upholding stringent security standards. By prioritizing robust security measures, charging stations not only enhance user trust and confidence but also contribute significantly to the overarching goal of fostering a safe, reliable, and sustainable electric transportation network (Luis, H. R. J., & Skármeta, A., 2020). As the adoption of EVs continues to surge, the imperative for secure charging infrastructure becomes increasingly paramount, underscoring the pivotal role that these stations play in shaping the future of transportation.

III. Goal of the Project

The EV Charging Station Security Assessment encompasses a thorough examination of infrastructure,

systems, and data security measures, encompassing a holistic approach that evaluates both physical and policy aspects. This comprehensive evaluation delves into the intricacies of the charging station's design, configuration, and operational protocols to identify vulnerabilities and establish robust defense mechanisms. By scrutinizing the physical infrastructure, including hardware components and access control measures, as well as the underlying systems and software architectures, the assessment ensures a comprehensive understanding of potential security risks.

Furthermore, by addressing policy frameworks, such as authentication procedures, data handling practices, and compliance with regulatory standards, the assessment establishes a solid foundation for safeguarding against evolving threats and ensuring compliance with industry best practices (Mastoi, M. et. Al., 2022). Through this meticulous examination, stakeholders can gain insights into the effectiveness of existing security measures and implement targeted strategies to fortify the resilience of EV charging infrastructure against emerging cyber threats and operational challenges.

IV. Objectives

The investigation entails a comprehensive examination of security risks prevalent in electric vehicle (EV) charging sites and their associated supporting systems. It involves assessing the efficacy of existing security measures implemented in charging stations, with a focus on identifying vulnerabilities and potential weaknesses. Special attention is directed towards addressing issues related to unauthorized access and cyber threats within the charging infrastructure, aiming to enhance protection against malicious activities and ensure the integrity and reliability of EV charging operations. Through this multifaceted approach, stakeholders can proactively mitigate risks and bolster the overall security posture of EV charging networks.

V. Functionality

Through simulation and demonstration, the efficacy of RFID authentication as a cybersecurity enhancement in charging stations is evaluated, aiming to fortify the security framework. This examination extends to identifying vulnerabilities prevalent in public EV stations, analyzing their associated risks comprehensively (Meng, W., Lee, W. H., Murali, S. R., & Krishnan, S. P. T. (2015). By pinpointing weaknesses within these stations' infrastructure and operational protocols, targeted measures can be implemented to bolster security measures effectively. The overarching goal is to enhance the resilience of EV charging networks against potential cyber threats and unauthorized access attempts, ensuring the continued safety and reliability of electric vehicle charging infrastructure.

VI. Technical Research

The selection of C++ within the Arduino framework for the Tinkercad EV charging system underscores a deliberate choice aimed at ensuring robustness, compatibility with IoT (Internet of Things) standards, and efficient code execution. By leveraging C++ in the Arduino environment, the design and implementation of the charging system are optimized for functionality and performance. This strategic decision not only facilitates the creation of a functional demonstration within Tinkercad's simulation platform but also highlights the system's ability to seamlessly integrate with IoT technologies (Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C., 2022). Additionally, the incorporation of RFID integration further enhances the security features of the charging station, showcasing a practical application of cybersecurity principles. Through this approach, the Tinkercad Arduino simulation serves as a valuable educational tool, fostering hands-on learning experiences and driving advancements in cybersecurity awareness within the context of electric vehicle infrastructure (Jung, D., Shin, J., Lee, C., Kwon, K., & Seo, J. T., 2023).

VII. PROTOTYPE ONE – Basic Charging Station

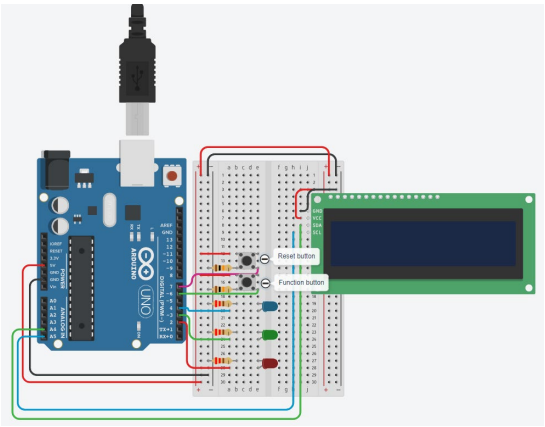

Figure 1: Screenshots of Prototype one - Basic Charging Station

The concept of prototype one serves as a simulated model, replicating the fundamental functions of a real-world charging station.

The schematic view of the circuit above explained is a basic, streamlined charging system that is easy for anyone to use. A welcome sign, "Welcome to EV Charging," is shown on an LCD screen to start the system. When the first button is pressed to start the process, a series of events happen.

While the button is being hit, the LCD quickly reacts by showing "Processing..." and a red LED light up to show the beginning phase. After a short 3-second break, the LCD changes to the word "Start Charging," and at the same time, a green LED turns on to show that the

charging process has begun. The system waits three seconds before showing "Finish Charging" on the LCD screen, which means the charging cycle is complete. At the same time, a blue LED lights up to show that the charging process is complete. The user has now been told that the payment process was successful.

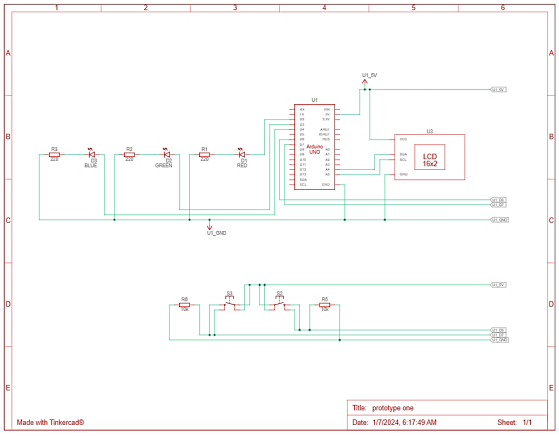

Figure 2: Design of Prototype one – Basic Charging Station

There is a second button built in to make it easy for users to restart the system and get it ready for the next charge cycle. If you press this button, the system goes back to its original state and the welcome message is shown on the LCD screen again. This easy-to-use reset button makes sure that the charging system works perfectly for future users. In conclusion, the circuit system mixes helpful visual feedback through the LCD display and matching LED signs to make the electric vehicle charging station easy to use and collaborative for users.

VIII. PROTOTYPE TWO – RFID Bypass

Prototype two demonstrate as the attacker or hacker successfully bypass the charging station and use it or steal private data from the EV.

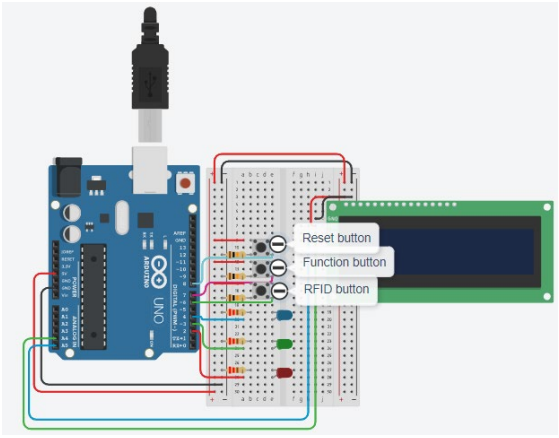

Figure 3: Screenshots of Prototype two - RFID Bypass

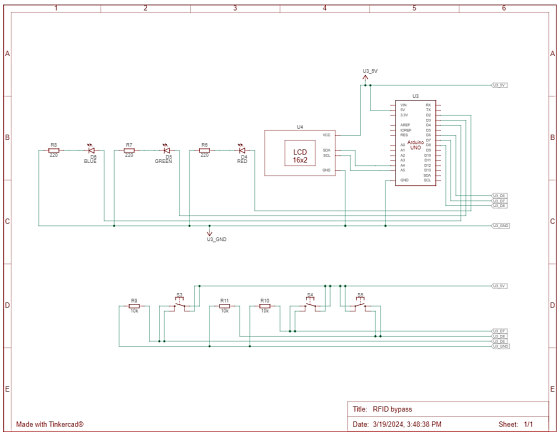

Figure 4: Design of prototype two - RFID Bypass

This prototype demonstrates as the attacker or hacker successfully bypass the charging station and use it or steal private data from the EV. In the coding part is where things start getting up to another level because this is when the system is power on, the whole system setup will be first focus on the boolean system authenticated before the setups of the code, as you can see that this has been set as false. This is because this simulation has no RFID module to be added to the system and that's why the author can modify his own RFID and act as if an attacker or hacker is able and could bypass this system which will be demonstrated later. The RFID button here is to prevent anyone to use the charging station which will now act as a locked system.

Along with the basic features of the simpler charging system, a new feature called RFID identification has been added to improve security and user interaction. The RFID authentication feature in this system doesn't exactly copy the full authentication process, but it does show how it works in a virtual way within the code framework.

As soon as the system is turned on, the LCD screen says, "Welcome to EV Charging." The first button does two things to simulate RFID verification. When hit, it not only starts the charging process as explained before, but it also acts like the RFID identification process. The LCD replies with a brief "Processing..." message, and a red LED light up to show that the identification process has begun. After a short 3-second pause, which is similar to how long RFID identification usually takes, the LCD changes to "Start Charging." At the same time, a green LED lights up to show that the identification process was successful, and that the device is ready to start charging.

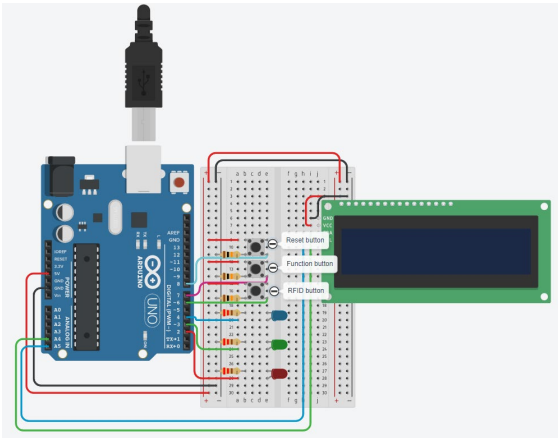

Figure 5: Screenshots of Prototype three - The Secure Code Enhancement

Prototype three acts as an improvement among all of the simulators and has the secure coding on the simulation.

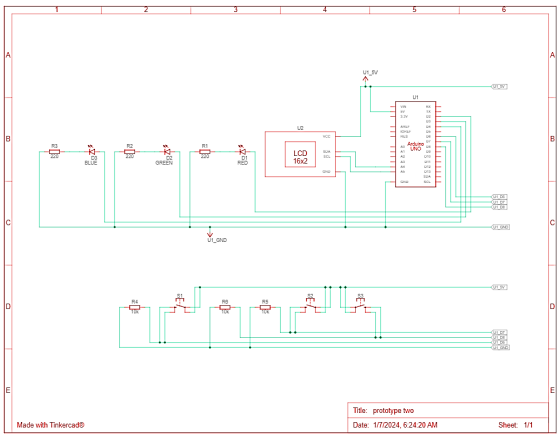

Figure 6: Design of Prototype three - The secure Code Enhancement

After simulation of RFID identification, the system goes through the usual charge cycle. After 3 seconds, "Finish Charging" appears on the LCD and a blue LED light up. The payment process is now finished with this step. A second button that resets the whole system has been added to make user contact even better. When you press this button, the system goes back to its original state and the welcome message shows up on the LCD. This reset function makes sure that the system is ready for the next person to use, making the experience smooth and easy.

In conclusion, the extended circuit system now includes RFID identification software, which lets users see how secure charging sites for electric vehicles are. This feature makes the system work better overall, giving users a more complete and interesting experience.

IX. Summary

The comprehensive testing journey undertaken for the Electric Vehicle (EV) charging station security assessment prototype has been notably fruitful, affirming the system's strength and user-friendly design. Throughout the rigorous unit testing phase, pivotal features, spanning system initiation, charging cycle progression, LED feedback, and RFID authentication, underwent meticulous scrutiny. The outcomes consistently mirrored anticipated results, marking a resounding "Pass" for all evaluated scenarios.

Transitioning to user acceptance testing, diverse user profiles—comprising electric vehicle owners, charging station operators, and educators well-versed on the Internet of Things (IoT)—actively engaged with the prototype. Electric vehicle owners lauded the intuitive interface, seamless responsiveness, and lucid guidance, contributing to an overall positive user experience. Charging station proprietors expressed satisfaction with the system's dependability, straightforward reset functionality, and the augmented security afforded by RFID authentication. Educators specializing in IoT recognized the prototype's alignment with IoT principles, scalability, and seamless integration capabilities.

The combined success in both unit and user acceptance testing serves as a robust validation of the prototype's functionality, reliability, and adaptability. The system not only proves itself capable but also exhibits considerable potential for further refinements, underscoring its prospective deployment as a secure, user-friendly, and IoT-ready solution for EV charging stations.

X. Unit Testing

User interaction with the Tinkercad EV charging system encompasses various testing scenarios, including the activation of the charging button, navigating through the complete charging cycle, triggering the reset button, and conducting multiple buttons presses to gauge system responsiveness. Furthermore, users engage with the RFID button, both with and without authentication, to evaluate its impact on system functionality. Throughout these interactions, feedback and display messages on the LCD screen provide crucial insights into the system's status and operations, enhancing user understanding. The simulation facilitates the execution of the entire charging process, allowing users to assess system responses to unexpected inputs and anomalies. This comprehensive approach to user interaction and system observation fosters a deeper understanding of EV charging station operations and reinforces practical cybersecurity education within the Tinkercad Arduino environment.

XI. Limitation

The primary limitation in executing my assignment lies in acquiring the necessary tools for simulating the simulator. Additionally, the chosen title is a novel subject in my country, given that electric vehicles and related companies recently commenced operations here.

XII. Conclusion

Evaluating an electric vehicle charging station is an important part of making sure that the rapidly growing world of electric transportation is safe, efficient, and lasts a long time. By looking at the charging station's physical, network, and working parts, this evaluation gives a full picture of its possible flaws, risks, and ways to make it better. The review results give charging station owners ideas on how to improve security and keep user data safe. They also give partners the tools they need to keep making the charging setting better for electric vehicles (EVs).

Peer review has many benefits besides its main goal of making sure safety. It creates a flexible framework that makes it possible for EV charging stations to grow, builds trust with customers, encourages technological progress, and makes sure that rules are followed. As more eco-friendly ways of getting around the world become popular, this review plays a big role in moving the business forward. It makes charging easier for people who use electric vehicle, gives station owners the tools they need to deal with new problems, and helps make the future more linked.

In the end, testing EV charging stations turns out to be an important part of building a strong, customer-focused, and safe charging network. This review gets us closer to a time when electric mobility is not only accepted, but also praised for how well it helps travel and the environment around the world. It works by dealing with many problems and taking advantage of chances that have been found.

References

1. Johnson, J., Anderson, B., Wright, B., Quiroz, J., Berg, T., Graves, R., Daley, J., Phan, K., Kunz, M., Pratt, R., Carroll, T., ONeil, L. R., Dindlebeck, B., Maloney, P., O'Brien, J., Gotthold, D., Varriale, R., Bohn, T., & Hardy, K. (2022, July 1). *Cybersecurity for Electric Vehicle Charging Infrastructure*. Cybersecurity for Electric Vehicle Charging Infrastructure (Technical Report) | OSTI.GOV. https://www.osti.gov/biblio/1877784

2. Acharya, S., Dvorkin, Y., Pandzic, H., & Karri, R. (2020). Cybersecurity of Smart Electric Vehicle Charging: A power grid perspective. *IEEE Access*, *8*, 214434–214453. https://doi.org/10.1109/access.2020.3041074

3. Sarieddine, K., Sayed, M. A., Jafarigiv, D., Atallah, R., Debbabi, M., & Assi, C. (2023). A real-time Cosimulation testbed for Electric Vehicle Charging and smart grid security. IEEE Security & Privacy, 21(4), 74–83. https://doi.org/10.1109/msec.2023.3247374

4. Luis, H. R. J., & Skármeta, A. (2020). *Security and privacy in the internet of things: Challenges and solutions*. IOS Press.

5. Mastoi, M. S., Zhuang, S., Munir, H. M., Haris, M., Hassan, M., Usman, M., Bukhari, S. S., & Ro, J.-S. (2022). An in-depth analysis of Electric Vehicle Charging Station Infrastructure, policy implications, and future trends. *Energy Reports*, *8*, 11504–11529. https://doi.org/10.1016/j.egyr.2022.09.011

6. Meng, W., Lee, W. H., Murali, S. R., & Krishnan, S. P. T. (2015). Charging me and I know your secrets! *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*. https://doi.org/10.1145/2732198.2732205

7. Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of Electric Vehicle Charging Station Management Systems. *Computers & Security*, *112*, 102511. https://doi.org/10.1016/j.cose.2021.102511

8. Jung, D., Shin, J., Lee, C., Kwon, K., & Seo, J. T. (2023). Cyber Security Controls in nuclear power plant by technical assessment methodology. IEEE Access, 11, 15229–15241. https://doi.org/10.1109/access.2023.3244991