Thesis Project Portfolio

Hijacking Power: Developing an Exploit for EV Chargers

(Technical Report)

The Creation and Building of Trust in an Online Voting System

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Thomas Windsor Antal

Spring, 2025

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Electric vehicles (EV's) have seen enormous growth over the last several years. This has led to a large uptick in the necessity for charging infrastructure, both on the road and at home. However, security is often the last thing users consider. My capstone project, which I conducted during an internship at Caesar Creek Software, was to reverse engineer a low-cost, at-home EV charger to find cybersecurity vulnerabilities. Ultimately, I developed an exploit that bypassed the RFID authentication and allowed anyone to charge their vehicle. The development process began with disassembling the charger, examining its internal components, and finding their datasheets. Next, I found that the creators of the charger had left serial wire debug (SWD) enabled, which allowed me to pull the device's firmware and decompile it using Ghidra. The device also had Joint Test Action Group (JTAG) enabled which allowed me to run a remote GDB server on the CPU. Together, these gave me both static and dynamic analysis of the firmware, and made developing an exploit significantly easier. I chose the RFID reader as my point of attack as it is the only part that takes input from the user. The exploit involved a minor edit in the firmware that overrode the validation and always opened the relay to allow for charging. The edited firmware can be installed in only a few minutes with the proper software and hardware, making it easy to deploy if physical access is possible. Future work would likely involve higher end models of the charger, which feature WIFI and Bluetooth, allowing for new attack vectors not present in my model.

In recent years, we have seen unprecedented attacks on the integrity of our nation's voting systems, particularly following the 2020 presidential election. Presidential elections have also seen record numbers of voters go to the polls, and yet over a third of eligible voters do not vote. This research paper dives into the feasibility of a new online voting system to rebuild trust and encourage voter participation. I utilized Actor-Network Theory to show the necessity for all human and non-human actors, as well as the fragility of the system. My research into the paper discusses the historical context of how election confidence has eroded from the 2000 presidential election, through the 2010s and up to the 2024 election. My research also examines failed attempts from other countries and the success of Estonia's permanent system. I also conducted a survey among college students to gauge public opinion, and 83% of responses indicated support for an online voting system. They were also asked about their biggest concern and the most common answers were fraud and security. My analysis shows that online voting could increase convenience and turnout primarily among college students, the disabled, and working-class individuals. However, an online only system could marginalize the poor and elderly as they may lack access to required personal technology. Building trust in a new voting system would be difficult and require grassroots efforts through those close to the system. Bipartisan support, open-source code, and legal safeguards against election denialism would be essential for this. In conclusion, online voting would not replace in-person voting, but rather supplement it to create a more equitable and convenient voting process. Future research should focus on technological infrastructure and increasing public awareness.

Critical government systems must go through rigorous penetration testing, or the process of simulating a cyberattack to see how a system performs. An online voting system would require a similar process, and likely be even more important if the code is open source. Reverse engineering can be performed on large scale infrastructure, not just physical devices. Government agencies or contractors could perform a reverse engineering project and use it as a way to catch issues before the system goes live. That team could be given full access to the source code and knowledge of how the pieces of the system interact. This would be difficult as the system would be enormous and likely take years, but this can be overcome with good coordination. The goal would be to prove that even perfect knowledge isn't enough to crack the system. If this is true, then a team of malicious hackers, who would have less knowledge, would not be able to damage the system. Hopefully, this would put the security concerns of individuals, especially those with cybersecurity experience, at ease and allow them to convince those close to them that it was secure as well. This kind of personal trust is extremely useful for tackling conspiracy theories, and could stop them before they begin.