2018

Threats and Mitigation of DDoS Cyberattacks Against the U.S. Power Grid via EV Charging

Glenn Sean Morrison
Wright State University

THREATS AND MITIGATION OF DDOS CYBERATTACKS AGAINST THE U.S. POWER GRID VIA EV CHARGING

A Thesis submitted in partial fulfillment of the
requirements for the degree of
Master of Science in Cyber Security

by

GLENN SEAN MORRISON

B.S.C.E., Wright State University, 2016

2018

Wright State University

WRIGHT STATE UNIVERSITY

GRADUATE SCHOOL

July 25, 2018

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY Glenn Sean Morrison ENTITLED Threats and Mitigation of DDoS Cyberattacks Against the U.S. Power Grid via EV Charging BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Science in Cyber Security.

_____

Yong Pei, Ph.D.
Thesis Director

_____

Mateen M. Rizki, Ph.D.
Chair, Department of Computer Science and Engineering

Committee on Final Examination:

_____

Yong Pei, Ph.D.

_____

Mateen M. Rizki, Ph.D.

_____

Vance M. Saunders, M.S.

_____

Barry Milligan, Ph.D.
Interim Dean of the Graduate School

ABSTRACT

Morrison, Glenn Sean. M.S.C.S., Department of Computer Science and Engineering, Wright State University, 2018. Threats and Mitigation of DDoS Cyberattacks Against the U.S. Power Grid via EV Charging.

Cars are an ever changing and integral part of modern society. Two of the biggest changes in vehicles today are their heavy integration with wireless communication and the push toward battery powered Electric Vehicles (EV). EV and EV charging stations have become a part of the Internet of Things (IoT). While this connectedness increases the convenience and functionality of the vehicles and charging stations, it also opens them up to a wide range of cyber threats.

This thesis examines the potential threats against the EV charging ecosystem through a historical analysis of past cyberattacks and identified vulnerabilities. As EV charging stations directly interface with the U.S. power grid, an attack initiated on EV and charging stations is capable of jeopardize the supply-demand balance of the power grid. If a large enough population is vulnerable to attack, then through a Distributed Denial of Service (DDoS) structured attack, the supply-demand balance can be exploited to cause widespread blackouts and grid instability. Using the historical analysis of cyberthreats, this thesis uses statistical analysis to hypothesize the feasibility of a DDoS cyberattack against the power grid using the EV charging ecosystem as an attack vector.

We then discuss potential mitigation strategies that can help reduce the chance of a DDoS style attack against the power grid using EVs.

Table of Contents

List of Figures

List of Tables

Acknowledgment

I would like to express my sincere gratitude to the following people, who have contributed to my knowledge through this thesis.

I would like to thank the Wright State University Department of Computer Science and Engineering faculty and staff for the teaching and guidance through my undergraduate and master's career. The knowledge obtained during my studies has helped shape the engineer I am today.

I would like to thank Dr. Yong Pei, my thesis advisor. His mentorship, expertise, and fun attitude helped guide and inspire me throughout my research. Working on this thesis has helped me find newfound interests in technology and cybersecurity.

Lastly, I would like to thank my friends and family who have encouraged and supported me every step of the way. This thesis would not be possible without them.

Chapter 1. INTRODUCTION

1.1 Vehicle Trends

Technology has been advancing exponentially since the 1960's. Most professionals in the technology and computing world are familiar with Moore's Law; the trend of transistors on a wafer doubling every couple years. This observation became a Manifest Destiny for the rate of progression for technology. Advancements in technology have impacted more than just the silicon in personal computers and laptops; it is now integrated into nearly everything humans use.

The spread of technology has forced vehicles to undergo an evolution of functionality and identity. Just as cell phones have become devices centered around everything but making calls, cars are no longer just a mechanical box with 4 wheels used for transportation. Modern cars are not focused on the destination, but the journey.

Cars have become a ubiquitous part of our lives and like most things, over the past few decades, technology has been slowly integrated into nearly every facet of cars. Almost all new cars come standard with automatic locks, automatic windows, cruise control, automatic braking, and sensors and warning systems for backing up and switching lanes. The infotainment systems have been upgraded from speedometers and odometers to include useful functions such as GPS navigation, voice control and feedback, performance and travel analysis, wireless communication, camera and sensor views, and a plethora of other technologies.

The future of today's modern, technology rich vehicles will involve even more technology integration. Two of the biggest trends in vehicles today are Autonomous Vehicles, fueled by the DARPA Grand Challenge [1]; and Electric Vehicles (EV), fueled by government regulation and the "Green Movement" [2]. This thesis will focus on EV, vehicles that run partially or entirely off battery power instead of using conventional fossil fuels and biofuels that most vehicles have used to date. Globally, EV sales have been increasing steadily, with the United States, China, and European countries such as the Netherlands showing the highest adoption rate, as seen in Figure 1. In the United States, California accounts for a vast majority of all EV in the country as seen in Figure 2. Although the timeframes differ slightly, both figures successfully demonstrate the overarching EV trends of today.

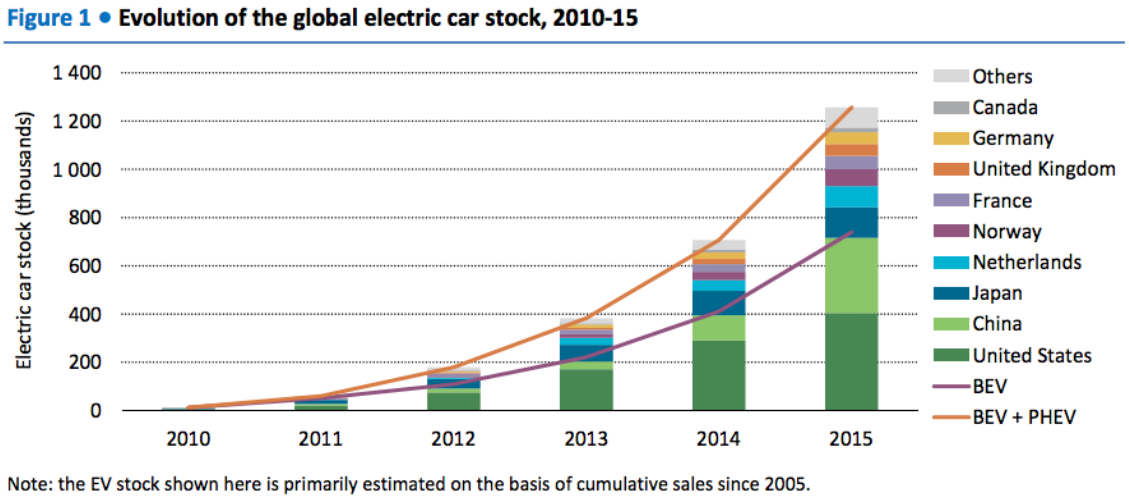

Figure 1.1 Global EV Trend 2010 - 2015 [3]

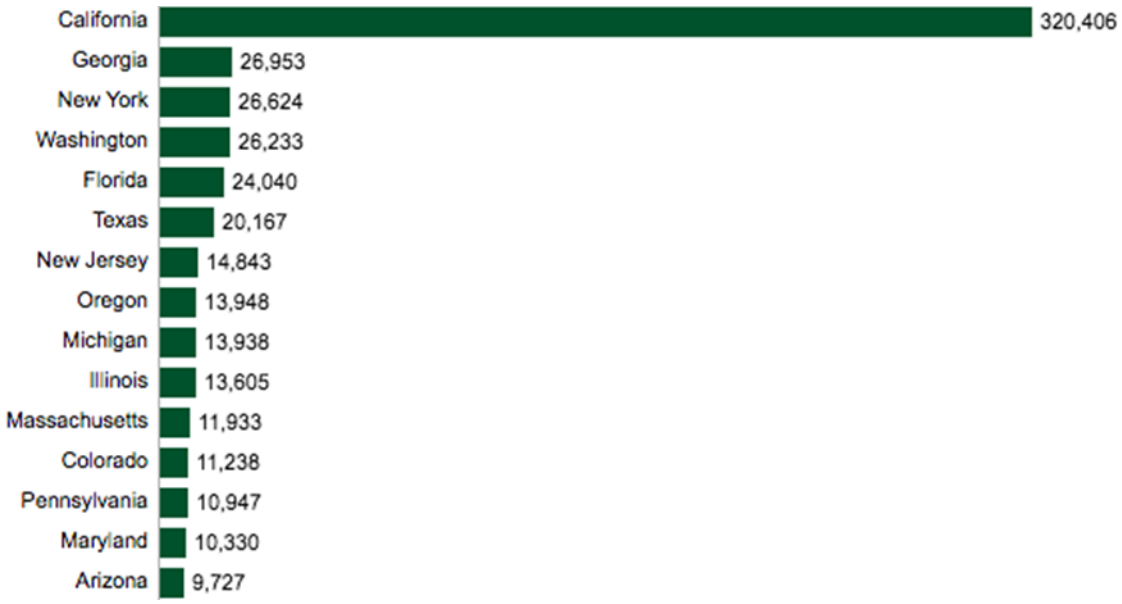

Figure 1.2 US EV Trend January 2011 - August 2017 [4]

1.2 Motivation

When conducting my research, I discovered that there are two topics that are being largely overlooked when discussing grid security and vehicle security:

1. Attacking the power grid indirectly by manipulating the systems connected to it and exploiting how the grid is designed to work
2. Attacking EV and charging systems for reasons other than stealing Personally Identifiable Information (PII) / billing information or commandeering vehicles and the associated safety implications

2.1 Analysis

The purpose of this thesis is to discuss potential cyberattack models on EV and EV charging stations and provide a statistical analysis of how they could be used as an avenue to attack the US power grid. Cybersecurity risks in EV pose social, economic, and political implications at the local, national, and global level. The power grid is the backbone of the US' critical infrastructure and much of the other critical infrastructures such as water, natural gas, communication, transportation, sanitation, and finance all rely on electricity to function properly.

This paper is broken into several sections.

- Chapter 1 served as an introduction to vehicles and their entrance into the cyber realm.
- Chapter 2 will provide the reader with pertinent background information regarding Cybersecurity, the US power grid, EV, EV charging, and the connections and relationships between them.
- Chapter 3 will discuss vulnerabilities and cyberattacks in vehicles, charging stations, standards, and the power grid to date.
- Chapter 4 will discuss realistic attack vectors, attack methodologies, build an attack tree, and analyze the scope and impact of a theoretical attack.
- Chapter 5 will discuss possible mitigation strategies to curb the feasibility of EV being used to attack the power grid.

- Chapter 6 will be a summary, conclusion, and discuss future work.

Chapter 2. BACKGROUND RESEARCH

2.1 Cybersecurity

Cars being integrated with technology, especially technology that involves communication, means that Cybersecurity needs to play an important role in its design and integration. Cybersecurity is a complex discipline. It is a relatively new subject whose scope and change of pace is far greater than nearly any other field. It is a recent byproduct of technological breakthroughs and the interconnectedness of the Internet in modern day society. As stated by Google's Eric Schmidt, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had [5]".

Over the past 40 years or so, technology and Internet has constantly changed and evolved. Many conventional items have been modified by the Internet. Fridges, coffee pots, lights, garage doors, thermostats, locks, surveillance cameras, and countless of previously "dumb" systems have been integrated with wireless communication for advanced features, convenience, and controllability. These systems have created a new group of devices called the Internet of Things (IoT). With the addition of wireless communication and control, cars have become an IoT device [6]. Being a part of the IoT group means that cars attack surface increases exponentially due to its connections to networks and other devices.

When discussing connected and communicating devices, the terms "cybersecurity", "threat", and "vulnerability" are often used. They are oftentimes interchanged, misused, and misinterpreted. The paper Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity by Jeff Hughes and George Cybenko [7] discusses key terms and concepts of cybersecurity today. The main points are briefly summarized below.

The basic characteristics that should be present in virtually any secure system: Confidentiality, Integrity, and Availability (CIA) [7] [8], sometimes called the CIA Triad [9].

- Confidentiality - Ensures that data is inaccessible, hidden, or unusable by anyone other than the owner or intended user.
- Integrity - Ensures that data is accurate and trustworthy and has not been modified or tampered with.
- Availability - Ensures that authorized parties can access their data at all times.

The basic characteristics of a Vulnerability: Susceptibility, Accessibility, and Capability [7].

- Confidentiality - Ensures that data is inaccessible, hidden, or unusable by anyone other than the owner or intended user.
- Integrity - Ensures that data is accurate and trustworthy and has not been modified or tampered with.

- Availability - Ensures that authorized parties can access their data at all times.

In order for a vulnerability to present, there must be a susceptibility that an attacker can gain access to and has the capabilities to exploit. Figure 3 below shows the relationship between the three characteristics.

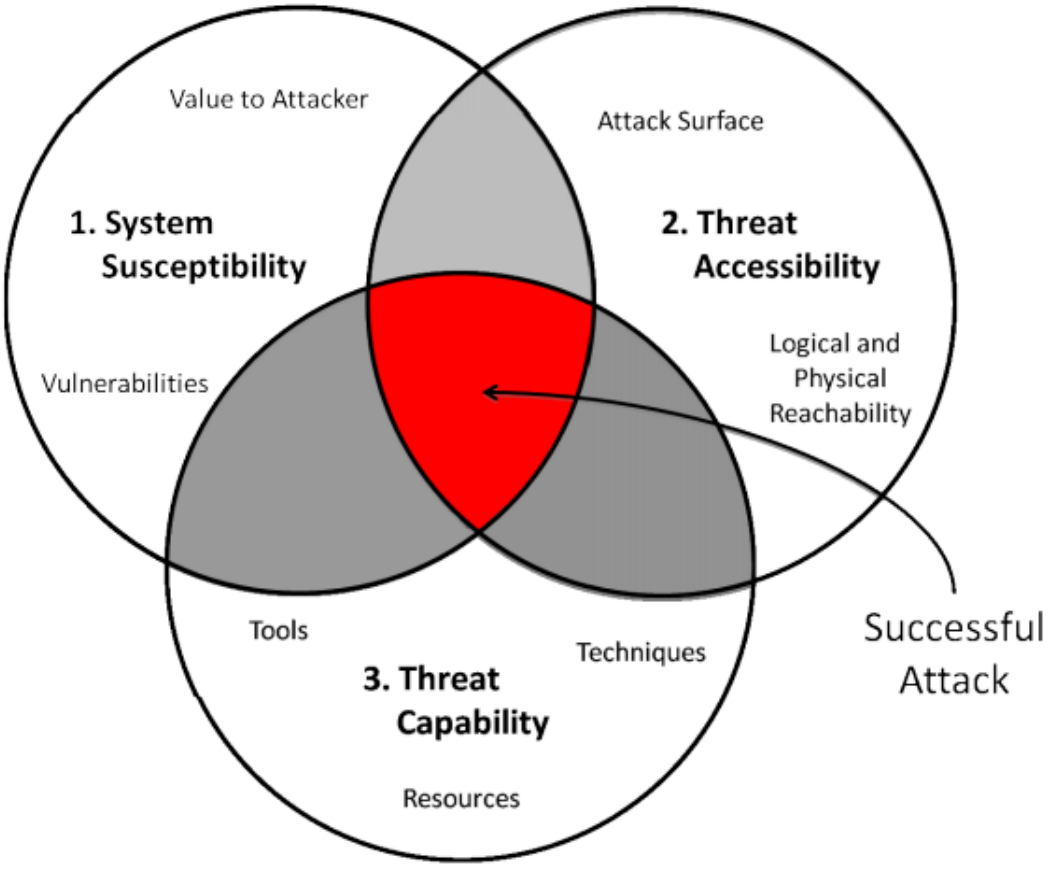

Figure 2.1 Characteristics of a Vulnerability [7]

As with all almost all technology, standardization, regulation, and security seem to be an afterthought and move at a much slower pace than technologies functionality

progression. Along with the uneven pace is the mantra of Murphy's Law extending into technology and cybersecurity; many experts argue that it is impossible to create a technology system that is completely secure. Much of cybersecurity is controlled by industry and capitalism. Instead of looking at cybersecurity from a traditional security viewpoint, cybersecurity is becoming a risk management exercise, and systems are designed as a sliding scale between usability, security, performance, and cost of a system.

- Usability is a subjective metric for how well humans can use and interact with a system.
- Security is a complicated metric that is usually based around CIA and any additional requirements. The required level of security is decided by the risk management analysis for a given system and varies greatly.
- Performance is an objective metric that is usually tied to specific requirements or performance benchmarks. As security increases it requires additional overhead which will impact the performance of the system.
- Cost is an objective metric that includes both the acquisition and sustainment cost of a total system.

Generally speaking, usability and performance are in direct contrast with security and cost, as demonstrated in Figure 4.

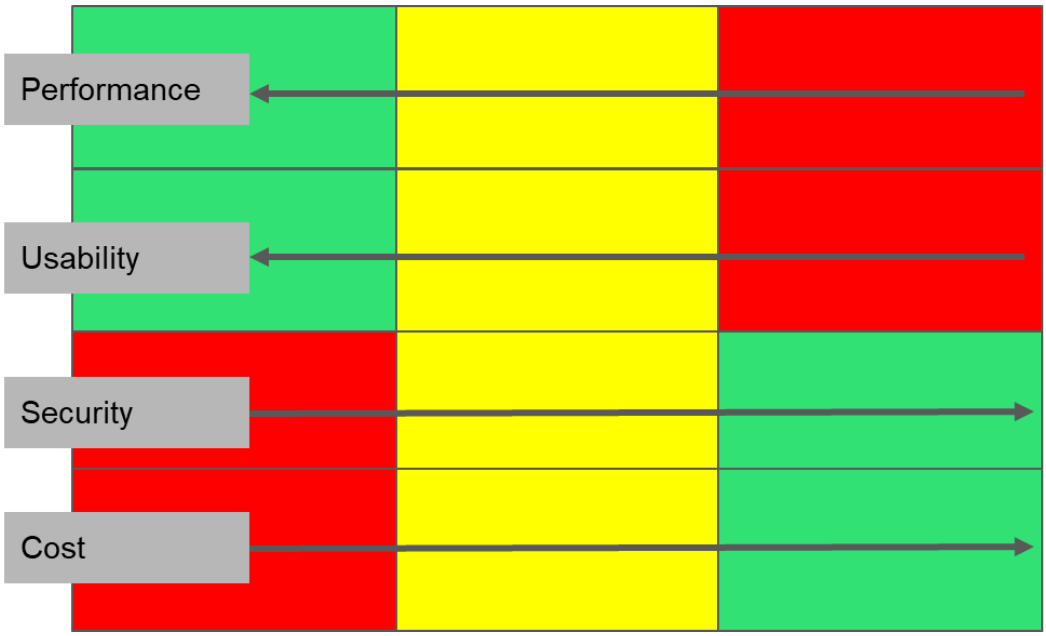

Figure 2.2 Cybersecurity Sliding Scale

Fundamentally, most entrepreneurs' goal is to maximize profit and provide a target level of quality, functionality, and security, with profit usually trumping all other characteristics. In order to maximize their profit, most systems are designed with the minimal amount of security possible. This practice will often create systems whose security is inadequate or becomes inadequate due to changes in technology. This approach is a major cause of a shortcomings or flaws in the CIA of a system and creates susceptibilities.

2.2 Electric Vehicles

2.2.1 Trend Analysis

Cars have been evolving for more than 200 years. Early models ran on steam, electricity, and internal combustion. During the early 20th century, almost 40% of American cars were powered by electricity. Due to the lack of electrical infrastructure, especially for charging, along with advancements in manufacturing and the cheapness of fossil fuels, internal combustion engine vehicles have dominated the market for a century. Vehicles like the Model T set a precedence for the vehicle ecosystem that we have today [10]. The internal combustion engine has shaped not only vehicles but national and global politics and economics. Manufacturing and processing capabilities as well as critical resource ownership has profoundly impacted the evolution of present day society [11].

Today, social, economic, and political motivations such as Global Warming and fossil fuel dependence have created a global drive for cars, and transportation in general, to transition to EV [12]. Over the past 20 years there have been economic and environmental pushes promoting hybrid and pure electric vehicles, especially in states like California, who are spearheading the development and integration of EV in the US [13]. As of January 2018, California aims to have at least 5 million EV on the road by 2030 [14]. With roughly 25.5 million registered cars in 2017, that would mean almost 20% of the current cars would be transitioned to EV [15]. As of October 2017, California had 337,482 pure EV [16].

As consumer trends continue to shift (as shown in Figure 1 & 2), big companies are responding by slowly moving to EV. Many companies are increasing their EV R&D budgets and have given public release statements regarding 10-year to 20-year plans aiming to move entire fleets to EV and hybrids [17]. These companies include big names such as Ford, GM, Toyota, Mazda, Daimler (Mercedes-Benz), Nissan, Mitsubishi, Jaguar Land Rover, Volvo, Volkswagen, Audi, and Porsche, and many more [18].

2.2.2 EV Classifications

There are three general types of EV: (1) HEV - Hybrid Electric Vehicles, (2) PHEV / EREV - Plug-in Hybrid Electric Vehicles / Extended-Range Electric Vehicles, (3) BEV / AEV - Battery Electric Vehicles / All Electric Vehicle [19].

1. HEV - Powered by petroleum engine at high speeds and battery engine at lower speeds and idle. Has rechargeable battery and petroleum fuel tank. The battery is recharged by regenerative braking [20].
2. PHEV / EREV - Powered by petroleum engine at high speeds and battery engine at lower speeds and idle. Has rechargeable battery and petroleum fuel tank. The battery is recharged by regenerative braking as well as plugging into a charging station.
3. BEV / AEV - Powered entirely by battery engine. Has large rechargeable battery. Utilizes regenerative braking and charging station to charge battery.

HEV and PHEV have a much smaller battery pack and much shorter electric engine travel range than a BEV. However, since the HEV and PHEV have a combustion engine, they have a far greater total travel range and are not limited by the lack of EV charging infrastructure [20]. All three use regenerative braking, a process that utilizes the kinetic and thermal energy lost during braking and transforms it into potential energy that is stored back into the battery. A graphic representation can be seen below in Figure 5.

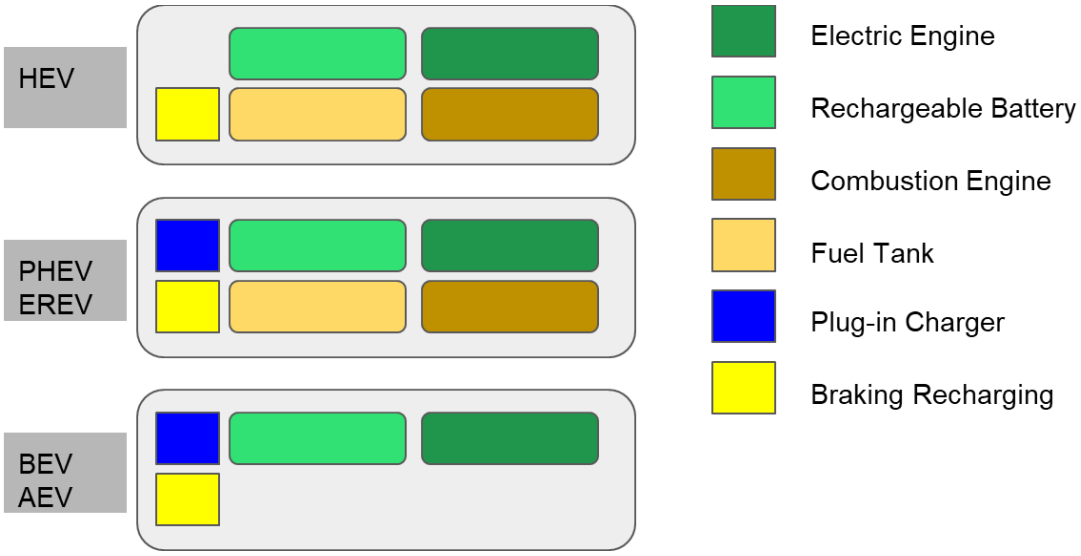

Figure 2.3 Types of Electric Vehicles

2.3 Power Grid

2.3.1 Basic Operation

The U.S. Power grid is a complex system of systems. “Local electricity grids are interconnected to form larger networks for reliability and commercial purposes. At the highest level, the U.S. power system in the Lower 48 states is made up of three main

interconnections, which operate largely independently from each other with limited transfers of electricity between them. [21]" They are divided as shown in Figure 6. The interconnect this paper will focus on is the Western Interconnection, which includes California.

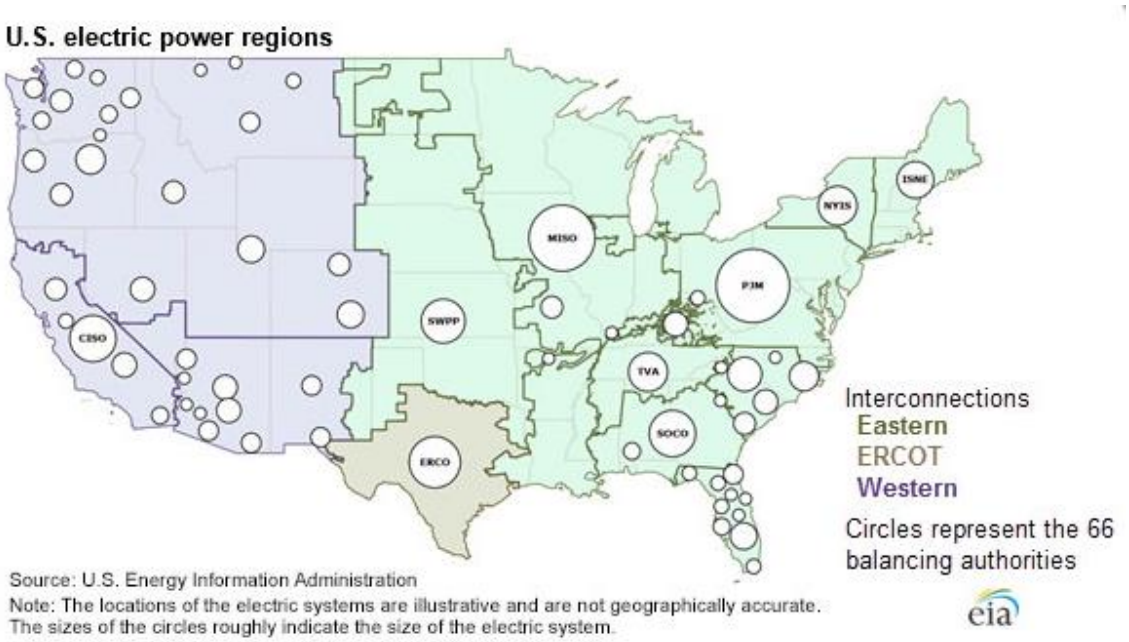

Figure 2.4 US Power Grid Regions [21]

The power grid is comprised of several systems that work to create, regulate, and distribute power. The main systems are [22]:

- Power plants - coal, nuclear, hydroelectric, geothermal, solar, wind, etc. In a majority of the cases, power source is harnessed in order to power a spinning electric generator, which is usually spun by a steam turbine.

- Substations - Regulate voltage from power station for transmission. Can be categorized into two kinds, step-up and step-down, which modify the voltage for transmission. In order to transmit power over great distances efficiently and reduce loss, the voltage must be stepped up to much higher than used by normal houses and businesses. Step-down substations are used to convert the voltage down to an easily usable level for most applications. Substations are also used as a pseudo circuit breaker for a general area it is distributing to.
- Transmission Lines - can be seen everywhere, varying load and size. Large high voltage lines carry load from power plant and substations great distances, several hundred miles. Power poles and underground lines carry power from transformers to their destination, usually not more than a few tens of miles. Can be 1, 2, or 3 phase power transmission. The main difference between the three types is the constancy of voltage delivery and the total amount of power that is able to be delivered in a single 360° cycle [23].
- Transformers - Look like metal trash cans on transmission poles. Used to regulate and maintain the voltage being sent into businesses and homes. Handles overcurrent and undercurrent conditions. Regulates the phase of power being sent, generally converting from 3 phase to 1 phase power.

Figure 7, below, is copied from *howstuffworks.com* and gives a very simple overview of how subcomponents of the grid are connected and interact. Real life implementations are more complex versions of interactions described above.

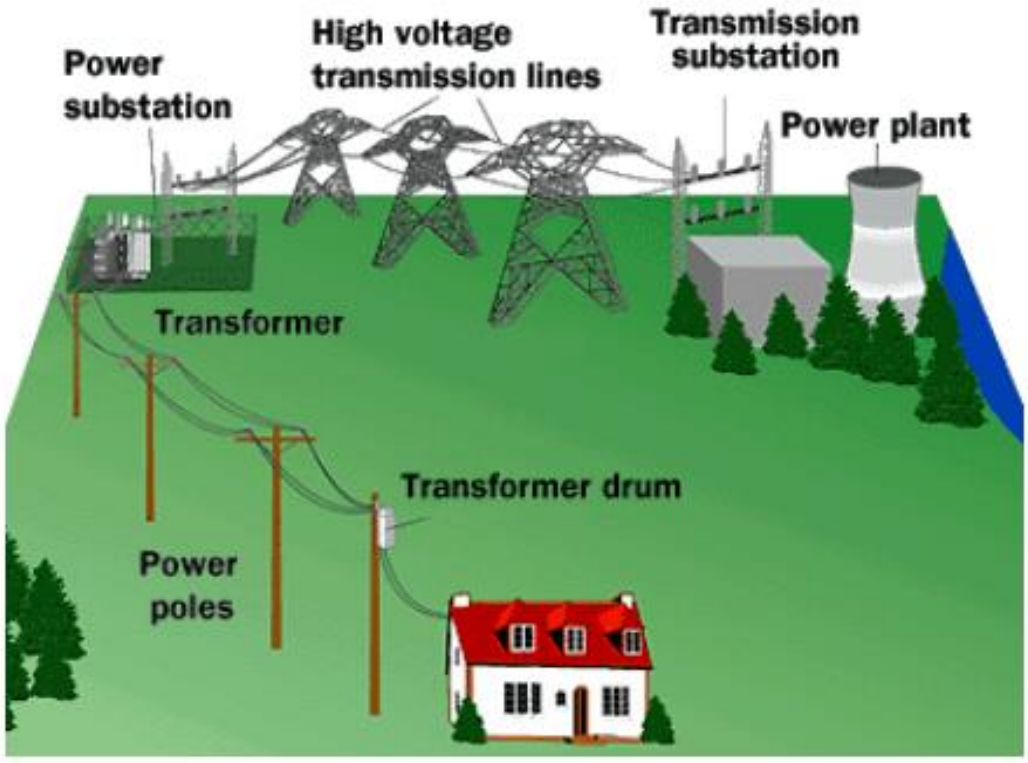

Figure 2.5 Power Creation and Transmission [22]

As mentioned, the U.S. power grid is a complex system of systems. One crucial part of that system not mentioned above are auxiliary power plants, sometimes called peak power plants. The continuously running power plants, simply referred to as power plants in this thesis, run 24/7, 365 days a year and make up a majority of the U.S. power grid. Auxiliary power plants are plants that are turned on and shut off to meet the daily

fluctuations in demand. The demand "... typically starts going up in the morning and peaks in the late afternoon and early evening [24]." Auxiliary power plants are generally small and designed to turn on and off to scale for the needs of target regions during peak hours. The size and number of auxiliary power plants for a given interconnect and sub-region is based on the many factors such as the population, climate, and social/cultural makeup of the region. Auxiliary power plants are also used to alleviate anomalies outside of the normal peak hour spikes.

Electric demand is made up of groups of stochastic and predictable variables. Every building, outlet, device, and person connected to the grid impact the demand. Power companies use statistical models, historical data, contextual data, and real time readings in order to loosely match power supply to the demand. Government regulations, industry standards, and capitalism all drive power companies to meet or exceed the power demand. Power consumption generally follows a rough bell curve, as shown in Figure 8 below [25]. Power consumption is at a low when the population is generally at home and sleeping. It steadily rises during the hours of a normal work day, mostly caused by establishments and workplaces. A large peak trend occurs in the afternoon when people would be coming home from work. Businesses will continue to draw steady power while residential usage such as electronics, appliances, and HVAC systems all cause this large spike. As the day progresses and turns to night, businesses close and people sleep, lowering the demand [26].

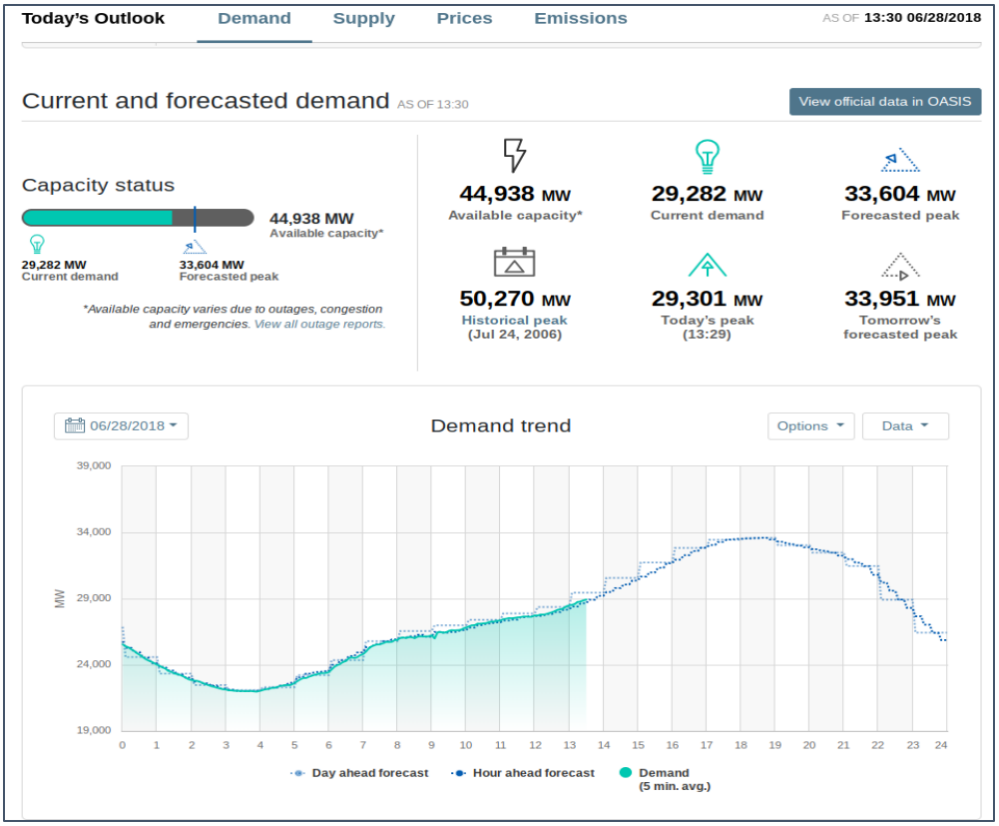

Figure 2.6 - California Supply-Demand Data (28 June 2018) [25]

2.3.2 Power Grid Properties and Contingencies

Electric supply-demand is an important variable for power plants. It plays a huge role on the economics, reliability, and quality of service being provided. The power supplied in the US is engineered to operate at a constant 60Hz throughout the entire system [27]. This frequency is used as a general indicator of grid health and supply-demand balance [28]. The relationship between supply-demand and frequency can be generalized to the relationships described in Table 1 below. Grid operators focus on frequency stability to maintain balance and protect the grid.

Supply-Demand Relationship	Impact on Frequency	Operation Nomenclature
Supply > Demand	Result Frequency > 60Hz	Overfrequency Event
Supply = Demand	Result Frequency = 60Hz	Frequency Balance
Supply < Demand	Result Frequency < 60Hz	Underfrequency Event

Table 2.1 Relationship Between Supply-Demand and Frequency (??)

Since it is practically infeasible to keep the frequency at a perfect 60Hz, each Interconnect has varying levels of operational tolerances. The accepted tolerance for the Western Interconnect is 60 Hz ± 0.036 Hz [29]. Operation is considered functional but degraded in the range $59.50 \leq freq \leq 59.97$. Operation is considered critical in the range if $freq < 59.50$ and extreme measures will be taken to attempt to restore balance and ensure safety of the grid. To ensure grid balance and safety, supply-demand fluctuations are controlled by 2 basic frequency response methods: Load Balancing and Demand Response.

Load Balancing is a supply-end approach, meaning it is deployed at the power plants. In a nutshell, load balancing is the predictive and reactive methods of generating power to match demand. Load balancing is used quite often in the form of powering up peak generators daily to match the peak power spike of the afternoon. During unpredicted and anomalous events, auxiliary generators are powered up to meet the demand [30].

The main issue with the load balancing is the timescale needed to get the generators up to speed to match the demand. It takes an incredibly long time to power up

generators, in comparison to the speed it requires consumers to increase the demand. Power generation is performed on the scale of minutes, hours, and even days. Power consumption is performed on the scale of seconds. Below is a breakdown of the main forms of power generation.

- During emergency situations, Ultra Fast Gas Generators, comparable to the turbines on airplanes, can be fired up within 5-10 minutes to react to the demand. Due to their intrinsic design and function, they are extremely expensive, inefficient, and produce a large amount of heat as a byproduct of power generation. Therefore, after roughly 15 minutes, they must be shut off to prevent damage. After being turned off, they cannot be used again until they have cooled down, been inspected, and undergone any required maintenance. This means that after running for a total interval of no more than 30 minutes, they require between 8-16 hours of downtime and inspection/maintenance [31].
- Internal combustion engine generators are another relatively fast and versatile power generation method but is relatively inefficient and expensive to use as a main source of power. Instead, they are generally used to help start other types of power plants start up and are used indirectly to heat steam to power steam generators [32].

- Conventional fossil fuel power plants such as a coal plant can take upwards of 4-8hrs to reach full power production depending on the size and integration of "fast start" mechanisms [33].
- Nuclear plants can take between 24-72 hours to start up and reach full operation. They are by far the most complicated and regulated power plants for startup procedures and pre-start inspection requirements [34] [35].
- Renewable forms of power generation are generally the most cost-effective methods of power generation and therefore are fully utilized in normal power generation and not used as responses to frequency events [36].

Due to the limitations of power generators, there must be faster measures in place to help balance the grid. That is where Demand Response (DR) comes into play. Demand response is a demand-end adaptation to grid imbalance. Essentially, DR comprised of a host of balancing strategies that will attempt to meet or curtail the demand in order to maintain a healthy frequency. Demand response is designed to operate on the scale of seconds to minutes, reaching full effectiveness between 30 seconds and 1 minute, and operating for about 15 minutes to allow a transition period for Load Balancing to kick in [28].

The first layer of DR is the Interconnection Frequency Response Obligation (IFRO), as mandated by the North American Electric Reliability Corporation (NERC), the governing body for power reliability in North America. IFRO is the minimum

capacity value that interconnects are required to have in order to handle large changes in demand without contingencies and failsafe's being triggered. It is essentially the requirement for the entire interconnect region as a whole to create a certain amount of surplus power that can be used to handle atypical, non-peak underfrequency events. The IFRO value is different for interconnect and is reviewed and updated accordingly by the NERC [37]. The values are summarized in Table 2 below. The importance and implications of the Western Interconnects IFRO value will be discussed further in Chapter 4.

Interconnect	Load (MW)	Frequency Deviation (Hz)	Contingency Trigger Deviation (Hz)
Eastern	1015	0.1	0.5
Western	841	0.1	0.5
ERCOT	380	0.1	0.7

Table 2.2 IFRO Minimum Requirements for Interconnects [37]

When IFRO fails to manage spikes in demand, two contingencies are in place to help achieve balance and protect the grid: Under Frequency Load Shedding and Under Frequency Generator Protection.

Under Frequency Load Shedding (UFLS) is a protective measure that is triggered when frequency response methods have failed to stabilize or correct a drop in frequency. It is tightly calibrated with IFRO and designed to initiate if IFRO fails [38] It is designed primarily as a contingency for islanded generators during a power imbalance and is

comprised of several stages. It will begin shedding the load from predetermined customers in a hierarchical order. It will continue to drop service until all stages have been iterated through. If UFLS fails, a second contingency will trigger [39].

Under Frequency Generator Protection (UFGP) is a protective measure that will trip the generator if it is exposed to sustained low frequencies or large spikes in low frequency. Depending on the severity and duration of the frequency imbalance, UFGP may be triggered before UFLS has finished its shedding procedures [39]. Essentially, if the generator begins to operate in a range that is deemed a safety hazard to the generator or other power components it is connected to, it will be disconnected from the grid and powered down to a safe state.

While UFLS is designed to automatically recover and restore the system to normal operation over a period of time if balance can be achieved, triggering UFGP is much more serious as it is designed as a final failsafe and requires human intervention and safety protocols to be performed before the generator can be spun up and reattached to the grid. UFGP can also cause a cascading effect on other generators in the network, exacerbating the grid imbalance [39]. Below, Figure 9 shows the underfrequency response relationships.

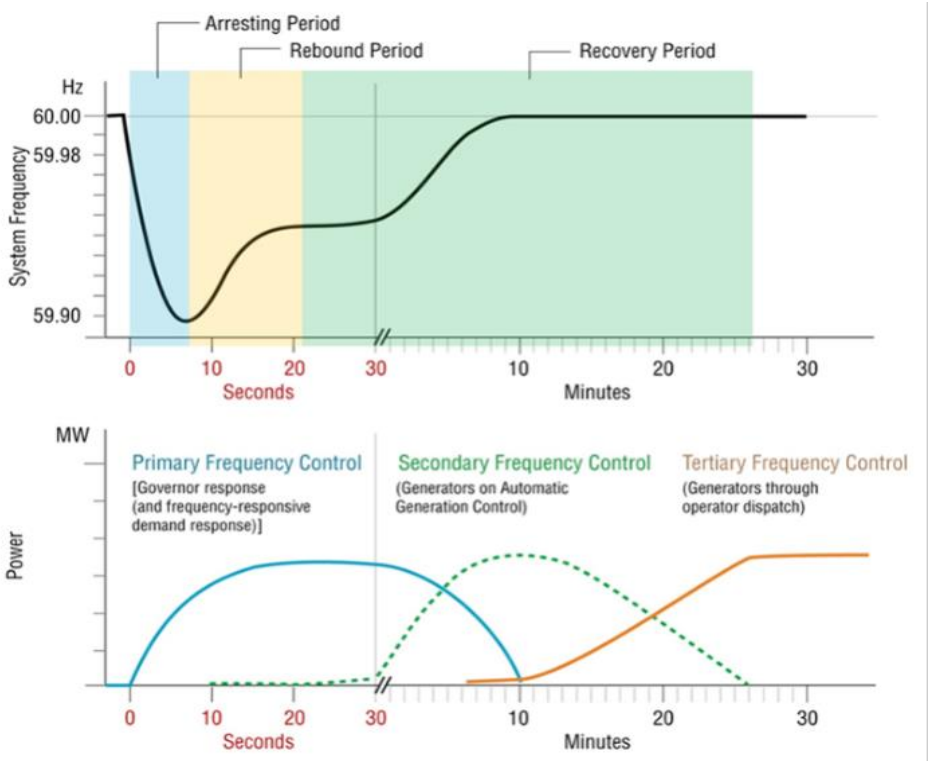

Figure 2.7 Power System Frequency Control [40]

2.3.3 Power Grid Failure Modes

The following section provides a brief description of key failure modes associated with power plants and the power grid. The two main modes of failure are overcurrent and undercurrent scenarios. This thesis focuses on undercurrent induced failures. Refer back to Table 1.

- Overcurrent is caused by a drop in demand, causing more supply of power than is needed. Overcurrent events are uncommon and can usually be controlled by simply putting the excess power to ground or power storing methods. Under

extreme circumstances, the current will force contingencies such as circuit breakers to trip in order to protect components [41].

- Undercurrent is caused by a spike in demand, causing there to be not enough power to meet the demand. The undercurrent control methods have been explained above, including Load Balancing and DR.

Overcurrent and Undercurrent situations have the potential to cause severe impacts on the grid, including [42]:

- Brownout - A degraded service state where partial or complete power loss will happen intermittently, usually caused by frequent and large oscillations in power. This can be noticed by the dimming of light bulbs and appliances being power cycled and reset.
- Blackout - A complete loss of power to a given service area. Can be cause by an emergency event or intentionally by power distributors.
- Rolling Blackout - A complete loss of power to several service areas where the blackout period is split among the regions, usually caused intentionally by power distributors.
- Cascading Failures - An event or series of events that causes the systematic failure of a system until a steady state can be reached or total system failure has occurred. This is considered the most severe of the failure modes of a system [43].

2.4 EV Charging Stations

EV chargers are the “gas stations” that EV use to recharge their batteries. The charging stations are the medium through which power created at power plants is measured, regulated, and distributed to EV. Charging stations can be broken up into 3 tiers [44] [45]:

- Level 1 - The charging interface is your standard home outlet, using a normal 3 prong adapter to plug into the wall. The peak power that can be drawn from most standard residential breakers is roughly 1.5 - 2.0 KW [46], with each outlet in the house set at a substantially smaller portion of that. Roughly speaking, it takes somewhere between 12 - 24 hours to fully charge most EV today, providing a Range Per Hour (RPH) charging rate of 4.5 miles/hour [44].
- Level 2 - The charging interface will require a control box and a 240V connection, equivalent to what many household appliances use. The peak power of these boxes ranges greatly, from around 1-2 KW all the way to 19 KW. The average charge rate usually associated with these chargers during discussion and analysis is 7 KW. The charge rate that the stations are able to produce is highly dependent on the EV being plugged in and most models cannot utilize a rate above 7.7 KW. As a generalization, Level 2 chargers can provide up to 25 -30 RPH using 7 KW station, reducing the full charge time to just a few hours [47].

- Level 3 - The charging interface will require a control box and custom interface to the power grid via a 480V DC plug. Level 3 charging is often referred to as DC Fast Charging [45]. There are several notable physical standards for DC Fast charging, including CHAdeMO, SAE, CCS, and Tesla Supercharger [48]. The similarities and differences between the Level 3 chargers are irrelevant to this thesis. What is important is they provide incredibly fast charging, being able to provide an 80% RPH value in is as little as 30 minutes. Level 3 charging can reach up to a 90KW peak when charging

Global industry and research interest focused on increasing the RPH rate and greatly increasing the peak power rate, with the "European Commission's trans-European transport network (TEN-T)" being a driving force, aiming to create 350KW superchargers [49]. While massive superchargers could have enormous implications on power grid management and stability, this thesis is focusing on Level 2 chargers. Level 1 chargers pose the same level of risk that a toaster or microwave does. Today's Level 3 superchargers are not readily available to the public, costing near $100,000 in many cases. Level 2 chargers do not require any extensive changes to install and are relatively cheap, with units costing several hundreds of dollars to a few thousand, making them similar to buying an appliance like a dryer or fridge. With level 2 operating at a rate of 7 KW, they have the ability to draw the same amount of peak power that 3 - 4 residential homes could.

When discussing the overall operation of any level of charger, there are two main standards. The first is ISO 15118 - Vehicle to grid communication interface [50]. The most current version of the ISO was published in 2013. Industry has essentially taken over standardization of EV charging with the Open Charge Point Protocol (OCPP), managed by the Open Charge Alliance, "a global consortium of public and private electric vehicle (EV) infrastructure leaders that have come together to promote open standards [51]" for EV charging. The OCPP is separate from ISO 15118, however much of OCPP is loosely based on ISO 15118 standards, with OCPP version 2.0 having direct interface modules for compatibility ISO 15118 devices [52]. OCPI is another protocol that will not be covered in this thesis, which is designed as a communication procedure for different charging providers to communicate and share information, much like how ATMs allow different financial institutions to use them [53].

The standard interface used by most Level 2 chargers [54] [55] is the SAE J1772 standard, which defines the socket and interface of a charging source and an EV. Competing Level 2 standards such as Tesla [56] have begun supporting the J1772 standard. CHAdeMO and SAE CCS as well as Tesla's interface still dominate the Level 3 charging domain, which remains largely divided [57]. The charging point and EV communicate with each other via Pulse Width Modulation (PWM) over the J1772 interface. Requests for charging, charging rates, current rectification, and other charging management is decided by the EV and sent to the charging station [58].

Chapter 3. THREATSCAPE

This chapter will discuss and enumerate the threatscape for the Power Grid, EV, and EV charging. To date, there has been no recorded attack on the power grid using EV. However, an in-depth threat analysis will be presented in order to help explain the vast threatscape surrounding the scenario. Analysis from this chapter will used in Chapter 4 to discuss possible attack scenarios based off of the current threatscape. The attacks and vulnerabilities discussed will be separated into separate groups to provide simple delineation and categorization.

3.1 History of Power Grid Vulnerabilities

The purpose of this section is to discuss threats and vulnerabilities against the power grid. It separated into cyber and no cyber vulnerabilities.

3.1.1 Weather and Natural Disasters

Although unrelated to cyber, the impacts and trends of nature induced scenarios can be used in impact analysis.

Natural disasters are a constant threat to the power grid, especially its transmission systems. Large storms, hurricanes, tsunamis, earthquakes, and other disasters can cause long lasting and serious impacts on power generation and transmission. One of the most notable power disasters during my lifetime was the Northeast blackout of 2003. A large storm paired with system contingency failures cause most of the Midwest and parts of Canada, around 50 million people, to experience a

widespread blackout [59]. While most only experienced a blackout for around 2-4 days, my housing development was in the dark for almost 6 days. It had a huge impact on my family and community. Although the cause of the blackout isn't relevant to this thesis, its impact has served as a first-hand basis for how big of an impact wide scale power loss can have. Hurricane Maria is another notable crisis, where up to 400,000 Puerto Ricans are still without power 6 months after the disaster. Grave social, cultural, and economic issues have stemmed from the prolonged power loss [60].

Seasonal weather patterns can also have a large impact on the grid. Historically, during the summer months, heatwaves can put a huge strain on power plants [61] [62], especially in states like California [63], and some have even been attributed to blackouts [64]. This strain is primarily caused by Heating, Ventilation, and Air Conditioning (HVAC) units. On especially warm and humid days, AC units will begin running earlier, run for longer periods of time, and continue running past their expected daily runtime. This spike in demand has not caused any wide scale, prolonged blackouts to date, however the peak electricity being used has exhausted a large portion of California and the Western Interconnects peak, auxiliary, and contingency power generation and frequency balancing [65]. The ability to use AC units in order to perform localized cyberattacks is something that is currently being investigated [66].

3.1.2 Cyberattacks Against the Power Grid

Arguably the first cyberattack against critical infrastructure systems was Stuxnet, a covert malware deployed in 2010 by the US and Israel against Iran. The malware caused equipment in Iranian nuclear refinement facilities to become damaged, halting their refinement efforts. The overall motivation behind it's deployment was to prevent war, specifically nuclear warfare from triggering between Israel and Iran [67] [68]. While the effort can be considered a political success, many consider the event to be a Pandora's Box, ushering in a new age of cyberattack [68]. Below is a summary of cyberattacks against power grids in recent history. As explained below, the frequency and severity of the attacks is increasing. Attacks have been attributed to individuals, groups, and nation states, with Russia being the most infamous in targeting the power grid.

3.1.2.1 Havex

Starting in 2007 and ending in 2014, a malware dubbed Havex was discovered, targeting SCADA and Industrial Control Systems (ICS), systems in Europe. Although it did not cause any blackouts and no damaging payloads were delivered does not mean the attack isn't serious. It was a "Stuxnet like" Advanced Persistent Threat (APT) that was designed to harvest critical data from SCADA and other industrial systems [69]; data that could be used to craft very sophisticated and specific attacks. It also provided data that would be necessary for attackers to analyze in order to understand the systems operation, layout, dependencies, and other situational information only known to the ICS operators. Although mostly found mostly in Germany, Switzerland, and Belgium, Havex was also

discovered in an isolated case in California. The malware was spread using a waterhole technique, where victims were drawn to an array of spoofed or infected pages which used scripts or trojan downloads to infect their targets [70].

3.1.2.2 Dragonfly

For several years leading up to 2014, A variant of the Havex malware, called Dragonfly, is attributed to attacks across ICS and Pharmaceutical systems in Europe and the US [71]. Like the original Havex malware, it was a APT cyberespionage tool used to gather critical information. Aside from general improvements and adaptations to improve functionality and infection, the main difference between Havex and Dragonfly are the targets. It targeted Switzerland, Turkey, and the US, with a majority of the infections occurring in the US [72].

3.1.2.3 Blackenergy

Starting in 2014, a variant of Havex and Dragonfly called Blackenergy was discovered. Blackenergy has targeted SCADA systems across multiple ICS, focusing power generation and transmission systems [73]. Mostly found spread across Ukraines energy sector, Blackenergy has managed to show up across the globe. The attacks have been attributed to Sandworm, an alleged Russian Hacking Group who has been tied to a wide range of cyberattacks [74]. Blackenergy at its core is an APT who provides attackers with Backdoor, Rootkit, Arbitrary Code Execution, and Botnet functionality. It is delivered via spear phishing attacks against carefully selected individuals. A modified

Blackenergy has also been discovered that performs additional cyberattacks such as cyber extortion, data destruction, PII theft, and spam distribution [75].

3.1.2.4 Attack on Ukraine

Russia and Ukraine have been in an “undeclared war” since 2014 when Ukraine and the rest of the Crimean Peninsula was forcefully annexed by Russia. Since then, Ukraine has been under all forms of attack and repression, including cyberwarfare. This cyberwarfare is far reaching, and according to Ukraine's Chief of Cyberpolice, occurs every day and targets all aspects of society [76]. Some have described the attacks as “a digital blitzkrieg”, alluding to the war strategies of the the Nazi’s during WWII [77]. One of the most notable attacks were during During 2015 and 2016, when Russia attacked Ukraine’s power grid several times, targeting several major power companies. These attacks used a combination of malwares and attack techniques, including spear phishing using Blackenergy. The attacks were able to successfully Distributed Denial of Service (DDoS) and damage the software in SCADA systems, causing widespread blackouts for prolonged periods of time [78].

3.1.2.5 Dragonfly 2.0

Beginning in 2015, a new strain of Dragonfly called Dragonfly 2.0 was discovered. It has been tied to most of the critical infrastructure cyberattacks across the globe over the past 3 years [79]. Like its predecessors, Dragonfly 2.0 is an improved APT

whose strains make use of all the latest malwares, infection techniques, zero-days, and known but unpatched exploits [80].

3.1.2.6 Attack on Ireland

The state-owned Irish power supplier EirGrid targeted by cyberespionage attacks during mid 2017. After discovery, experts estimated that the systems had been infected a few months prior to discovery [81]. Although little information has been released, many experts believe that the breaches are likely caused by the Dragonfly 2.0 malware [82].

3.1.2.7 Attack on US

According to the Department of Homeland Security and the FBI, the US has been closely investigating and tracking cyberattacks against critical infrastructure since 2016 [83]. During May of 2017, the Wolf Creek nuclear power plant in Kansas was penetrated. While no operational systems were commandeered, the extent of the network penetration and what information was stolen remains unclear [84]. Although there was no official attribution for the attacks, reports from security experts conclude that modified strain of Dragonfly 2.0 was used [85].

During March of 2018, US critical infrastructure underwent a wave of cyberattacks, impacting “electric, nuclear, water, aviation, and critical manufacturing sectors” [86]. Security experts believe that version of Dragonfly 2.0 was also used in the wide array of attacks which show extreme levels of sophistication and specialization [85].

In response, the Trump Administration has publicly accused the Russian Government for the wave of cyberattacks against US critical infrastructure [83] [86].

Although no serious damage has occurred as a result of recent cyberattacks against the US, the malware responsible, Dragonfly 2.0 or a newer strain, is an adapted version of the Blackenergy malware that has been used in serious attacks that caused blackouts for extended periods of time in Ukraine. It is likely that the malware used in recent attacks have had the ability to disrupt power but lacked the information for a successful attack to be carried out. Originally, in 2014 the NSA briefed congress that "China" and "one or two other countries" could have the ability to launch a cyberattack on the US power grid [87]. China has been conducting cyberespionage with APTs for a while now, however most of the efforts to date have been focused on R&D data, intellectual property, and financial and trade secrets, not critical infrastructure [88]. On the world stage, Russia appears to be at the spearhead of developing critical infrastructure cyberattacks.

Security experts and government agencies are not the only people concerned with cyberattacks against the grid. Lloyd's of London, and insurance firm, put together a financial report that discusses a plausible attack scenario and discusses implications [89]. Their research was focused on the Eastern Interconnect, which is comprised of 15 different states and Washington D.C. [90]. Based on their analysis of grid operations and connections, Lloyd's determined that it would only take the removal of 50 out of the 700

power generators, roughly 7.15%, in the Eastern Interconnect in order to cause widespread blackouts [91]. In another scenario, only 9 transformers would need to be disabled [89]. The attacks could leave an upwards of 93 million people without power and cost insurance companies 10's of billions of dollars [91]. The scenario in the report is described as a "fictionalized account based on several historical and publicly known real-world examples" [92]. While their attack scenario, termed "Erebos" does not provide any technical instruction on how to carry out an attack, it has many of the same characteristics as the Russian APT's enumerated above. Their attack also is modeled to take place during the summer due to the increased electric demand and strain that HVAC systems put on the power grid [92].

3.2 History of Vehicle Vulnerabilities

The purpose of this section is to discuss threats and vulnerabilities associated with non-EV and EV to date. While their propulsion systems are different, there are similarities between their control, safety, and infotainment systems.

3.2.1 CAESS

Cybersecurity concern and analysis of cars essentially started around 2010 when researchers at the Center for Automotive Embedded Systems Security (CAESS) published a paper titled Experimental Security Analysis of a Modern Automobile, which focused on finding out just how secure the electronic components in cars were [93] [94]. The results of their research indicated that nearly every aspect of cars were insecure. The

main limitation of their research was that direct physical connection to the vehicle via the ODB-II and other busses was required at some point to attack the system [95].

One year later in 2011, the same group from CAESS published a second paper called Comprehensive Experimental Analyses of Automotive Attack Surfaces, which built upon their original attack model from 2010. Instead of requiring physical connection to the car, they were able to attack it using the mp3 player, the Bluetooth module, and telematics unit [95] [96]. The authors concluded that cars could be hacked and exploited remotely, however they did not provide explicit details, only a demo.

3.2.2 Miller and Valasek

The main shortcoming of the CAESS research was that they did not provide the tools, methodologies, or attack details in their papers. DARPA became interested in vehicle cybersecurity and in 2012, two researchers, Charlie Miller and Chris Valasek were awarded a DARPA grant to produce a "library of tools that would aid in continuing automotive research and reduce the barrier of entry to new researchers into the field" [95]. The two were able to create a cyber analysis toolkit and released step by step technical documentation demonstrating a wide array of attacks on a 2010 Ford Escape and 2010 Toyota Prius, including taking control of the steering wheel and disabling the brakes [97]. Although they created a toolkit and demonstrated attacks, industry downplayed their research because they had not been able to figure out the secrets that

CAESS had in order to remotely hack and control the car and all of their work was done via a physical connection.

Pleased with their work, DARPA awarded the two another grants in 2013 to continue their research and expand their tool kit to function to include simulated vehicle systems. Even with their free introductory toolkit, vehicle security research was incredibly cost intensive due to the need to purchase a vehicle to use as a testbed. Their solution was to create a starter framework for Electronic Control Units (ECU), sensors, and other standard hardware in vehicles. Instead of spending thousands of dollars on a vehicle, researchers could spend a few hundred dollars buying sample hardware from critical systems inside vehicles. Their research, titled “Car Hacking: For Poories” [98] provided all of the technical data needed to get mini-testbeds up and running.

In 2014, after expanding their toolkit, they began to gather data on vehicle architecture in an attempt to classify and group vehicles based on their expected attack surface, design complexity, and overall security present in the communication busses. Their analysis landed them on a 2014 Jeep Cherokee [95]. Over the next year, Miller and Valasek were able to hack into the Jeeps WiFi unit through its hardcoded password, which is based on the model and year of the car. After connecting to the WiFi unit via the Sprint cellular network, they were able to discover a connection between the multimedia system the vehicles Controller Area Network (CAN) bus. The multimedia system was not designed to talk to the CAN bus, but the found a loophole through an ECU called the

V850, which was designed as a listen only device that monitors the CAN bus for specific messages. The V850 was designed to accept firmware upgrades with no authorization requirements. Over WiFi, they were able to update the V850's firmware and begin sending communication to the CAN bus [99]. After establishing this connection, they were able to send any command they desired, and therefore control the vehicle as they saw fit [100]. The 2014 Jeep Cherokee hack remains one of the most famous and well documented vulnerabilities discovered to this day.

3.2.3 Mathew Solnik

During 2014, another DARPA grant winner named Mathew Solnik, was also able to demonstrate remote car hacking and control. Using the cellular network, Solnik was able to gain remote access to a Honda Accord and manipulate its CAN bus [101]. The attack leveraged vulnerabilities he discovered in the implementation of the client-side GSM/CDMA protocols in the cellular unit of the car. By jamming the cellular signals, the car was expecting such as 3G or LTE, the cellular unit would broadcast information on earlier versions of the cellular protocol, such as 2.5G. Using these broadcasts, he was able to abuse the protocols functionality and crack the authentication and transport security measures. Once connected, he was able to rewrite the firmware to allow complete control of the cellular unit [102]. The method in which Solnik gained control of the CAN bus were not included in his Blackhat 2014 presentation.

3.2.4 BMW

During 2014, the German Automobile Association did a research study on the cybersecurity of BMWs. Using the cellular unit and its connection to Connected Drive, they performed a Man in the Middle (MitM) attack that gained them access in a matter of a few minutes. Due to the nature of the attack, the breach was undetectable. Their research excluded any interaction with the CAN bus, although remote hacking of a communication module is serious and plays a key role in crafting a more serious attack [103].

3.2.5 DARPA

During February of 2015, DARPA gave a presentation on 60-Minutes showing the remote hacking of a Chevy Impala that leveraged security flaws in General Motors (GM) OnStar systems [104] [105]. The special showed DARPA's Dan Kaufman remotely controlling the Impala's acceleration and braking. No technical details were released during the news broadcast; however it can be reasonably assumed that any and all of Miller, Valasek, and Solnik's research could have been used to craft the attack.

3.2.6 Tesla

During 2015, Kevin Mahaffey and Marc Rogers presented a Tesla Model S hack at the DEF CON hacking conference. The duo found 6 unique security flaws that allowed them to conduct their attack [106]. Vulnerabilities included the digital car keys being stored in an insecure tar file, plaintext passwords stored in insecure folders, and static

WiFi security procedures that allowed easy spoofing of a trusted connection. The overall severity of the attack was low with little CAN bus control, and the hack required physical access in order to gain all of the necessary information [107[. Nonetheless, they worked with Tesla and the issues were patched over the air within a week.

In 2016, researchers at Keen Security Lab were able to remotely connect several versions of Tesla's model S and assume full control of the cars infotainment and CAN busses in both park and drive mode. Details of the attack were not disclosed due to the "responsible disclosure" policies of the organization [108].

3.2.7 Hacking Community Trends

As vehicle cybersecurity have become more prevalent, so has the hacking community. There are a wide array of tools designed to analyze, control, and distort physical vehicles, ECUs, and CAN busses, as well as emulators and training tools [98] [109] [101] [110]. The hacking community believes that the best way to promote security is to remove obscurity and get as many people involved as possible. However, there is always the possibility that these tools can be used as the foundation for more nefarious actors.

This hacking trend can also be loosely compared to the seemingly harmless culture "motorheads", or car enthusiasts. There are underground communities of those seeking to modify their vehicles control systems for top performance. Usually, their modifications involve electronic control of the drivetrain or fuel system and removing

governor that limits the top speed of the car. In order to perform many of these operations, very specific information is required such as hard coded security values, admin information, and maintenance information [111]. This community has been hacking their cars for years, and as vehicles evolve, they likely begin to use and contribute to the hacking and security communities that analyze EV.

3.3 History of Charging Station Vulnerabilities

There is a wide array of vulnerabilities present in charging stations. This section will focus on covering vulnerabilities related to the remote access of charging stations and the protocols used for remote access. Most charging stations are equipped with wireless communication to manage charging, perform billing, and update the systems. The communication technology includes WiFi, cellular, Bluetooth, and RFID [112]. The addition of networking means that like EV, EV chargers can also be considered an IoT device. Being an IoT devices means the device becomes susceptible to a wide array of attacks [113].

3.3.1 Germany

In December of 2017, Mathias Dalheimer, a technical expert from Fraunhofer Institute for Industrial Mathematics ITWM [114], conducted extensive research regarding the current charging infrastructure of charging stations all over Germany [114]. The country as a whole saw an increased average of a few hundred percent per state, with Berlin experiencing an astonishing 3700% increase in charging infrastructure, a trend we

will likely start seeing in large American cities [115]. He developed a custom Level 2 charger interface that allowed him to analyze and manipulate information being sent to and from the charging station and has provided technical instructions to make your own [116]. His research concluded that the charging stations were plagued with security vulnerabilities.

A majority of his analysis was focused on the information share between the phone app, the vehicle, and the charging point to the billing backend that manages the charging. The issues touched at least 4 unique charging services including New Motion, BMW Charge Now, E-Wald, and Ladenetz, and he suspects that many more have the same issues. He found several issues such as:

- Storing the UID as plaintext length 20 char (sole authentication variable), where 8 bytes are the ID token and the rest of the bytes can be set based on the service provider.
- Using a provably insecure cryptosystem called Mifare for transmission
- No challenging methods in authentication of UID

He also focused on testing the security of a Hager and KEBA charging modules, both popular and widespread across Germany. In both systems, network information regarding the charging can be viewed on port 8080, which is HTTP, meaning it is unencrypted. All charging activity, control messages, and requests are sent over port 8080 or 8081. By performing a MitM attack, he was able to sniff the traffic and parse all messages, as well

as send spoofed messages [115]. Using Shodan, a simple tool that can be used to discover IoT devices, he was able to find the charging station as well. With the IP:Port known, he could craft any messages he wants to the charging station, for example starting and stopping charging [117].

The stations are also equipped with USB ports. Their purpose is for service technicians to be able to troubleshoot and update the systems. By plugging a FAT32 USB drive into the station, he was able to discover everything about the charging station, including the firmware version, ifconfig data, and admin username and password, which were factory defaults. Security flaws included [115] [116] [118]:

- The only requirement for overwriting the system configuration was to name the new configuration file the same name and replace it. Update process requires no authentication
- The same update process could be initiated via HTTP. Just initiate a Telnet connection and launch the shell
- All processes run by the system had root privileges
- Updated configuration files can be used to enable arbitrary code execution, using string concatenation was able to run custom scripts (buffer overflow). In this case he just ran an 8-bit display with messages such as “pwnd” and “charge free today”, but much more serious actions can be performed on power control and charging systems including simulating artificial charging events.

A new charging feature called Autocharge can initiate charging events using only the MAC address of the car as an authentication token. While MAC address space iteration suffers from computational infeasibility issues, the MAC addresses are auto generated at the factory that the NIC is created and therefore the make, model, and year of the car can be used to narrow down the address space. Using Spoofed MAC addresses is currently only a concern for energy theft, since a physical device is required to initiate charging [116].

In his closing remarks, he described the current charging infrastructure as a "loose collection of technologies". Due to the current architectures of the charging stations and EV, drastic changes to improve the security of the charging process are not likely. He made references to solutions such as standing up PKI infrastructure, which could not be supported by the current ARM based systems used in the charging process. Certified smart meter gateways, which would be standalone modules that maintain regulation and security of electric transfer, would need integrated into the charge points, and would be incredibly costly to certify, integrate, and maintain [116].

3.3.2 Hack in the Box

Ofer Shezaf, founder of OWASP Israel presented charging station hacking methodologies at Hack in the Box. His main findings determined that charging stations had several vulnerabilities that would normally be protected by even the simplest of administrators in a traditional networking setting [119].

Like most researchers, he found that the security of RFID billing procedures were missing. Most of the information was sent in the clear and easily captured via MitM attacks. Some stations were protected by symmetric encryption. After further examination, he discovered that the symmetric key was the same for all stations of the same type, meaning that once you extracted it via physical interactions with the station, you could then perform a MitM attack on the encrypted traffic [120]. He also found that the WiFi wireless communications were HTTP and could be subject to MitM attacks as well as Injection attacks [120]. He concluded that weaknesses in wireless communication allowed for DoS and data theft cyberattacks.

3.4 History of Protocol Vulnerabilities

The protocol vulnerabilities covered in this section are focused on OCPP. The charging station ecosystem is comprised of mostly OCPP based systems. Big issue and reason why OCPP rules the charging protocol battle is because ISO standards are expensive to obtain and OCPP is open source. This costliness of ISO standards is also reflected in my ability to find sources. A majority of the vulnerability analysis I found is focused on diagnosing and treating OCPP vulnerabilities. The version of OCPP found in nearly all charging stations today is OCPP v1.5, which was released in 2012. A newer version, OCPP 2.0 was released during April of 2018, and is not included in the scope of this assessment [121]. From this point, the phrase ‘OCPP’ implies OCP v1.5.

3.4.1 OCPP

The OCPP protocol is designed to coordinate communication between a charging point, power manager, and EV. The main focus of the protocol is to provide a clear method for charging to be metered and controlled and a majority of its structure is comprised of communication between the charge point and power manager. OCPP is "mainly concerned with reservations and management of charging processes with restricted security considerations, principally limited to ensuring that charging is performed only when authorized by a billing system" [122]. OCPP communication utilizes Simple Object Access Protocol (SOAP), an Extensible Markup Language (XML) extension over HyperText Transfer Protocol (HTTP) via Transmission Control Protocol (TCP)/Internet Protocol (IP). All communication and data requests within the protocol are performed using the SOAP framework which facilitates the sending and receiving functions in human friendly plaintext [123]. The protocol recommends that securing critical information by implementing Transport Layer Security (TLS) or WebSockets (WS) where needed but does not explicitly implement it within OCPP [122].

As described previously in vulnerabilities found in charging stations, sending messages via HTTP means that data is vulnerable to packet sniffing. This packet sniffing allows for MitM type attacks including [122] [124] [125] [126]:

1. Eavesdropping
2. Packet spoofing, sinkhole attacks, and session hijacking

3. DoS, both communication and charging
4. Financial impersonation and energy theft
5. Impact charging station power stability

Sending messages via HTTP is the most common communication method. As a solution, charging station developers can implement low level security implementations such as TLS. This encryption only provides the illusion of security. If an attacker is performing reconnaissance on the network traffic around the charging station, they will see the initial bootstrapping and node commissioning messages sent via HTTP. In a race condition, the attacker can send a spoofed packet using the obtained public key and nonce value to establish a secured connection with the charging station [122].

TLS does not provide end-to-end security since the attempt at a secure tunnel described above would only be between the charging point and the initial interface of the billing back end. Any intermediate points in the billing back end is only required to use HTTP, therefore there is no way to guarantee the integrity of the response [125].

Using the RFID UID as the sole token of authentication in the billing scheme with weak challenging allows for credential theft in the form of [125]:

1. Eavesdropping
2. Brute force

Encapsulating existing and familiar protocols into OCPP helps provide familiarity and robustness in its use and implementation [123]. However, utilizing existing protocols means that the encapsulated protocol runs the risk of inheriting vulnerabilities from the underlying protocols. For example, after exploiting the insecure nature of HTTP, attackers could perform XML Injection, potentially altering the intended logic of the protocol and allow for code injection. The TCP/IP protocol itself is also vulnerable to TCP RST and SYN flood attacks [122]. It is also worth mentioning that Injection attacks rank #1 on the list of top security risks of 2017 [127].

3.4.2 SAE J1772

During my research, I found no documentation describing vulnerabilities or exploits of the J1772 connection between EV and charging stations. The interface is a physical link, with low level communication link, and does not directly impact decision making or power management.

3.5 History of Application Vulnerabilities

A common trend becoming available to most vehicles is increased convenience and control through the use of phone applications. Used to control location data, lock/unlock, and starting ignition. Most charging stations are also equipped with phone apps. The following section will discuss recent vulnerabilities discovered in vehicle related phone apps.

3.5.1 Tesla

In 2014, Nitesh Dhanjani found two vulnerabilities in Teslas phone app. The app can perform a wide array of features including monitoring the location, starting and stopping the car, controlling charging, controlling the headlights, locking and unlocking the doors, and even control the sunroof [128].

The first vulnerability was the password system. The Tesla app is secured with a 6-digit password and the app did not force a lockout due to multiple failed login attempts. This allowed for easy brute forcing [129]. The most challenging part of hacking into the app was knowing the attacker's login email. Obtaining an owners email could be accomplished relatively easily using spear phishing attacks or other forms of social engineering [130].

The second vulnerability was Tesla's REST API. Tesla users email, and password are stored in a cleartext data token in the apps directory. Although it was not Tesla's intention, 3rd party app makers started to create Tesla apps that invoked parts of the Tesla REST API. Essentially, app makers could create apps that were able to make a get() API call that would retrieve the owners login information. Once this information was retrieved, it could be redirected to the 3rd party apps folder, stealing the password and allowing them to do whatever they want with it [129].

3.5.2 Nissan

In 2016, vulnerabilities in the Nissan Leaf's companion phone app were discovered. The vulnerability was centered around the phone apps implementation and some social engineering paired with brute forcing. The major issue with the app was that it did not use any form of authorization to validate requests. The only thing required for the app to function was the cars VIN number, which is stenciled into most car's windshield dashboard [131]. Aside from walking up to the car and copying the number, brute forcing the VIN number would not be too hard. Most of the VIN number digits can be assumed based on the cars make, model, year, and country of origin [132]. This could reasonably narrow down the guess space to 5 digits. After further research, it was also determined that commands could be sent from a web browser, making brute force all the more feasible. The attack could not be carried out while the car is moving, however.

3.5.3 Hyundai

In 2017, a vulnerability in the Hyundai Blue Link phone app was discovered that allowed attackers to locate, unlock, remote start, and steal vehicles. The technical details of the attack were not released, however the research firm who found the vulnerability said the exploit was made possible by a bug implemented in one of the app updates. The bug could allow attackers to steal the owners account information from user WiFi transmissions and use the legitimate app functionality to steal the car [133].

3.5.4 Android

In September of 2017, Kaspersky reviewed “nine mobile apps from the largest car manufacturers” [134]. Their analysis focused on analyzing app security against the 3 largest security threats that malicious Android apps have historically used: malicious rooting, malicious overlay, and malicious code injection. Their analysis found that 0 of the 9 apps protected against any of the 3 forms of malware. Using malicious rooting, the security researchers at Promon were able to create a nefarious version of the Tesla app that would steal the owner’s username and password. The app would broadcast the information to attackers, and they even stood up a fake Tesla server which allowed them to initiate the keyless driving function, allowing the car to be stolen [135].

3.5.5 Charging Station Considerations

I was unable to find any documentation regarding vulnerabilities in charging station phone apps. One thing to consider is indirect exploitation through charging apps dependencies. A star example is ChargePoint’s companion app, which provides a wide array of charging control features. In order to increase the capabilities and convenience of the app, they have integrated it with 3rd party services like Nest and Alexa [136]. Adding trusted functionality for 3rd party apps could be a potential susceptibility for the companion app.

3.6 History of IoT Vulnerabilities

Because EV and EV charging stations are now a part of the IoT category, this section will provide a brief overview of a few IoT vulnerabilities.

3.6.1 DEF CON

The IoT Village at DEF CON held an IoT hacking competition. The results of the competition found 47 IoT vulnerabilities across 27 unique devices. The vulnerabilities affected a wide range of devices, including door locks, thermostats, refrigerators, wheelchairs, WiFi range extenders, routers, and even solar panel arrays. Vulnerabilities included insecure and hardcoded passwords, buffer overflows, command injection, password sniffing, replay attacks, and cross site request forgery. To date, the IoT Village efforts have discovered 113 total IoT vulnerabilities over the past few years [137].

3.6.2 Dyn DDoS Attack

During October of 2016, Dyn, one of the world's largest Domain Name Server (DNS) providers, fell victim to one of the largest DDoS attacks ever recorded. The attack was able to bring down many big-name domains such as Twitter, Amazon, Netflix, Reddit, CNN, BBC, Paypal, and Github [138]. DNS is a critical component in the Internet's infrastructure, managing the relationship between human friendly domains such as www.google.com and its respective IP address.

The attack was carried out by the Mirai Botnet [139]. Using a worm to spread itself across the Internet, it targeted IoT devices. The worm exploited a wide variety of

poor security implementations ranging from poor design, hard coded passwords, factory default passwords, hidden admin access points, and even some which had no authentication process. Once the worm gained access to the device, it deployed the botnet code into the RAM of the device, which would take control of the device. Once fully infected, the new IoT bot would notify the C&C server and scan the Internet for a new device to infect [140]. A key to Mirai's success was that it did not remove the IoT devices functionality, so the DVRs, IP cameras, thermostats, baby monitors, routers, and other IoT devices continued to work as intended. This was important because the malware was running from RAM; if a user cycled the power on the device in an attempt to fix it, Mirai would be removed from the device [141].

Mirai was used to perform thousands of attacks over a few months. Several attacks were record breaking, with the attack on Dyn being the largest and most impactful, with its effects being felt globally. The attack on Dyn spanned a period of about 8 hours, was deployed in 2 phases, and is estimated to have used roughly 100,000 compromised IoT devices [142]. The second phase of the attack, dubbed a "water torture" attack, indirectly attacked the domains by targeting the operation of DNS itself. The attack focused on overwhelming the targeted domains authoritative DNS server, sending a loop of recursive queries [143].

The attack on Dyn was the first of its kind in both complexity and magnitude. The root cause of the attack was the poor security and management of IoT devices. Today,

many of the security issues found in Mirai are still ranked at #1 for the OWASP vulnerability chart [144]. IoT botnets are a huge problem today and will continue to be a problem until manufactures and users start taking serious measures to secure their devices.

Chapter 4. REALISTIC ATTACK SCENARIO

The purpose of this chapter is to discuss a realistic attack scenario based on the historical analysis of vulnerabilities and attacks mentioned in Chapter 3. The complexity of the relationship between EV, EV chargers, charge managers, the Internet, phone applications, and the power grid makes crafting cyberattacks a nontrivial task. Creating a successful attack will likely require an incredibly complex attack path that makes use of several vulnerabilities across several components in the charging path. Figure 10 is a graphical representation of the interconnectedness of the charging process. An important trend to notice is that all parts of the system are directly or indirectly connected to the Internet.

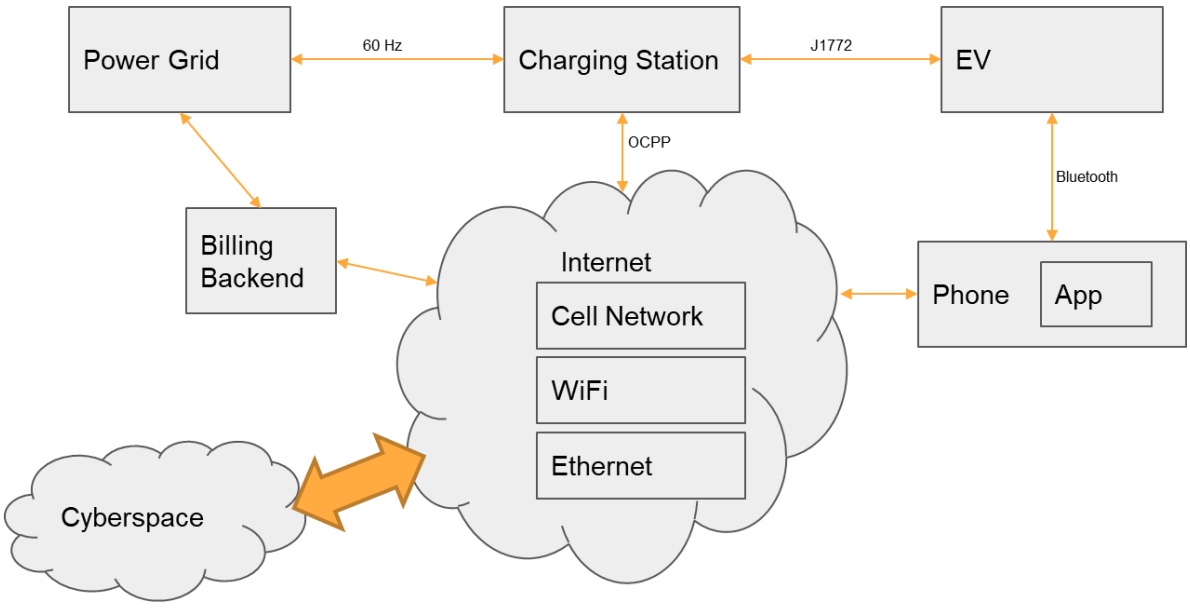

Figure 4.1 Relationship Between Components

The current ecosystem of home chargers do not include a billing backend tied to a charging manager. This further reduces the attack scope and attack constraints of the possible scenarios. Without the billing backend, there are less connections to the power grid and charging stations. However, this is favorable for an attacker because it further reduces the authentication and management of the charging process.

The only requirements for standing up a Level 2 charger in your home is a dedicated 240V circuit in your home breaker and compliance with US Fire Code and other safety regulations regarding the stations placement and installation [145]. At most, electrical contractors may need to expand the current electrical infrastructure of your house if your breaker cannot support a dedicated 240V circuit, however this is rare since many common home appliances such as stoves and washers/dryers use the same circuit.

Once installed, home chargers generally need to be connected to the Internet in order for them to provide their full range of services; the popular ChargePoint home station is a good example. After connecting to the home breaker, the charging station needs to be configured. Using their phone app, you are required to create an account and provide your personal information. Then, using your phone, you find your home charger and connect it to WiFi. Once connected to the network, the station can be controlled remotely. It can be configured to to auto charge, by time, by price, or be manually controlled using the phone or web app [146]. Other brands, such as EV Box [147], Blink [148], and Tesla [149], use similar methods of setting up and managing home chargers.

The ability to control charging over the Internet without the need to talk to the billing backend [150] gives attackers more freedom to conduct their attacks, as described in the section below.

4.1 Attack Goals and Possible Attack Paths

The DDoS cyberattack against Dyn was described in Chapter 3. Using a botnet of IoT devices, the attackers were able to indirectly attack domains by attacking the fundamental functionality of the DNS service upon which they relied. The goal of the following attack scenario is to discuss a similar attack: DDoS cyberattack against the US power grid indirectly by creating a botnet that can manipulate the supply-demand balance of the grid. In order to be able to manipulate the supply-demand of the grid, attackers must be able to remotely control the charging behaviors of charging stations in a scalable manner. This can be done by:

- Directly controlling the charging station via the Internet
- Indirectly controlling the charging station via phone applications
    - Directly controlling the charging station via vehicle companion app
    - Indirectly controlling the charging station via charging applications

4.1.1 Directly via Internet

Threat scenarios discussed in Chapter 3 regarding current charging stations and OCPP showed a wide range of vulnerabilities. This attack focuses on directly communicating

with the charging station. Charging stations are vulnerable to [115] [116] [118] [122] [124] [125] [126]:

1. Eavesdropping and credential theft
2. Packet Spoofing and other MitM based attacks
3. Sinkhole attacks
4. Unchallenged/unauthenticated remote firmware updates
5. Remote arbitrary code execution via Injection and Buffer Overflows
6. Remote control of charging events
7. Remote simulation of charging events
8. Defeat TLS via race conditions

The charging station is connected to the Internet so that it can receive updates and management remotely. The Internet can be used to remotely update the firmware and remotely manage the device providing functions such as restarting the system or starting and stopping charging events. Using the remote firmware update process, an attacker could install a malicious update that modifies the firmware to accept commands [123]. Updating the firmware would allow for injection of additional functionality to the attacker, such as methods for maintaining communication with the C&C Server.

To start an update, all you need to do is send the charging station an UpdateFirmwareRequest.req() message. The message only includes the URL where the update can be downloaded and control variables such as date and time. During the

update, the managing party can send FirmwareStatusNotification.req() to monitor the update progress. The final FirmwareStatusNotification.conf() message will notify the managing party that the update is complete. During a normal operation, the managing party is the vendor that creates the charging station. However, if an attacker is able to identify the IP address of the charging station, they will be able to craft their own malicious update request. Since no authentication is required to initiate a firmware update, it will automatically attempt to update after the date and time in the message [151]. The Web Service Description Language (WSDL) for the functions can be seen in Figure 11.

```
216
217         <s:complexType name="UpdateFirmwareRequest">
218           <s:sequence>
219             <s:element name="retrieveDate" type="s:dateTime" minOccurs="1" maxOccurs="1" />
220             <s:element name="location" type="s:anyURI" minOccurs="1" maxOccurs="1" />
221             <s:element name="retries" type="s:int" minOccurs="0" maxOccurs="1" />
222             <s:element name="retryInterval" type="s:int" minOccurs="0" maxOccurs="1" />
223           </s:sequence>
224         </s:complexType>
```

Figure 4.2 Firmware Update WSDL [152]

The attacker can control the charging behavior using RemoteStartTransaction.req() and RemoteStopTransaction.req(). RemoteStartTransaction.req() requires a unique charging ID and the ID of the charging connector being used [151], as shown in the WSDL of Figure 12 [152]. When used by a public charge point, the unique charging ID is sent to the billing backend for verification.

However, at home charging stations, there is no billing backend so the devices are set to default accept whatever the charging ID is. The only thing that the attacker needs to get right is the device ID and charging port ID. By performing eavesdropping, the attacker can determine necessary information to craft spoofed charging request packets. The attacker also could have modified the firmware to accept specialized control packets that can be used to control charging events.

```
259         <s:complexType name="RemoteStartTransactionRequest">
260           <s:annotation>
261             <s:documentation>Defines the RemoteStartTransaction.req PDU</s:documentation>
262           </s:annotation>
263           <s:sequence>
264             <s:element name="idTag" type="tns:IdToken" minOccurs="1" maxOccurs="1" />
265             <s:element name="connectorId" type="s:int" minOccurs="0" maxOccurs="1" />
266           </s:sequence>
267         </s:complexType>
```

Figure 4.3 Charging Event WSDL

4.1.2 Indirectly via Phone Application

Companion phone apps for charging stations and electric vehicles are an incredibly common feature today. While phone apps add convenience, they also add another layer of vulnerabilities. Specifically, the Android platform has a long history of vulnerabilities and exploits. A study by Kaspersky [134] determined that of the “top” 9 vehicle apps, none of them provided protection against the 3 most common Android attacks:

1. Malicious rooted apps

2. Malicious overlays
3. Malicious Code Injection

Researches at Promon were able to demonstrate that, using existing malicious rooted apps, they could easily replace the Tesla app on a persons phone and enable total control of the car and steal their login credentials [135]. Although there are no reported cases of charging station credential or vehicle credential thefts reported in the wild, that does not mean its not a threat. In 2017, Google took down 700,000 malicious apps from the Google Play Store [153]. That still didn't stop roughly 50 malicious apps from slipping through, which resulted in millions of downloads [154]. Malicious apps that can steal credentials or subvert apps will also commonly sell their abilities to the highest bidder. After the app is established, they will transfer it to a new entity that will use the malware for whatever they want.

If a phone can be compromised, an attacker could attempt to remotely control the charging through either the vehicle or through the station itself. The charging can be controlled by EVs in a scenario where charging is configured to auto charge; the charging station will begin charging once plugged into an EV with no charging credentials required [155]. If the attacker can control the vehicles charging behavior, they can start and stop charging regardless of the charging station. This situation is less likely as EV owners will likely try to obtain premium rates for charging by scheduling it for non-peak hours such as late at night.

The second and more powerful attack would be gaining control of the charging stations phone app. Using stolen credentials or a subverted app, the attacker could directly control charging events. Stolen credentials can be used to log into the charging stations web application and send charging commands. Using network analysis tools, the attacker could figure out how the web application sends the commands and use the stolen credentials to create a script that will automate the commands to all the stolen accounts. Using a subverted app, the attacker could add additional functionality that silently listens to a C&C server for instructions on when to launch the attack.

4.2 Attack Feasibility

The attacker is not constrained to one attack path. Using all 3 attack methods will give the attacker the highest chance of success. Diversity of charging stations will not help as many versions of stations have been found to be incredibly insecure. As realized in the Dyn attack, there are a large number of device owners that do not go through the proper measures to secure their IoT devices. Using a tool such as the Shodan command line library [156] allows for easy searching for vulnerable charging stations. Tools such as wireshark [157] can be used to monitor the traffic at vulnerable IPs and libraries like pcap [158] or netwox [159] can be used to send attack packets. The authors of Mirai posted its source code publicly available online [160], giving attackers pointers on how a similar attack structure could be designed.

The C&C server should be managed and operated outside of the zone that is being attacked to ensure that the connection persists. As power is restored to areas, charging stations will come back online and can be directed to begin charging again, exacerbating the power recovery efforts.

The attacker could use other situational variables to enhance their chance of success. If they chose to perform the attack during a heatwave in the summer, HVAC units would be putting extra strain on the power grid. This could be used to help ensure that the spike exhausts the resources the power grid has available, since a majority of their peak generation capabilities will already be used to handle the peak caused by HVAC units.

The attacker should also conduct the attack during peak hours of the day, when people are using the most energy and EVs are likely to be home and connected to their chargers. During peak hours, EV charging trends follow a general pattern, where a small percentage of users will charge during peak hours, while most of the charging occurs in intervals over the night during non-peak hours [161]. Using multiple attack vectors and exploiting environmental and consumer trends, an attacker could create an attack scenario that allows for the compromise and control of a large amount of unsupervised consumer home charging stations.

The attack scenario mentioned above is reasonable because current research has done modeling and analysis of a similar problem. As mentioned in Chapter 3 [61] [64]

[66], AC units have historically been a non-cyber threat to the stability of the power grid. Further research has also been performed regarding the cybersecurity of "smart" AC units, connected to either the Internet or an Internet controlled smart meter. In their analysis, they determined that vulnerabilities in the operation of the smart AC units allowed for a DDoS attack against the local power grid [28]. Other research efforts have concluded that EV charging is the next vector destabilizing the power grid both through non-cyber and cyberattack vectors [162] [163].

The research from [28] based their analysis on the ability for smart AC units to cause sustained underfrequency to the power grid. Their work compared the frequency of the grid to the amount of load required to cause an underfrequency event. "The relationship between the impact (Hz) and the required load (MW) can be used to evaluate the resilience of the smart grid to cyber-physical attacks based on the acceptable level of impact imposed on the power system [28]".

Using the power grid research from Chapter 2, this thesis will use the same relationship from [28] to determine the required scale of EV Level 2 chargers needed to impact the Western Interconnect, based on California population statistics alone. This is reasonable because of the analysis provided in Chapter 1; California makes up a large majority of total US EV ownership at nearly 58% [4].

4.3 Statistical Analysis

Using the statistics from Chapter 2 [14] [27] [30] [37] [38] [39], the following general formula in Figure 13 is a derivative of [28] study that describes the relationship between IFRO, frequency variation, charge rate, and the total number of EV:

$$\frac{IFRO \ * \ \Delta freq \ * \ 100}{Charge\ rate \ * \ 5{,}000{,}000} = Infection\ Percentage$$

IFRO	841MW/0.1Hz
$\Delta freq$ UFLS	0.5Hz
$\Delta freq$ UFGP	0.9Hz
Charge rate	7KW
CA Theoretical Population	5,000,000

Figure 4.4 DoS Threshold Formula

The power grid is designed to handle gradual fluctuations in demand. The main goal of the DDoS attack is to cause a large, instantaneous spike in demand. This spike will trigger frequency responses. IFRO will be the immediate response, reaching its full potential within 10s of seconds. If the spike exceeds the IFRO value, then UFLS will initiate, providing reduced QoS and dropping service to customers in a hierarchical fashion. If UFLS or the frequency variation is too great, UFGP will initiate. UFGP will begin to island power generators from the grid in order to protect the turbines. Initiating

UFGP will incur noticeable penalties to QoS with the likelihood of blackouts being very likely. After tens of minutes, the quick and expensive supply producing methods such as gas turbine generators will be forced to shut off and be out of commission for extended periods of time. Loss of the quick response generators will cause the frequency to drop even more, and the likelihood of widespread UFGP and generator islanding is very likely.

If the EV chargers are able to cause a sustained, large spike in demand then the EV can be used to cause a supply-demand imbalance that will cause the cascading disconnection of power supply from the power grid. The power plants would be forced into restart conditions, which range anywhere from 4 hours to 72 hours depending on the type. These disconnections would cause widespread blackouts across immediate local areas. The impacts would be felt across the Western Interconnect. As portions of it fail, the entire region would enter a state of imbalance, and the potential for further service disruption is likely.

Using this formula, the goal is to determine the total number of infected EVs required to trigger UFLS and UFGP contingencies. This is analyzed using both the required and perfect case IFRO values for the Western Interconnected evaluated by NERC for 2017. The following table provides a summary of the variables and results, as well as the percentage of the 5 million EV goal for California.

IFRO (MW/0.1Hz)	Delta f (Hz)	Contingency	Infected EV	Percentage
841	0.5	UFLS	600,714	12.0%
841	0.9	UFGP	1,081,285	21.6%

Table 4.1 Infection Results

The results from this table do not include any outside factors such as time of day or season, which could both be used in the attackers favor when launching an attack. The minimum infection rate required to induce localized DDoS is 12.0%. The minimum infection rate required to induce generator islanding and widespread blackouts is 21.6%. The most popular charging networks in the US are ChargePoint, Tesla, and the Blink network, making up roughly 66% of the nation's charging infrastructure [164]. ChargePoint accounts for 39.3% of the chargers. This means that theoretically, an attacker would only need to be able to compromise a little more than half of all the ChargePoint chargers in order to launch an attack.

4.4 Impact

The impact of a DDoS attack against the US power grid would be serious. Loss of power would have an immediate impact on other critical infrastructure such as water, natural gas, communication, transportation, sanitation, and finance. Many people's homes would be without the resources they rely on. Hospitals, fire stations, police departments, and other important services would be without power and operating at reduced levels.

Many of these services have forms of backup power, but depending on the duration of the blackout, lives could be at risk.

I learned firsthand during the 2003 blackout that local supplies become scarce during a blackout. Those without backup power lost the contents of the fridges and freezers during the first the first 24 - 48 hours. Local gas stations and supermarkets were completely sold out of ice and coolers within the first 8 hours. Flashlights, batteries, bottled water, and nonperishables were wiped from the shelves. The only way to pay for anything was with physical currency, which was an issue because my family rarely carried cash.

When blackouts are caused by natural disasters, it causes people to react irrationally out of fear or desperation. Looting and crime are at a high in situations such as hurricanes when blackouts happen for long periods of time. People will hoard resources in an attempt to ensure that they do not run out.

In the past, blackouts have been tied to nature and therefore, the earth is at fault for the impact on people. A cyberattack is different. It would likely cause intense political pressure. People could possibly begin to doubt the government if it is unable to protect people's critical resources from human based attacks. If attribution can be made, there will probably be intense feelings of anger and retribution, similar to those that happened during the terrorist attacks on 9/11. In the event that an attack is tied back to a nation state, a new political precedence will need to be formed. Is a cyberattack an act of war?

Will military action be used in reaction to a cyberattack? How would the US look if it does not react with strong measures after being attacked [89]? An attack of this nature would have serious impacts on politics and foreign policy.

Chapter 5. MITIGATION

There are several ways that the threat of a cyberattack against the grid can be mitigated. The two strategies of increasing grid security are through:

1. Charging Infrastructure
2. Power Grid

5.1 Power Grid

5.1.1 OCPP

Arguably the most important solution will be to implement OCPP v2.0 and all of its optional security functionality [165]. OCPP v2.0 has added the implementation of security profiles, allowing owners to configure the security of their device, including key management, certificate management, and the use of HTTPS. It has also added the ability to integrate the charging stations into smart grid topologies and allow for remote station management outside of the current billing focused management. The architecture of OCPP v2.0 is also designed to fully compatible with ISO 15118, allowing for better portability and functionality [166].

OCPP v2.0 adds multiple security features, but its integration will not that easy. Vendors and the billing backend will need to modify and update their systems to handle the increased requirements. Some stations may also require hardware updates in order to

meet the additional overhead required to interface with smart grid technology and certificate/key management [167].

5.1.2 Intelligent Design with Security in Mind

Charging station designers should also focus on total security of the system, not just the protection of billing information. Current security is based around a charging account and verification performed by the billing backend. Administration and maintenance should use functionalities within the security profiles to ensure things such as signed firmware updates and encryption and signatures be used on charging control messages and not just billing messages. Data stored on the charging stations, such as signatures and keys, should also be encrypted and obfuscated to further increase the difficulty required to obtain information. Also, critical security data such as keys should not be hardcoded or derivatives of a reasonably guessable pattern by using data such as vendor, model, or year of production [168].

5.2 Power Grid

5.2.1 Smart Grid

Some Argue that integration of smart grid technology will be better suited to handle undesirable behavior and attacks against charging infrastructure. Smart grid technology allows operators greater visibility and control of the supply-demand balance [169]. The two main drawbacks are scope and level of complexity. Power grid operation will need to have the ability to take the massive amount of constantly changing data and

use it to make calculated decisions. The behavioral modeling and contingency management will be incredibly hard to perfect. The addition of smart grid technology will also increase the attack surface on which the grid can be manipulated and attacked. Greater control will also create greater chance of attack [170].

Smart grid integration also need to ensure that manual controls and overrides remain in the grid. Operators ability to manually control the grid is an important functionality that is commonly used in emergency events. There is a noticeable trend of reduced human controllable inputs in newer smart grid technology that is being proposed and trialed [89].

5.2.2 Smart Charging Algorithm

Smart charging algorithms added to charging stations can be used to more efficiently and economically charge EVs. In a paper published by WSU's SMART Lab, they were able to prove that a smart charging algorithm can be used to mitigate undesirable behavior in charging patterns to more efficiently manage the load by treating EV as peak demand home appliances [171]. The algorithm uses deep learning to efficiently schedule the users charging behavior in relation to the current demand on the power grid and from learned predictions based on the users charging habits. This algorithm could also be modified to manage individual charging stations to quickly react to large spikes in charging demand.

Chapter 6. Conclusion

6.1 Conclusion

Cars are an ever changing and integral part of modern society. Technology has been slowly integrated into nearly every facet of cars. Almost all new cars come standard with automatic locks, automatic windows, cruise control, automatic braking, and sensors and warning systems for backing up and switching lanes. The most notable technological advances in cars are the integration of wireless communication, the use of phone applications to control cars, and the push towards EV replacing fossil fuel internal combustion engine vehicles. Wireless communication in EV and charging stations has turned them into IoT devices, bringing all of the convenience and attack vectors that the Internet provides. EV will replace HVAC and become the next generation of residential appliance that can put large strains on the power grid.

This thesis discusses the functionality and relationship between EV, EV charging stations, the power grid, and the Internet. A historical analysis of cyber vulnerabilities that impact the power grid, cars, charging stations, vehicle phone apps, cell phones, and IoT devices was presented. Using past attacks, this thesis discussed a theoretical cyberattack that is closely related to the Mirai botnet that was used to DDoS Dyn in 2016. Using vulnerabilities in charging station wireless communication and smartphone applications, an attacker could create a botnet of charging stations and cellular devices that can be used to launch an indirect cyberattack against the U.S. power grid by causing

extreme fluctuation in the supply-demand balance, using the functionality of the power grids contingency measures against it.

Using statistical analysis, this malicious spike in demand will need to exceed the IFRO value and be large enough to cause a 0.9Hz underfrequency event. This will cause UFLS and UFGP to be initiated and wide scale DoS to consumers. The analysis is based off of metrics for 2017 NERC values for the Western Interconnect and California's 2030 goal to have 5 million registered EV. Using these numbers, it will only require control of roughly 21.6% of California's EV population to launch an attack that could cause wide scale blackouts.

6.2 Future Work

There are several possibilities for future work based off of the preliminary research performed in this thesis. These topics include:

1. The Smart Grid
2. Implementation of OCPP 2.0
3. Home use of Super Chargers
4. Use of wireless charging mediums
5. Overfrequency based attack (power dumping)
6. Public charging station based attack
7. Geographical locations outside of Western Interconnect

REFERENCES

1. "The Grand Challenge". *DARPA.* [Online] Available: https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles . [Accessed: 19-Jul-2018].
2. Lallanilla, Marc. "The History of the Green Movement". *ThoughtCo.* 5-Feb-2018. [Online] Available: https://www.thoughtco.com/what-is-the-green-movement-1708810 . [Accessed: 19-Jul-2018].
3. Plumer, Brad. "The rapid growth of electric cars worldwide, in 4 charts". *Vox.* 6-Jun-2016. [Online] Available: https://www.vox.com/2016/6/6/11867894/electric-cars-global-sales . [Accessed: 19-Jul-2018].
4. "EV Statistics of the Week: Californian's Have Purchased 12 Times More EVs Than the 2nd Highest State". *EVAdoption.* 16-Dec-2017. [Online] Available: http://evadoption.com/ev-statistics-of-the-week-californians-have-purchased-12-times-more-evs-than-the-2nd-highest-state/ . [Accessed: 19-Jul-2018].
5. "Eric Schmidt Quotes". *BrainyQuote.* [Online] Available: https://www.brainyquote.com/quotes/eric_schmidt_102325 . [Accessed: 19-Jul-2018].
6. "Automotive Cyber Security". *Automotive Cyber Security.* [Online] Available: https://automotivecybersecurity.iqpc.com/ . [Accessed: 19-Jul-2018].
7. Hughes, Jeff; Cybenko, George. "Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity". *timreview.* Aug-2013. [Online] Available: https://timreview.ca/sites/default/files/article_PDF/HughesCybenko_TIMReview_August2013.pdf . [Accessed: 19-Jul-2018].
8. "What is Security Analysis?". [Online] Available: https://www.doc.ic.ac.uk/~ajs300/security/CIA.htm . [Accessed: 19-Jul-2018].
9. "confidentiality, integrity, and availability (CIA triad)". *WhatIs.com.* [Online] Available: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA . [Accessed: 19-Jul-2018].
10. "History Of The Automobile". *Encyclopedia Britannica.* [Online] Available: https://www.britannica.com/technology/automobile/History-of-the-automobile . [Accessed: 19-Jul-2018].
11. "". *Place.* Date. [Online] Available: http://theconversation.com/how-the-car-fueled-global-economic-and-foreign-policy-63079 . [Accessed: 19-Jul-2018].
12. "How the car fueled global economic and foreign policy". *The Conversation.* 27-Jul-2016. [Online] Available: https://www.theguardian.com/environment/2017/feb/02/electric-cars-cheap-solar-power-halt-fossil-fuel-growth-2020 . [Accessed: 19-Jul-2018].

13. “Drive clean and save”. *Clean Vehicle Rebate Project.* [Online] Available: https://cleanvehiclerebate.org/eng . [Accessed: 19-Jul-2018].
14. Shepardson, David. “California looks to ramp up electric vehicle sales”. *Reuters.* 26-Jan-2018. [Online] Available: https://www.reuters.com/article/us-autos-emissions-california/california-looks-to-ramp-up-electric-vehicle-sales-idUSKBN1FF2XG . [Accessed: 19-Jul-2018].
15. “Department of Motor Vehicles Estimated Vehicles Registered by County for the Period of January 1 Through December 31, 2017”. *DMV.* [Online] Available: https://www.dmv.ca.gov/portal/wcm/connect/add5eb07-c676-40b4-98b5-8011b059260a/est_fees_pd_by_county.pdf?MOD=AJPERES . [Accessed: 19-Jul-2018].
16. “California continues to lead the way on electric vehicles”. *Curbed.* 30-Jan-2018. [Online] Available: https://www.curbed.com/2018/1/30/16950118/electric-vehicles-ev-california-tesla . [Accessed: 19-Jul-2018].
17. Carey, Nick. “Ford plans $11 billion investment, 40 electrified vehicles by 2022”. *Reuters.* 14-Jan-2018. [Online] Available: https://www.reuters.com/article/us-autoshow-detroit-ford-motor/ford-plans-11-billion-investment-40-electrified-vehicles-by-2022-idUSKBN1F30YZ . [Accessed: 19-Jul-2018].
18. Williams, Brett. “Here's how every major automaker plans to go electric”. *Mashable.* 3-Oct-2017. [Online] Available: https://mashable.com/2017/10/03/electric-car-development-plans-ford-gm/#tdSaUD5mEiqN . [Accessed: 19-Jul-2018].
19. “Types of electric vehicles”. *Ergon.* [Online] Available: https://www.ergon.com.au/network/smarter-energy/electric-vehicles/types-of-electric-vehicles . [Accessed: 19-Jul-2018].
20. “Types of electric cars”. *energysage.* 16-Nov-2017. [Online] Available: https://www.energysage.com/electric-vehicles/101/types-of-electric-cars/ . [Accessed: 19-Jul-2018].
21. “How Electricity Is Delivered To Consumers”. *eia.* [Online] Available: https://www.eia.gov/energyexplained/index.cfm?page=electricity_delivery . [Accessed: 19-Jul-2018].
22. Brain, Marshall; Roos, Dave. “How Power Grids Work”. *howstuffworks.* [Online] Available: https://science.howstuffworks.com/environmental/energy/power1.htm . [Accessed: 19-Jul-2018].
23. “What's the Difference Between Single Phase and Three Phase AC Power Supplies?”. *Aegis.* 12-Mar-2015. [Online] Available: http://aegispower.com/index.php/blog/179-what-s-the-difference-between-single-phase-and-three-phase-ac-power-supplies . [Accessed: 19-Jul-2018].

24. LaMonica, Martin. “Turning off the Power to Run the Grid”. *MIT Technology Review.* 5-Apr-2013. https://www.technologyreview.com/s/513356/turning-off-the-power-to-run-the-grid/ . [Accessed: 19-Jul-2018].
25. “Today’s Outlook”. *California ISO.* [Online] Available: [Online] Available: http://www.caiso.com/TodaysOutlook/Pages/default.aspx . [Accessed: 19-Jul-2018].
26. “Energy and the Environment”. *EPA.* [Online] Available: https://www.epa.gov/energy/electricity-customers . [Accessed: 19-Jul-2018].
27. “Learn More About Interconnections”. *ENERGY.GOV.* [Online] Available: https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/transmission-planning/recovery-act-0 . [Accessed: 19-Jul-2018].
28. AlMajali, Anas. “Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats”. *MDPI.* 28-Dec-2016. [Online] Available: https://pdfs.semanticscholar.org/8b4d/0a3518ce34d6412c58cc5e2971c112dc6bad.pdf . [Accessed: 19-Jul-2018].
29. “Reliability Guideline Primary Frequency Control”. *NERC.* 2015. [Online] Available: https://www.nerc.com/comm/OC/Reliability%20Guideline%20DL/Primary_Frequency_Control_final.pdf . [Accessed: 19-Jul-2018].
30. “How to balance supply and demand on new electricity markets”. *Next Kraftwerke.* [Online] Available: https://www.next-kraftwerke.com/energy-blog/how-to-balance-supply-and-demand-on-new-electricity-markets . [Accessed: 19-Jul-2018].
31. “Combustion Engine vs Gas Turbine: Startup Time”. *Wartsila.* [Online] Available: https://www.wartsila.com/energy/learning-center/technical-comparisons/combustion-engine-vs-gas-turbine-startup-time . [Accessed: 19-Jul-2018].
32. “Combustion Engine for Power Generation: Introduction”. *Wartsila.* [Online] Available: https://www.wartsila.com/energy/learning-center/technical-comparisons/combustion-engine-for-power-generation-introduction . [Accessed: 19-Jul-2018].
33. Kemp, John. “COLUMN-To survive, coal power plants must become more flexible: Kemp”. *Reuters.* 19-Nav-2013. [Online] Available: https://www.reuters.com/article/coal-power-generation-idUSL5N0J42YG20131119 . [Accessed: 19-Jul-2018].
34. “Why does it take so long to restart a nuclear power plant?”. *StackExchange.* [Online] Available: https://engineering.stackexchange.com/questions/7394/why-does-it-take-so-long-to-restart-a-nuclear-power-plant . [Accessed: 19-Jul-2018].

35. Laris, Mark. “What is the procedure to start up a nuclear power plant and why does it take weeks?”. *Quora.* 25-Sep-2017. [Online] Available: https://www.quora.com/What-is-the-procedure-to-start-up-a-nuclear-power-plant-and-why-does-it-take-weeks . [Accessed: 19-Jul-2018].
36. Greenwood, D.M. “Frequency response services designed for energy storage”. *ScienceDirect.* 1-Oct-2017. [Online] Available: https://www.sciencedirect.com/science/article/pii/S0306261917307729 . [Accessed: 19-Jul-2018].
37. “2017 Frequency Response Annual Analysis”. *NERC.* Nov-2017. [Online] Available: https://www.nerc.com/comm/oc/bal0031_supporting_documents_2017_dl/2017_fraa_final_20171113.pdf . [Accessed: 19-Jul-2018].
38. “Primary Frequency Response and Control of Power System Frequency”. *FERC.* Feb-2018. [Online] Available: https://www.ferc.gov/industries/electric/indus-act/reliability/frequency-control-requirements/primary-response.pdf . [Accessed: 19-Jul-2018].
39. “EPRI Power System Dynamics Tutorial”. *EPRI.* 27-Jul-2009. [Online] Available: https://www.epri.com/#/pages/product/1016042/?lang=en . [Accessed: 19-Jul-2018].
40. Eto, Joseph. “Use of Frequency Response Metrics to Assess the Planning and Operating requirements for Reliable Integration of Variable Renewable Generation”. *Lawrence Berkeley National Laboratory.* 17-Apr-2012. [Online] Available: http://mydocs.epri.com/docs/publicmeetingmaterials/4-17-2012/04-Use-of-Frequency-Response-Metrics-Joseph-Eto.pdf . [Accessed: 19-Jul-2018].
41. Miller, Dean. “Cold Load Pickup Issues”. *IEEE Power Engineering Society.* [Online] Available: http://www.pes-psrc.org/Reports/Cold_Load_Pickup_Issues_Report.pdf . [Accessed: 19-Jul-2018].
42. “Energy Dictionary”. *energyvortex.* [Online] Available: https://www.energyvortex.com/energydictionary/blackout__brownout__brown_power__rolling_blackout.html . [Accessed: 19-Jul-2018].
43. Jun, Yi. “Model of Cascading Failures in Power Systems”. *IEEE Xplore.* 26-Feb-2006. [Online] Available: https://ieeexplore.ieee.org/abstract/document/4116173/ . [Accessed: 19-Jul-2018].
44. “Understanding Electric Vehicle Charging”. *Plug In America.* 31-Jan-2011. [Online] Available: https://pluginamerica.org/understanding-electric-vehicle-charging/ . [Accessed: 19-Jul-2018].

45. “Levels of Charging”. *EVTown.* [Online] Available: http://www.evtown.org/about-ev-town/ev-charging/charging-levels.html . [Accessed: 19-Jul-2018].
46. “What's the electrical limit of an outlet, circuit, or panel?”. [Online] Available: http://michaelbluejay.com/electricity/maxload.html . [Accessed: 19-Jul-2018].
47. “ELECTRIC CAR CHARGING 101 — TYPES OF CHARGING, CHARGING NETWORKS, APPS, & MORE!”. *EVObsession.* 10-Sep-2-15. [Online] Available: https://evobsession.com/electric-car-charging-101-types-of-charging-apps-more/ . [Accessed: 19-Jul-2018].
48. “EV DC Fast Charging standards – CHAdeMO, CCS, SAE Combo, Tesla Supercharger, etc”. *GreenTrasportation.* [Online] Available: https://greentransportation.info/ev-charging/range-confidence/chap8-tech/ev-dc-fast-charging-standards-chademo-ccs-sae-combo-tesla-supercharger-etc.html . [Accessed: 19-Jul-2018].
49. Berman, Brad. “Is 350-Kilowatt Ultra-Fast Charging the Future of EV Refueling?”. *plugincars.* 20-Oct-2016. [Online] Available: http://www.plugincars.com/350-kilowatt-ultra-fast-charging-future-ev-refueling-132296.html . [Accessed: 19-Jul-2018].
50. “Road vehicles -- Vehicle to grid communication interface”. *ISO.* 2013. [Online] Available: https://www.iso.org/standard/55365.html . [Accessed: 19-Jul-2018].
51. “Open Charge Point Protocol”. *OCA.* [Online] Available: https://www.openchargealliance.org/ . [Accessed: 19-Jul-2018].
52. “Open Charge Alliance launches OCPP 2.0”. *Cision.* 17-Apr-2018. [Online] Available: https://www.prnewswire.com/news-releases/open-charge-alliance-launches-ocpp-2-0--300631772.html . [Accessed: 19-Jul-2018].
53. “Open Charge Point Interface OCPI”. *NKL.* Jan-2017. [Online] Available: https://www.nklnederland.com/projects/our-current-projects/open-charge-point-interface-ocpi/ . [Accessed: 19-Jul-2018].
54. “Electric Vehicle Charging Guide”. *ChargeHub.* [Online] Available: https://chargehub.com/en/electric-car-charging-guide.html . [Accessed: 19-Jul-2018].
55. “Vehicle Communications and Charging Control”. *Pacific Northwest.* [Online] Available: https://www.energy.gov/sites/prod/files/2014/07/f18/vss142_pratt_2014_p.pdf . [Accessed: 19-Jul-2018].
56. “New Tesla to J1772 adapter allows other electric cars to charge at Tesla’s Destination Chargers”. *electrek.* 20-Jun-2017. [Online] Available:

https://electrek.co/2017/06/20/tesla-j1772-adapter-electric-cars-destination-chargers/ . [Accessed: 19-Jul-2018].
57. Marcucci, Todd. “How the J1772 charging standard for plug-in vehicles works”. *EDN Network.* 17-Sep-2013. [Online] Available: https://www.edn.com/electronics-blogs/automotive-currents/4421241/How-the-J1772-charging-standard-for-plug-in-vehicles-works . [Accessed: 19-Jul-2018].
58. Mathoy, Arno. “Definition and implementation of a global EV charging infrastructure”. *BRUSA Elektronik.* Date. [Online] Available: https://www.yumpu.com/en/document/view/39489467/definition-and-implementation-of-a-global-ev-park-charge . [Accessed: 19-Jul-2018].
59. Minkel, JR. “The 2003 Northeast Blackout--Five Years Later”. *Scientific American.* 13- Aug-2013. [Online] Available: https://www.scientificamerican.com/article/2003-blackout-five-years-later/ . [Accessed: 19-Jul-2018].
60. Kenderdine, Melanie. “US power grid needs defense against looming cyber attacks”. *The Hill.* 23-Mar-2018. [Online] Available: http://thehill.com/opinion/energy-environment/379980-us-power-grid-needs-defense-against-looming-cyber-attacks . [Accessed: 19-Jul-2018].
61. Feuer, Alan. “City Dims Lights as Heat Strains the Power Grid”. *New York Times.* 2-Aug-2006. [Online] Available: https://www.nytimes.com/2006/08/02/nyregion/02heat.html . [Accessed: 19-Jul-2018].
62. Galbraith, Kate. “Spreading Demand Thinner on the Power Grid”. *New York Times.* 19-Sep-2012. [Online] Available: https://www.nytimes.com/2012/09/20/business/energy-environment/20iht-green20.html . [Accessed: 19-Jul-2018].
63. Huff. Ethan. “California power officials beg customers to stop using air conditioning as West Coast power grid reaches critical failure”. *Power Grid News.* 11-Sep-2017. [Online] Available: https://www.powergrid.news/2017-09-11-california-power-officials-beg-customers-to-stop-using-air-conditioning-as-west-coast-power-grid-reaches-critical-failure.html . [Accessed: 19-Jul-2018].
64. “Power Outages Attributed to Heat”. *AccuWeather.* 8-Jul-2010. [Online] Available: https://www.accuweather.com/en/weather-news/be-alert-for-power-outages-in-1/33594 . [Accessed: 19-Jul-2018].
65. “California ISO Peak Load History 1998 through 2017”. *California ISO.* [Online] Available: https://www.caiso.com/documents/californiaisopeakloadhistory.pdf . [Accessed: 19-Jul-2018].

66. Wang, Sheng. “Cooperation of Demand Response and Traditional Power Generations for Providing Spinning Reserve”. *Science Direct.* Dec-2017. [Online] Available: https://www.sciencedirect.com/science/article/pii/S187661021736157X . [Accessed: 19-Jul-2018].
67. Beaumont, Peter. “Stuxnet worm heralds new era of global cyberwar”. *The Guardian.* 30-Sep-2010. [Online] Available: https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar . [Accessed: 19-Jul-2018].
68. Fruhlinger, Josh. “What is Stuxnet, who created it and how does it work?”. *CSO.* 22-Aug-2017. [Online] Available: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html . [Accessed: 19-Jul-2018].
69. Khandelwal, Swati. “Dragonfly Russian Hackers Target 1000 Western Energy Firms”. *The Hacker News.* 1-Jul-2014. [Online] Available: https://thehackernews.com/2014/07/dragonfly-russian-hackers-scada-havex.html . [Accessed: 19-Jul-2018].
70. Walker, Danielle. “'Havex' malware strikes industrial sector via watering hole attacks”. *SC Media.* 25-Jun-2014. [Online] Available: https://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/538721/ . [Accessed: 19-Jul-2018].
71. “The Impact of Dragonfly Malware on Industrial
72. Control Systems”. *SANS Institute.* 18-Jan-2016. [Online] Available: https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672 . [Accessed: 19-Jul-2018].
73. “Dragonfly: Western energy sector targeted by sophisticated attack group”. *Symantec.* 20-Oct-2017. [Online] Available: https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks . [Accessed: 19-Jul-2018].
74. “BlackEnergy APT Attacks in Ukraine”. *Kaspersky.* [Online] Available: https://usa.kaspersky.com/resource-center/threats/blackenergy . [Accessed: 19-Jul-2018].
75. Hultquist, John. “Sandworm Team and the Ukrainian Power Authority Attacks”. *FireEye.* 7-Jan-2016. [Online] Available: https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html . [Accessed: 19-Jul-2018].
76. “Frequently Asked Questions: BlackEnergy”. *Trend Micro.* 11-Feb-2016. [Online] Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy . [Accessed: 19-Jul-2018].

77. Miller, Christopher. “What's Ukraine Doing To Combat Russian Cyberwarfare? 'Not Enough'”. *RadioFreeEurope RadioLiberty.* 7-Mar-2018. [Online] Available: https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html . [Accessed: 19-Jul-2018].
78. Greenberg, Andy. “HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR”. *Wired.* 20-Jun-2017. [Online] Available: https://www.wired.com/story/russian-hackers-attack-ukraine/ . [Accessed: 19-Jul-2018].
79. Farmer, Ben. “Russia was behind 'malicious' cyber attack on Ukraine, Foreign Office says”. *The Telegraph.* 15-Feb-2018. [Online] Available: https://www.telegraph.co.uk/news/2018/02/15/russia-behind-malicious-cyber-attack-ukraine-foreign-office/ . [Accessed: 19-Jul-2018].
80. Kumar, Mohit. “Dragonfly 2.0: Hacking Group Infiltrated European and US Power Facilities”. *The Hacker News.* 7-Sep-2017. [Online] Available: https://thehackernews.com/2017/09/dragonfly-energy-hacking.html . [Accessed: 19-Jul-2018].
81. “Dragonfly: Western energy sector targeted by sophisticated attack group”. *Symantec.* 20-Oct-2017. [Online] Available: https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks . [Accessed: 19-Jul-2018].
82. Uchill, Joe. “Irish power grid compromised by foreign actor: report”. *The Hill.* 8-Aug-2017. [Online] Available: http://thehill.com/policy/cybersecurity/345836-irish-power-grid-compromised-by-foreign-actor-report . [Accessed: 19-Jul-2018].
83. Paganini, Pierluigi. “Irish electricity transmission system operator EirGrid targeted by a nation-state actor”. *Security Affairs.* 8-Aug-2017. [Online] Available: https://securityaffairs.co/wordpress/61800/cyber-warfare-2/eirgrid-targeted-nation-state-actor.html . [Accessed: 19-Jul-2018].
84. Volz, Dustin. “In a first, U.S. blames Russia for cyber attacks on energy grid”. *Reuters.* 15-Mar-2018. [Online] Available: https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3 . [Accessed: 19-Jul-2018].
85. Perlroth, Nicole. “Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say”. *New York Times.* 6-July-2017. [Online] Available: https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?_r=0 . [Accessed: 19-Jul-2018].
86. Greenberg, Andy. “HACKERS GAIN DIRECT ACCESS TO US POWER GRID CONTROLS”. *Wired.* 6-Sep-2017. [Online] Available:

https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/ . [Accessed: 19-Jul-2018].
87. Ibelle, Bill. “RUSSIAN CYBERATTACK ON US POWER GRID MEANT TO BE SHOW OF POWER, RESEARCHERS WORKING TO THWART THE NEXT ONE”. *News Northeastern.* 21-Mar-2018. [Online] Available: https://news.northeastern.edu/2018/03/21/northeastern-researchers-address-russian-power-grid-attack/ . [Accessed: 19-Jul-2018].
88. Crawford, Jamie. “The U.S. government thinks China could take down the power grid”. *CNN.* 21-Nov-2014. [Online] Available: https://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/index.html . [Accessed: 19-Jul-2018].
89. Murdock, Jason. “U.S. TARGETED BY SUSPECTED CHINESE CYBER ESPIONAGE GROUP, FIREEYE RESEARCH WARNS”. *Newsweek.* 16-Mar-2018. [Online] Available: http://www.newsweek.com/us-targeted-suspected-chinese-cyber-espionage-group-fireeye-research-warns-847984 . [Accessed: 19-Jul-2018].
90. Knake, Robert. “A Cyberattack on the U.S. Power Grid”. *CFR.* 3-Apr-2017. [Online] Available: https://www.cfr.org/report/cyberattack-us-power-grid . [Accessed: 19-Jul-2018].
91. “New Lloyd’s study highlights wide ranging implications of cyber attacks”. *Lloyd’s.* 8-Jul-2015. [Online] Available: https://www.lloyds.com/news-and-risk-insight/press-releases/2015/07/business-blackout . [Accessed: 19-Jul-2018].
92. “Business Blackout”. *Lloyd’s.* 6-Jul-2015. [Online] Available: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout . [Accessed: 19-Jul-2018].
93. “Business Blackout: The insurance implications of a cyber attack on the US power grid”. *Lloyd’s.*
94. “A Brief History of Car Hacking 2010 to the Present”. *Smart!.* 30-Aug-2017. [Online] Available: https://smart.gi-de.com/2017/08/brief-history-car-hacking-2010-present/ . [Accessed: 19-Jul-2018].
95. “Experimental Security Analysis of a Modern Automobile”. *CAESS.* 2014. [Online] Available: http://www.autosec.org/pubs/cars-oakland2010.pdf . [Accessed: 19-Jul-2018].
96. Miller, Charlie; Valasek, Chris. “Remote Exploitation of an
97. Unaltered Passenger Vehicle”. *Illmatics.* 10-Aug-2015. [Online] Available: http://illmatics.com/Remote%20Car%20Hacking.pdf . [Accessed: 19-Jul-2018].

98. “Comprehensive Experimental Analyses of Automotive Attack Surfaces”. *CAESS.* 2016. [Online] Available: http://www.autosec.org/pubs/cars-usenixsec2011.pdf . [Accessed: 19-Jul-2018].
99. “Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)”. *Forbes.* Greenberg, Andy. [Online] Available: https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/ . [Accessed: 19-Jul-2018].
100. Miller, Charlie; Valasek, Chris. “Car Hacking: For Poories”. *Illmatics.* 2016. [Online] Available: http://illmatics.com/car_hacking_poories.pdf . [Accessed: 19-Jul-2018].
101. “Black Hat USA 2015: The full story of how that Jeep was hacked”. *Kaspersky.* 6-Aug-2015. [Online] Available: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ . [Accessed: 19-Jul-2018].
102. Greenberg, Andy. “HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT”. *Wired.* 21-Aug-2015. [Online] Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ . [Accessed: 19-Jul-2018].
103. “We Drove a Car While It Was Being Hacked”. *Motherboard.* 29-May-2014. [Online] Available: https://motherboard.vice.com/en_us/article/ae33jk/we-drove-a-car-while-it-was-being-hacked . [Accessed: 19-Jul-2018].
104. “MATHEW SOLNIK”. *BlackHat.* [Online] Available: https://www.blackhat.com/us-16/speakers/Mathew-Solnik.html . [Accessed: 19-Jul-2018].
105. “BMW Hack: the auto industry's big cyber-security warning sign [w/video]”. *autoblog.* 6-Feb-2015. [Online] Available: https://www.autoblog.com/2015/02/06/bmw-hack-cyber-security-warning-feature-video/ . [Accessed: 19-Jul-2018].
106. “Car hacked on 60 Minutes”. *CBS.* 6-Feb-2015. [Online] Available: https://www.cbsnews.com/news/car-hacked-on-60-minutes/ . [Accessed: 19-Jul-2018].
107. “DARPA Shows How To Hack a Car Through OnStar”. *Popular Mechanics.* 9-Feb-2015 [Online] Available: https://www.popularmechanics.com/cars/news/a13997/darpa-hackers-can-control-your-vehicle/ . [Accessed: 19-Jul-2018].
108. “Tesla Model S being hacked and patched blazing-fast”. *Kaspersky.* 10-Aug-2015. [Online] Available: https://www.kaspersky.com/blog/tesla-s-hacked-and-patched/9516/ . [Accessed: 19-Jul-2018].

109. "Tesla hackers explain how they did it at Defcon". *RoadShow*. 9-Aug-2015. [Online] Available: https://www.cnet.com/roadshow/news/tesla-hackers-explain-how-they-did-it-at-def-con-23/ . [Accessed: 19-Jul-2018].
110. "Car Hacking Research: Remote Attack Tesla Motor". *Keen Security Labs*. 19-Sep-2016. [Online] Available: https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/
111. "$60 DIY car hacking device is an inexpensive and easy way to hack cars". *Computerworld*. 30-Mar-2015. [Online] Available: https://www.computerworld.com/article/2903714/60-diy-car-hacking-device-is-an-inexpensive-and-easy-way-to-hack-cars.html . [Accessed: 19-Jul-2018].
112. Said, Carolyn. "Comma.ai releases hacker tools for DIY self-driving features". *SFGATE*. 7-Jul-2017. [Online] Available: https://www.sfgate.com/news/article/Comma-ai-releases-hacker-tools-for-DIY-11271240.php . [Accessed: 19-Jul-2018].
113. Wiens, Kyle. "WTF! IT SHOULD NOT BE ILLEGAL TO HACK YOUR OWN CAR'S COMPUTER". *Wired*. 23-Jan-2015. [Online] Available: https://www.wired.com/2015/01/let-us-hack-our-cars/ . [Accessed: 19-Jul-2018].
114. Smith, Scott. "Smart charging stations for electronic cars are extremely vulnerable to hacking". *Quartz*. 22-May-2013. [Online] Available: https://qz.com/87385/smart-charging-stations-for-electronic-cars-are-extremely-vulnerable-to-hacking/ . [Accessed: 19-Jul-2018].
115. Fireman, Jerry. "Growing a Connected Network of EV Charging Stations". *ptc*. [Online] Available: https://www.ptc.com/en/product-lifecycle-report/growing-a-connected-network-of-ev-charging-stations . [Accessed: 19-Jul-2018].
116. "Expert from Fraunhofer ITWM uncovers security vulnerabilities of charging stations". *Fraunhofer*. 31-Jan-2018. [Online] Available: https://www.fraunhofer.de/en/press/research-news/2018/January/security-vulnerabilities-of-charching-stations.html . [Accessed: 19-Jul-2018].
117. "Don't be sure charging your electric car is secure enough". *Kaspersky*. 9-Jan-2018. [Online] Available: https://www.kaspersky.com/blog/electric-cars-charging-problems/20652/ . [Accessed: 19-Jul-2018].
118. Dalheimer, Mathias. "Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit - english translation". *YouTube*. 27-Dec-2017. [Online] Available: https://www.youtube.com/watch?time_continue=109&v=szYeqOIQ9Bw . [Accessed: 19-Jul-2018].

119. Dalheimer, Mathias. “EVSim: Tester für Ladestationen”. *EVSim.* [Online] Available: https://evsim.gonium.net/ . [Accessed: 19-Jul-2018].
120. “Chaos Computer Club hacks e-motor charging stations”. *CCC.* 27-Dec-2017. [Online] Available: https://www.ccc.de/en/updates/2017/e-motor . [Accessed: 19-Jul-2018].
121. “How to hack an electric car-charging station”. *Naked Security.* 17-May-2013. [Online] Available: https://nakedsecurity.sophos.com/2013/05/17/how-to-hack-an-electric-car-charging-station/ . [Accessed: 19-Jul-2018].
122. Shezaf, Ofer. “Who can hack a plug?”. *XIOM.* 2013. [Online] Available: https://conference.hitb.org/hitbsecconf2013ams/materials/D2T2%20-%20Ofer%20Shezaf%20-%20The%20Infosec%20Risks%20of%20Charging%20Electric%20Cars.pdf . [Accessed: 19-Jul-2018].
123. “Open Charge Alliance launches latest protocol”. *Electrive.com.* 18-Apr-2018. [Online] Available: https://www.electrive.com/2018/04/18/open-charge-alliance-launches-latest-protocol/ . [Accessed: 19-Jul-2018].
124. Alcaraz, Christina. “OCPP Protocol: Security Threats and Challenges”. *IEEE Xplore.* 15-Feb-2017. [Online] Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7857099 . [Accessed: 19-Jul-2018].
125. “OCPP v1.5”. *OCA.* [Online] Available: https://www.openchargealliance.org/protocols/ocpp/ocpp-15/ . [Accessed: 19-Jul-2018].
126. Eekelen, Marko. “An end-to-end security design for smart EV-charging”. *ElaadNL.* 2-Dec-2014. [Online] Available: https://www.elaad.nl/uploads/files/Smart_Charging_-_End2End_security_design_-_LaQuSo_-_Final_-_1Dec2014_2.pdf . [Accessed: 19-Jul-2018].
127. Broek, Fabian. “Securing the information infrastructure for EV charging”. *Radboud University, Netherlands.* 2015. [Online] Available: https://www.cs.ru.nl/E.Poll/papers/EVcharging.pdf . [Accessed: 19-Jul-2018].
128. “Securely connecting Electric Vehicles to the Smart Grid”. *Siemens AG.* 2016. [Online] Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.683.7333&rep=rep1&type=pdf . [Accessed: 19-Jul-2018].
129. “Top 10-2017 Top 10”. *OWASP.* 2017. [Online] Available: https://www.owasp.org/index.php/Top_10-2017_Top_10 . [Accessed: 19-Jul-2018].

130. "How a hacked password can unlock a Tesla car". *Graham Cluley*. 31-Mar-2014. [Online] Available: https://www.grahamcluley.com/hack-password-tesla-car/ . [Accessed: 19-Jul-2018].
131. Dhanjani, Nitesh. "Cursory Evaluation of the Tesla Model S: We Can't Protect Our Cars Like We Protect Our Workstations". *Nitesh Dhanjani*. 2014. [Online] Available: http://www.dhanjani.com/blog/2014/03/curosry-evaluation-of-the-tesla-model-s-we-cant-protect-our-cars-like-we-protect-our-workstations.html . [Accessed: 19-Jul-2018].
132. Neal, Meghan. "Hacking a Car Shouldn't Be as Easy as Hacking a Computer". *Motherboard*. 31-Mar-2014. [Online] Available: https://motherboard.vice.com/en_us/article/xywdkw/hacking-a-car-shouldnt-be-as-easy-as-hacking-a-computer . [Accessed: 19-Jul-2018].
133. "Hacker controls Nissan Leaf using smartphone app vulnerability". *Alphr*. 2016. [Online] Available: http://www.alphr.com/cars/1002800/hacker-controls-nissan-leaf-using-smartphone-app-vulnerability . [Accessed: 19-Jul-2018].
134. Kelion, Leo. "Nissan Leaf electric cars hack vulnerability disclosed". *BBC*. 24-Feb-2016. [Online] Available: http://www.bbc.com/news/technology-35642749 . [Accessed: 19-Jul-2018].
135. Sharp, Alastair. "Hyundai app exposed vehicles to high-tech thieves: researchers". *Reuters*. 25-Apr-2017. [Online] Available: https://www.reuters.com/article/us-autos-cyber-hyundai/hyundai-app-exposed-vehicles-to-high-tech-thieves-researchers-idUSKBN17R1OF . [Accessed: 19-Jul-2018].
136. "Are connected car apps secure?". *Kaspersky*. 20-Sep-2017. [Online] Available: https://www.kaspersky.com/blog/connected-car-apps-revisited/18548/ . [Accessed: 19-Jul-2018].
137. "Tesla cars can be stolen by hacking the app". *Promon*. 23-Nov-2017. [Online] Available: https://promon.co/security-news/hacking-tesla-app-stolen-car/ . [Accessed: 19-Jul-2018].
138. "Charge Faster, Go Farther". *ChargePoint*. [Online] Available: https://www.chargepoint.com/drivers/home/ . [Accessed: 19-Jul-2018].
139. Constantin, Lucian. "Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON". *CSO*. 13-Sep-2016. [Online] Available: https://www.csoonline.com/article/3119765/security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html . [Accessed: 19-Jul-2018].
140. Woolf, Nicky. "DDoS attack that disrupted Internet was largest of its kind in history, experts say". *The Guardian*. 26-Oct-2016. [Online] Available:

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet . [Accessed: 19-Jul-2018].
141. Hilton, Scott. “Dyn Analysis Summary Of Friday October 21 Attack”. *Oracle*. 26-Oct-2016. [Online] Available: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ . [Accessed: 19-Jul-2018].
142. “Mirai Botnet DDoS Attack Type”. *Corero*. [Online] Available: https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html . [Accessed: 19-Jul-2018].
143. Fruhlinger, Josh. “The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the Internet”. *CSO*. 9-Mar-2018. [Online] Available: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-Internet.html . [Accessed: 19-Jul-2018].
144. “Mirai botnet Minecraft scam brought down the Internet”. *Wired*. [Online] Available: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-Internet/ . [Accessed: 19-Jul-2018].
145. “WATER TORTURE: A SLOW DRIP DNS DDOS ATTACK”. *Secure64*. 25-Feb-2014. [Online] Available: https://secure64.com/water-torture-slow-drip-dns-ddos-attack/ . [Accessed: 19-Jul-2018].
146. “OWASP TOP 10 IOT VULNERABILITIES BASIC IDEA FOR TESTING”. *IoT PenTest Lab*. 5-Jan-2017. [Online] Available: http://iotpentest.com/owasp-top-10-iot-vulnerabilities-basic-idea-for-testing/ . [Accessed: 19-Jul-2018].
147. “Charging at Home”. *ENERGY.GOV*. [Online] Available: https://www.energy.gov/eere/electricvehicles/charging-home . [Accessed: 19-Jul-2018].
148. “General ChargePoint Home FAQs”. *ChargePoint*. [Online] Available: https://www.chargepoint.com/products/home/general/ . [Accessed: 19-Jul-2018].
149. “Elvi Brochure”. *EVBox*. [Online] Available: https://info.evbox.com/elvi-brochure?__hstc=12195819.149c474c2ee75d0ca3e9a5d814c30468.1531181601009.1531181601009.1531181601009.1&__hssc=12195819.1.1531181601009&__hsfp=3303712018 . [Accessed: 19-Jul-2018].
150. “Blink Pedestal and Wall Mount Level 2 EV Chargers”. *Blink*. [Online] Available: http://www.blinkcharging.com/l2-charging . [Accessed: 19-Jul-2018].
151. “Home Charging Installation”. *Tesla*. [Online] Available: https://www.tesla.com/support/home-charging-installation?redirect=no . [Accessed: 19-Jul-2018].

152. “Questions for Discussion and Additional Stakeholder Comment”. *ChargePoint.* [Online] Available: http://www.ripuc.org/utilityinfo/electric/PST_UBM_SC_18.pdf . [Accessed: 19-Jul-2018].
153. “OCPP Downloads”. *OCA.* [Online] Available: https://www.openchargealliance.org/downloads/ . [Accessed: 19-Jul-2018]. Open Charge Point Protocol v1.5
154. “ocpp_chargepointservice_1.5_final.wsdl”. *GitHub.* 18-Aug-2013. [Online] Available: https://github.com/knutster/OCPP/blob/master/ocpp_chargepointservice_1.5_final.wsdl . [Accessed: 19-Jul-2018].
155. “Google took down over 700,000 bad Android apps in 2017”. *The Verge.* 30-Jan-2018. [Online] Available: https://www.theverge.com/2018/1/30/16951996/google-android-apps-removed-security-2017 . [Accessed: 19-Jul-2018].
156. Goodin, Dan. “Malicious apps with >1 million downloads slip past Google defenses twice”. *Ars Technica.* 14-Sep-2017. [Online] Available: https://arstechnica.com/information-technology/2017/09/malicious-apps-with-1-million-downloads-slip-past-google-defenses-twice/ . [Accessed: 19-Jul-2018].
157. “General ChargePoint Home FAQs”. *ChargePoint.* [Online] Available: https://www.chargepoint.com/products/home/general/ . [Accessed: 19-Jul-2018].
158. “Shodan Command-Line Interface”. *Shodan.* [Online] Available: https://cli.shodan.io/ . [Accessed: 19-Jul-2018].
159. “Wireshark Remote Capturing”. *HowtoForge.* [Online] Available: https://www.howtoforge.com/wireshark-remote-capturing . [Accessed: 19-Jul-2018].
160. “TCPDump Documentation”. *TCPDUMP*. [Online] Available: http://www.tcpdump.org/ . [Accessed: 19-Jul-2018].
161. “Netwox”. *Netwox.* [Online] Available: http://ntwox.sourceforge.net/ . [Accessed: 19-Jul-2018].
162. “Mirai-Source-Code”. *GitHub.* 15-Jul2017. [Online] Available: https://github.com/jgamblin/Mirai-Source-Code . [Accessed: 19-Jul-2018].
163. “An Analysis of Electric Vehicle Trends in Developed Nations: A Sustainable Solution for India”. *University of Illinois, Chicago.* Date. [Online] Available: https://journals.uic.edu/ojs/index.php/JUR/article/download/8014/6400 . [Accessed: 19-Jul-2018].
164. “Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems”. *IEEE Xplore.* 18-Dec-2016. [Online]

Available: https://ieeexplore.ieee.org/document/7929019/ . [Accessed: 19-Jul-2018].
165. Sperling, Daniel. “Plug-in vehicles generate new variables for power grids”. *TEC*. Jan-2014. [Online] Available: https://tec.ieee.org/newsletter/january-2014/plug-in-vehicles-generate-new-variables-for-power-grids . [Accessed: 19-Jul-2018].
166. “Analyzing Key Factors That Will Drive Mass Adoption of Electric Vehicles”. *EVAdoption*. [Online] Available: http://evadoption.com/statistics-of-the-week-us-electric-vehicle-charging-stations-chargers-and-networks/ . [Accessed: 19-Jul-2018].
167. “OCPP v2.0”. *OCA*. [Online] Available: https://www.openchargealliance.org/protocols/ocpp/ocpp-20/ . [Accessed: 19-Jul-2018].
168. “THE CASE FOR ISO 15118 AND OCPP 2.0: PREVENTATIVE SOLUTIONS TO HACKING CHARGING INFRASTRUCTURE”. *V2G*. 17-Jan-2018. [Online] Available: https://www.v2g-clarity.com/en/blog/iso15118-mitigates-hacking-charging-infrastructure/ . [Accessed: 19-Jul-2018].
169. “Open Charge Alliance launches OCPP 2.0”. *CISION*. [Online] Available: https://www.prnewswire.com/news-releases/open-charge-alliance-launches-ocpp-2-0--300631772.html . [Accessed: 19-Jul-2018].
170. “The need for cybersecurity within the electric vehicle infrastructure”. *ElaadNL*. Oct-2017. [Online] Available: https://www.elaad.nl/uploads/files/EVS30_Paper_-_The_need_for_cybersecurity_within_the_electric_vehicle_infrastructure.pdf . [Accessed: 19-Jul-2018].
171. “The Increasing Importance of Security for the Smart Grid”. *ELP*. 4-Jan-2011. [Online] Available: https://www.elp.com/articles/powergrid_international/print/volume-16/issue-4/features/the-increasing-importance-of-security-for-the-smart-grid.html . [Accessed: 19-Jul-2018].
172. Shivakumar, Ashutosh. “Individualized Smart Charging to Mitigate the Growing Electrical Peak Demand from EVs as Home Appliances”. *SMARTWorld*. May 2018.