Project ParkAid

Marcos Luchetti

Old Dominion University

CYSE 494: Entrepreneurship in Cybersecurity

Akeyla Porcher, MS Ed

December 2, 2022

Project ParkAid

I. Introduction

Ever since its inception, the automobile has greatly improved our productivity and quality of life, as they help us get from point A to point B much faster. In recent times, however, as population density increased, so too has automobile ownership. In some of the most densely populated metropolitan cities along the coastlines of the United States, such as Washington, D.C., New York City, Atlanta, and Los Angeles, the traffic and congestion on the roads and parking areas are exceptionally insufferable. A great portion of this traffic and congestion is a result of difficulty in finding accessible parking spots in many places within metropolitan areas, such as airports, transit stops, retail malls, etc. The lack of easily accessible parking, inefficient parking, and smaller parking areas are just some of these difficulties that drivers face. The problem of parking inefficiency goes much further beyond the factor of inconvenience. Take, for instance, the impact on local commerce and the quality of life for local inhabitants. Inefficient parking schemes result in reduced customer engagement with businesses, and businesses having to pay for unused parking spaces. In addition, as cars are becoming bigger, the amount of available parking spots decreases, as they are too small to fit such vehicles. This places an additional burden on businesses in metropolitan areas, that are already dealing with the rapid growth in population density, to have enough resources to meet the demand of their customers. Moreover, parking inefficiency is also very taxing on the environment, since drivers are essentially releasing more pollutants into the environment as they drive around looking for available parking spaces. Drivers are also susceptible to parking fines, whether it be because they are unaware of parking rules in certain locations, or they forget when their parking time is set to expire.

As a result of these problems related to parking inefficiency, several private companies have attempted to improve the parking experience by creating parking applications, or apps. These apps are installed on the user's smartphone and they allow the user to discover and even reserve available parking spots, thus eliminating the hassle of searching for a spot themselves. Smart parking apps solve the issue of heavy traffic through advanced parking space booking or providing information on vacant parking spots in the area. Thanks to these applications, drivers are now more aware of just how many accessible parking spots are available in the city, saving time and preventing unneeded stress. As useful and effective as these apps are, they often lack proper security implementations, which can lead to a confidentiality and privacy breach of the user's data. For instance, some applications are guilty of lacking adequate authentication controls; meaning, anyone could track the location of any vehicle simply by entering a license plate number into the app, without even proving that they are the owner of said vehicle. As one can imagine, cyber criminals and stalkers can easily exploit this feature to view a target's current parking sessions and receipts. For many authentication systems, a phone number and license plate number are sufficient to authenticate the identity of a user to the system. Application developers cannot overlook security, it needs to be the top priority during development.

The problem of parking inefficiency in United States metropolitan regions and compromised security in smart parking applications must be addressed through a system that promotes security, privacy, and intuitiveness. The solution to this problem will be manifested through a security-focused cyber-physical platform called ParkAid. This innovation in smart parking will simplify the parking experience for people living in densely populated areas. The ParkAid cyber-physical platform will use a smartphone app that communicates directly with GPS technology to analyze and process the positioning and navigation information of a vehicle

with absolute precision. The app will work in real time to quickly find the most accessible parking locations in any given region in the United States. The ParkAid app will also make it easier for users to track the remaining time in a parking space, thus eliminating feelings of worry and uncertainty in the user, as well as decreasing the likelihood of parking fines. With this app, drivers will spend less time looking for parking spaces, thereby decreasing the pollution of the environment. As its top priority, ParkAid will effectively address security and privacy concerns by employing the security-by-design approach and implementing cybersecurity policies and procedures. ParkAid will provide the efficiency and ease of use that today's hard working professionals yearn for and will put their security and privacy above all else.

II. Literature Review

A. Traffic Congestion

Parking inefficiency in metropolitan areas is becoming a more concerning issue as vehicle ownership continues to increase. This problem has many effects on society, such as traffic congestion, environmental pollution, and detrimental impacts on local commerce and on the local inhabitants' quality of life. Traffic congestion is caused by many factors, including population growth, inexpensive downtown parking, urban sprawl, and inadequate infrastructure investment (Lewis, 2008, p. 7). A research study of urban traffic congestion in 2005 discovered that the average peak-period traveler "spends an extra thirty-eight hours of travel time and consumes an additional twenty-six gallons of fuel a year, amounting to a cost of $710 per traveler" (p. 7), or $1,083.40 in 2022 adjusted for inflation. The so-called "external costs" of traffic congestion also include "the economic value of time wasted in delayed and unreliable conditions, the extra gas and other vehicle operating costs of stop-and-go driving, and the environmental damage and related costs to human health" (p. 8). These delays are considered an

economic cost because it counts as time that could have been used for productivity and/or recreation. Furthermore, to circumvent delays caused by unreliable conditions on the road and to avoid being late for work/appointments, people try to get on the road earlier. However, this also sacrifices valuable time that could be spent with family or other personal business. In 2005, it was reported that traffic delays, and time spent to circumvent these delays, caused people to lose approximately a combined 4.2 billion hours. When equated to the monetary value of these losses, and combined with the 2.9 billion gallons of fuel wasted in traffic-congested conditions, approximately $78 billion was lost during that year (Texas Transportation Institute, 2007), or $119 billion in 2022 adjusted to inflation. This is without even taking the environmental cost into account. A 2006 analysis of traffic in New York City found that traffic congestion cost the metropolitan economy over $13 billion (or $20 billion today) a year, including $6 billion (or $9 billion today) in wasted time and workday productivity (Lewis, 2008, p. 8). All of these numbers have only increased as automobile ownership has risen as well. In addition to the enormous time spent on roads, the price of traffic congestion in urban areas is also felt in the increasing fuel consumption that results in air pollution from carbon-dioxide (CO_2) emission. In fact, traffic carbon emission has become the main influencing factor of environmental pollution and is a major factor affecting climate change (Qi & Duan, 2022, p. 67). Research points out that CO_2 generated by traffic carbon emissions accounts for 25% of the total global carbon emissions (p. 67). The results of these emissions are not only felt in climate change but also in the increasing pollution of particulate matter content in the air environment that, over the long term, will contribute to a variety of respiratory diseases and endanger human health (p. 67). Metropolitan cities are in need of some innovation and infrastructure overhauls that would significantly reduce the immense economic, social and environmental costs of traffic congestion.

B. Smart Parking Systems

Cyber-physical systems are “the systems of systems that combine the physical world with the world of information processing” (ur Rehman & Gruhn, 2017, para. 1). For instance, smart parking, or real-time parking space occupancy monitoring, is an efficient cyber-physical system that was invented to aid in identifying available parking spaces. In recent times, this has become an important and effective solution to the problem of parking inefficiency in traffic-congested areas. This system is significantly lower in cost compared to commercial systems that use LEDs and sensors to indicate the occupancy of parking spaces. This technology can also be applied to both indoor and outdoor parking. In smart parking systems, parking spaces are managed and operated through the following processes:

(1) Management of parking space access; (2) Monitoring parking space occupancy; (3) Assistance for the driver to find spaces; (4) Assistance to find a specific vehicle previously parked; (5) Payment; (6) Parking exit management; (7) Method to monitor and extract information about all these processes. (Giampaoli & Hessel, 2021, p. 7)

Some smart parking systems often use wireless sensor nodes equipped with cameras to monitor the occupancy of parking spaces. The availability of each parking space is determined not by a human but by an algorithm, and the results are sent to a central controller, which can be seen via a graphical interface by the end-user (p. 7). However, the need for a camera makes the system more expensive to implement. To reduce costs while maintaining proper functionality, some smart parking systems have instead opted for geometric or ultrasonic sensors that detect the presence of vehicles. The most efficient systems, however, use a combination of cameras, sensors, and advanced artificial intelligence to monitor the occupation of parking spaces. This

system is more expensive, but it is more reliable in different environments, such as urban areas and outdoor or indoor parking. The general architecture of smart parking systems involves a control center where parking administrators can use the Management and Visualization System (MVS) that is installed on servers located in the Datacenter Cloud Infrastructure (DCI) (p. 8). Then, the Vehicle Detection Devices (VDD) and the Communication and Contextualization Gateway (CCG) are installed in the field, or the parking itself. The data center and the devices present in the field communicate through the backhaul network. As the name suggests, the VDD is the component that detects the presence of vehicles in the parking spaces. A Raspberry Pi3 that is connected to a camera via its serial camera interface (CSI) will perform the VDD function, and an occupancy detection algorithm will determine the un/available state of the parking spaces (p. 8). IoT middleware will record information about the status of parking spaces and operating settings. The VDD communicates with the MVS through the CCG, and the communication between each VDD and CCG occurs over the wireless network interface (IEEE 802.11 WLAN) (p. 8). The CCG is the gateway between the local network formed by the VDDs and the IP network used as a backhaul between the control center and the VDD installation site, or the field (p. 8). A Raspberry Pi3 will act as the CCG, and will consolidate and contextualize information about the status of each parking space and record the VDD operating settings locally in the embedded IoT middleware (p. 8). Located at the control center, the MVS houses a set of utilities that are used to provide an interface for system operation. There are three modules implemented into this MVS: one is the image capture module which is embedded in each VDD—this is responsible for “digitizing the image of the parking where the VDD is installed” (p. 8). This image is then passed on to the second module, or the interface that “displays the demarcation of parking spaces by drawing polygons on the image” (p. 8). Finally, the web

application serves as the third module of the MVS and it provides the administrator with a dashboard that presents useful information, such as: “counting the total number of vehicles in the parking and information on the occupancy of individual spaces in real time” (p. 8). On the end-user side, a smart phone app will be used to place a request for a parking space, once it has been determined that the spot is available. At the admin level, the app is used to manage the whole procedure of the car parking management system. The application server is responsible for storing the user and web server information and responding to requests from the system. The web application “sends a request to the app server that will be viewed by different users who will confirm [the] allocation slot after doing some basic checks” (ur Rehman & Gruhn, 2017, p. 3). The geometric or ultrasonic sensors will be equipped with a microcontroller that senses the presence of the vehicle in the parking lot, and will convert the signal from analogue to digital, before finally transmitting it to the server. The status of the parking spot is constantly updated in the database.

C. Cybersecurity Concerns

Today, there seems to be a mobile application for just about any service that we need. These apps are intuitively designed to make daily activities easier, by enhancing the user’s overall productivity and efficiency in all sorts of environments. As mentioned before, we have seen mobile apps intersected with smart parking systems and they have worked quite well. This Internet-of-Things (IoT) approach to parking considerably increases the efficiency of parking lots in densely populated areas. There are many mobile applications like these that are being developed, but they often lack proper security implementations. Unfortunately, some mobile application developers focus more on improving the user experience at the expense of security

(Abdullah & Zeebaree, 2021, p. 148). This can lead to significant information security and data privacy issues that can seriously impact end-users as well as organizations.

Take the Android operating system (OS), for example. This operating system has a considerably large install base of over 2 billion devices, which will have downloaded more than 228 billion mobile applications by the end of 2022 (p. 148). Given these circumstances, addressing the security issues of Android mobile applications is a challenging and complex undertaking. In addition, when developers have a lack of security awareness, this only increases the potential for security vulnerabilities. Because of this, mitigating application vulnerabilities has become an unmissable necessity. Vulnerabilities to Android applications include denial of service (DoS), sniffing, privilege escalation and non-authenticated access (p. 149). The permission mechanism that is built into Android security performs very well at protecting the privacy of users as well as preventing malicious acts. Essentially, Android "forces applications to request permissions from users to access sensitive information" (p. 149). However, this mechanism can still be vulnerable to threats such as intent spoofing, privilege escalation, phishing, etc.

Mobile applications must be developed with security in mind, as developers should be aware of the vulnerabilities and how to mitigate them. According to the Open Web Application Security Project (OWASP), the ten most prevalent mobile application vulnerabilities include: weak server-side controls, insecure data storage, insufficient Transport Layer protection, unintended data leakage, poor authorization and authentication, broken cryptography, client-side injection, security decisions via untrusted inputs, improper session handling, and lack of binary protections (pp. 149-150). Research shows that these vulnerabilities are caused by: 1. a lack of security awareness and bad coding practices by developers working on mobile applications, 2.

Android's flawed permission mechanism and its improper usage that can also potentially lead to data leakage, and 3. many mobile applications using APIs incorrectly (p. 151). However, the most likely reason behind mobile application vulnerabilities is mainly permission-related flaws that stem from the user or developer's lack of knowledge and misuse of application permissions (p. 151). Experts on the matter have emphasized the importance of "considering security issues by developers at the development phase of mobile applications" (p. 152)—this concept is dubbed as security-by-design. To achieve adequate security in Android, it is important that users understand permissions so as to not grant malicious software access to their data, as well as updating their device to the latest firmware that brings with it the most recent vulnerability patches. Also, mobile application developers must employ security-by-design principles when developing apps that have access to the user's personal data and information.

D. ParkAid Concept

ParkAid will use GPS technology to analyze and process the positioning and navigation information of a vehicle with absolute precision. ParkAid geometric sensors and cameras will be used to detect the occupancy status of parking spaces. The ParkAid platform will include a smartphone app that will work in real time to quickly find the most accessible parking locations for its users in any given region in the United States. With the ParkAid app, users will be notified of the remaining time they have left in a parking space, eliminating worry, uncertainty, and the potential for parking fines. This solution provides all the economical and eco-friendly benefits mentioned earlier, but it will go a step beyond by effectively addressing security and privacy concerns. The app will be developed by a team of cybersecurity experts who understand cyber threats and vulnerabilities, and how to mitigate risks posed by hackers. ParkAid will make paying for parking hassle-free thanks to the encrypted in-app payments. Users can also find the

parking spot that best suits their preference by using the filter feature that can define certain criteria, such as the number of available parking spots, the cost of parking per hour, and the maximum amount of time a vehicle can be parked in a spot. ParkAid will utilize in-pavement antennae and cameras across a multitude of parking services which will be used to detect when and where spots become available (Giampaoli & Hessel, 2021, p. 8).

The IoT component of the ParkAid platform, which includes all the devices that will communicate with each other as well as the app itself, will be designed with security as its top priority. All ParkAid users will have to create an account with an email address, phone number, username, password to login into the application, as well as the vehicle license plate number and the Vehicle Identification Number (VIN) issued by the Department of Motor Vehicles (DMV) upon registration of the automobile in the state of residence. To confirm the creation of the account, the user can choose to have a code sent to them via SMS or email, to which they submit on the app or on the web. The user will then be required to set up two-factor authentication (2FA) with a 2FA app of their choice that creates a time-based one-time password (TOTP) that expires after 30 seconds. The user must use this code to authenticate themselves to ParkAid, thus eliminating the poor authorization and authentication vulnerability, as well as providing proper session handling. All data that is transmitted and stored will be encrypted through the use of the RSA security algorithm, which generates public and private keys that make it much more difficult for cyber attackers to gain access to confidential data and information. To prevent weak server-side controls, the ParkAid cybersecurity team will scan the application and its libraries with scanning tools such as Nessus and SQLmap. These tools will also be used to scan for vulnerabilities in the ParkAid servers and databases which store sensitive information. In addition, to prevent insecure data storage, the sensitive data of users will not be stored in mobile

applications unless necessary, and all local files will be encrypted, with the encryption keys stored securely. ParkAid will also use trusted certificates with the mobile application service as a way of providing sufficient Transport Layer protection. Caching and clipboard access will be blocked as a way of mitigating unintended data leakage. To prevent malicious client-side code injection, all data inputs will be validated, and parameterized queries will be used when accessing the database (Abdullah & Zeebaree, 2021, p. 150). Lack of binary protections is another common mobile application vulnerability that ParkAid addresses by storing sensitive API keys on the server, and by preventing passwords from being stored in the mobile applications binary (p. 150).

E. Benefits of Smart Parking Systems

I believe that ParkAid will gather broad appeal from its users who would welcome the benefits of an economical and eco-friendly parking program. Implementing a smart parking system such as this would aid towards eliminating 30% of traffic congestions that on average are "produced due to cars circulating around buildings for finding parking vacancies in an urban environment" (Shoup, 2006, p. 480), and would save approximately 3.5 to 14 minutes of time spent finding a parking space. This also makes the air around buildings less polluted and greatly benefits drivers, non-drivers, and car park owners (Yang & Lam, 2019, p. 786). For drivers, having the ability to check vehicle parking space and service information before driving into a car park entrance would significantly help in optimizing their driving routes by avoiding wasting mileage, time and gasoline consumption. As for local commerce, the reduced traffic from there being less cruising for parking "makes it easier for businesses to gain higher efficiency in their meetings, operations and transactions" (p. 786). Furthermore, non-drivers would also benefit from several quality-of-life improvements, including less accidents, air pollution, carbon

emission and noise produced with parking space search, such as using car horns to alert other cars and pedestrians, all being reduced substantially (Caicedo et al., 2016, p. 126, 128). Evidently, citizens need an advanced technological solution to solve the increasing traffic problems. With more and more services and information becoming digital, implementing a smart parking system would likely be the easiest approach towards improving the traffic management program and the parking sector, while also being able to integrate seamlessly into the community.

III. Outside Perspectives

A. Leadership

The problem of parking inefficiency and cybersecurity concerns regarding mobile applications can also be viewed from the lens of leadership. No matter which way you look at it, it would take a considerable amount of leadership knowledge and expertise to properly develop the concept of cybersecurity in an organization. This semester, I have learned a lot about the different leadership styles and how to best apply them to a given situation. The class I took is called CPD 416 - Trends & Issues in Leadership. Taking into account all that I learned from that class, I am now more confident in identifying the right leadership approach given the current state of affairs. In this circumstance, I would implement a combination of contingency and contemporary approaches to leadership, through the path-goal theory of leadership (contingency) and transformational leadership style (contemporary). With the path-goal theory of leadership, it is important to motivate employees and/or team members by selecting the appropriate leadership style for each member. Some members may need a directive, supportive, participative, or achievement-oriented leadership style in order to feel motivated to be productive and achieve certain goals. Cybersecurity and environmental conditions are always subject to change, and

therefore it would be useful for ParkAid leadership to be able to change styles depending on the circumstances. Transformational leadership will be needed to give employees inspirational motivation and intellectual stimulation to achieve the collective goals of the organization. For ParkAid, it is important that the team members are encouraged to think creatively and work harder to solve issues related to parking inefficiency and cybersecurity, namely the social, economic, and environmental impacts. Also, when employees work together for the collective wellbeing of the organization and for the success of the mission, then that serves as a motivational boost to deliver and even exceed expectations.

B. Economics

It is also important for companies to understand the economic-benefit returns on cybersecurity investments. One of the insights I researched in ECON 200S - Basic Economics was the macro-analytic method for measuring economic-benefit returns on investments called the Table Top Approach. When evaluating the impacts of cyber intrusion events on the ParkAid platform as well as countermeasure investments, the table top approach helps in determining the greatest cost-benefit gains in cyber defense and why (Garvey et al., 2012, p. 315). With the table top analysis, we can assess cyber-event probabilities which enables us to calculate a return-on-investment on the implementation of countermeasures to cyber risks, such as DoS attacks. Investing in cybersecurity risk mitigation methods is important, but an economic outlook is paramount to ensuring that ParkAid will have a properly adjusted budget that can accommodate other business factors.

C. Ethics

Ethics is considered to be one of the most challenging areas in regards to information technology applications. As I learned in PHIL 230E - Introduction to Ethics, ethics are determinant on the community environment in which they are present. Meaning, the community environment of the digital world differs significantly from the community environment of the world of everyday, physical real life. In the digital world, the "anonymity and distancing of time and space increase the difficulty of taking account of the other" (Bodi, 1998, p. 459). This is why so many application developers often overlook security when designing their applications, as they have no regard for ethical values such as honesty, responsibility, confidentiality, trust, accountability, and fairness. In order for ParkAid to successfully address cybersecurity concerns on the platform, we must follow a code of ethics that respects the security and privacy of our customers and stakeholders.

IV. Effectiveness Assessment

The ParkAid program's success can be measured by tracking parking records stored on the ParkAid app and observing metrics such as the amount of parking spots found per week, how many spots were filled, reviews on the iOS/Android app store and social media, etc. This information can then be used to identify trends in the usage of the app and determine its success in being an effective solution to the parking problem. Also, by identifying user trends, we can gain useful insights into how our users behave, and how we should continue developing the platform to meet their demands. If we find that users have lost interest in the platform, consumer research and reputable surveys will be utilized to discover the reason(s) behind this behavior. The resulting data will be analyzed and it will inform strategic solutions accordingly. Security assessments of the mobile application will be conducted to expose security gaps, and we will subsequently address any vulnerabilities that appear.

For instance, to determine the environmental effectiveness of ParkAid, we will take into account all the time saved through the parking reservation and navigational system on the app. This information will give us an idea as to how much CO_2 emissions were avoided, thanks to the smart parking system preventing cruising for parking spaces. To determine the effectiveness of ParkAid on local commerce, we can track where users have reserved parking and identify what local businesses have encountered more customers due to the parking spots made more accessible thanks to our app. Lastly, to determine the social effectiveness of ParkAid, we can observe the number of app downloads over a specific period of time, check how many new users have appeared in a day, week, month, etc., monitor the user retention rate, etc. It would also help to come up with a social media hashtag, such as "#ParkAid", as this would indicate to us our users' praises and criticisms of the application. These metrics would indicate to us if the app is having the desired social impact and is improving the users' quality of life or not.

V. Realizing the Innovation

It would take considerable support from the city to implement the ParkAid program, which is not easily attainable, especially given the present economic circumstances. For example, to achieve support for the platform in Washington, D.C., we would need the support of the mayor, who is the chief executive officer with executive sponsors typically located in the mayor's office. This is because Washington, D.C.'s governance structure is that of mayor-council. Under the mayor-council form of governance, Washington D.C. has a Chief Innovation Officer (CIO) and a Chief Data Officer (CDO). The Chief Innovation Officer reports to the city manager or mayor and is responsible for "generating and recognizing new ideas, and coordinating innovation efforts within the city and with the outside community" (Greenberg, 2015, p. 14). The Chief Data Officer reports to the CIO or city manager or mayor, and is

responsible for “database system planning, governance, data quality and standards, open data, and transparency” (p. 14). To gain support for ParkAid, we would need to pitch our innovation to the CIO of Washington, D.C., who is responsible for recognizing new ideas. Furthermore, there are several funding models that support new technology and governance efforts. To turn ParkAid into a reality, I think that the department funding or department/partner funding model would be the best option. Through this model, an assessment of the innovation or technology will be carried out by management to determine if it would be appropriate for more than one department, before each department then determines how much of the cost it will cover. There are many benefits to this funding model, such as “cost sharing, leveraging technology and service contracts, and perpetuating a consistent infrastructure” (p. 15). It is important to pick a densely populated city like Washington, D.C., because I feel that this type of environment is where ParkAid would likely be most effective. As an entrepreneur, it is important to have a good start into whatever industry you are entering. We can then scale it up as the application improves on itself as well as the lives of others.

Once ParkAid has secured investment from the city with an appropriate funding model, we can then focus on what the platform needs in order to function at all times. It would take a significant amount of financial resources to broadly implement the program over large metropolitan areas. The ParkAid platform would require enormous IT infrastructure support from local providers, as well as the support of local car park owners. The IT infrastructure consists of all the physical and digital structures and devices that are needed to operate the ParkAid platform. This includes, but is not limited to, power supplies to data centers, servers, networking equipment, storage systems, software applications, operating system platforms, etc. The IT infrastructure provider is also responsible for ensuring that the components work together

without issues so as to avoid unwanted downtime. Another important aspect that is needed for businesses with integrated IT is compliance with Payment Card Industry (PCI) Data Security Standard (DSS). PCI DSS is “a global information security standard designed to prevent fraud through increased control of credit card data” (Mazzoli et al., 2022, para. 1). As a business that accepts payment cards from the five major credit card brands, Visa, MasterCard, American Express, Discover, and the Japan Credit Bureau (JCB), as well as storing, processing, and transmitting payment and cardholder data, ParkAid will need to ensure compliance with PCI DSS so as to gain trust from users and stakeholders alike. In order to fulfill PCI DSS compliance, ParkAid will be committed to maintaining security of its assets and applications, protecting and encrypting cardholder data, implementing and documenting cybersecurity policies and procedures, tracking and monitoring access to the network, protecting information systems against malware, and making annual revisions to security policies and procedures to keep up with the latest trends and threats in cybersecurity.

VI. Next Steps

Following this experience, the next step in the entrepreneurship would be refining the ParkAid platform concept by thinking about alternative strategies and methods that would better suit the innovation, and discarding any deficiencies before they become serious obstacles later on in the development process. The next step would be to prepare to enter the parking industry by conducting research on existing companies and services that they offer, identifying areas in which we can improve upon. We can also prepare by researching the market demand for this type of service and identify what more we can offer to our customers, and what we can trim off. After that, the next step would be to create numerous prototypes until we arrive at a product that is capable of solving the problem of parking inefficiency and data insecurity efficiently and without

error. If the prototype does not meet the standards required by the industry, then we will try again until we achieve that standard. This will require various testing methods, including the functioning of IoT components, user feedback from using the app, as well as vulnerability scanning and penetration testing. Once the final ParkAid prototype is completed and presentable, then the next step would be to pitch the innovation to the CIO of Washington, D.C. If the city is willing to back this project, then we can then proceed to the implementation phase. With the funding of the city, we can now consult with IT infrastructure providers to install ParkAid sensors in indoor and outdoor parking spaces across metropolitan areas, and have them optimized. If the innovation is successful over a long period of time, then we can move on to the expansion phase. The goal would be to implement ParkAid into other large metropolitan areas as well, and possibly experiment with less densely populated cities. As another step in the innovation process, we can invest in learning and renovation so as to provide impetus for the next cycle of innovation. The insights we have gathered up to this point will be very useful in greatly improving ParkAid as a solution to problems in the transportation sector, whose importance to society and the economy cannot be overstated.

VII. Self-reflection

To the Director of the ODU Advanced Technology Center,

Hello, my name is Marcos Luchetti and I am a Cybersecurity student here at Old Dominion University. Over the course of the Fall 2022 semester, I have participated in an entrepreneurship project in which I worked with two other students to create an innovation to a current problem in our society. For this project, we decided to pursue a solution to the problem of parking inefficiency in metropolitan areas and compromised security in smart parking applications. After brainstorming for ideas, we came up with a solution that has taken the form of a security-focused cyber-physical platform called ParkAid. A smart parking solution such as this would consist of several Internet-of-Things (IoT) components, including sensors, GPS, a smartphone app, and IoT middleware. When thinking about how it should be developed, I used my knowledge in cybersecurity to come up with a plan to have ParkAid follow the security-by-design approach, which would essentially prioritize the security and privacy of its users.

I read many scholarly articles to prepare myself to address all the issues related to the ParkAid problem statement. For instance, I learned quite a bit about the negative impacts of constant traffic congestion on metropolitan areas. These detrimental effects are felt not only by drivers, but also just as much, if not more, by non-drivers. You will find that traffic congestion often leads to heavy pollution which is bad for the environment and for our health, it detracts business from local commerce, and it can worsen the local inhabitants' quality of life, due to all the noise and obstruction. Furthermore, I learned how smart parking solutions work on a technological level and how security vulnerabilities are mitigated. I found these devices, like the

geometric sensors and cameras, as well as the method in which all these components communicate with each other, to be very interesting. I also found it useful to learn about cybersecurity implementation in smart parking technology. Looking at the problem from the perspective of fields not related to my major was also very eye-opening and reminded me that there is always room for interdisciplinary thinking. Overall, just putting this entire project together felt like a great experience that I can use to my advantage as I enter and progress into the cybersecurity field.

In regards to my project, students might find value in the innovation itself as well as the way I produced the project as a whole. In regards to ParkAid, students can find value in its mission to improve peoples' quality of life. As for how I made this project, students may find value in the attention to detail I put into every aspect, supported by comprehensive research and independent thinking, planning, and execution. If I were to do things differently, I would have liked to create a mini-prototype to show how the innovation actually works. I feel like I would have learned even more if I had been willing to make a real functioning prototype for ParkAid. Nevertheless, this was an unforgettable experience, and in the end I created an entrepreneurial project that I am very proud of.

Sincerely,

Marcos Luchetti

References

Abdullah, H., & Zeebaree, S. R. (2021). Android mobile applications vulnerabilities and prevention methods: A review [Paper presentation]. 2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA), Baghdad, Iraq. https://ieeexplore.ieee.org/document/9773615

Bodi, S. (1998). Ethics and information technology: Some principles to guide students. The Journal of Academic Librarianship, 24(6), 459-463. https://doi.org/10.1016/s0099-1333(98)90007-6

Caicedo, F., Lopez-Ospina, H., & Pablo-Malagrida, R. (2016). Environmental repercussions of parking demand management strategies using a constrained logit model. Transportation Research Part D: Transport and Environment, 48, 125-140. https://doi.org/10.1016/j.trd.2016.08.014

Garvey, P. R., Moynihan, R. A., & Servi, L. (2012). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. Systems Engineering, 16(3), 313-328. https://doi.org/10.1002/sys.21236

Giampaoli, L. E., & Hessel, F. (2021). Parking space occupancy monitoring system using computer vision and IoT [Paper presentation]. 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA. https://ieeexplore.ieee.org/abstract/document/9595935

Greenberg, S. R. (2015). Using innovation and technology to improve city services. IBM Center for The Business of Government. https://www.businessofgovernment.org/sites/default/files/Using%20Innovation%20and%20Technology%20to%20Improve%20City%20Services.pdf

Lewis, D. (2008). America's traffic congestion problem: Toward a framework for nationwide reform. Hamilton Project: Discussion Papers, 6, 2-36. http://proxy.lib.odu.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=34562011&scope=site

Mazzoli, R., Vukos-Walker, C., Sriraman, & Buck, A. (2022, September 20). Payment card industry (PCI) data security standard (DSS). Microsoft Learn. Retrieved December 2, 2022, from https://learn.microsoft.com/en-us/compliance/regulatory/offering-pci-dss

ur Rehman, S., & Gruhn, V. (2017). Recommended architecture for car parking management system based on cyber-physical system [Paper presentation]. 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia. https://ieeexplore.ieee.org/document/8272987

Shoup, D. C. (2006). Cruising for parking. Transport Policy, 13(6), 479-486. https://doi.org/10.1016/j.tranpol.2006.05.005

Texas Transportation Institute. (2007, September 18). Press release: Annual study shows traffic congestion worsening in cities large and small. https://mobility.tamu.edu/ums/media_information/press_release.stm

Qi, S. N., & Duan, M. (2022). Study on the impact of traffic carbon emission on environmental pollution considering time constraints. Advances in Transportation Studies, 2, 67–76. https://doi-org.proxy.lib.odu.edu/10.53136/97912599481137

Yang, W., & Lam, P. T. (2019). Evaluation of drivers' benefits accruing from an intelligent parking information system. Journal of Cleaner Production, 231, 783-793. https://doi.org/10.1016/j.jclepro.2019.05.247