Current Status of Art

Hardware and Hackers

Obinna Okonkwo, Isaac Mbappe

10/12/17

This report will choose to show the importance and basic needs for ethical hacking and hacker security in today's social, and give a brief knowledge on a society where without these key components of computer software defense could lead to a negative showing. This will be the core of our project which is to construct a hardware security device that will be implemented in our devices to improve our environment.

In today's economy, it is a major issue within producers as to how much security strength is place upon their product because of the constantly upgrading hackers and the vulnerabilities within different products. These businesses then recruit experts with hacking skills to then in sense destroy the product to rebuild.The basis of ethical hacking allows for any organization's interior security and information to be analyzed objectively. The group of ethical hackers have no previous knowledge but compile together information about the business by the data that is collected by the group. The job of ethical hackers is to examine the organization's main frame for different entry points, weaknesses, important targets that could be the main objectives for intruders, then begin to develop and design ways to defend against outside intruders from the information they have collected.

While, this report is to give light upon the principle and core of ethical hacking, but that is not to be confused with what malicious hackers. When it comes to this research project we choose to hack into the autonomous car from a malicious aspect but will learn from an ethical hacking position. Some might think that the difference between ethical and malicious hackers is basically a good and bad decision. As stated before Ethical hacking is based on the idea that a hacker uses their skills to obtain and improve an organization's interior technology. While the main goal of a malicious hacker is to obtain access unauthorized by the manager usually to gain sensitive information that would lead to personal gain. Malicious hackers can be known to cause chaos on a website or crash servers, just for notoriety. So in a sense we will be using different methods to gain access into the different autonomous cars and cause chaos, and then proceed to find better ways of strengthen our defensive systems within our cars.

The essence of this research project is ethical hacking as we have stated previously and with that we will be stating the advantages and disadvantages with in society when it comes to ethical hacking. The advantages of ethical hacking on a big scale could include the procedures that are taken to fend off national security breaches in regards to terrorism, while also on a lower scale is necessary for restricting access to malicious hackers which is crucial because of the

increase in the Internet of things in today's society. While the advantages allows for protection within national security, the same people we task with protecting our interior infrastructure could easily be swayed in the opposite direction. The disadvantages of ethical hacking, could potentially lead to financial and personal information being taken by the same hackers who placed the exact defensive measures in place to stop the breach, that also goes for bigger scaled hacks in regards to national security.

A product like the one being looked at within this VIP team would allow for us as undergraduate students to understand the basics of hacking within a microcomputer, as this is just the lowest of what could possibly be an ongoing, constantly updating, general safety hack for the foreseeable future. We understand that we are at least another 5 - 10 years before we will full computerized vehicles for everyday uses. When that time come, research like the one that this group is doing, would allow for greater defense against malicious hackers. As of right now, most cars come equipped with push-to-start as one of the only "hack able" source in the vehicle, but soon vehicles will start coming off the assembly-line with cellular use capabilities. Automated and connected vehicles are becoming a major platform for third party software and hardware. In this case, the security is proving a problem. Hackers had have the chance to demonstrate that they could take control of a vehicle having a velocity of seventy miles per hour. That happened in 2015. Once an intruder or attacker is in the system, that person can interfere with almost any protocol in the vehicle through different electronic controls units such as control steering, acceleration, braking, wireless connectivity, and some other function units. So in order to prevent that type of situation to happen, the security of our designated system must be well developed and quite unbreakable for the attackers. In order to do that, we must develop a system while having the mentality of an attackers.

Security is all around, for example, it is in identification, private communication, software protection, access control, electronic signature and so on. Security is the state of being free from threat. Autonomous vehicles are using multiple wireless sensors securities and quite some hardware securities. First of all, wireless sensors network is a group of transducers with the ability to communicate with infrastructure for recording and monitoring conditions at different locations. Wireless sensor network should be well protected especially, because it is a big concern for the society. Wireless sensor networks use different nodes that are able to detect, calculate, and communication different phenomena. Wireless sensors network is against a wide variety of unstable security due to the hardware limitations of the sensor nodes, large number of node, the weight of the application environmental conditions, and cost. Security should be prioritized in order to confidentially send a packet over the wireless network.

Confidentiality is the goal of security, quite basic, that provides one of the most important obstacles to achieve to satisfy the integrity and availability and the achievement of vital goals and time critical. There are different type of techniques to secure the information. There is an

encryption-decryption as a technique that is applied for the traditional wired networks and not for wireless sensor networks. But it is used to hide the content of a message while. And Steganography is used to hide the existence of the message. Wireless sensor networks are very weak and susceptible to many types of security attacks cause to the broadcast reason it will be better to implement another type of security such as hardware security.

Hardware security plays critical roles now that computing is integrated into many of our daily activities. Hardware security deals with data in hardware devices. A hardware security device will be manufactured and placed inside our autonomous vehicles or devices. That hardware security will work together with the software security that will already be developed and implemented into the autonomous car or devices microprocessors or micro-chips. That hardware device will execute specific tasks such as improving the security of the required device, being able to save the data then shut the system down in order to provide a counter attack to the intruder, being able to have a recoverable memory, so data will not be lost after a system shut down.

In the market, we found people who have ideas about making hardware-based security, meaning, the security will be built directly into the silicon and install it into the central processing unit (CPU). Based on our research, hardware-based security is not a new concept. It was just not successful because that hardware-based security was designed as a closed system, which eliminate the possibility of the third party to detect any security flaws.