HACK

Isaac Mbappe

Obinna Okonkwo

Faculty Advisor: Dr. Michaela Amoo

Wednesday 25th April, 2018

Abstract: The research I am conducting will give my audiences some information related to Data Integration in Wireless Sensors Network for autonomous vehicles. I have been interested in the hardware security area, reason I have decided to conduct a research in that field. This research will cover at least one factor that shows how wrong data are being read by wireless sensors, based on a conducted experiment. And how those wrong data can be a major factor in autonomous vehicles.

Summary:

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. In this project, we capture a frequency signal using a Radio Frequency device from a car key to reverse engineer it to hijack that specific car.

Problem Statement:

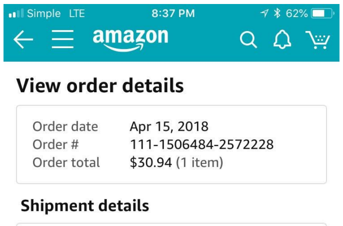
At the start of this school year our long term goal was to build a well constructed autonomous vehicle to perform specific task with the help of sensors as an attachment. Secondly, would like to also testing the security perimeters by hacking through the vehicle to building increase the security measure with the use of hardware defense. While that was our Long term goal, our Academic Year Goal was, with the help of a Software Defined Radio to design a hardware security measure that would stop the a recorded frequency from unlocking the vehicle.

As we matriculate through this technological society, everything in this world strives for protection from what we're not 100% with. In sports, we are told to always wear protective head gear, and when on strolling through your laptop, they stress to get Spyware to protect from harmful viruses. Just like society, this group's main goal is to research for an increase defensive perimeters to better provide safety for future consumers.

Design Requirement:

For the project, we'd required the use of a Software-Defined Radio (SDR) and computer software to connect to the radio in order to capture the signal that we would use from a car key.

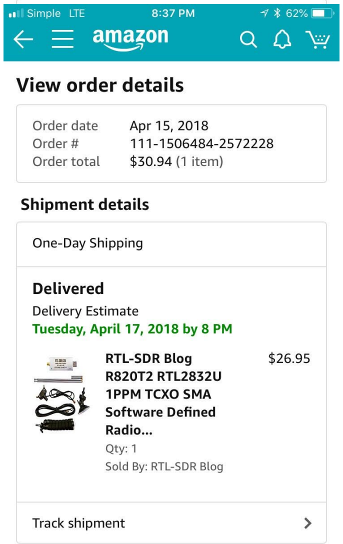
The budget that we place on my partner and I, because we were buying the equipment ourselves, was $200. We search different sites like Amazon, EBay, and sites that specialized in frequency devices. We were able to find different SDRs, the best ones soaring out of price range, but were able to come to agreement on one that would cost us roughly $90. We later came to find that this product was not compatible with our laptops, which forced us to go further and buy another; we would find one for $30. The software we were able to use for the project was small server software that was developed to allow users to share their radios over the internet or simply over their own remote shacks, which works with just a single user or up to a few hundred users.



View order details

Order date Apr 15, 2018
Order # 111-1506484-2572228
Order total $30.94 (1 item)

Shipment details



View order details

Order date Apr 15, 2018
Order # 111-1506484-2572228
Order total $30.94 (1 item)

Shipment details

One-Day Shipping

Delivered
Delivery Estimate
Tuesday, April 17, 2018 by 8 PM

RTL-SDR Blog R820T2 RTL2832U 1PPM TCXO SMA Software Defined Radio... $26.95
Qty: 1
Sold By: RTL-SDR Blog

Track shipment

In this paragraph I will discuss the different constraints within the project can be classified as such:social, cultural, political, environmental, economic, and time. As a social constraint, the questions whether the purpose is ethical or unethical. This type of research could be used wrongly by thieves to record key frequencies , to be used to gain entry into a vehicle. Within society , as we progress into the future technology like this needs to be researched and invested within as we try to plan on how to stop attacks when it comes the wrong side of the law. Another constraint that we faced as a group was the inaccessibility to experiment with more than one, due to the fact that between both me and my partner we only own one. On the side of Intellectual Property, we purchased the SDR that was used from www.nooelec.com , while the software is from https://airspy.com/spy-servers. The SDR that was used within this project stayed in line with the rules and regulation brought forth within in FCC part 15, that regulates everything that has to do with radio frequency devices.

Current Status of Art:

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.

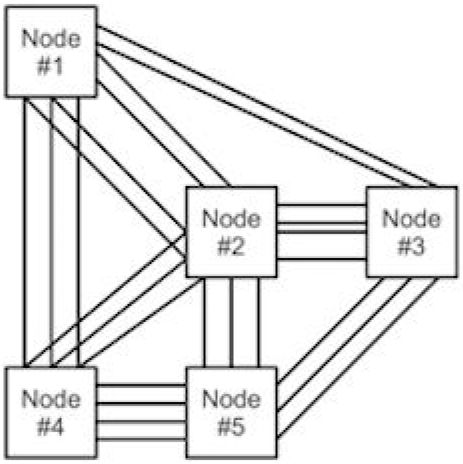
In the market, we found people who have ideas about making hardware-based security, meaning, the security will be built directly into the silicon and install it into the central processing unit (CPU). Based on our research, hardware-based security is not a new concept. It was just not successful because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

Solution Design:

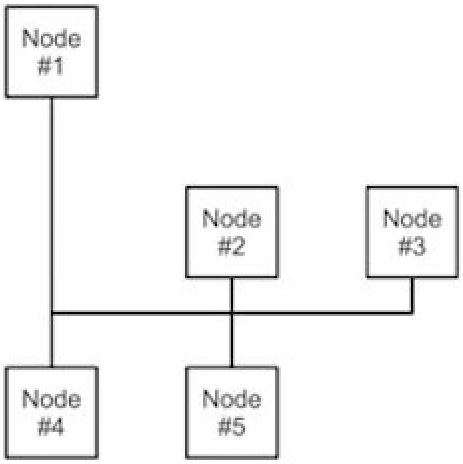
In today's economy, it is a major issue within producers as to how much security strength is place upon their product because of the constantly upgrading hackers and the vulnerabilities within different products. These businesses then recruit experts with hacking skills to then in sense destroy the product 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.

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.

We will prevent our system by protecting the CAN bus network.



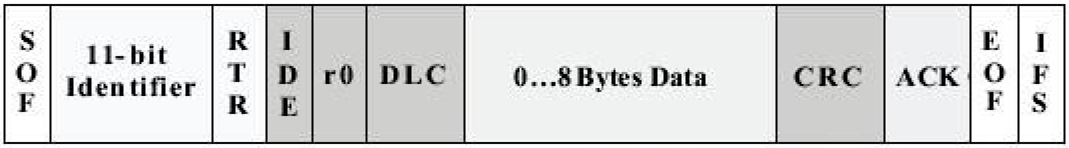
ECU



CAN

Before the CAN bus network, the engine control unit(ECU) was the main source connecting everything micro controllers to devices in the car. Reason there were many wires. But the CAN bus dramatically reduce the amount of wires used.

Every signal sent through the CAN bus has to go through the CAN frame before reaching the designated device.

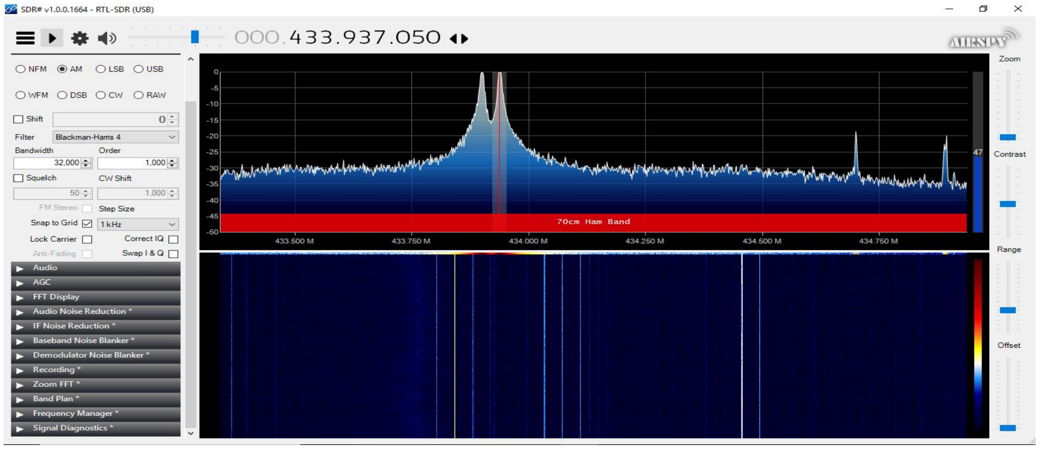


S O F	11-bit Identifier	R T R	I D E	r0	DLC	0…8 Bytes Data	CRC	ACK	E O F	I F S

Standard CAN frame Structure

Implementation:

We assemble all the pieces of the device together to capture the signal from a car key in order to replicate the same exact signal. Then signal that replica to hijack that specific car. Our main goal is to create a security that will prevent people to hijack autonomous system by reading a signal or by directly attacking the CAN bus located in an autonomous system.



SDR# v1.0.0.1664 - RTL-SDR (USB)

000.433.937.050

○ NFM ● AM ○ LSB ○ USB

○ WFM ○ DSB ○ CW ○ RAW

□ Shift 0

Filter: Blackman-Harris 4

Bandwidth: 32,000 Order: 1,000

□ Squelch 50 CW Shift 1,000

FM Stereo □ Step Size: 1 kHz

Snap to Grid ☑

Lock Carrier □ Correct IQ □

Anti-Fading □ Swap I & Q □

Reading a car key frequency signal.

Conclusion

To conclude, this school year while doing this research project, was one of learning and more learning. While we came in with a empty head, at this moment we have learned so much of the technical side of autonomous vehicles and methods of hacking into vehicles , such as through the CAN Bus and OBD-2 port. Understanding what is needed to receive and record signal frequencies with the software defined radio, gave us valuable knowledge as we journey towards our post graduate career.