CAR HACKING: THINK NOT, WHY HACK A DESKTOP WHEN YOU HACK A CAR?

Author: Anjana S Murthy
Assistant Professor
Dept of BCA
New Horizon College, Marathalli,
Bangalore, India.

Abstract :As time passes by the scale of technology grows larger and smarter, this applies to vehicles too. In the present-day cars are increasingly being implemented with computers or ECU's which are driven by millions of lines of code and control most of the critical systems even to an extent where the cars could drive by themselves. Completely packed under a interconnected internal networks most of the modern ECU's now come with a "socketCAN / CAN bus" which have given an added advantage for exploiters. In the past a car could only be hacked if it had an vulnerable ECU but with introduction of "socketCAN / CAN bus" as a few vulnerabilities closed new ones we're discovered, even though there exist IDS or intrusion detection systems it is practically very difficult for them to detect such attacks. Here in this paper as a proof of concept we're going to present multiple ways to exploit different vulnerabilities using the "socketCAN / CAN bus" in a car which would also show how the vulnerabilities are exploited and executed and what can be taken over and answer a few intriguing questions such as can the throttle, breaks and steering would be controlled?, is it viable to control the car while it's moving? , is it possible to lock up a person inside the car? And many more. And we would also present how a computer/ECU that was designed for safety be used for destruction with a few lines of code and tiny modifications to the system. And finally we try to find the best possible counter measures to overcome such attacks.

Keywords: socket CAN, CAN bus, exploits, vulnerability, car.

I Introduction:

In the ever changing world of technology as every possible device known to mankind are being turned smart so do automobiles. As vehicles grow day by day computers in them become smarter too or in other words they are being driven by computers to automate the maximum number of processes possible which has gone to an extent where car drive by themselves or have an autonomy level 4. But the real question is how is all this even driven? It is driven by something known as an ECU or in other words the brain of the car which pretty much controls everything, now here let's take a look at the basic ECU functionalities.

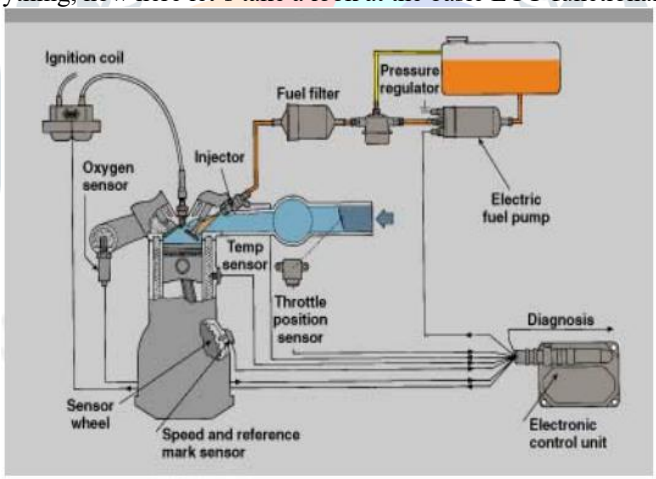


Figure 1: Engine Management System (Eyal, 2007)

Here a ECU works by interfacing with different engine components including the fuel pump, fuel injectors, throttle body, spark plugs, and various sensors, The ECU receives inputs from the sensors and makes slight adjustments for controlling the function of the engine's physical components accordingly. This allows for ignition timing and fuel/air mixture to be dynamically adjusted in real-time, which can save fuel and enhance performance. Prior to the use of ECUs for engine management, these functions had to be controlled mechanically, but with the introduction to an ECU things got a lot simpler. Today, in the automotive systems security is a trending topic is the recent high profile car hacking demonstrations have grabbed the attention to the fact that the modern automobile is highly vulnerable, which is an insecure platform that the public relies on, and one which plays an integral role in most people's lives? Unfortunately, this type of stance by the big automakers does nothing to improve vehicle security. It is clear that a more aggressive action is needed to address vulnerabilities and make the modern automobile a better platform all over.

2. Interconnected car network:

No here to understand the intercity of the problem that the modern day automobiles are facing, first let's take a look at how the hardware/sensor is interconnected with each other for the ECU to control them.

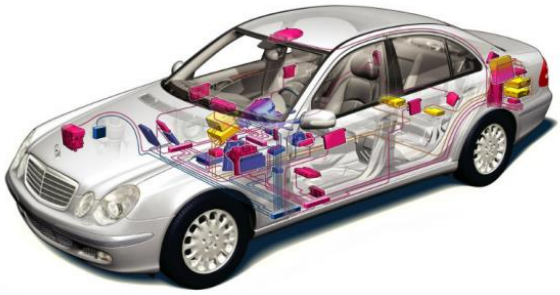


Figure 2: Diagram of electronic components in a car, courtesy of the Mercedes-Benz

Here in the above picture we can identify the components that are interconnected to the physical device which are seen blue in color, where as the safety components which are connected are seen pink in color and at the end all the entertainment systems that are connected are seen to be yellow in color. The interconnected devices contain the vehicles engine management system, Breaks, Airbags/ safety controls, door locks, all the gauges, entertainment systems, seat controls and more. As all the devices are interconnected to each other it makes the job of the attacker easier as exploiting just one of those many components would give the attacker access to all the devices or in other words the whole car.

3. The Architecture of CANBUS:

Before we get in to problem and exploitation let's first understand how what the architecture of CANBUS/ CAN socket is and how it works for a better point of understanding. In the brain of the modern-day vehicle's the inter connected systems in the controlled area network bus or in other words the CANBUS is a central network on "bus" on which the data traffic would be broadcasted, which commands everything from applying the brakes to lowering the windows. The CANBUS was brought into to reduce the complexity while reducing the wiring cost. Here let's take a look at the above explanation with the help of a picture:

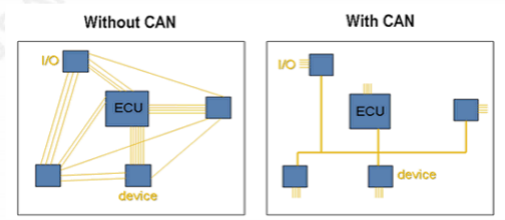


Figure 3: Can Networks Significantly Reduce Wiring (National Instruments, 2014)

Before the introduction of the CANBUS technology the communication b/w two devices had to be point-to-point connected, the diagram above demonstrates the efficiency of the CANBUS Socket. In a vehicle where the majority of the components being connected via the CAN, the "bus" receive a large amount of traffic, here now let's take a look at pictorial representation of the connection.

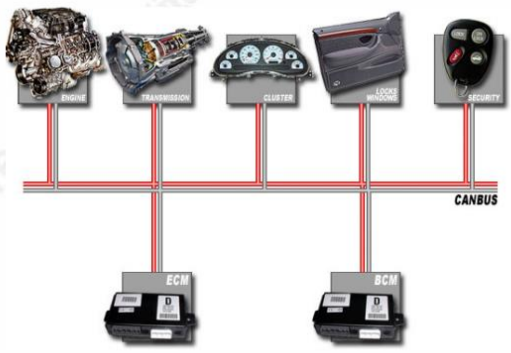


Figure 4: CAN Bus Network (Fortin Electronic Systems, 2006)

So then why is the CAN technology so different from the "bus" topologies in which the traffic constantly flows?CAN bus whether it is actually requested or not. An example of this can be illustrated using the vehicle's tachometer, which displays the number of revolutions per minute (RPM) being performed by the engine. For the tachometer to display the engine RPM, it does not first need to send a query to the engine; instead, the engine's ECU constantly broadcasts the engine RPM out over the CAN bus to any listening controllers. All the tachometer's controller needs to do is monitor CAN bus traffic for RPM messages, and when one is detected, the tachometer's display is updated with the new information. By repeating this action many times per second, the driver sees a tachometer readout that appears to change dynamically in real time.

Now let's take a look at the internal circuit of the CANBUS socket

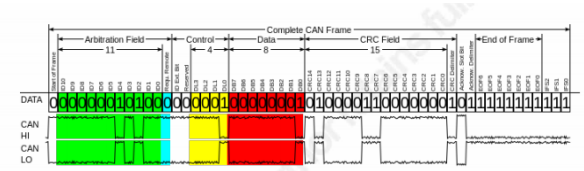
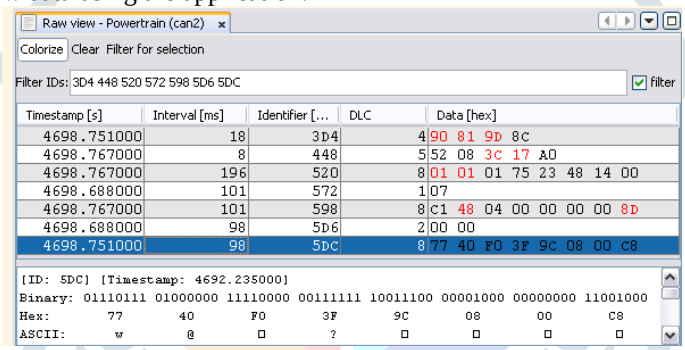


Figure 5: Complete CAN Frame (Wikipedia, 2014)

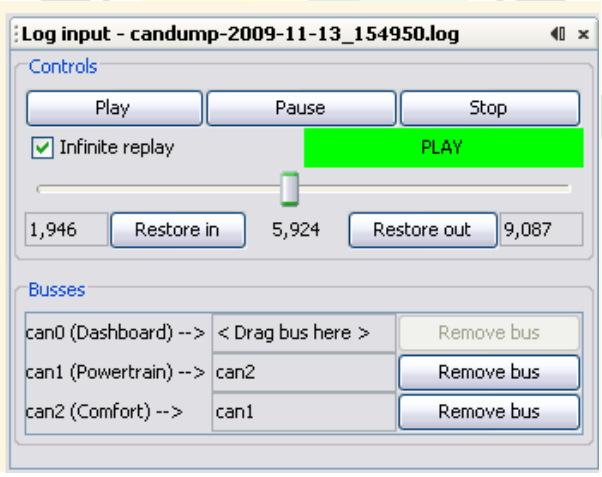
The first bit represents the start of a new data frame and is known as the SOF bit. The 11 bits that follow are used for the identifier. The next bit, shown in blue, is the remote transmission request (RTR) bit. Although CAN data is typically broadcast out onto the CAN bus without being solicited, it is also possible for a CAN controller to request data from another controller by utilizing the RTR bit. Following the RTR bit is an extended ID field bit and a reserved bit. Next comes to a 4-bit data length field, shown in yellow, whichis used to signify the length of the data which follows. The data portion, shown in red, comes next and can be anywhere from 0 to 64 bits (8 bytes) in length. Following the data field is a CRC field used for message integrity. The two bits that follow the CRC field are message acknowledgment (ACK) bits. Finally, the end of frame (EOF) bits is used to signify the end of the CAN data transmission.

4. Exploiting using CANBUS:

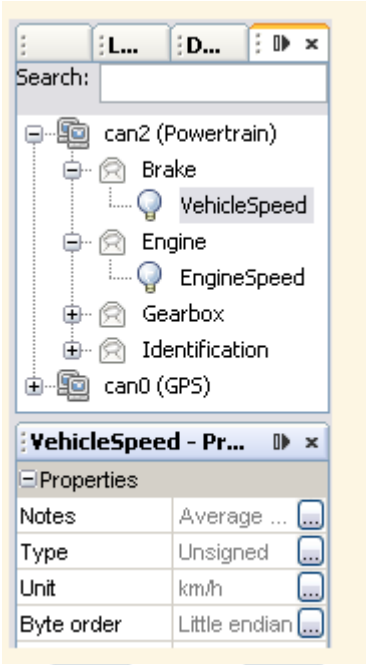
Here in this section we're going to take a look at how the exploitation is done using the CANBUS socket using a popular tool known as "Kayak". Kayak uses a compatible CAN adapter to create a new bus socket which means there would be additional hardware for exploitation. Assuming that kayak is installed and configured, we move forward to connect to the hardware that is connected to the car or in other words the new bus socket which was created earlier. Once connected the device automatically recognizes and makes a tree of the current session assuming that all the connection is done using the socket://busname@host:port we move forward to reading the raw data using the application.



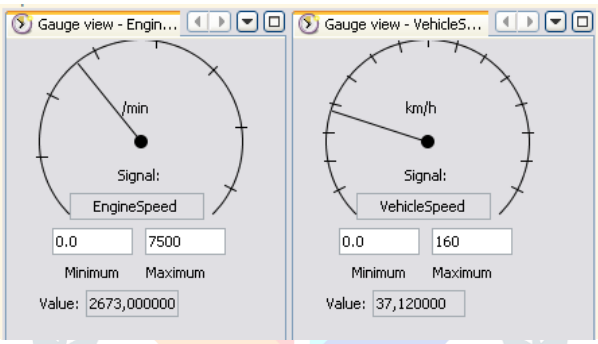
Here in the above picture we see the raw data post exploitation. Moving forward we use the application to record a log file and play a log file as shown in the picture below :



Moving forward towards the main objective of the session we try to manipulate the data that is flowing.



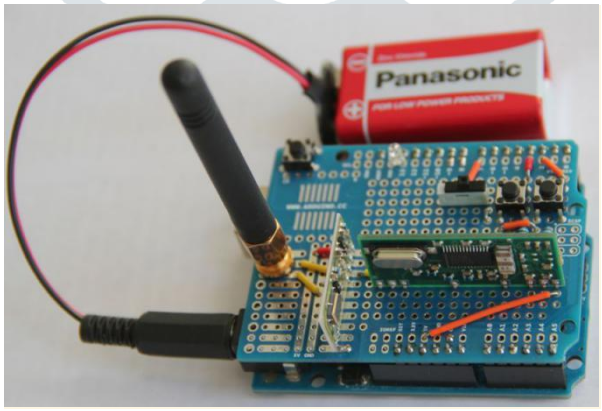
Let us look at picture below:



Here in the above pictures we see the manipulated data where the control is taken over.

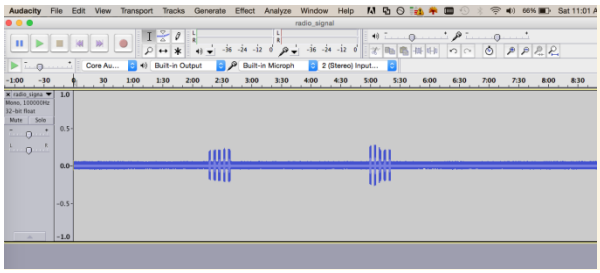
5. Exploiting using SDR:

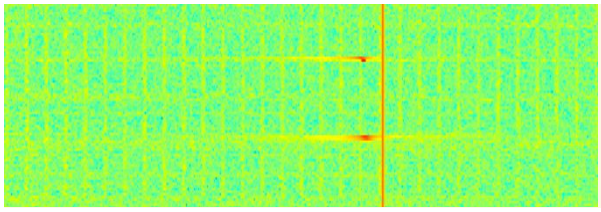
Using the CANBUS is not the only possible way exploiting a car and CANBUS exploitation also requires additional hardware too. But in this method we use a technique to capture radio waves for exploitation while the user unlocks the car using the remote; the exploitation tools and methodology are pretty much the same but with a external device for exploitation instead of an internal connection.



Here this 3000 rs device is capable enough to capture the radio waves from the car for attacker to exploit it.

Here's how the graph of the signal would look like :



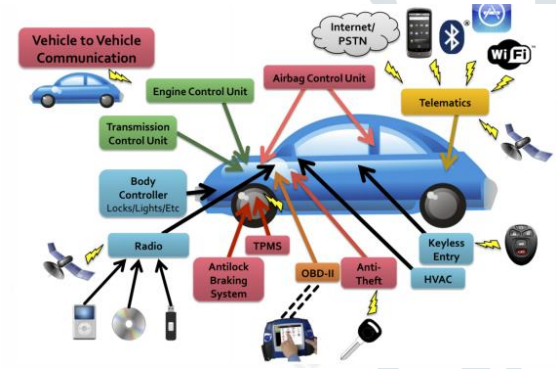


In the above picture the peak points in the graph is the time when there was access by the user and then the packets were captured at that moment for exploitation.

6. Post hacking effects:

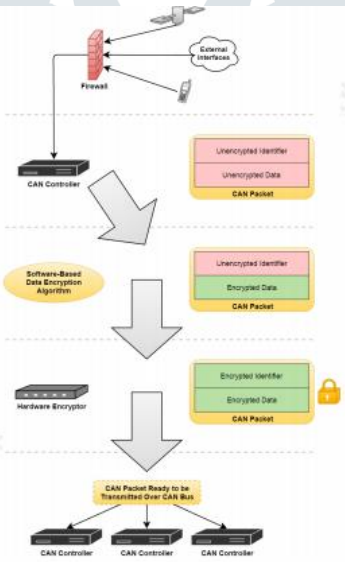
Once the attacker gains access to the car the hack could : steer the car, break without the knowledge of the user, control windows, control entertainment system, remotely turn off the car, disable the breaks, steal the car and many more all remotely without physical contact.

And here's a pictorial representation of the above statement:



5. Possible Solutions:

The most relevant solution for problem is to add a firewall, encrypt the traffic on the bus and enhance the IDS or intrusion detection system for an easier understanding here's a pictorial representation of it :



VI Conclusion:

As the automobile industry grows and updates itself the threats over car hacking decreases and as major car manufacturers have been briefed about the problem, as research is being carried on there would many more simpler ways to secure a car from being hacked and as time passes even cars would be secure and hard to hack.

REFERENCE:

[1]https://www.washingtonpost.com/news/wonk/wp/2013/07/25/heres-how-hackers-could-crash-your-car/?utm_term=.4c4cfa00b42a

[2]https://www.wired.com/story/car-hack-shut-down-safety-features/

[3]https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[4]https://interestingengineering.com/what-is-car-hacking-what-can-you-do-prevent

[5]http://www.eweek.com/security/parrot-security-os-3.5-improves-linux-security-tools-distribution/car-hacking-with-kayak

[6]https://makezine.com/2016/04/08/car-hacking-tools-trade/

[7]https://github.com/ParrotSec/car-hacking-tools

[8]http://samy.pl/opensesame/

[9]https://github.com/Hive13/CANiBUS

[10]http://linklayer.github.io/cantact/

[11]http://kayak.2codeornot2code.org/

[12]http://www.vanheusden.com/O2OO/

[13]https://github.com/zombieCraig/UDSim/

[14]http://octane.gmu.edu/

[15]https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platorm-For-Auditing-CAN-Devices-wp.pdf

[16]http://www.carknow.me/carduino/

[17]http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf

[18]http://opengarages.org/handbook/

[19]http://www.mcafee.com/de/resources/white-papers/wp-automotive-security.pdf

[20]http://www.syssec-project.eu/m/page-media/3/connectedcar-iv-2011.pdf