Summary of Article is as follows.

In-Vehicle networks used for inter-ECU communication, most commonly the CAN bus, were not designed with cyber-security in mind. As a result, communication by corrupt devices connected to the bus is not authenticated. IVAS is an in-place cryptographic scheme: the first CAN messaging solution to ensure both authentication and confidentiality without additional data such as authentication tags. The IVAS solution stands out in its ability to authenticate sender integrity and data integrity, blocking malicious messages without adding payloads

<https://trid.trb.org/view/1598171>

* 2.This Articles describes the attack and security of trucks and cars being used in United States today. Summary is as follows:
* All modern heavy duty trucks and buses in the United States use the SAE J1939 standard (J1939) for their internal networks. We show how the openness of the standard gives easy access for safety critical attacks. We demonstrate how simple it is to replicate the kinds of attacks used on consumer vehicles. We conclude with a discussion for possibilities of additional attacks and potential remote attack vectors. We are the first to experimentally demonstrate that heavy vehicle networks are vulnerable to heavy vehicle attacks to similar to consumer car attacks.

<https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf>

1. In this paper, a security situation awareness model is proposed based on the stacked denoising auto-encoder (SDAE) and bidirectional long short-term memory (Bi-LSTM) By fusing the domain data and expert knowledge, the proposed model has better accuracy and intelligence. The situation awareness processes of this model are divided into three stages: situation extraction, situation prediction and situation assessment. The model is officially used to predict the future of the CAN bus

<https://www.mdpi.com/2079-9292/11/1/110/htm>

1. The study of capacity optimization and costing models is an important research topic that deserves contributions from both the practical and theoretical perspectives. This paper presents and discusses a mathematical model for capacity management based on different costing models (ABC and TDABC) A generic model has been developed and it was used to analyze idle capacity and to design strategies towards the maximization of organization’s value. The trade-off capacity maximization vs operational efficiency is highlighted and it is shown that capacity optimization instead of maximization.

<https://reader.elsevier.com/reader/sd/pii/S2351978918312794?token=DA1C3C0207B03FB18451543176FDC436655EE242FE4B998952AFB1EE3063A5E028A087CE9047385BEDBF398D6FB7E6EA&originRegion=eu-west-1&originCreation=20220426085842>

1. In this Articles Two main computers are discussed along with their features and comparison being used in automobiles.

The two main computers that will be discussed in this paper are the Engine Control Unit and Power train Control Module. The ECU is one of the computers in the car that is most dominant and powerful. The PCM is a multi-layered circuit that adjusts and monitors all the mixtures such as fuel and air. It is in charge of monitoring the system's inputs, some parameters such as the fuel economy, and the emissions' management. In this section, we will discuss the different computers a car has, the research that has been done on car hacking, and finally the future expectations. We will explain some of the different aspects of the security aspects that have been done by universities, when it comes to cars.

http://misc.schattorie.nl/roadster/SMARTProject/Documentation/Car%20Hacking%20-%20eel%206931%20final.pdf

1. This articles is putting up some light on hacking techniques used in automobile Industry. How can we ethically hack cars , deploy patches and can raise awareness about Car Hacking Among people.

Summary of Article is as Follows:

The Controller Area Network (CAN-Bus) the de facto standard in modern cars is susceptible to cyber-attacks. The purpose of this research is to shed some light to the security and vulnerabilities patches that exist in the CAN-Bus and to make the public aware of such. An actual but ethical hacking is performed using an Instrument Cluster Simulator (ICSim), leading to taking control of various car controls such as opening and locking of door. This study seeks to assess the vulnerabilities in vehicular network that would be exploited by hackers to gain access and control in the automobiles.

<https://static1.squarespace.com/static/5ff7438c9d45b97785d3aa4a/t/607f306a3abd493f5c3703f6/1618948202993/JoanJohn_poster.pdf>

1. In this article author is describing features of Can and How can we enhance it’s security using different methods. Summary is as Follows:

Controller Area Network (CAN) is the most extensively embedded network protocol in vehicles. In the last decade, security attacks in vehicles have been increasing and have been reported in several papers. Authors propose centralized authentication system in CAN with improved CAN controller. The objective of the proposed security monitoring system is to prepare against spoofing attacks. The system proposed in this paper is schematically illustrated in Figure 3. Our experimental results demonstrate that our proposal method is effective on real in-vehicle network environments. It is essential to install a special purpose CAN controller that uses an error frame to overwrite spoof messages on a real time basis.

<https://global-sei.com/technology/tr/bn81/pdf/81-01.pdf>

8.

The Controller Area Network is a main standard for the in-vehicle network. However, lack of security features of CAN protocol makes vehicles vulnerable to attacks. The message injection attack is a representative attack type which injects fabricated messages to deceive original Electronic Control Units or to cause malfunctions. In this paper we propose a method able to detect four different type of attacks targeting the CAN protocol adopting fuzzy algorithms. We obtain encouraging results with a precision ranging from 0.85 to 1 using the fuzzy NN algorithm.

<https://ieeexplore.ieee.org/abstract/document/8015464>

9

In 2015, researchers exploited a vulnerability in the head unit that was produced by the supplier Harmon Kardon. They were able to control physical aspects of the car such as steering and braking at speed. This required no user interaction or special setup on the vehicles. The attack was nearly invisible to the driver and left behind almost no forensic evidence. No matter how hard we try and how we make the security solutions on vehicles, it is impossible to make something perfectly secure and un-hackable. A vehicle's security should not rely solely on preventing attacks, but should also design systems that can detect attacks and take appropriate actions.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8890036>

10/

The National Highway Traffic Safety Administration (NTHSA) released their policy on automated vehicle development in 2013. The Society of Automotive Engineers (SAE) released the international standard J3016 in 2014, where they defined six levels of automated driving. The prediction for SAE level five automation varies depending on who is asked. The infrastructure constraints to provide Vehicle to Everything (V2X) is still being developed including the standards for the Dedicated Short Range Communications (DSRC) which will enable the secure information sharing with the automotive Internet of Things (IoT).In this article Author is demonstrating an attack and concluding that we should design systems that can detect attacks research, we successfully attacked the Jeep hun- We exploited a vulnerability in the head unit Secure Automotive Systems Tesla Model S that can give you the total control of the vehicle. Tesla has now patched the Vulnerability,

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7815712>

11.Our anomaly detector works by calculating statistics about ongoing network traffic and comparing them with historical data. The collections of statistics are called flows. flows contain statistics about a complete com­ munication between two endpoints. We trained a one-class support vector machine (OCSVM) to classify flows flows. The OCSVM learns the distribution of a single class from training data [8]. data as in or out of the training class. We use same flows above as a basis for feature vectors for the OCSV

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7420322>

12.

CAN bus, data sniffers and car hacking development are finding increasing use in. The drawback is the possibility of unauthorized access to the data sent via the network. The system relies on two CAN network nodes. CAN networks seem to be the easiest way of Data transmission in Automobiles but direction is difficult to identify in a CAN network. It is impossible to determine in a simple way which data frames in a CAN network are sent via which nodes are to determine the data flow direction. Further the articles has some calculations for this problem resolution.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7284005>

13.

CAN Track are sophisticated Computer Aided Design (CAD) competitive tools. It not only supports planning, development, testing and finally starting-up; but also incorporates the unique features of CAN bus security enhancement and tool Network. (CAN) bus security feature is implemented using an encryption mechanism to encrypted message unique at any instance of time to avoid replay attacks. The algorithm is tested thoroughly on an experimental setup using Vector Canoe; with the results of two Index Terms – CAD, CAN, Automotive, Security, Encryption

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7934878>

14.

The most used protocol for communication of different components in automotive system is the Controller Area Network(CAN) This paper proposes a method based on deep learning aiming at discovering attacks toward the CAN-bus. It also validates our approach

by analysing a real-world dataset with the injection of messages from different types of attacks:denial of service,fuzzy pattern attacks,and attacks against specific components.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9325944>

15.

Paper proposes a hybrid anomaly detection system for CAN bus based on patterns of recurring messages and time interval of messages. The proposed system is evaluated on real CAN bus trafﬁc with simulated attack scenarios. The key idea is to model the recurring patterns in CAN bus messages and time interval range of individual CAN IDs. Injection attacks may not be detected by payload based systems as it only this work. Compromised apps connected to vehicles can can. to remotely control critical vehicle systems such as steering.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9342791>

Now The Idea We are gonna Implement:

Car Hacking: Accessing and Exploiting the CAN

Bus Protocol

Car Hacking: Accessing and Exploiting the CAN Bus Protocol is an easy-to-understand first attack on automobile. Using only free, open-source software and either a Raspberry Pi, an Android phone, or a free Kali Linux virtual machine running on an existing laptop, hackers can test for vulnerabilities and potentially attack a car be attached to the on-board diagnostic port (OBD-II) of a target vehicle for direct Car hacking itself is surprisingly similar to hacking other networked devices

In this article we are going to download some open source tools. Then we are going to capture CAN messages of the Car and then using some reverse Engineering Tools we are going to hack the car. Using these capture packets we can either go for replay attacks or In some severe cases we can even control the whole car remotely. The more explanation and Practical of this Article will be demonstrated in upcoming weeks.