Security Flaws in Autonomous Cars

Pranjal Page[1], Ujjwal Sirothia[2], Gautam Singla[3]

[1,2,3]SVKM's NMIMS (Deemed to be University), V. L. Mehta Road, Vile Parle, West Mumbai, Maharashtra, India, Pin Code - 400 056

---***---

ABSTRACT - *Development of autonomous vehicle is an upcoming disruptive technology in the field of Science. While there have been plenty of cases of accidents but all of them have been on account of information processing but it doesn't reflect the ambiguous threat hovering over implementation of autonomous vehicles i.e. security flaw.*

Going by the security triad, , availability is what keeping the researcher on toes as it directly affects human lives and confidentiality being the major issue in today's world its implication in autonomous vehicle is threatening user's mental and physical wellbeing.

Key-words: Security Flaws, Autonomous Cars, Data Privacy, Route Tracing

1. INTRODUCTION

Development of fully automated vehicles has to go through an array of complex issues. These issues are concerned with the security, legal, infrastructure and environment surrounding the autonomous cars. Security threats discovered till date make cars as vulnerable as any existing computer network. It could be data breach, spoofing and possible fatal attacks like taking full access over the car and shutting it down.

If we see a future filled with autonomous cars running on the road then this is the high time, the cyber security agencies working upon the security improvements because even though the threats are similar to the current network system but their impact would be much severe putting billions of life at stake. Advancement in technology for sustaining the autonomous vehicle industry is adding up new cyber threats which could be exploiting different sensors present in the vehicle. Without robust, sophisticated, bullet-proof cyber security for automated vehicles, mass market for these vehicles simply won't come into being.

2. AUTOMOTIVE NETWORK

As discussed earlier this cars are vulnerable to many cyber-attacks. The reason can be understand by studying the cars In-vehicle architecture and threats related to sensors used in this architecture. Different sensors works as a control unit known as the ECU's (Electrical Control Unit). Communication takes place between different ECU to efficiently monitor and configure different vehicular subsystems. Fig. 1 shows that the in-vehicle network is composed of several different subsystems like Vehicle safety, Powertrain, etc.

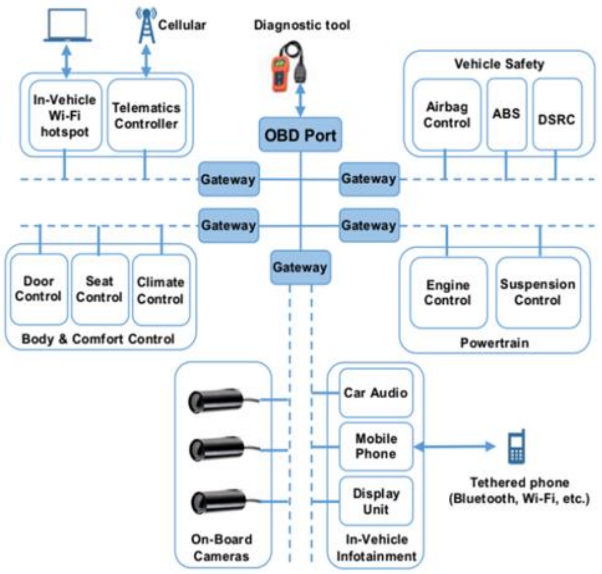


Figure 1: In-Vehicle Network Architecture

In functioning of self-driven cars, provision for its on road application with respect to its system architecture is classified in basically two networks. CAN (control area network) is used for motion sensor system such as the cars ABS system and Steering controls whereas the LIN (local interconnect network) functions for communication in the in vehicle network related to the features of cars. Here CAN network is responsible for cars functioning related to its travel purpose as this network coordinates between the service provider and connected vehicle. Vehicles for communication contain various ports such as the OBD, DSRC etc. This ports contains the details related to vehicle initial point address to destination address, the travel route and the time required to complete the journey. Therefore, the increasing number of connection points in each in-vehicle network subsystem make the vehicle more accessible from the outside world. Hence, more vulnerable to different cyber-attacks. Even if these entry points are secured separately can result in similar securing functions on connected vehicle. Restrictions such as limited computational power and storage capabilities should be considered.

3. CYBER THREAT VECTORS

Cyber threat vectors are the parameters due to which these self-driven cars can become victims of the cyber-attack. Bluetooth, OBD dongles, Transmission ECUs, Auto Mobile Apps are some vectors which can be attacked in order to control these connected vehicles. Such are illustrated in figure 2.

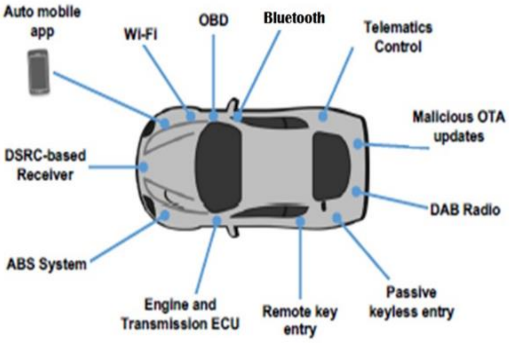
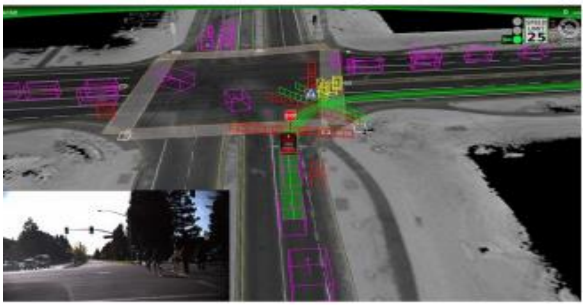


Figure 2. Cyber Threat Vectors

3.1 OBD PORT

OBD port consists of the procedure algorithm required for the connected vehicles in the respect of their infrastructure and travelling information in coordination with the service providers using gateways. As soon as this information is received at the server side of the service provider, a response related to the functioning of the vehicle is generated following the conditions and policies defined while framing the working algorithm of connected vehicle. This response in the form of packets are transferred to the OBD dongles acting as commands for vehicles. As we can see OBD port of vehicle consists almost a lot of information about the vehicle its security becomes a greater concern as it can be entry point for attackers and it also routes the attacker to its main ECU which is connected to the main CAN network. Also, its control is based on the application functionalities and it eventually turns into threat. The OBD dongles are connected to open source Road-side network and Secondly low level encryption can allow the attacker to edit the algorithm. Thus it can be a major security flaw at its real-time application.

3.2 DSRC PORT



In connected vehicles the working algorithm for communications between the service provider and connected vehicle are V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). Now for these communications the DSRC port manager is responsible. The DSRC delivers the communication packets in terms of On-Board Unit (OBU). As these packets are delivered on basis of connection network, it exposes too many packet-related attacks such as packet dropping, man-in-middle attack, even sometimes man-in-middle attack can invade the packet details and edit them and send them to receiver. Now let us understand one such attack. For an autonomous car a particular route is defined, the route is saved as car drives on the same route. Now suppose an attacker framed a fake object present on the road through which the car is being travelled. Now for an obstacle, an exception code routine is already defined which gets automatically called which in result makes the route changed, by such the attacker can control the vehicle. Such security flaw can cause sensitive data leakage causing a great privacy issue.

3.3 APP THREATS

Original Equipment Manufacturer (OEM) endorsed connected car solutions such as Apple's Car Play and Google's Android Auto interfaces will bring more integrated, but potentially vulnerable mobile apps into the connected vehicle. Recent reports about attacks on connect vehicle have a significant ratio of have been attacked by the auto-mobile apps. So the app's level of security against this threats becomes a major aspect. For apps utilizing web service authentication of host service provider should be verified at each route gateway communication before allowing its remote access to service provider.

4. PRIVACY ASPECTS

With the rapid development in self-driving it can be said the in future privately-owned autonomous cars can be in trend. Thinking of the privacy aspect, such issues can become a great concern for reliability. Below are some privacy issues that are needed to be addressed before these vehicles grab a full-fledged position in auto-mobile market

4.1 OWNER IDENTITY

As we studied earlier the self-driven cars collects the user information such as the destination address, route map of roads, etc. Thus, it becomes a great concern for connected vehicles functioning here. Attackers by hacking the ports sensors such as OBD Dongles, DSRC etc. used in cars can become a threat in terms of security.

4.2 ROUTE TRACING

Location Tracking is another concern as the route map derived for these autonomous cars are pre-defined and are governed by the host service provider. Now if this service provider is not secured enough, then the route map consisting the cars destination address, routes, speed, etc. is an entry point for attacker to get access of such information making it a privacy issue to be taken care of.

4.2.1 SENSITIVE LOCATION DATA

A dataset that contains sensitive location coordinates such as medical center, private bunkers and any other private trips socially unconventional places is prone to get exposed which might cause the owner mental and physical stress.

4.2.2 ADVERTISING

So far we have studied about the location tracking being a threat as the data can be used for deriving user's location and frequently visited places. Here, Marketing companies have a role play as if they get the location data and frequently used routes of user. They tend to post their marketing banners on those routes to gain customers. Another usage of such data could be providing best in vehicle experience by taking the route record which have business of their interest. E.g. if the owner usually travel to the electronic shop in his/her area then it may suggest the high rated shop in the nearby area.

4.3 SENSOR DATA

As discussed earlier OBD Dongles, DSRC port, Apps details etc. contains information related to travel, destination address. Now in the algorithm there is also a provision where similar routes or pattern of travel are recorded, it is fielded as an activity. Here, privacy the treat can be explained as e.g. suppose a user stops at coffee shop every day at a same period of time on his way to destination then this sub activity is also recorded in database in which location data, span of time, etc. are stored. Now this information describing user work schedule can be a type of private information issue. Besides this, as we discussed in Advertising, once the frequently used routes are figured out, Advertising companies tend to post their banners on those routes to gain customers. Thus we can say sensors data can be concern issue to secure vehicle's and user's information.

5. CONCLUSION

Hence, we can conclude that autonomous vehicles are far from being deployed on public roads as their security threats is still a concerned issue in its full-fledged implementation. They can provide a great support in terms of reliable travelling and transportation given that they are free from any life threatening security flaws. Security threats are the big obstacle on the road of implementation of autonomous cars but also we are sure that the self-driving enthusiasts will resolve this and come up with the best they have. We are pretty sure that someday and sometime the fictitious world of autonomous cars running on road would be a real thing.

ACKNOWLEDGEMENT

The work was mainly done at the campus of NMIMS, Shirpur. We would like to thank Mr. Ritesh Dhanare for his guidance and immense support. He encouraged us further for development of this paper. We would also like to thank our family for moral support.

REFERENCES

[1] Norton Rose Fulbright, the Privacy Implications of Autonomous Vehicles, June 2017.

[2] Qiang Ni and Mahmoud Hashem Eiza, Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security, February 2017.

[3] Christopher H. Grigorian and R. Nicholas Englund, Cybersecurity: Yes, They Will Hack Your Car, March 2017.

[4] Todd Litman, the Many Problems with Autonomous Vehicles, October 2017

[5] Anthony Jones, Autonomous Cars: Navigating the Patchwork of Data Privacy Laws That Could Impact the Industry, 2017

[6] Rob Toews, the biggest threat facing connected autonomous vehicles is cybersecurity, 2017

[7] By Kersten Heineke, Philipp Kampshoff, Armen Mkrtchyan, and Emily Shao, Self-driving car technology: When will the robots hit the road? 2017