International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: http://doi.org/10.31695/IJASRE.2018.32849

Volume 4, Issue 8
August - 2018

Enhancing Connected Vehicle Security with Block chain

Yamunaa Balasubramaniam[1] and Sathyanarayanan PSV[2]

[1]Business Architect, Ford Motors, India

[2] Project Manager, Wipro

India.

ABSTRACT

With millions of cars getting connected with OEM / Other vehicles in coming years, there is an increasing demand in ensuring that the consumers are rightly protected from any cyber threats. Vehicle to Vehicle communication such as Smart intersection, Traffic light control and Collision avoidance need the ultra-quick response after handling the security validation. Built-in security and architecture design are required to mitigate any threat. This paper discusses the need for a holistic approach to looking at the deep insight of hackable components in the connected vehicle ecosystem using Blockchain technology. It focuses on security services with Intrusion protection throughout the life cycle of the vehicle. All this ensures a comprehensive and end to end protection. Adhering to the proposed architecture provides proactive measures for any vulnerability thereby building trusted and secure vehicles.

Keywords: Block Chain, Connected Vehicles, Enhanced Security.

1. INTRODUCTION

1.1 Vehicle to Vehicle Communication

Most commonly proposed vehicular-ad-hoc-networks (VANET) concepts focus on centralized network structures which are similar to the road traffic regulations of the pre-VANE Tage, controlled by governmental institutions. As often in computer networks, centralized control structures result in several downsides: Central control units are single points of failures and especially worthwhile targets for attackers. Besides outside attackers, centralized systems are also particularly interesting for entities which perform (non)-governmental surveillance. As a consequence, the following section introduce an alternative decentralized and self-managed VANET structure based on the concept of Ethereum and a challenge-response-based authentication mechanism. Ethereum's contract system provides a framework for self-organization and self-management of the network using distributed applications on top of the blockchain technology.

1.2 Ethereum

Ethereum is a decentralized platform which is based on Bitcoin's block chain concept. "What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing complete programming language that can be used to create 'contracts'" [3]. In the context of Ethereum, a contract is an instance of an application which runs on the block chain and consists of its program code, storage and an account balance [4]. Contracts are created by posting them (and their code) to the blockchain. "The contract's code is executed whenever it receives a message, either from a user or from another contract. While executing its code, the contract may read from or write to its storage file. A contract can also receive money into its account balance, and send money from its account balance to other contracts or users. The code of a contract determines how it behaves when it receives messages, under what conditions (and to whom!) it sends money out and how it interacts with other contracts by sending messages to them" [4]. Contracts are powered by "gas", Ethereum's internal fuel. Each computational step of the code execution requires a certain amount of gas and therefore prevents accidental or hostile infinite loops [3]. Contracts are implemented in one of Ethereum's high-level languages (e.g Serpent), afterwards compiled into bytecode and posted to the blockchain. The execution of the contract code itself "is part of the definition of the state

transition function, which is part of the block validation algorithm, so if a transaction is added into block B the code execution spawned by that transaction will be executed by all nodes, now and in the future, that download and validate block B" [3].

2. RELATED WORKS

Previous work has proposed the use of hardware related side-channels [4] as a mitigation to this interference and eavesdropping problem in vehicular networking. Of particular interest, and one of the initial motivators for our work, was the observation that both ultrasonic systems (parking aid) and visual camera technology (adaptive headlight cornering camera) already exist on the front of many modern vehicles. More extensive camera capabilities are also available through the impact and accident logging devices that are increasingly incorporated in new vehicles. Ultrasonic audio and CMOS camera visual light devices exhibit high levels of directionality, and favorable signal attenuation properties that make it physically more difficult for an attacker to eavesdrop, intercept, inject or generate interference in these channels. A drawback to the use of these "commodity" hardware side-channels, however, is that they have a relatively low throughput, thus requiring the development and implementation of protocols that minimize the throughput requirement across the channels. In this paper we explore the feasibility of establishing the secure infrastructure for low data rate inter vehicular communications, using blockchain, in the absence of continuous RF or wireless infrastructure support.

3. CONNECTED VEHICLE ECOSYSTEM

Connected Vehicles, as the name goes, enables interoperable wireless communication of vehicles with each other and the world around them. The ecosystem includes everything, right from smart phones to infrastructure with the vehicles as the core of the system.

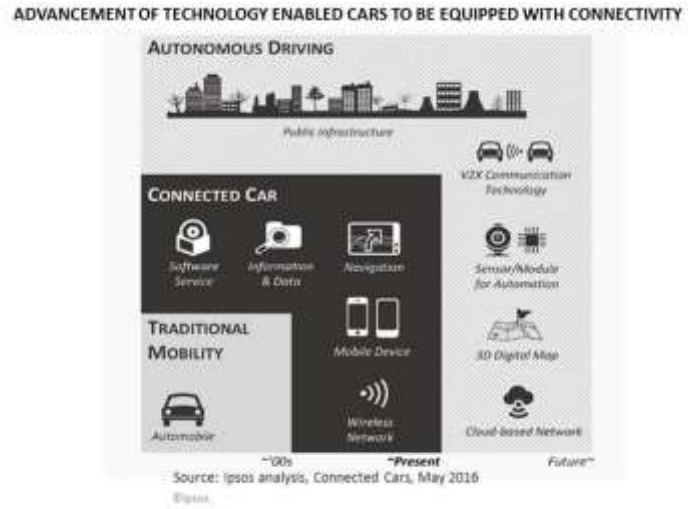

Fig 1. Autonomous Driving Illustration

Fig 1 illustrates how connected cars would be the predecessor of Autonomous Driving. It also depicts the components in the ecosystem. This drives the necessity of ensuring security across the ecosystem which triggers from the connected vehicle.

4. THREATS

In July 2015, researchers Charlie Miller and Chris Valasek, who have since accepted jobs at Uber, remotely disabled a Jeep Grand Cherokee on a highway after hacking into its Uconnect-based infotainment system. Shortly after, FCA carried out a voluntary recall of 1.4 million Uconnect-enabled vehicles to install a software patch.

A second hack was carried out in August 2016; this time, the car's braking, acceleration and steering could be manipulated at any speed. Both instances were reported in the press.

In February 2016, a UK-based Nissan Leaf was hacked over the Internet, demonstrating that a remote cyberattack can come from anywhere in the world. In this instance, Troy Hunt, a Microsoft Most Valuable Professional (MVP) for Developer Security, gained access to vehicle data and controlled certain vehicle systems from his home in Australia.

DOI: 10.31695/IJASRE.2018.32849

Then in June 2016, a Mitsubishi Outlander PHEV was hacked via its Remote Control smartphone app, which allows the user to lock or unlock doors, edit charger settings and control non-driving critical elements such as air conditioning.

Tesla has fallen victim to several hacks, most recently at the hands of Chinese cyber security firm Keen Security Lab. Researchers were able to control the brakes, doors, and mirrors of a Model S from 20km (12miles) away.

In August, a string of vehicle thefts in Houston marked what is reported as the first example of criminal cyberattacks. Two car hijackers appeared to replicate techniques used by academics by connecting a laptop to the vehicles' on-board diagnostics (OBD) ports. More than 100 SUVs were reportedly hacked and stolen.

All these incidents do not indicate one particular area that needs security but the whole ecosystem must be made secure for a safe environment.

Security is necessary to provide integrity, authentication and availability.

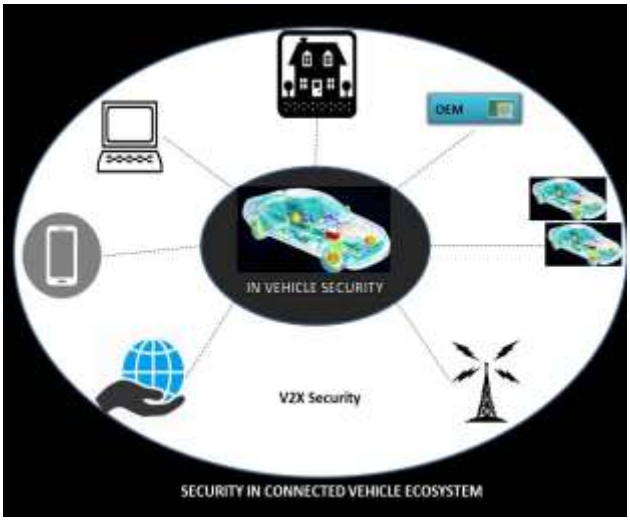

Fig 2. Security in Connected Vehicle system

5. THREAT LAYERS

Connected vehicle threat landscape includes multiple layers which clearly encompasses all possible areas that can be exploited by the attack vectors.

Fig 3 Layers of Threat and Security

5.1 HARDWARE SECURTIY

Securing Hardware components from being tampered is the first and foremost step towards security in connected vehicles. Various units like the Electronic Control Unit (ECU), Human Machine Interface (HMI), Sensors and many others must be protected as they are the secure anchors for next layer. This includes ensuring the code the board is running is authentic and the supply chain that built the product is secured.

This is followed by the security of software that is installed on the hardware.

5.2 SOFTWARE SECURITY

Software is everywhere – In Vehicle and in the Cloud. The market for intelligent connected cars will see a sharp rise by 2020. For the largest part these cars will be differentiated by the embedded software applications that run in the vehicle, as well as backend services that run in the cloud. Software systems can be attacked to steal information, monitor content, introduce vulnerabilities and damage the behavior of software. Ensuring privacy and appropriate user controls, promotes software security.

5.3 FIRMWARE SECURITY

Though infecting firmware is much harder than infecting regular software, corruption is possible with firmware. This can be counteracted with built-in protections in hardware, against any unauthorized firmware modification.

5.4 COMMUNICATION SECURITY

Hardware and software security alone have proven inadequate to protect against known threats. Communications security is the prevention of unauthorized access to telecommunications traffic, or to any written information that is transmitted or transferred. It should take into consideration the trusted over untrusted components to ensure that confidential information does not flow in an unintended way. Communication security includes Transmission security, Cryptographic Security, Physical Security and Emissions Security.

5.5 DATA SECURITY

Connected vehicles will produce larger volumes of data than ever. The data that is being collected from the connected vehicles should be used safe. Data security covers privacy and protection of personal data, vehicle specific data and telematics data. It also prevents corruption of data. Compromise of this data, poses just as much a threat to the overall security of connected vehicles. Classifying the data and securing sensitive and vulnerable data kick starts data security.

6. BLOCKCHAIN IN ACTION

A single solution to all this would be implementing block chain in the ecosystem. Block chain provides immutability and consistency by capturing every transaction with timestamp and all the transactions are validated before entering into a block. The distributed ledger enables every participant to have their copy of the ledger thus providing the key security properties of Confidentiality, Integrity and Availability to data in a distributed system. We introduce a blockchain protocol layer and a blockchain application layer to the base IoT architecture layers, as shown in Fig. 4.

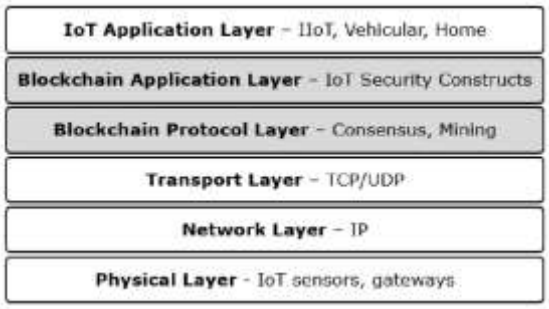

Fig 4. Blockchain With IoT Application

DOI: 10.31695/IJASRE.2018.32849

6.1 BLOCKCHAIN PROTOCOL LAYER

The blockchain protocol layer encompasses the consensus algorithm for nodes in the network. We define certain categories of messages in this layer to help achieve a common view of the blockchain among all participating nodes.

6.2 BLOCKCHAIN APPPLICATION LAYER

The blockchain application layer defines the IoT security specific transactions and their semantics for the higher layers. The core function provided by our proposed application model is authentication and authorization for devices on IoT networks.

7. CHALLENGES

In spite of all the security that blockchain offers, there are some challenges needing out attention. The speed to process transactions is low. Though Ethereum has better performance, will it suit for V2X communications which is real time? The computational power of all the participating nodes also has to be looked at.Finally, the size of the block; with so many transactions happening every millisecond, the number of transactions getting into a block is determined by the block size. This eventually contributes to the number of blocks in the chain.

8. CONCLUSION

Securing the software execution within the vehicle and the interfaces, communication to the vehicle provides protection end to end in the connected vehicle ecosystem. Automakers and the government together have major roles to put in place a strategy and tackle any vulnerability. Blockchain is a relatively unexplored area in the IoT security space, and we show that it is a viable solution to the IoT security problem. The key properties of tamper-resistance and decentralized trust allow us to build a secure authentication and authorization service which does not have a single point of failure.

REFERENCES

[1] Gartner. ”Report on IoT security spending”, Gartner Newsroom. 2016.
[2] ScorexFoundation. ”A treatise on Blockchain concepts + Scorex 2.0 tutorial.” https://github.com/ScorexFoundation/ScorexTutorial, 2017.
[3] S. Nakamoto. ”Bitcoin: A peer-to-peer electronic cash system.” https://bitcoin.org/bitcoin.pdf, 2008.
[4] Open Web Application Security Project. ”Internet of Things Project - Attack surfaces.” https://www.owasp.org/, 2017
[5] Abera, Tigist, et al. ”Things, trouble, trust: on building trust in IoT systems.” 53rd Annual Design Automation Conference. ACM, 2016.
[6] V. Buterin. ”On Stake” https://blog.ethereum.org/, 2014
[7] A. Varga and R. Hornig. ”An overview of the OMNeT++ simulation environment.” Simulation tools and techniques for communications, networks and systems & workshops, Simutools 08, 2008.
[8] Dorri, Ali, et al. ”Blockchain for IoT security and privacy: The case study of a smart home.” IEEE International Conference on Pervasive Computing and Communications Workshops, 2017.