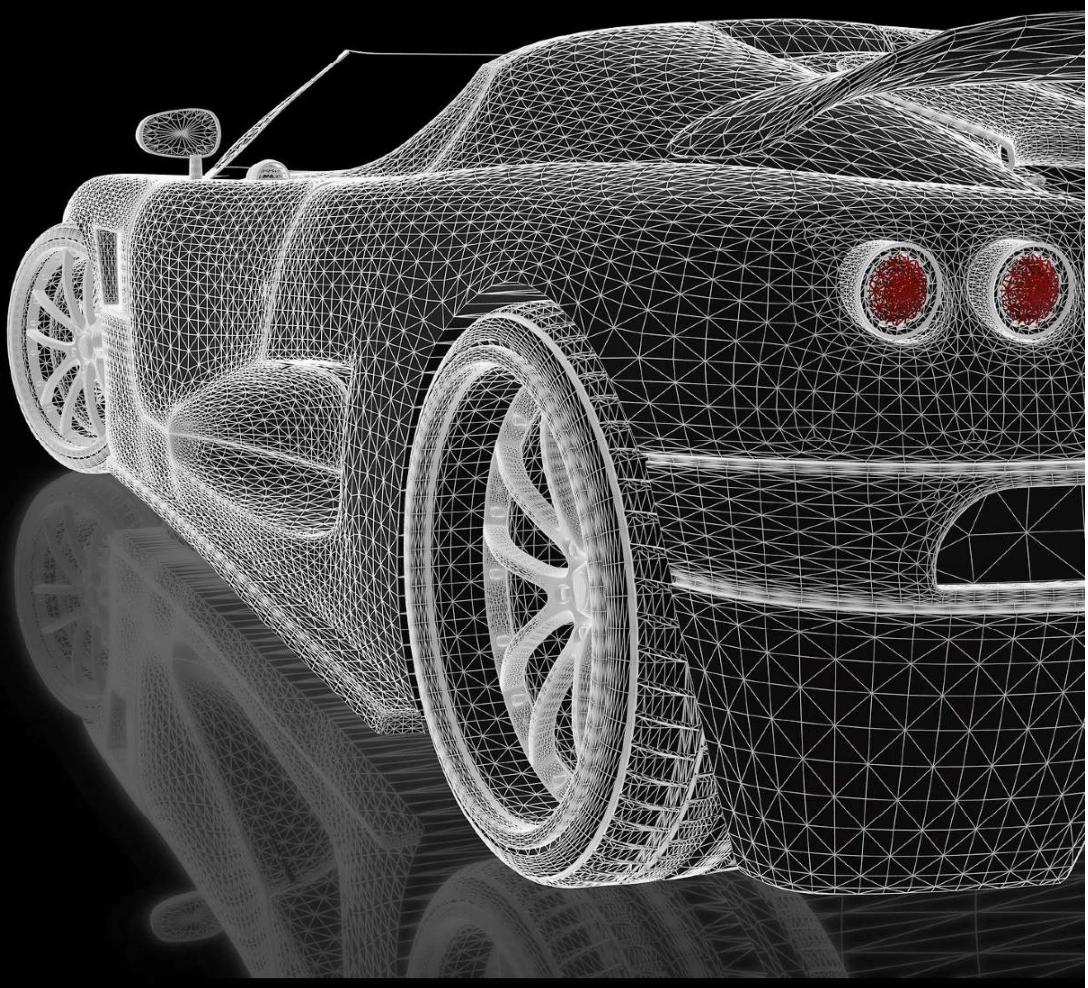
AUTOMOTIVE CYBER SECURITY CHALLENGES

A Beginner's Guide



Dr. Yasir Imtiaz Khan
Institute for Future Cities & Transport
Coventry University, United Kingdom

ISBN-13: 979-8617419612

Important Information

If you are a researcher/student and wants a free copy of the full book. Kindly send me an email at khan.yasir@outlook.com

To cite this book:

Khan, Y. I. (2020). Automotive Cyber Security Challenges: A Beginner's Guide. (1 ed.) Amazon Kindle, Feb 2020, ISBN 979-8617419612. https://www.amazon.co.uk/dp/B0852SMHLP

Bib

```
@article{khan2020automotive,
  title={Automotive Cyber Security Challenges: A Beginner's Guide},
  author={Khan, Yasir Imtiaz},
  year={2020},
  publisher={Amazon Kindle}
  ISBN={979-8617419612}
  url = {https://www.amazon.co.uk/dp/B0852SMHLP}
}
```

AUTOMOTIVE CYBER SECURITY CHALLENGES

A Beginner's guide

Dr. Yasir Imtiaz KHAN
Institute for Future Cities and Transport
Coventry University, United Kingdom

To Ammi and Abu

CONTENTS

PREFACE

This book explores the need for cyber security in automotive and what all the stakeholders e.g., Original Equipment Manufacturers (OEMs), users, security experts could do to fill the cyber security gaps. In particular, it looks at the security domain changes and how threat modelling and ethical hacking can help to secure modern vehicles. Furthermore, it examines the skills and tools that everyone who wants to work as automotive cyber security personal needs to be aware of, as well as how to think like an attacker and explore some advanced security methodologies.

This book could serve very well as a text book for undergraduate (year 3) and postgraduate modules for automotive cyber security. The book is organized into six chapters excluding the introduction. A brief description of each of the chapters follows:

Introduction highlights the importance of cyber security in modern vehicles by discussing critical security challenges that are faced by the automotive industry. Furthermore, some potential risks posed to modern vehicles are identified and discussed.

Chapter 1: This chapter starts with the history and evolution of modern vehicles over the years. Then, various standards proposed by the automotive industry to build secure vehicles are discussed. The learning objectives of this chapter include: understanding the automation levels in vehicles by comparing different proposed models, and learning the automotive standards to understand the need for automotive cyber security.

Chapter 2: This chapter establishes the automotive cyber security language. All the important concepts and definitions are provided in this chapter that are necessary to understand

the overall security situation in modern vehicles. Furthermore, the famous Jeep Cheroke attack along with other case studies are discussed that forced automotive industry to take cyber security seriously. The learning objectives of this chapter include: critical awareness of the key theoretical concepts underpinning cyber security threats in automotive context, and understanding current security loop holes in vehicles using real world case studies.

Chapter 3: The focus of this chapter is to study the most common in-vehicle networks e.g., Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay and media oriented system transportation (MOST). How these networks are connected and transmit data across electronic control units. Furthermore, an industrial tool named CANoe is explored to model the intended electronic control units and see how data transmission happens in the simulated environment. The learning objective of this chapter includes deep understanding of in-vehicle networks.

Chapter 4: The most common vulnerabilities and potential attacks on the controller area network are discussed in this chapter. Then, a practical demonstration of attack is shown through simulated tools. The learning objectives of this chapter include: critical awareness of error handling techniques of controller area network & their exploitations, and how to do reverse engineering of the real data.

Chapter 5: This chapter establishes threat modelling language in general and then focusing on automotive threat modelling. A new automotive threat modelling approach is proposed and used in this book. Through practical case studies the proposed approach is exemplified. Then, the attack trees are discussed in general and in the automotive context through examples. The learning objectives of this chapter include: deep understanding of core concepts of the structured approach to allow automotive cyber security threats to be modelled & classified, and how to do automotive threat modelling, and attack trees generation of automotive assets.

Chapter 6: The last chapter discusses the vehicle perimeter security. Different proposals of firewalls, intrusion detection systems, and encryption in the automotive context are explored and discussed. The learning objectives of this chapter include: understanding core concepts of perimeter security in general and automotive, and evaluating current perimeter security measures in automotive.

Y. I. KHAN

Coventry, United Kingdom
February, 2020

ACKNOWLEDGMENTS

To all the wonderful people I owe a deep sense of gratitude especially now that this project has been completed.

Y. I. K.

INTRODUCTION

Today, we see vehicles with fascinating features such as interactive telematics unit where you could use GPS, play your favourite songs and connect your phones to make calls. They offer lane assistance, power windows and seat warming. Behind these rich features of vehicles, there are millions of lines of code that are running on embedded systems commanding each element to act correctly.

[Example Scenario] Imagine, you are driving your sports utility vehicle or any vehicle on national highways or motorways and suddenly your vehicle speed starts to increase without you pushing the accelerator, your door windows roll down and your breaks are not operational any more. Unfortunately, this is a harsh reality not a Hollywood movie script.

[How is this possible?]

The simple answer is due to lack of security in automotive. There are many vulnerabilities that could be exploited to launch cyber attacks on vehicles either physically or remotely. One example attack is to exploit the vulnerabilities of the controller area network (CAN) using OBD-2 port (i.e., on-board diagnostics port, which has been left open for everyone by law for vehicle diagnostic purposes). CAN is the main backbone in-vehicle network, which does not have any encryption or authentication mechanism embedded. Many cheap CAN loggers are available to record the in-vehicle communication, which can be easily reverse engineered. These loggers have made it very easy to get human-readable live OBD2 data from the vehicles on speed, revolutions per minute, throttle position and more. Furthermore, these loggers can facilitate transmitting crafted messages into the CAN bus. Now the question is how can we connect these loggers to vehicles? There are two ways: 1) we

physically connect the CAN logger through the OBD-2 port, 2) we connect the CAN logger remotely for example, this could be achieved by taking control of the infotainment system.

To be fair, when automotive industry was growing, the only requirements were fast, comfortable, safe vehicles. Unfortunately, the security was not considered as a prime requirement and there was not any legislation forcing manufacturers to build secure vehicles.

Let us discuss security challenges that modern vehicles are facing.

The computation power of vehicle is low due to environmental conditions. The embedded computers i.e., ECUs are designed for specific functionalities, therefore, the computation power by design is very limited, which can be an advantage for the adversaries as they can leverage the power of better computers. Another drawback with vehicles is that they could run easily for a decade and the technology on the other hand grows exponentially, which makes them easy to be exploited.

It is not feasible to monitor any vehicle if it is not connected. Whenever there is a problem with your car, you need to go to the garage for possible diagnostics, which is very cumbersome. What if vehicle is connected all the time and all the updates and diagnostics are done remotely?

Software testing is considered one of the most expensive phases in the software development life cycle. To make all the vehicle secure, it is important to perform exhaustive testing, since, companies need to employ more people to change the entire development if there are problems discovered late.

The intelligent transportation system demands connectivity of vehicles and communication from vehicle to vehicle/infrastructure. Appartently, the connected and autonomous vehicles are the future. In general, vehicular connectivity is very similar to computers, where there is a complex software architecture and many new applications. Modern days vehicles have millions of lines of codes enabling ECUs (Electronic Control Unit) to perform different functionalities. Software updates of ECUs are inevitable to prevent discovered vulnerabilities. In the automotive world, software updates are very crucial as it could be very dangerous for the safety and security of passengers. The challenge for software update in automotive is that every vehicle cannot be brought back to garage every time there is a patch available. Many companies/researchers are working to find ways for secure over-the-air updates [1, 2, 3].

As we are heading towards more connectivity e.g., vehicle to vehicles and vehicles to infrastructure. One infected vehicle will be a potential risk to many other vehicles. We need to secure all the functionalities of a single car to protect the rest.

As discussed above, vehicles can be attacked either physically or remotely. There is an immense need to isolate remote connectivity with the internal communication in vehicle. Usually, remote connectivity is limited to certain specific components in vehicles e.g., infotainment system should not have access to the in-vehicle networks such as CAN, FlexRay. The AUTOSAR recommends automotive cyber security architectural design must consider the issues of how to isolate, deploy and manage these connectivity interfaces in a secure

way.

Connected and autonomous vehicles will be using more and more personal information e.g., GPS locations, biometric information and linking it to the cloud. This is a challenging task to protect the personal data theft and possible alterations. The attacker could easily use such data to launch remote or physical attacks.

[Reflection] Now that you have read the security challenges, who do you think is responsible for automotive cyber security, vehicle manufacturers or owners?

The ideas of connected and autonomous vehicles and intelligent transportation are fascinating but carries huge burden of cyber security. The communication between vehicles to vehicle/infrastructure needs confidentiality, integrity and availability. Some example of risks posed to modern vehicles are as follows:

Identity/personal information theft: Owner details, GPS logs, credit cards, etc.

Unauthorised access: Keyless door entry system through mobile apps or electronic key fobs.

Creation of mobile bots: Large number of vehicles could be excellent candidates for bots, which can be used to launch cyber attacks.

Installation of ransomware: Victims must pay money to regain control of their vehicles.

REFERENCES

1. McAfee Labs. Mcafee labs report 2016 threats predictions. Intel Security, 2016. `www.mcafee.com/mx/resources/reports/rp-threats-predictions-2016.pdf`.
2. Bernardeschi C. and Din G. Security modeling and automatic code generation in AUTOSAR. Universit di Pisa Dipartimento di Ingegneria dellInformazione Corso di Laurea Magistrale in Computer Engineering, 2016.
3. ADI KARAHASANOVIC, Threat modeling of the AUTOSAR standard. Master Thesis. Department of Computer Science and Engineering Chalmers University of Technology University of Gothenburg, Sweden 2016.