APPLIED COMPUTER SCIENCES

FH JOANNEUM
University of Applied Sciences

Student: Markus Wolf
Supervisor: FH-Prof. DI Dr. Klaus Gebeshuber
Degree Programme: IT & Mobile Security 2018

Automotive Cyber Security Toolkit

Car Hacking Based on Android Infotainment Systems

Rationale:

Modern cars contain tens of thousands of lines of code inside their Electrical Control Units and almost every contains a central ECU that is a fully functional computer. For a long time, these components were only developed focusing on functionality and not on security. Therefore, many vulnerabilities in automotive exist that propose mayor threats to IT- and physical security [1, 2]. Miller and Valasek made such vulnerabilities public in 2015 when they hacked a Jeep Cherokee over the internet and drove it off the road. This led to a recall of 1.4 million vehicles to fix the issue, but many others may have not been discovered by now [3]. Moreover, the attack surface of vehicles consists of different entry points like the telematic control unit, the OBD Interface, the Tire Pressure Monitoring System or the mentioned Infotainment System, resulting in a broad field of potential topics for scientific research [2, 3, 4, 5]. AVL List GmbH is currently starting with research projects in the field of automotive security. Therefore, a so called “automotive cyber security toolkit” is needed to identify possible entry points, evaluate security levels, and perform security tests of different kinds of automotive systems. In addition, a PoC of an Android In-Vehicle Infotainment System exploit will demonstrate security vulnerabilities in modern vehicles [6, 7].

Research Questions:

- Which available hardware and software can be used for security assessments on vehicles?
- Which attack surface do modern vehicles provide?
- What are the key aspects of an automotive vehicle penetration testing scenario?
- What vulnerabilities do In-Vehicle Infotainment Systems provide?

Methodological Design:

The first step consists of gathering software and hardware tools for penetration testing in relation to automotive vehicles by performing an online literature research. The tools are afterwards categorized in a matrix that includes different kinds of information like purpose, target interface, author, licence model, costs and documentation for every item. As a practical part a proof of concept is created, where the CAN-Bus of a car is accessed by exploiting a retrofitted Android infotainment system in a case study.

Objective:

The main objective of the project is to identify, evaluate and categorize existing software and hardware tools in the field of automotive security to create a collection as start point for further research in the AVL List GmbH. In relation to this, a list of automotive interfaces that exist in modern cars for security tests is gathered. Each interface is assessed in terms of robustness, security mechanisms and access difficulty. The practical part consists of a case-study in which a Mazda model 3 with a retrofitted In-Vehicle Infotainment System with Android 7.1 will be tested. As a conclusion, a matrix that contains important information e.g. costs, license model, documentation and targeted interface per tool is created.

Literature:

[1] Smith C. The Car Hacker’s Handbook: A Guide for the Penetration Tester, 2016, No Starch Press, USA.
[2] Miller C. & Valasek C.: Survey of Remote Automotive Attack Surfaces, In http://illmatics.com/remote%20attack%20surfaces.pdf, 2014 [Acc. 01.01.2020]
[3] Miller C. & Valasek C.: Remote Exploitation of an unaltered Passenger Vehicle, In http://illmatics.com/Remote%20Car%20Hacking.pdf, 2015 [Acc. 01.01.2020]
[4] Checkoway S. et. al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security Symposium, USENIX Association, 2011
[5] Foster I. et.al.: Fast and Vulnerable: A Story of Telematic Failures, WOOT’15, USENIX Association, 2015
[6] Keuper & Alkemade: The Connected Car. Research Rapport, Computest, 2018
[7] Constantino G. & Matteucci I.: Demo Candy Cream, In https://www.iit.cnr.it/sites/default/files/Costantino-Matteucci2019_Chapter_DemoCANDYCREAM.pdf, 2019 [Accessed 1 Jan. 2020]

Contact:

markus.wolf@edu.fh-joanneum.at

source: auto-pumpkin.com

source: pentest-standard.org

source: flaticon.com