CAR HACKING AT DEF CON 26

by: Mike Szczys

9 Comments

August 11, 2018

Hackaday

August 2018

Keen Security Lab

August 2017

Tencent 腾讯 KEEN security lab

black hat

FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

Sen Nie, Ling Liu, Yuefeng Du
Keen Security Lab of Tencent
{snie, dlingliu, davendu}@tencent.com

ABSTRACT

In today's world of connected cars, security is of vital importance. The security of these cars is not only a technological issue, but also an issue of human safety. In our research, we focused on perhaps the most famous connected car model: Tesla.

In September 2016, our team (Keen Security Lab of Tencent) successfully implemented a remote attack on the Tesla Model S in both Parking and Driving mode.[1-3] This remote attack utilized a complex chain of vulnerabilities. We have proved that we can gain entrance from wireless (Wi-Fi/Cellular), compromise many in-vehicle systems like IC, CID, and Gateway, and then inject malicious CAN messages into the CAN Bus. Just 10 days after we submitted our research to Tesla, Tesla responded with an update using their OTA mechanism and introduced the code signing protection into Tesla cars.

REGULAR EXPLOITATION OF A TESLA MODEL 3 THROUGH CHROMIUM REGEXP

December 19, 2019 | Jasiel Spelman

TO THE BLOG

This is the fourth in our series of Top 5 interesting cases fro[m]
bugs has some element that sets them apart from the more
released by the program this year. Today, we look at the expl[oit]
Model 3 in Vancouver at Pwn2Own this year.

Zero Day Initiative

December 2019

New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars

by Tencent Keen Security Lab

After conducting the intensive security analysis of multiple BMW cars' electronic control units, Keen Security Lab has found 14 vulnerabilities with local and remote access vectors in BMW connected cars. And 7 of these vulnerabilities were assigned CVE (Common Vulnerabilities and Exposures) numbers.

Introduction

The research of BMW cars is an ethical hacking research project. In the research, Keen Security Lab performed an in-depth and comprehensive analysis of both hardware and software on in-vehicle infotainment Head Unit, Telematics Control Unit and Central Gateway Module of multiple BMW vehicles. Through mainly focusing on various external attack surfaces, (including GSM network, BMW Remote Service, BMW ConnectedDrive System, Remote Diagnosis, NGTP protocol, Bluetooth protocol, USB and OBD-II interfaces), Keen Security Lab has gained local and remote access to infotainment components, T-Box components and UDS communication above certain speed of selected multiple BMW vehicle modules and been able to gain control of the CAN buses with the execution of arbitrary, unauthorized diagnostic requests of BMW in-car systems remotely.

Keen Security Lab

August 2018