Automotive Cybersecurity
From perceived threat to stark reality

SHAMIK GHOSH
July 2016
## Contents

1. **The automotive cybersecurity conundrum** 1
   1.1 Introduction 1
   1.2 What needs to be done? 3

2. **Nuts and bolts of cyberattacks** 5
   2.1 Why would one hack a vehicle? 5
   2.2 Hacker’s motivational factors 5
   2.3 CAN – the holy grail for hackers 7
   2.4 Who is responsible if a vehicle is hacked? 9

3. **Remote attack surfaces in modern vehicles** 10
   3.1 If it’s CONNECTED; it’s HACKABLE 10
   3.2 In-vehicle Infotainment units 11
   3.3 OBD-II dongles 12
   3.4 Bluetooth (Paired devices) 14
   3.5 In-car Wi-Fi 14
   3.6 Tyre Pressure Monitoring Systems (TPMS) 14
   3.7 Remote Keyless Entry (RKE) 15
   3.8 In-car apps/content 16
   3.9 External links (V2X communications) 17
   3.10 EV charging 18

4. **Perspective: the vehicle manufacturers’ take on cybersecurity** 19
   4.1 Is security a priority for the automotive industry? 19
   4.2 Automotive industry investing in cybersecurity, but ROI? 20
   4.3 Security by design: From reactive to pre-emptive 22
   4.4 Security & Privacy: Dealing with two different worlds 23

5. **Regulatory landscape for automotive cybersecurity** 25
   5.1 How government authorities can help? 25
   5.2 Legislation on automotive cybersecurity – help or hindrance? 26
   5.3 Cybersecurity related standards for automotive 27

6. **Securing our connected vehicles** 30
   6.1 Learning from other industries 30
   6.2 Automotive cybersecurity best practices: the four ‘S’s 31
6.3 OTA management 33
6.4 Don't FORGET your suppliers! 34

7. Automotive cybersecurity projects and solutions 35
7.1 Introduction 35
7.2 Auto-ISAC (Information Sharing Advisory Centre) 35
7.3 Cyber Security Consortium for Connected Vehicles (CCV) 36
7.4 I Am the Cavalry (IAtC) 36
7.5 Trustworthy Software Initiative (TSI) 36
7.6 GENIVI Alliance 37
7.7 Intel's Automotive Security Review Board (ASRB) 37
7.8 Transport Research Laboratory (TRL) 38
7.9 Argus Intrusion Prevention System (IPS) 38
7.10 TowerSec ECUSHield 38
7.11 NCC-SBD Automotive Secure Development Cycle (ASDL) 39
7.12 Symantec's Embedded Security: critical system protection 39
7.13 Blackberry's Professional Cybersecurity Services 40

References 41

List of figures

Figure 1 Charlie Miller (driver) and Chris Valasek with the Jeep Cherokee 1
Figure 2 Replacement of an authentic CAN program by a malicious one 8
Figure 3 1978 Cadillac Seville's dashboard 10
Figure 4 NissanConnect EV app for LEAF 16
Figure 5 Automotive cybersecurity investment 20

List of tables

Table 1 Car hacking value chain analysis 6
Table 2 Available intra-vehicle networking protocols 7
Table 3 Ramifications of SPY Car Act 27
Table 4 Security Development Lifecycle 31