Automotive Cybersecurity
From perceived threat to stark reality

Shamik Ghosh
ABOUT Automotive

Since 2002, our exclusive network of industry specialists has ensured an unrivalled resource to bring you comprehensive coverage of the automotive supplier industry. Each report gathers individual perspectives from within the industry, and formulates ABOUT Automotive's own definitive forecasts, generally to a 5–7 year horizon.

All ABOUT Automotive authors have a proven track record, having written for leading management consultancies, financial institutions and publishers. ABOUT Automotive reports are used by the major automotive suppliers, as well as the leading vehicle manufacturers. They are also used by banks and management consultants, as well as academic institutions.

SAE International

SAE International is a global professional society that provides technical resources for the ground vehicle and aerospace engineering community. Since 1905, SAE has connected engineers and the technical content needed to provide the solutions to improve vehicle technology and advance the mobility industry.

SAE International sets the standards for vehicle engineering and delivers a lifetime of learning. By uniting over 128,000 engineering professionals and technical experts world-wide through a comprehensive collection of programs, products, and services, SAE International drives both expertise and knowledge to the vehicle engineering community.

The Author

Shamik Ghosh is an experienced professional with a diverse knowledge of the automotive industry. He has swiftly acquired a thorough understanding of the disruptive trends in automotive technology like autonomous driving, connected cars, IoT and smart mobility. Shamik has written over 2,000 articles and is also a frequent participant in major industry studies, and has advised numerous clients on strategy and competitive issues.
# Contents

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

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

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

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

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

6. Securing our connected vehicles  
   6.1 Learning from other industries  
   6.2 Automotive cybersecurity best practices: the four ‘S’s
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