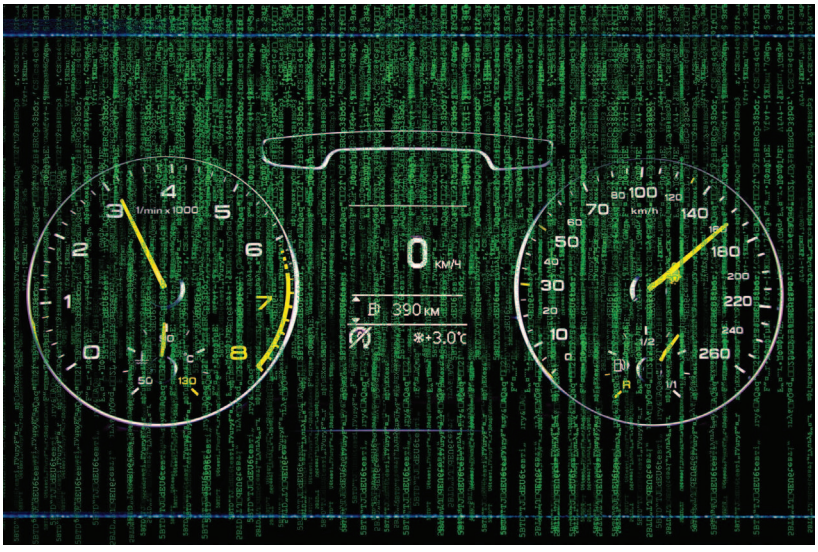
Yoshiyasu
Takefuji

Connected Vehicle Security Vulnerabilities

In the history of mandatory regulation of computerized vehicles, an E-Letter entitled, "Black box is not safe at all," was published in *Science* [1] in 2017. It mentioned that on-board diagnostics (OBD-II) specifications were made mandatory for all cars sold in the United States in 1996. The European Union made European OBD (EOBD) mandatory for all gasoline (petrol) vehicles sold in the European Union starting in 2001.

The problem is that the OBD-II and EOBD specifications contain "black boxes" that cannot be fully tested by car manufacturers. There is also no security provided in the OBD-II and EOBD specifications. In other words, for more than fifteen years, we have been neglecting security problems of the naked (unsecured) cars [1].

Before considering autonomous vehicles [2], we must understand such unsecure mandatory specifications. Why have we been forced to live with black-box testing without understanding the details of the black box? We all know that black-box testing is not suitable for identifying defects in hardware or software in the black box. However, open source is not automatically more secure than closed source [3]. The difference is with open source code you can verify for yourself (or pay someone to verify for you) whether the code is secure [3]. With closed source programs it needs to be taken on faith that a piece of code works properly. Open source allows the code to be tested and to be verified to work properly [3]. Open source also allows anyone to fix broken code, while closed source can only be fixed by the vendor [3]. The open source hardware/software movement has been navigating in a good direction to remove all black boxes and to enhance security and incremental innovations [1].



ISTOCK/ET1972

However, cyber-security expert Gene Spafford has a slightly different view of the open/closed issues on security: "I agree that we should be concerned about having unknown components in our systems. We (historically) had some vendors who

Digital Object Identifier 10.1109/MTS.2018.2795093
Date of publication: 2 March 2018

did extensive and formal testing of their software for high-assurance applications. The current market doesn't support that kind of examination, and few vendors know how to do it, but that doesn't mean it can't be done. Vendors might test better if we had a legal or economic means of holding them liable for defects. Right now, if they do a poor job verifying security, they simply release a patch and do it again!"

Why have we been forced to live with black-box testing without understanding the details of the black box?

A second serious security problem is with vehicle electronics and engine control units (ECUs). ECUs include the electronic/engine control module (ECM), powertrain control module (PCM), transmission control module (TCM), brake control module (BCM or EBCM), central control module (CCM), central timing module (CTM), general electronic module (GEM), body control module (BCM), suspension control module (SCM), and others. Some modern vehicles have up to 80 ECUs where new features are added. More new features are then patched into the existing systems, making the systems more vulnerable to attack.

An in-vehicle/external network makes it more vulnerable. An in-vehicle infotainment (IVI) system often uses Bluetooth technology and/or smart phones to help drivers control the system with voice commands, touch screen input, or physical controls [4]. In addition to IVI systems, smart phone links, vehicle telematics, diagnostics, and autonomous vehicles make the system more vulnerable through external applications.

We must understand and define vehicle security buzzwords including "maps," "ECU-remapping," and "re-flashing." Engine ECUs contain "maps" which are basically multi-dimensional lookup tables of minimum, maximum, and average values for various engine sensors [5]. The software on an engine ECU interprets the information from those tables and sends an appropriate signal to the relevant engine sensors so that the appropriate performance is delivered during the drive [5]. The practice of downloading a different map into the vehicle's ECU is often called "re-flashing" [5]. A process to refine the vehicle's engine map is called "ECU-remapping." According to Dave Blundell's "ECU hacking" [6], ECU attacks are classified into front door attacks, back door attacks, and exploits, respectively:

Front door attacks: Commandeering the access mechanism of the original equipment manufacturer (OEM).

Back door attacks: Applying more traditional hardware hacking approaches.

Exploits: Discovering unintentional access mechanisms.

Hackers or crackers can use inexpensive commercial tools for ECU attacks.

In this article, potential hackings are classified into "vehicle sensors attacking" and "vehicle access attacking." We must protect our autonomous vehicles against potential hackings, detailed in the following sections.

We are not prepared for potential vehicle sensor attacks. Vehicle sensor attacks can include global positioning system (GPS) jamming/spoofing attacks, millimeter wave radar jamming/spoofing attacks, light detection and ranging (LiDAR) sensor relay/spoofing attacks, ultrasonic sensor jamming/spoofing attacks, and camera sensor blinding attacks.

Vehicle access attacking affects not only autonomous vehicles but also conventional vehicles. Vehicle access attacking includes key fob clone and telematics service attacking.

Vehicle Sensor Attacking

Autonomous vehicles use the following sensors: GPS, millimeter wave (MMW) radar, LiDAR sensor, ultrasonic sensor, and camera sensor. We must protect current and future autonomous vehicles against these types of sensor attacks. Vulnerabilities and attack methods are briefly described below. Potential countermeasures are also noted where possible.

GPS Jamming and Spoofing

GPS spoofing became very popular after Pokémon GO hacks. GPS signal spoofing must be mentioned first. Protecting GPS from spoofers is critical to autonomous vehicle navigation. Conventional GPS systems are vulnerable to spoofing attacks. Using inexpensive software defined radio (SDR), GPS signal spoofing can be easily achieved [7], [8]. Advanced spoofing technology might pose defense challenges even to very sophisticated victim receivers. There is a need for more research and development in the area of spoofing defenses, especially concerning the question of how to recover accurate navigation after the detection of an attack. More importantly, however, there is a need for receiver manufacturers to start implementing and embedding spoofing defenses [9]. In other words, the current GPS is vulnerable to GPS signal spoofing.

Psiaki's team has found that combining strategies can provide a

reasonably secure countermeasure that could be commercially deployed [9].

As far as we know, there is no commercial anti-spoofing GPS system available in the market.

MMW Radar Attacking

Millimeter wave (MMW) radar uses the following frequency bands: 24.0–24.25 GHz, 76–77 GHz, 77–81 GHz, and a UWB band of 21.65–26.65 GHz. The 76.5 GHz band is exclusively for automotive radar worldwide. There are jamming and spoofing attacks against MMW radars. MMW radar jamming and spoofing attacks were demonstrated in Defcon24 in 2016 [10]. Using off-the-shelf hardware, they were able to perform jamming and spoofing attacks, which caused blinding and malfunction of the Tesla, which could potentially lead to crashes and impair the safety of self-driving cars [10].

As far as we know, there is no commercial anti-jamming / spoofing MMW radar available in the market.

LiDAR Sensor Attacking

Petit *et al.* have demonstrated effectiveness of relay attacks and spoofing attack on LiDAR (ibeo LUX 3), respectively [11]. A cheap transceiver was able to inject fake objects that are successfully detected and tracked by the ibeo LUX 3. These attacks prove that additional techniques are needed to make the sensor more robust to ensure appropriate sensor data quality [11]

However, combining multiple wavelength LiDAR makes it harder for the attacker to attack both signals at the same time [11].

Ultrasonic Sensor Attacking

Liu *et al.* have tested Tesla, Audi, Volkswagen, and Ford using ultrasonic sensor attacks: jamming and spoofing attacks. They showed that all tested vehicles were able to be jammed and spoofed [10].

As far as we know, there is no commercial anti-jamming/spoofing ultrasonic sensor available in the market.

Camera Sensor Attacking

Petit *et al.* have tested a camera sensor (MobilEye C2-270) by blinding the camera with laser and LED matrix. The attacks confused the auto controls [11]. For the MobilEye C2-270, a simple laser pointer was sufficient to blind the camera and prevent detection of vehicle ahead [11].

As far as we know, there is no commercial anti-blinding camera sensor available in the market.

Vehicle Access Attacking

Key Fob Clone

In order to gain access to a vehicle, a key fob clone technique can be used. Two distinct vulnerabilities were reported in the existing keyless entry system that could affect 100 million vehicles [12]. Affected vehicle keyless entry systems included VW group remote control, Alfa Romeo, Chevrolet, Peugeot, Lancia, Opel, Renault, Ford, and others [12]. By eavesdropping a single signal sent by the original remote, an adversary is able to clone a remote control and gain unauthorized access to a vehicle [12]. A correlation-based attack on Hitag2 allows us to clone the remote control within a few minutes using a laptop computer [12]. The wireless carrier frequency is currently 315 MHz in the U.S./Japan and 433.92 MHz (ISM band) in Europe. In Japan the modulation is frequency-shift keying (FSK), but in most other parts of the world, amplitude-shift keying (ASK) is used. Since the publication of a key fob clone paper [12], there has been no solution provided by manufacturers. We should immediately prepare for this key fob clone problem.

Telematics Service Attacking

Burakova *et al.* have found that the SAE J1939 Standard with Bluetooth, cellular, and WiFi through telematics service used for trucks can allow easy access for safety-critical attacks [13]. In other words, an adversary with network access can control safety critical systems of heavy vehicles using the SAE J1939 protocol.

The open source hardware/software movement has been navigating in a good direction to remove all black boxes and to enhance security and incremental innovations.

Tesla has talked publicly about implementing a co-designing feature where only a trusted code signed with a certain cryptographic key works [14]. Cars' internal networks will need better internal segmentation and authentication, so that critical components don't blindly follow commands from the OBD2 port [14]. They need intrusion detection systems that can alert the driver — or rider — when something anomalous happens on the cars' internal networks [14].

All of these security problems arise because vehicle designers are not expert enough in network security. They have not paid attention to the security problem. We must embed security protection to guard against a variety of attacks.

Exploitation Case Studies

Wireless Carjacking

Wireless penetration using cellular connection, Bluetooth bugs, a rogue Android App, and a malicious audio file on a CD were reported in 2010 [15]. White hat hackers revealed nasty new car attacks [16]. White hat hackers killed a jeep on the highway in 2015 [17]–[19]. Because of simple authentication of ECUs, hackers can control ECUs. For example, the steering wheel of the 2010 Ford Escape's parking assist module can be controlled by CAN command 0x0081 [17]–[19]. The power steering of the 2010 Toyota Prius with lane keep assist (LKA) can be controlled by controller area network (CAN) command 0x02E4 [17]–[19]. By plugging an Internet-connected gadget into a car's OBD2 port, researchers could take control of a Corvette's brakes in 2015 [20]. Because of vulnerabilities, Fiat Chrysler recalling 1.4 million vehicles amid concerns over remote hack attacks [21]. High-tech thieves could steal Hyundai cars via its mobile APP in 2017 [22]. Cyber security expert Kevin Mahaffey said: "Automakers that transform themselves into software companies will win. Others will get left behind" [23].

Known and Unknown Vulnerabilities

There are currently security problems of connected vehicles that we must solve immediately. Jamming/spoofing problems on vehicle sensor attacking should be resolved. An immediate solution is needed for vehicle access attacking, including key fob cloning and telematics service attacks.

There are many known/unknown vulnerabilities in the current connected vehicles. The connected vehicles must be also protected against wireless carjacking. Otherwise, the connected vehicles, and self-driving cars, will become the next crime frontier.

Author Information

Yoshiyasu Takefuji is with the Faculty of Environment and Information Studies, Keio University, 5322 Endo, Fujisawa 2520882 Japan. Email: takefuji@sfc.keio.ac.jp.

References

[1] Y. Takefuji, "Black box is not safe at all," *E-Letters of Science*,2017; http://science.sciencemag.org/content/352/6293/1573/tab-e-letters.

[2] 1. Jean-François Bonnefon *et al.*, "The social dilemma of autonomous vehicles," *Science*, vol. 352, no. 6293, pp. 1573-1576, Jun. 24, 2016.

[3] J. Lynch, "Why is open source software more secure?," *Infoworld*, Sept. 22, 2015; http://www.infoworld.com/article/2985242/linux/why-is-open-source-software-more-secure.html.

[4] V. Beal, "In-Vehicle Infotainment (IVI)," *Webopedia*, 2018; http://www.webopedia.com/TERM/I/in-vehicle-infotainment-ivi.html.

[5] C. Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester*. No Starch Press, 2016.

[6] D. Blundell, "ECU hacking," *The Car Hacker's Handbook: A Guide for the Penetration Tester*, 2016, ch. 6; http://publicism.info/engineering/penetration/7.html.

[7] Software-Defined GPS Signal Simulator, Github; https://github.com/osqzss/gps-sdr-sim, accessed Dec. 15, 2017.

[8] S. Kiese, "Gotta Catch 'Em All! – WORLDWIDE! (or how to spoof GPS to cheat at Pokémon GO), *Insinuator*, 2016; https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/.

[9] M.L. Psiaki and T.E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol.104, no. 6, pp.1258-1270, Jun. 2016.

[10] C. Yan *et al.*, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles," presented at DEFCON24, 2016; https://assets.documentcloud.org/documents/3004659/DEF-CON-whitepaper-on-Tesla-sensor-jamming-and.pdf, https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles.pdf.

[11] J. Petit *et al.*, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. of Blackhat-EU15*, 2015; https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf.

[12] F.D. Garcia *et al.*, "Lock it and still lose it —On the (in)security of automotive remote keyless entry systems," in *Proc. USENIX*, 2016; https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf.

[13] Y. Burakova *et al.*, "Truck hacking: An experimental analysis of the SAE J1939 Standard," in *Proc. USENIX*, 2016; https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf.

[14] A. Greenberg, "Securing driverless cars from hackers is hard. Ask the ex-uber guy who protects them," *Wired*, 2017; https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.

[15] J. Markoff, "Researchers show how a car's electronics can be taken over remotely," *New York Times*, Mar. 10, 2011; http://www.nytimes.com/2011/03/10/business/10hack.html?_r=0.

[16] A. Greenberg, "Hackers reveal nasty new car attacks – With me behind the wheel" (Video), *Forbes*, Jul. 24, 2013; https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#6677f02228c7.

[17] A. Greenberg, "Hackers remotely kill a Jeep on the highway—With me in it," *Wired*, Jul. 2015; https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[18] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Aug. 10, 2015; http://illmatics.com/Remote%20Car%20Hacking.pdf.

[19] C. Valasek and C. Miller, "Adventures in automotive networks and control units," *IOActive*, 2014; https://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf.

[20] A. Greenberg, "Hackers cut a Corvette's brakes via a common car gadget," *Wired*, Aug. 2015; https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/.

[21] M.B. Quir, "Fiat Chrysler recalling 1.4M vehicles amid concerns over remote hack attacks," *Consumerist*, Jul. 24, 2015; https://consumerist.com/2015/07/24/fiat-chrysler-recalling-1-4m-vehicles-amid-concern-over-remote-hack-attacks/.

[22] Reuters, "High-tech thieves could steal Hyundai cars via its mobile app: Researchers," *Hindustan Times*, May 17, 2017; http://www.hindustantimes.com/autos/high-tech-thieves-could-steal-hyundai-cars-via-its-mobile-app-researchers/story-zQ6R1Vouy5bAH1I72shu6I.html.

[23] N. Perlroth, "Why car companies are hiring computer security experts," *New York Times*, May 7, 2017; https://www.nytimes.com/2017/06/07/technology/why-car-companies-are-hiring-computer-security-experts.html?mcubz=1&_r=0.