International standards are needed for securing autonomous vehicles

- Yoshiyasu Takefuji, Professor, Keio University

(14 September 2018)

Andrew Robinson wrote an article entitled "Looking ahead" (1). Autonomous vehicles (AVs) will play a crucial role in our society in the self-driving age. However, current AVs have unsolved security vulnerabilities so that we must overcome the vulnerabilities and resolve all the problems. I have collected the known security vulnerabilities for AVs or connected vehicles (CVs) (2). There are two kinds of potential vehicle attacks: forged vehicle communications (in-vehicle network, inter-vehicle network or telematics, and vehicle access attacks), and sensor attacks. We must devise and develop several new technologies for nullifying those potential vehicle attacks where the fact of AVs security problems must be disclosed by scientists and engineers. In order to use autonomous vehicles in our society, international standards for securing sensors are highly demanded and needed.

Forged vehicle communications:
In-vehicle network attacks
In OBD2 (On Board Diagnostics level 2) standard, no security is embedded or provided. Therefore, in the in-vehicle network communications, security functions including encryption / decryption between ECUs (electronic control units) must be embedded in OBD2 or the OBD2 standard must be replaced with the better standards for AVs or CVs.

Inter-vehicle network attacks
In the inter-vehicle network or telematics, since 4G/LTE/3G hijacking has been reported (3,4), the new communications networks including 5G or other robust networks must be created and used.

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 (7). Affected vehicle keyless entry systems included VW group remote control, Alfa Romeo, Chevrolet, Peugeot, Lancia, Opel, Renault, Ford, and others (7). Currently we have no protection against key fob clone.

Jamming/Spoofing/Quieting attacks against sensors

Vehicle sensor attacks can include global positioning system (GPS), millimeter wave radar, light detection and ranging (LiDAR), ultrasonic sensor, and camera sensor. There are three kinds of attacks against vehicle sensors: jamming, spoofing, and quieting. Jamming is to generate noises causing denial of service for disturbing the original signals. Spoofing is to craft fake signals in order to alter the original signals. Quieting is to diminish the echoes in order to hide obstacles. Therefore, attacks against sensors include the total of 15 attacks: 15 = 3 (jamming, spoofing, quieting) x 5 (GPS, millimeter wave radar, LiDAR, ultrasonic sensor, camera).

Since the widespread popularity of Pokémon Go on smart phones, cheap GPS spoofers have been available in the market. A GPS spoofer sends a fake signal to GPS receivers within a certain distance. The spoofed GPS receivers always indicate the wrong location because of the GPS faked signals. As far as we know, there is no commercial anti-spoofing GPS system available in the market.

Camera is very weak against blinding (jamming) attacks. The goal of blinding attacks is to blind the camera fully or partially, by emitting light into the camera in order to hide objects (5). For the MobilEye C2-270, a simple laser pointer was sufficient to blind the camera and prevent detection of vehicle ahead (5). As far as we know, there is no commercial anti-blinding camera sensor available in the market.

A LiDAR can only see things that are reflected by the signal. If the signal does not return (due to absorption, transparent objects or range limits), it will assume there is ‘nothing’ (5). Jamming / spoofing / relay attacks against a LiDAR device have not been nullified yet. As far as we know, there is no commercial anti-jamming/spoofing LiDAR available in the market.

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

In order to use autonomous vehicles in our society, international standards for securing sensors are highly demanded and needed. There are many known/unknown vulnerabilities in the current AVs or CVs. The connected vehicles must be also protected against wireless carjacking. Otherwise, the connected vehicles, and self-driving cars, will become the next crime frontier.

References:

1. Andrew Robinson, Looking ahead, Science 14 Sep 2018: Vol. 361, Issue 6407, pp. 1079

2. Y. Takefuji, "Connected Vehicle Security Vulnerabilities [Commentary]," in IEEE Technology and Society Magazine, vol. 37, no. 1, pp. 15-18, March 2018
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8307141

3. Yuwei ZHENG et al., "Ghost Telephonist Link Hijack Exploitations in 4G LTE CS Fallback," Black hat USA 2018
https://www.blackhat.com/docs/us-17/thursday/us-17-Yuwei-Ghost-Telephoni...

4. Syed Rafiul Hussain et al., "LTEInspector：A Systematic Approach for Adversarial Testing of 4G LTE," Proc. of Network and Distributed Systems Security (NDSS) Symposium 2018 18-21 February 2018, San Diego, CA, USA
http://dx.doi.org/10.14722/ndss.2018.23113

5. Petit. J et al., "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," Black Hat Europe, 11/2015
https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f6187...

6. C.Yan et al., "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles," presented at DEFCON24, 2016

7. 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