Before the
National Highway Traffic Safety Administration
Washington, DC

In the Matter of:

Federal Automated Vehicles Policy and Cybersecurity Best Practices for Modern Vehicles	)	NHTSA-2016-0090-001
	)	NHTSA-2016-0104-001

Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems

by

Samuelson-Glushko Technology Law & Policy Clinic (TLPC)

Zachary Goldberg
Student Attorney

Blake E. Reid
Director

tlpc@colorado.edu
303.492.0548

via upload to regulations.gov
November 21, 2016

Table of Contents

Discussion

Autonomous vehicle technology is vulnerable to physical-layer jamming and spoofing attacks. However, the guidance reports regarding autonomous vehicle safety and modern vehicle cybersecurity in the above-referenced dockets do not substantially address these threats.[1] We urge the Administration, and agencies such as the Federal Communications Commission (FCC) and Department of Defense (DOD) as appropriate, to emphasize the importance of researching and counteracting physical-layer jamming and spoofing attacks to which autonomous vehicles are uniquely susceptible.

We fully acknowledge that attacks directed toward autonomous vehicles' network and application layers present a serious—and perhaps more serious—threat. However, jamming and spoofing attacks pose undeniable risks that must be addressed. For example, an attacker could blind an autonomous vehicle by jamming its cameras and sensors with a laser. An attacker could also spoof an autonomous vehicle into traveling off-course in order to steal the vehicle or its cargo.

Although the technologies, vulnerabilities, and defenses described below are not exhaustive, and in-depth technical explanation exceeds this comment's scope, the sections that follow outline basic autonomous vehicle systems, ways criminals can attack these systems using jamming and spoofing, and possible defenses against these attacks, as a blueprint for the Administration and other agencies to address these issues in further actions in the dockets.

I. Autonomous Vehicle Technology

Autonomous vehicles must "see" their surrounding environment and exchange information with one another in order to maneuver safely and reach desired destinations using a variety of

[1] *See Federal Automated Vehicles Policy*, Guidance Report, Docket No. NHTSA-2016-0090-001 p. 20-22 (Sep. 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf (referencing vehicle cybersecurity only generally, and neither jamming nor spoofing threats specifically); *Cybersecurity Best Practices for Modern Vehicles*, Docket No. NHTSA-2016-0104-001 §§ 6, 6.7.8 & fns. 31, 32 (Oct. 24, 2016), http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf (no mention of jamming; mention of spoofing only in connection with vehicles' network layers, not physical layer spoofing attacks).

systems: wireless spectrum-based communication systems, Lidar, radar, ultrasonic and odometry sensors, Global Positioning Systems (GPS) and Global Navigation Satellite Systems (GNSS).

A. Wireless Communication

Vehicle-to-Vehicle communication enables autonomous vehicles to send and receive information regarding one another's location, direction, travel rate, and to alert one another as to potential dangerous road conditions and other hazards.[2] Some autonomous vehicles use IEEE 802.11p interfaces to communicate with one another, and receive information from roadside transmitters, using the Dedicated Short Range Communication band ranging from 5.850 to 5.925 GHz.[3] The specific mechanisms by which autonomous vehicles exchange such information include peer-to-peer and multi-hop communications, which enable cooperative traffic monitoring, route optimization, crash prevention, weather monitoring, and alerts.[4]

B. Lidar, Radar, Ultrasonic and Odometry Sensors, and Video Cameras

Several types of monitoring devices and sensors enable autonomous vehicles to detect and respond to their surroundings.[5] A system of mapping lasers, light detection and ranging (Lidar), radar sensors, and video cameras detect other vehicles, the road, pedestrians, and other objects.[6]

---

[2] Julie Goodrich, *Driving Miss Daisy: An Autonomous Chauffeur System*, 51 Houston L. Rev. 1 265, 274, (Sep. 22, 2013, 1:28 pm), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2330549 (last visited Nov. 19, 2016) (Describing autonomous vehicle wireless communication mechanisms and capabilities).

[3] Muhammed Tilal & Rashid Minhas, *Effects of Jamming on IEEE 802.11p Systems,* at 2, (Master of Science Thesis in Comm. And Engineering) (Chalmers University of Technology, Department of Signals and Systems, Göteborg, Sweden, Report # Ex 086/2010) (Nov. 2010), http://publications.lib.chalmers.se/records/fulltext/133747.pdf (last visited Nov. 19, 2016).

[4] Bassem Mokhtar & Mohammed Azab, *Survey on Security Issues in Vehicular Ad Hoc Networks*, 54 Alexandria Engineering J. 4, at 1116 (Dec. 2015) http://www.sciencedirect.com/science/article/pii/S1110016815001246 (last visited Nov. 19, 2016).

[5] Alex Davies, *Turns Out the Hardware in Self-Driving Cars is Pretty Cheap*, Wired.com (Apr. 22, 2015, 9:00 am) https://www.wired.com/2015/04/cost-of-sensors-autonomous-cars/ (last visited Nov. 18, 2016).

[6] *Id.*

Ultrasonic sensors measure the position of very nearby objects, and odometry sensors (in conjunction with GPS) precisely track travel rate and distance.[7]

C. GPS and GNSS Navigation

Fully-autonomous vehicles rely upon GPS and GNSS for navigation to desired locations.[8] Satellites send the vehicles information, which their on-board receiver equipment then uses to calculate their position.[9] Signal accuracy and the manner in which fully-autonomous vehicles receive and respond to signals are critical to proper functionality and public safety.[10]

II. Physical-Layer Cybersecurity Threats to Autonomous Vehicles

The systems outlined above operate on the physical layer of autonomous vehicle technology, meaning that attacking these systems does not require hacking into a vehicle's internal computer networks or those with which the vehicle interfaces. Criminals could use physical-layer cyberattacks to steal autonomous vehicles and their freight, cause crashes, or imperil passengers and pedestrians.

While an attacker can remotely seize control of the brakes, acceleration, and steering in partially-autonomous vehicles, seizures are less detectible in the fully-autonomous vehicle context.[11] Because fully-autonomous vehicle communication networks ("vehicular ad hoc networks") lack fixed infrastructure and move around at varying speeds, those networks also lack reliable paths of end-to-end communication conducive to efficient data transfer.[12] This makes them inherently vulnerable to interference (unintentional jamming) and deliberate jamming and spoofing attacks.[13]

---

[7] *Id.*
[8] *Id.*
[9] GPS.gov, User Segment, http://www.gps.gov/systems/gps/ (last visited Nov. 18, 2016).
[10] Davies, *supra* note 4.
[11] Alex Hern, *Self-Driving Cars Irresistible to Hackers, Warns Security Executive*, TheGuardian.com (Jan. 28, 2014), https://www.theguardian.com/technology/2014/jan/28/self-driving-cars-irresistible-hackers-security-executive (last visited Nov. 18, 2016).
[12] *Id.*
[13] Tilal & Minhas, *supra* note 2, at 12.

A. Jamming

Jamming involves bombarding receivers with noise—signals or messages that cause interference.[14] Transmitting a signal of sufficiently high power on the same frequency as another signal can cause interference, and is neither complicated nor expensive to execute.[15] This technique can prevent autonomous vehicle communication systems from receiving intended messages clearly, and in some cases, even entirely.[16]

Autonomous vehicles' susceptibility to jamming attacks results largely from their reliance on the inherently open wireless medium for communication.[17] Jamming can interfere with or block an autonomous vehicle's ability to receive GPS or GNSS signals.[18] Attackers can use jamming attacks to disrupt autonomous vehicles' short range and long-range wireless communication.[19] Attackers can also blind autonomous vehicle radar systems by jamming the RF signals that their radar emitters send and receive using signal generators.[20]

Autonomous vehicles are also vulnerable to less-sophisticated signal-jamming attacks. Attackers can disable autonomous vehicles' onboard cameras using off-the-shelf lasers.[21] Alternatively, attackers can execute blocking attacks by diverting fully-autonomous vehicles into parking garages or

---

[14] Garu Wollenhaupt, *How Cell Phone Jammers Work*, HowStuffWorks.com, http://electronics.howstuffworks.com/cell-phone-jammer2.htm (last visited Nov. 19, 2016).
[15] *Id.*
[16] Mokhtar & Azab, *supra* note 3, at 1115.
[17] Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuur, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer & Jeffrey H. Reed, *A Communications Jamming Taxonomy*, IEEE Security and Privacy (Jan/Feb 2016), at 47.
[18] Jean-Pierre Hubaux, Srdjan Capkun & Jun Luo, *Making Wireless Work: The Security and Privacy of Smart Vehicles*, IEEE Security and Privacy (May/Jun 2004), at 52, https://infoscience.epfl.ch/record/49853/files/HubauxCL04.pdf (last visited Nov. 19, 2016).
[19] Chris Lu, *Security of Autonomous Vehicles* (Dec. 15, 2014) at 5-6, http://www.cse.wustl.edu/~jain/cse571-14/ftp/vehicle_security.pdf (last visited Nov. 19, 2016).
[20] John Torchinsky, *Hackers Show that Tesla Autonomous Sensors Can Be Fooled, But It's All a Bit Stupid* (Aug. 4, 2016, 1:50 pm), Jalopnik.com, http://jalopnik.com/hackers-show-that-tesla-autonomous-sensors-can-be-foole-1784825823 (last visited Nov. 19, 2016).
[21] Paul Szoldra, *Hackers Show How They Tricked a Tesla into Hitting Objects in its Path*, BusinessInsider.com (Aug. 8, 2016, 3:23 pm), http://www.businessinsider.com/defcon-tesla-jamming-spoofing-autopilot-2016-8 (last visited Nov. 19, 2016).

other structures with thick concrete walls containing embedded metal fragments or steel framing that block wireless signals from propagating.[22] These blocking attacks cut off the vehicles' cellular communication ability by preventing them from emitting or receiving wireless signals from outside the structure.[23]

B. Spoofing

Spoofing attacks involve tricking sensors, cameras, and receivers with false information. Spoofing attacks on autonomous vehicle communication systems involve sending false messages, warnings, or signals to alter the recipient vehicles' courses or behavior, and attackers can spoof autonomous vehicles with relative ease and at low expense.[24] Attackers can spoof autonomous vehicle cameras and Lidar and systems using a low-power lasers and pulse generators to trick them into slowing down, changing course, or remaining stationary to avoid hitting nonexistent objects.[25] Attackers can also spoof autonomous vehicles using Arduinos, open source electronics platforms that can receive inputs from sensors and control lights, motors and other actuators.[26] Attackers can fool ultrasonic driving and parking sensors into "seeing" nonexistent objects using Arduinos connected to ultrasonic transducers.[27] Attackers can also blind ultrasonic sensors using sound-deadening foam.[28]

Inputting counterfeit measurements and manipulating satellite health status bits can fool GPS and GNSS receivers into believing imposter signals or rejecting legitimate ones.[29] While military GPS

---

[22] Wollenhaupt, *supra* note 13.
[23] *Id.*
[24] Mokhtar & Azab, *supra* note 3, at 1117, 1122-24; Hubaux, *supra* note 16, at 52.
[25] Mark Harris, *Researcher Hacks Self-driving Car Sensors*, IEEE Spectrum (Sep. 4, 2005, 19:00 GMT), http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors (last visited Nov. 11, 2016).
[26] Arduino.cc, What Is Arduino, https://www.arduino.cc/ (Last visited Nov. 17, 2016).
[27] Torchinsky, *supra* note 18.
[28] *Id.*
[29] Ali Jafarnia-Jaharomi, Ali Broumandan, John Nielsen & Gerald Lachapelle, *GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques*, Int'l Journal of Navigation and Observation

and GNSS signals are encrypted to defend against unauthorized use and counterfeiting, the civilian GPS and GNSS signals that guide autonomous vehicles "were designed as an open standard, freely accessible to all."[30] Advances in software-defined radio tool technology enable increasingly less-sophisticated criminals to create effective GPS and GNSS spoofing apparatuses, and even the most effective of known spoofing defenses are not infallible.[31]

III. Protecting Autonomous Vehicles from Jamming and Spoofing Attacks

Manufacturers have equipped many of the vehicles currently on the market with autonomous braking, lane recognition, and parking assist features.[32] Google, car manufacturers, and automotive industry analysts believe that fully-autonomous vehicle technology will be ready for mass distribution as soon as 2020.[33]

However, considerable research and development efforts may be necessary to effectively defend against jamming and spoofing threats. Protecting autonomous vehicle technology and rendering fully-autonomous vehicles safe for large-scale deployment will require more effective safeguards. Active counter-interference measures, tailored data authentication, encryption, and sender-vehicle identification requirements may be necessary to counteract jamming and spoofing attempts perpetrated to steer the vehicles off-course or weaken their communications and interactions with one another.[34]

(Feb 24, 2012) at 1-3, https://www.hindawi.com/journals/ijno/2012/127072/ (last visited Nov. 19, 2016).

[30] Todd Humphries, *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing* (July 18, 2012), at 2-3, 10, http://rnl.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf (last visited Nov. 19, 2016).

[31] *Id.*

[32] Ratan Hudda, Clint Kelly, Garrett Long, Jun Luo, Atul Pandit, Dave Philips, Lubab Sheet & Ikhlaq Sidhu, *Self Driving Cars* (Univ. of CA, Berkeley College of Engineering, Fung Institute for Engineering Leadership) (May 29, 2013), Abstract, http://slidepapers.in/wp-content/uploads/2016/03/Selfm-Driving-Cars.pdf.

[33] *Id.*

[34] Mokhtar & Azab, *supra* note 3, at 1117, 1120, 1125.

Some have called for a mechanism for disabling autonomous software in the event of a spoofing attack to be a requisite feature on all autonomous vehicles.[35] Such a feature would enable a passenger to bypass autonomous functionality in the event of an attack by using the steering wheel or pedals to course correct or safely pull over and park the vehicle rather than continuing on the attacker's desired route.[36]

However, defending against spoofing attacks directed toward autonomous vehicle GPS or GNSS systems may require ensuring that the signals they use have cryptographic authentication signatures.[37] Improvements to Receiver Autonomous Integrity Monitoring, and complementary and backup systems, may be required to adequately defend against jamming and spoofing attacks targeting satellite-based autonomous vehicle communication systems.[38] Additionally, remaining cognizant of vulnerabilities that anti-jamming or anti-spoofing mechanisms themselves possess that make them susceptible to attack will be critical to their efficacy.

* * *

Public safety, consumer privacy, and theft prevention depend upon proper consideration of the cybersecurity and safety threats that autonomous vehicle jamming and spoofing attacks pose. We urge the Administration to acknowledge in greater detail in its future guidance revisions the threat that autonomous vehicle jamming and spoofing attacks pose. We urge those who are involved in developing and deploying autonomous vehicle technology to take steps toward counteracting potential jamming and spoofing threats sooner rather than later, and the Administration and other agencies to encourage such efforts. Keeping these considerations in mind in early design stages, and

---

[35] Goodrich, *supra* note 1, at 288-89.
[36] *Id.*
[37] Humphries, *supra* note 28, at 10.
[38] Anne Ju, *'Spoofed' GPS Signals Can Be Countered, Researchers Show*, Cornell Univ. Chronicle, (Jul. 23, 2012) http://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attacks (Last visited Nov. 19, 2016); Alan Cameron, *Munich Summit Will Emphasize GNSS Backup – GPS World*, Resilient Navigation and Timing Found. (Sep. 29, 2016) http://rntfnd.org/2016/09/29/munich-summit-will-emphasize-gnss-backup-gps-world/ (last visited Nov. 19, 2016).

well in advance of widespread fully-autonomous vehicle deployment, is critical both to public safety and the success of the autonomous vehicle industry.

Respectfully submitted,

/s/

Zachary Goldberg
Student Attorney

Blake E. Reid
Director

blake.reid@colorado.edu
303.492.0548

Samuelson-Glushko Technology Law & Policy Clinic