CHAPTER 11

THE THREAT FROM INSIDE . . . YOUR AUTOMOBILE

Isaac R. Porche III

INTRODUCTION

Automobiles have a cybersecurity risk. The vulnerabilities stem from the abundance of software, computers, and networks that have been designed into automobiles beginning several decades ago. Published experimental results and real-world incidents substantiate the existence of vulnerabilities in today's commercial automotive fleet. Like the vulnerabilities of the Internet, these automobile-based ones are likely to persist. Security standards, federal motor vehicle regulations, and a new patching regimen by car owners will be needed to help mitigate the risk. Until then, it is not hard to imagine a day when a portion of the American automobile fleet is taken over by nefarious actors.

This chapter is organized into three parts. The first part is about the risks that exist from the computers and networks that are onboard today's commercial automobiles. The second part describes the implications of the risks. The third part presents a contrived scenario, where the vulnerabilities described are exploited to produce a catastrophic event.

AUTOMOBILES HAVE (CYBER) RISK

The first part of this chapter discusses the risks.

Embedded Computers and Networks in Automobiles Make Them Vulnerable.

Vulnerabilities have existed in automobiles for some time because of all of the software, computers, and networks that have been embedded in automobiles over the last 30 years. The Cadillac brand has hosted onboard networks since the 1980s.[1] The data rates on these networks continue to grow.[2] Today, modern automobiles literally run on millions of lines of software code and 30 to 100 computers.[3]

A big push for onboard networks—that spanned the entire U.S. automotive sector—came in the mid-1990s and was driven by new emission regulations. It was the start of regulations in the United States requiring an onboard physical connector to allow access to vehicle electronics.[4] These are called onboard diagnostic (OBD) connectors. They enable a mechanic, an inspector, or even the car owner to connect to the vehicle's onboard computers. These connectors have existed on U.S. vehicles for many years.

More recently, connectivity has expanded from the wired medium to the wireless world. Today, wireless communication devices are common on vehicles. University researchers[5] have explored the viability of exploiting all of the communication systems that reside in vehicles. The researchers showed that exploitation is possible using:

> Onstar-like cellular connections, Bluetooth bugs, a rogue android application that synched with the car's network from the driver's smartphone, or even a malicious audio file in the cars stereo.[6]

This finding is significant because these links enable access to onboard computers, which can control the vehicle via drive-by-wire systems (DBW).

A DBW trend is evident, i.e., automobiles are increasingly controlled electronically and not mechanically. "Active Park Assist" will parallel park a car using sensors to measure distances to the curb.[7] Other DBW features available today include electric power steering, electric throttle, and braking for adaptive cruise control. Ford plans a "Traffic Jam Assist" feature, perhaps in 2017,[8] to steer, throttle, and brake the vehicle automatically via computer control. The Berkeley PATH project demonstrated automated driving over 20 years ago[9] using vehicle-to-vehicle communication and onboard radars. Today, Google is actively demonstrating its own driverless car.

In the future, there will be more and more automation of the functions previously performed by the driver. All of this means that computers and networks are performing the functions and issuing the driving commands to the vehicle. Published experimental results[10] substantiate the existence of vulnerabilities in today's commercial automobile fleet. Table 11-1 below summarizes their findings.

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium
	CD	Special song Windows media audio (WMA)	Yes	Medium	Yes	Medium-High
	PassThru	Wi-Fi or wired control connection to advertised PassThru devices	No	Small	Yes	Low
	PassThru	Wi-Fi or wired shell injection	No	Viral	Yes	Low

Table 11-1. Attack Surface Capabilities.[11]

Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium
	Bluetooth	Sniff media access control (MAC) address, brute force personal identification number (PIN), buffer overflow	No	Small	Yes	Low-Medium
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High

Source: Checkoway *et al*., 2011.
Note: According to their notes, "the Visible to User column indicates whether the compromise process is visible to the user (the driver or the technician); we discuss social engineering attacks for navigating user detection in the body. . . . The Scale column captures the approximate scale of the attack. . . . The Full Control column indicates whether this exploit yields full control over the components connected controller area network (CAN) bus (and, by transitively, all of the engine control units in the car). Finally, the Cost column captures the approximate effort to develop these attack capabilities."

Table 11-1. Attack Surface Capabilities.(cont.)[11]

History of Local Area Networks within Automobiles.

In-vehicle networks were introduced decades ago to enable diagnostic queries, emission checking, and the sharing of the sensors and other data between multiple in-vehicle computers.[12] A predominant networking protocol used for automobiles today is the CAN bus. It was developed by Bosch in the 1980s and became an International Organization for Standardization standard a decade later. Many new European and North American cars have a CAN bus.[13] CAN

was designed to handle up to 800 kilobits per second (kbps) of network traffic. For higher data rates, there are other networks onboard like media oriented systems transport (MOST).[14] CAN is known as a standard which makes it easy to access and exploit. Specifically, these networks are well-studied by car enthusiasts and computer hackers alike.[15] For example, there was a workshop on how to hack into CAN. It was held at DEFCON (defense readiness condition) 19, which is a well-known annual hacker conference. A website (*www.canbushack.com*) still exists.

Protocols and Standards for In-vehicle Networking Are Defined.

Government and industry standards have enabled a degree of interoperability between available devices and commercial in-vehicle networks. A sample of some are listed below:

- **SAE J1962 –** The OBD-II connector standard has been required on most vehicles since 1996. It allows a hand-held scanner to plug physically into a car's networks easily from the passenger compartment. The connector can be converted into a USB port to enable any ordinary laptop to be connected. Today, this connector is not relied upon as much for diagnostics but is being increasingly used to log data for insurance companies and others.
- **SAE J1850 –** This is a network protocol used with the OBD-II connector.
- **SAE J2534 –** The "PassThru" standard for reprogramming engine and other onboard computers is the newer prevailing standard for diagnostic and vehicle interrogation.

These standards promote universal connectivity and ease of use. However, this invites security compromise.

In-vehicle Networks Are Designed for Easy Physical Access.

The use of onboard connectors and the existence of onboard networks and networking protocols makes it easy to interrogate vehicle networks and reprogram vehicle computers. Mechanics use commercially available devices to read the networks for trouble codes, as do clerks at many auto parts stores.

Potential Consequences of Exploiting These Networks Has Been Demonstrated.

In 2010, a 20-year-old disgruntled employee remotely disabled over 100 vehicles.[16] He did so by illegally accessing a website that could send wireless signals to the security systems installed on these vehicles.

In an article published by the Institute of Electrical and Electronics Engineers (IEEE), University of Washington researchers[17] exposed numerous flaws in the prevailing standard for in-vehicle networks. The flaws enable a bypass of "rudimentary network security protections." The researchers were able to embed malicious code in safety-critical systems sufficient to facilitate disablement of the braking system.

In 2013, two Defense Advanced Research Projects Agency-funded researchers in Indiana demonstrated how to "exploit" a Ford Escape. They connected a MacBook laptop to the OBD connector to override the driver's commands and divert the vehicle into a vacant field.[18] The same researchers co-opted a Toyota

Prius and controlled its acceleration, steering, seatbelt tightness, horn, and brakes.

Parallels with Insecurity of Internet.

There are similarities when comparing the modern security problems of the Internet and the emerging security problems of networked vehicles. Two reasons are: (1) both have to support multiple access points (physical and virtual), and (2) have to support connection with unknown entities. These requirements result in the complexity of the system design. As the saying goes, "complexity is the bane of security." The second reason is that vehicle networks increasingly are a part of the Internet. They are interconnected through handheld devices and other wireless communication nodes embedded in the vehicle to support telematics, vehicle diagnostics, and other functions.[19] Vehicle networks and the Internet inherit each other's security posture.

In the field of information technology, there is an established history of adopting operating systems that are easier to work with but less secure. Arguably, the Internet itself grew from a design philosophy where the need for interoperability, usability, and connectivity trumped the need for a more secure design.

An important example from 50 years ago is Multiplexed Information and Computing Service (MULTICS), which was replaced by a family of multitasking, multiuser computer operating systems known as UNIX. Early on, UNIX was the operating system used by many of the Internet's servers. Developers chose the name UNIX because it is an "emasculated MULTICS." The original name was spelled UNICS, which stood for UNiplexed Information and Computing Service.[20]

Bruce Scheier summarized the advantages of MULTICS: "MULTICS was an operating system from the 1960s, and had better security than a lot of operating systems today."[21] According to a review by Paul Karger and Roger Shell, "MULTICS had a primary goal of security from the very beginning of its design."[22] Their review, completed 20 years ago, asserted that MULTICS security features from the 1960s were not designed into products current today (i.e., those developed around the millennium). MULTICS was replaced with UNIX due to usability. According to Ken Thompson, the esteemed co-developer of MULTICS and UNIX, "[MULTICS was] . . . overdesigned and overbuilt and over everything. It was close to unusable."[23]

For these reasons, it is fair to say that the Internet was not designed with the most robust security design. This flaw can be blamed on the usability of security in general.[24] The bottom-line is this: There is no reason to hope that vehicle networks will "grow up" to be any more secure than the Internet, which is not very secure.

Risk from the Computerized Transportation Infrastructure.

Increasingly, risks also come from the information technology (IT)-laden road infrastructure, which, in some cases, is coupled to vehicle technology. This includes:

- Computer controlled traffic lights that are either:
  - hard-wire networked to enable updates and changes,

  - dynamically changeable via wireless communication devices (for emergency responders and police),
  - and/or updated by plugging in a laptop.
  - This includes ramp meters at freeway entrances.
- Advanced traveler information systems (ATIS), which includes their websites. Note: A transit system's ATIS was recently hacked in 2011 by the group, Anonymous.[25]
- Other field devices like "toll tag readers, cameras, and roadside equipment [that] are quite susceptible to tampering."[26]

Edward Fok provides a more complete overview of the cybersecurity issues in modern transportation systems.[27]

IMPLICATIONS

The second part of this chapter speculates on the implications of the risk.

The Role of Cars in Society is Large.

What would be the impact on the economy if no commuter's car started in the morning? According to the census bureau, the average driver's commute to work is just under a half-hour. We can assume this means driving is a necessity for a large portion of automobile commuters. Although many large metropolitan areas have mass transit, it is not likely that many cities could handle the ridership increase if a significant fraction of automobile commuters switched modes.

The economic impact of the attacks that occurred on September 11, 2001, is estimated to be over $100 billion.[28] The reasonable question is to ask, "Will the same magnitude of loss occur after a temporary loss of automobile usage and highway access due to a massive cyberattack on the commercial fleet?" Arguably, an equal amount of economic paralysis seems possible if any transportation sector becomes of limited use, even for a few days.

The Automobile is a Cyber-Physical System.

The National Science Foundation uses the term "cyber-physical system," to describe "a system of collaborating computational elements controlling physical entities."[29] Supervisory control and data acquisition (SCADA) systems come to mind, and there is considerable research on the robustness and cybersecurity of SCADA systems.

Automobiles today are "mobile cyber-physical systems." As argued by Qaisar Shafi,[30] the robustness of such systems to threats posed is critical. This threat is critical because the increased electronic content that controls an automobile today can render it, literally, into a remotely controlled precision guided missile. It is a missile that is laden with liquid fuel.

A coordinated cyberattack on a large number of automobiles could crash the road network they traverse by congesting it with remotely triggered accidents or remotely triggered disablements. The psychological impact on highway commuters of even a small demonstration of this vulnerability could persuade most drivers to abandon automobile use at least temporarily.

SCENARIO

Given the risks described in this chapter and speculation on the implications of the risks, a scenario is developed for consideration.

Threat from Automobiles.

Consider a future scenario that involves:

- thousands of multi-ton projectiles,
- laden with liquid fuel and explosives,
- loitering in a holding pattern at high speeds,
- around sensitive targets in the national capital region (e.g., Metro, DC),
- waiting for electronic instructions to seek and destroy assets important to the U.S. Government.

Many people would think this is referring to a new smart weapon employed in a Hollywood movie. However, it could refer to rush hour traffic on the DC beltway, leveraging vehicles that could be exploited and controlled. In Steven King's 1973 short-story titled *Trucks*, the story-line is similar.

The Road to Calamity.

The year is 2019, 1-year before the calamity.

(Day-365): Foreign operatives, educated and living in the United States, join FakeCompanyScanX (FCS-SXN) as software developers. FCS-SXN is a maker of a device sold in auto parts stores. When that device (or tool) is plugged into a vehicle's onboard network, the device will report on the health of the automobile. It allows individual car owners to monitor and check

their own cars for repair issues. The FCS-SXN scanner is also used in many auto repair shops. In Virginia, it is used by nearly all the repair shops and dealerships for annual vehicle inspections.

The operatives, working as developers at the company, design the FCS-SXN scanner so that, upon connection to a vehicle, it will surreptitiously upload malicious code into each car's computer system, where it will remain dormant. The FCS-SXN device works in almost all commercial vehicles sold in the United States as a result of standards and protocols adopted over several decades.

Around the same time, a free, popular "smart-app" is circulating on the Internet. It is designed to work on any Android or iPhone. The smart-app was also created by FCS-SXN, and it allows the smartphone it resides on to "pair" with most vehicles that use Bluetooth. The smart-app provides an automatic status check to the owner's phone and other helpful features. Unknown to the owners of the phone, the smart-app can "talk" to the malicious code inside the infected vehicle. The smart-app also talks to a central server over the Internet (using the phone's wireless connection).

(Day-30): It is the year 2020. Over the last year, 10 percent of commuters in the Metro, DC, area have had their cars scanned by the FCS-SXN tool and have become infected. In addition, many of those car-owners have been solicited by FCS-SXN with advertisements offering them the free smart-app. Ten percent of them have downloaded it to their smartphone.

(Day-0 or D-Day): At 7:30 a.m., a central server under the control of foreign adversaries issues a command over the Internet to all cell phones running the smart-app. The smart-app commands any infected vehicle in the range of its blue-tooth signal to set the vehi-

cle's throttle to the maximum opening. This command affects 0.5 percent of the commuting vehicles in the DC area. These cars are instantly accelerated. By 8:00 a.m., there are over 5,000 accidents across the Metro, DC, area. Witnesses report that in nearly all cases, the drivers' cars suddenly accelerate out of control. This begins the attack. In the aftermath, disabled cars, collisions, or emergency responders snaking through the calamity block all major throughways.

(Day+1): The congestion is overwhelming, and the road network is unusable in many parts of the Metro, DC, area.

(Day+2): The nefarious actors send text messages to the affected smartphones to take credit for the auto cyberattack. This is reported by the media and commuters and confirms many suspicions.

(Day+3): Drivers in many metropolitan areas across the United States abandon their use of automobiles and flock to other forms of transportation that are perceived to be "safe" like rail or bicycle.

(D+180): Software patches to cars and smartphones are sufficiently distributed, and normalcy is returning to the DC area. However, the economic consequences are devastating.

CONCLUSIONS AND RECOMMENDATIONS

There is a growing awareness of the need for cybersecurity in automobiles[31] and transportation systems in general.[32] Officials in the government are certainly alarmed. In his testimony to the Senate in May of 2013, David Strickland, head of the National Highway Traffic Safety Administration (NHTSA) said, "These interconnected electronic systems are creating opportunities to improve vehicle safety and reliability, but

are also creating new and different safety and cybersecurity risks." According to the testimony, "hackers could potentially tap into these systems to steal cars, to eavesdrop on conversations or even to cause collisions."[33] Strickland is proposing a new division in NHTSA to address the concerns.

This newfound awareness of the need for automobile cybersecurity is news.[34] What is not new is the vulnerability, which has existed for some time and is likely to persist. This chapter highlights cybersecurity risks in modern automobiles and explores the implications. A scenario is presented that considers how the risks could be exploited. The purpose of presenting such a scenario is to make the point that the transformation of automobiles over the last few decades from mechanical drive to electronic drive, has also transformed them into millions of critical cyber-physical systems.

To prevent such a scenario from possibly occurring in the future, a number of things need to take place. First, revised motor vehicle safety standards are needed that address the cybersecurity of the modern automobile. Second, increased consumer awareness of the need for proper "auto-cyber-hygiene" is needed. In addition, higher consumer expectations are needed to allow market forces to pressure automakers to provide more guarantees. Third, there is a need for a commercial base of providers of anti-malware software that scans and secures vehicle computers and networks.

DISCUSSION: OTHER THREATS AND IMPLICATIONS

As noted by Isaac Porche, Jerry Sollinger, and Shawn McKay, similar threats apply to many other physical systems including smart homes and smarter cars:

> Neither 'wire' nor consent is required for one to be represented in cyberspace. Air gaps are difficult to maintain and thus no longer sufficiently protect devices from nefarious actors who operate in cyberspace . . . [a]s long as a device is not dumb (that is, as long as it contains a processor and some memory), it can be accessed, affected, and controlled to some degree by anyone who can overcome the air gap.[35]

The list of at-risk systems that fall into this category is long and includes medical devices, home automation systems, and other appliances being integrated into automobiles.

Smart thermostat products, like Nest (see *https://nest.com/thermostat/life-with-nest-thermostat/*), offer the user a monitoring system that tracks home activity. The system automatically adjusts the in-home temperature accordingly. Similar systems allow users to adjust home temperatures (or appliance settings or door locks) remotely from a smartphone. In a *Forbes Magazine* article,[36] Kashmir Hill describes her ability to turn on the bedroom lights of a complete stranger. These homes are only as secure as the underlying software and smartphones that facilitate access.

As noted in a 2013 article in *The Telegraph*, theoretically, "hackers need only to obtain the serial number of a pacemaker to force it to deliver an 830-Volt shock directly to a person's heart."[37]

ENDNOTES - CHAPTER 11

1. According to General Motors (GM):

> In Model Year 1981, all GM Passenger Cars for the U.S. market used a similar data link to a test connector for assembly line diagnostics. The value of this data in diagnosing emission systems after customer delivery was quickly identified and scanner tools were made to view and interpret the data stream. . . . In the 1985 model year, Cadillac FWD "C" vehicle had a electronic system that had point to point data links between five electronic modules and a dedicated assembly line diagnostic connector. . . . On the 1988 and 1989 model year Buick Reatta and 1986-89 model year Buick Riviera, touchscreen cathode ray tube (CRT) equipped vehicles, an 8,192 bit/sec data bus was implemented between the body computer module and the assembly line connector, climate control module, and CRT controller. This was GM's first multi-drop data bus.

Ronald Cox, "Development of First GM Vehicle Data Links," Detroit, MI: General Motors Corporation, available from *history.gmheritagecenter.com/wiki/index.php/Development_of_First_GM_Vehicle_Data_Links*.

2. In the early-1980s, the data rate on GM cars was 80 bits per second link. The data rate increased to over 8000 bits per second by the end of that decade. The controller area network (CAN) bus enables data rates to go up between 25 kilobytes per second (kbps) to one megabits per seconds on a single or dual-wire communication line (see canbuskit.com, undated).

3. According to Jim Motavalli, the first onboard computers in automobiles were in the mid-1970s: "The 1977 Oldsmobile Toronado had a very simple computer unit that was used for spark-plug timing, and the next year the Cadillac Seville offered an optional trip computer that used a Motorola chip." See Jim Motavalli, "The Dozens of Computers That Make Modern Cars Go (and Stop)," *The New York Times*, February 4, 2010. There is at least one European automaker with onboard computing or networking even earlier.

4. For the purpose of checking emissions through an onboard diagnostic (OBD) connector.

5. Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, "Experimental Security Analysis of a Modern Automobile," Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy, 2010, pp. 447-462; Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," San Diego, CA: Center for Automotive Embedded Security Systems, 2011, available from *autosec.org/pubs/cars-usenixsec2011.pdf*.

6. Andy Greenberg, "Hackers Reveal Nasty New Car Attacks--With Me Behind the Wheel," *Forbes*, August 12, 2013, available from *forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/*, accessed on October 2, 2014.

7. Stephen Edelstein, "Future Fords May Steer Owners Out of Traffic Jams," June 28, 2012, available from *digitaltrends.com/cars/future-fords-may-steer-owners-out-of-traffic-jams*, accessed on October 2, 2014.

8. *Ibid.*

9. Isaac Porche, Kwang Soo Chang, William Li, and Pravin Varaiya, "Real-Time Task Manager for Communications and Control in Multi-Car Platoons," Proceedings of the SAE and IEEE Intelligent Vehicles Conference, Detroit, MI, June 1992, pp. 409-414.

10. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," San Diego, CA: Center for Automotive Embedded Security Systems, available from *autosec.org/pubs/cars-usenixsec2011.pdf*, accessed on October 02, 2014; and Koscher *et al*., "Experimental Security Analysis of a Modern Automobile," pp. 447-462.

11. Checkoway *et al*.

12. Ronald W. Cox, "Local Area Network Technology Applied to Automotive Electronics Communications," *IEEE Transactions on Industrial Electronics*, Vol. IE-32, No. 4, November 1985, pp. 327-333.

13. "CAN History," *CAN in Automation*, available from *cancia.de/index.php?id=161*, accessed on October 2, 2014.

14. According to its supporting cooperative (e.g., Audi, Daimler, BMW, and others), MOST (media oriented systems transport) is "the de-facto standard for multimedia and infotainment networking in the automotive industry." MOST Cooperative, available from *mostcooperation .com/home/index.html*, accessed on October 2, 2014.

15. Robert Leale, "CanBusHack," undated, available from *canbushack.com*, accessed on October 2, 2014.

16. Kevin Poulson, "Hacker Disables More Than 100 Cars Remotely," Wired, March 17, 2010, available from *wired.com/threatlevel/2010/03/hacker-bricks-cars/*, accessed on October 2, 2014.

17. Koscher *et al*., "Experimental Security Analysis of a Modern Automobile," pp. 447-462.

18. Greenberg, p. 1.

19. Telematics is a widely used industry term relating to information technology functions being integrated into automobiles, e.g., navigation systems. See *telematicsresearch.com/PDFs/TRG_ITSWG-Telematics.pdf,* which associates the term with "solutions [i.e., capabilities] based on information flowing to and/or from a vehicle."

20. See discussion at *unix.org/what_is_unix/history_timeline.html*.

21. Bruce Schneier, "The Multics Operating System," September 19, 2007, available from *schneier.com/blog/archives/2007/09/the_multics_ope.html*, accessed on October 2, 2014.

22. Paul Karger and Roger Shell, "Thirty Years Later: Lessons from the Multics Security Evaluation," available from *acsac.org/2002/papers/classic-multics.pdf*, accessed on October 2, 2014.

23. This is according to an interview conducted by Peter Seibel, *Coders at Work: Reflections on the Craft of Programming*, New York: APress Publications, 2007.

24. J. D. Tygar, and Alma Whitten, "Why isn't the Internet Secure yet?" *ASLIB Proceedings*, Vol. 52, No. 3, March 2000, pp. 93-97.

25. Edward Fok, "An Introduction to Cybersecurity Issues in Modern Transportation Systems," *ITE Journal,* No. 7, July 2013, p. 18.

26. *Ibid.*

27. *Ibid*.

28. Shan Carter, and Amanda Cox, "One 9/11 Tally: $3.3 Trillion," *The New York Times*, September 8, 2011, available from *nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0*, accessed on October 2, 2014.

29. Edward A. Lee, "Cyber-Physical Systems—Are Computing Foundations Adequate?" 2006, available from *ptolemy.eecs.berkeley.edu/publications/papers/06/CPSPositionPaper/*, accessed on October 2, 2014.

30. Qaisar Shafi, "Cyber Physical Systems Security: A Brief Survey," 12th International Conference on Computational Science and its Applications, 2012, available from *ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6257627*, accessed on October 2, 2014.

31. Alberto Sangiovanni-Vincentelli, "Cybersecurity for the Automobile: Is the Car of the Future Still a Car?" presented at I&C Research Days, Lausanne, Switzerland, June 21, 2012, available from *ic.epfl.ch/files/content/sites/ic/files/pdfs/Presentations%20RD%202012/A.Sangiovanni.pdf*, accessed on October 20, 2014.

32. Fok, p. 18.

33. Brooks Hays, "Federal officials want to beef up cybersecurity for motor vehicle communication systems," Gimby.org, May 23, 2013, available from *gimby.org/blogs/gimby-news-focus/20130523/federal-officials-want-beef-cybersecurity-motor-vehicle*, accessed on May 23, 2012.

34. Jim Finkle, "Insight: Experts hope to shield cars from computer viruses," Reuters, August 20, 2012, available from *reuters.com/article/2012/08/20/us-autos-hackers-idUSBRE87J03X20120820*, accessed on October 2, 2014.

35. Isaac Porche, Jerry Sollinger and Shawn McKay, "*A Cyberworm that Knows no Boundaries*," Santa Monica, CA: RAND Corporation, 2011.

36. Kashmir Hill, "When 'Smart Homes' Get Hacked: I Haunted a Complete Stranger's House Via the Internet," *Forbes*, July, 2013, available from *forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/*, October 2, 2014.

37. "Pirates of Cyberspace," *The Telegraph*, March 10, 2013, available from *telegraphindia.com/1130310/jsp/7days/story_16654680.jsp#.U2E41PldX_E*, accessed on October 2, 2014.