JULY 2019

KILL SWITCH

WHY CONNECTED CARS CAN BE KILLING MACHINES AND HOW TO TURN THEM OFF

Consumer Watchdog

EXECUTIVE SUMMARY

For the past five months Consumer Watchdog worked with a group of car industry technologists and engineers concerned about the danger of Internet connectivity in modern non-self-driving cars and their susceptibility to hacking. The result is this investigative report exposing the perils of "connected cars" without compromising the identity of the industry insiders, who could lose their jobs as a result.

The report that follows, "Kill Switch," reflects the consensus concerns of these industry technologists about the security design flaws in the new fleet of connected cars. With tens of millions of these Internet-connected cars already operating on American roads, these automobiles will comprise the majority of new cars by the end of the year. This report is presented as a basis for conversation and new security protocols.

Background

While self-driving cars have received lots of attention, the auto industry is quietly installing components that carry similar risks into ordinary consumer automobiles. Widespread use of self-driving cars is years or decades away. However, 17 million new cars are deployed on American roads each year in which the mechanisms that control movement—accelerating, steering, and braking—can be overridden by computers and software.

This computerization has been accompanied by a growing trend of connecting cars to wide-area communications networks—making them part of the Internet of Things (IoT). This is a dangerous combination, as it creates the potential for hackers to take control of vehicles remotely. Unlike other "connected" technologies in which hackers can only steal information or money, hacked cars have the potential to cause property damage and deaths. Whereas the military and aviation industries carefully avoid connecting dangerous machines to the Internet, the auto industry has yet to learn this lesson.

Millions of cars on the Internet running the same software means a single exploit can affect millions of vehicles simultaneously. A hacker with only modest resources could launch a massive attack against our automotive infrastructure, potentially causing thousands of fatalities and disrupting our most critical form of transportation. Recent reporting about United States efforts to counter Russian cyber-attacks with its own online infiltration indicate that we increasingly live in the era of cyber warfare. An attack targeting transportation infrastructure is a growing possibility.

Most concerning is that automotive industry executives are aware of these risks, yet are proceeding nonetheless to deploy these technologies, putting corporate profits ahead of consumer safety and national security.

Main Findings of the Investigation

The top ten car brands in the U.S., accounting for 95% of car sales, all sell Internet-connected cars. The three top-selling carmakers in the U.S., GM, Toyota, and Ford, representing nearly half the U.S. auto market, will only sell Internet-connected cars by the end of this year.

The troubling issue for industry technologists is that these vehicles' safety-critical systems are being linked to the Internet without adequate security and with no way to disconnect them in the event of a fleet-wide hack.

Most connected vehicles share the same vulnerability. The head unit (sometimes called the infotainment system) is connected to the Internet through a cellular connection and also to the vehicle's CAN (Controller Area Network) buses. This technology dating to the 1980s links the vehicle's most critical systems, such as the engine and the brakes.

Experts agree that connecting safety-critical components to the Internet through a complex information and entertainment device is a security flaw. This design allows hackers to control a vehicle's operations and take it over from across the Internet.

By 2022, no less than two-thirds of new cars on American roads will have online connections to the cars' safety-critical system, putting them at risk of deadly hacks. Car makers have many economic motivations to connect vehicles to the Internet—from saving money on recalls by updating vehicle software over-the-air to collecting valuable data on how fast we drive to where we shop. While car companies market flashy new features, such as remotely starting cars from smartphones, technologists report the companies have not prepared for the grave security implications of a connected car fleet.

Car makers have even acknowledged to investors and shareholders the dangers of connected cars and their vulnerability to hacking. However, technologists report the companies are deceiving the public about the risks and their inability to eliminate them after nearly a decade of trying.

Technical experts explain that using smartphone technology in cars, technology that was never designed to protect safety-critical systems, is a recipe for disaster. A plausible scenario involving a fleet-wide hack during rush hour in major U.S. metropolitan areas could result in approximately 3,000 fatalities, the same death toll as the 9/11- attack.

Expert hackers report that time and money are the only things that stand between them and hacking a fleet of cars. Software design practices that result in frequent hacks of everything from consumer electronics to financial systems cannot be trusted in cars, which can endanger not only the lives of their occupants, but also pedestrians and everyone else on the road.

Connected cars have suffered more than half a dozen high-profile hacks in recent years. All have been benign demonstrations, not intended to cause harm. Hundreds more vulnerabilities have been reported to carmaker "bug bounty" programs. Experts report a hack of American vehicles designed to cause damage is inevitable without better security. The car industry's response when vulnerabilities are exposed is to patch individual security holes and ignore the design problems that underlie them.

Car hacking demonstrations to date have always focused on a single vehicle, but the networked nature of connected cars creates numerous avenues for a fleet-wide attack. Viruses can spread vehicle-to-vehicle. Malicious WIFI hotspots can infect any susceptible vehicle that passes within range. Cars can be infected with "sleeper" malware that wakes at a given date and time, or in response to an external signal, resulting in a massive coordinated attack.

Security-critical components in cars are black boxes. Even the car makers themselves often do not know the origins of the software they use, nor their true risks.

Vehicles from many major carmakers—including Tesla, Audi, Hyundai, and Mercedes—rely heavily on software written by third parties. This includes open source software, like Android, Linux, and FreeRTOS. This software often comprises contributions from hundreds or thousands of different authors around the world, and there is usually little accountability for flaws. For example, FreeRTOS, used in critical systems by Tesla, had major vulnerabilities discovered in October 2018, but Tesla never acknowledged using the software, the vulnerability, or whether it patched the problem.

The veil of secrecy surrounding automotive software and the ability to update it "over the air" without touching the vehicle lets automakers cover up safety problems and sloppy testing practices. Consumers are driving cars whose systems run on unfinished and under-tested software.

Despite working on the problem for more than a decade, carmakers have proven incapable of creating Internet-connected vehicles that are immune to hacking, which is the only standard that can keep consumers safe. With connected cars rapidly overtaking the market, consumers will soon have no haven from the online connections that threaten them.

To protect the public, carmakers should install 50-cent "kill switches" in every vehicle, allowing consumers to physically disconnect their cars from the Internet and other wide-area networks. Otherwise, if a 9/11-like cyber-attack on our cars were to occur, recovery would be difficult because there is currently no way to disconnect our cars quickly and safely. Mandatory "kill switches" would solve that problem.

Road Map Recommendations

The report offers the following road map for the industry and regulators to follow to ensure the safety and security of automobiles for the public.

As hacked cars have the potential to kill thousands of people, the industry must respond both immediately and in the long term to this threat.

The car industry should respond immediately with more transparency and consumer control.

- Regulators should require automakers to publicly disclose the authorship, safety certifications, and testing methodology used for all safety and security critical software, allowing for analysis by independent regulatory and testing agencies.

- CEOs of auto manufacturers should sign personal statements and accept personal legal liability for the cyber-security status of their cars.

- The industry should agree to a general standard protocol that cars not be connected to wide-area networks until they can be proven immune to hackers.

New car designs take three to five years to reach consumers. However, every carmaker should commit before year's end that:

- Each one of their cars at the earliest possible date will come with an Internet kill-switch that physically disconnects the Internet from safety-critical systems.

- Future designs will completely isolate safety-critical systems from infotainment systems connected to the Internet or other networks because connecting safety-critical systems to the Internet is inherently dangerous design.

If carmakers do not commit by December 31, 2019, legislators and regulators should mandate these protections.

Table of Contents

Most 2020 Model Cars are Connected to the Internet **6**

Figure I: Top Selling U.S. Carmakers' Connected Car Goals 7

Figure II: Vulnerable Connectivity Features in Top Models 9

The Threat: Internet Connectivity to Safety-Critical Systems **9**

Anatomy of a Remote Car Hack **10**

CEOs Acknowledge Hacking Risks To Investors **12**

Figure III: Investor Disclosures Acknowledge Hacking Risks 13

Even The Automakers Don't Know Who Writes Automotive Software **16**

Figure IV: Known Current and Future Open Source Operating Systems 17

Breeding Software Bugs That Can Be Exploited **18**

Figure V: List of Bug Bounties 20

The Mythological "White Hat" Hacker **20**

Over-The-Air Updates: Blessing or Curse? **22**

Anatomy and Scenarios of a Fleet-Wide Hack **26**

Recent History of Car Hackings **34**

Timeline of Notable Car Hacks **36**

Profits Over Security and Safety **39**

Potential Damage from a Large-Scale Hack **42**

The Future of Auto Safety: The Kill Switch & Beyond **44**

APPENDIX: Key Answers From Top Engineers **47**

Most 2020 Model Cars Are Connected to the Internet

There are about 50 million "connected cars"—cars that communicate with the cellular network or with each other—on U.S. roads today[1], representing about 20% of all cars in use, but those numbers are rising rapidly. About 17 million new cars are deployed on American roads each year[2].

Top-selling automakers including General Motors, Ford, and Toyota have committed to making all of their new models "connected cars" in upcoming model years. This makes connected cars a much more serious and immediate risk to public safety than self-driving cars.[3]

[1] "Stock of Connected Cars," *Statista*: https://www.statista.com/outlook/320/109/connected-car/united-states#market-users

[2] "Car Sales set another U.S. Record," Ahiza Garcia, CNN Business, Jan 2017 http://money.cnn.com/2017/01/04/news/companies/car-sales-2016/index.html

[3] "Market share held by selected automobile manufacturers in the United States in 2018," *Statista,* 2019 https://www.statista.com/statistics/249375/us-market-share-of-selected-automobile-manufacturers/

Figure I: Top Selling U.S. Carmakers' Connected Car Goals [4] [5] [6] [7] [8] [9]

Top-selling Makes in U.S.	U.S. Market Share	New cars at risk due to connectivity
General Motors (Chevy, Buick, Cadillac, etc.)	17.02%	All new vehicles today
Toyota	14.63%	All by 2020
Ford	14.44%	All by 2020
Fiat-Chrysler	12.98%	Next generation platform providing connectivity in all cars by 2022
Renault-Nissan-Mitsubishi	9.35%	90% of new cars by 2022
Honda	9.10%	Unknown
Hyundai/Kia	7.42%	Unknown
Subaru	3.94%	Unknown
Volkswagen	3.69%	Unknown
Daimler	2.06%	Unknown

In model year 2019, connected cars are already commonplace. The top ten car brands in the U.S., accounting for 95% of car sales, all sell Internet-connected cars. All of the top

[4] "Market share held by selected automobile manufacturers in the United States in 2018," *Statista*, 2019 https://www.statista.com/statistics/249375/us-market-share-of-selected-automobile-manufacturers/

[5] "GM's OnStar service explained," Jeremy Laukkonen, *Lifewire*, Jan 2019: https://www.lifewire.com/gms-onstar-service-534811

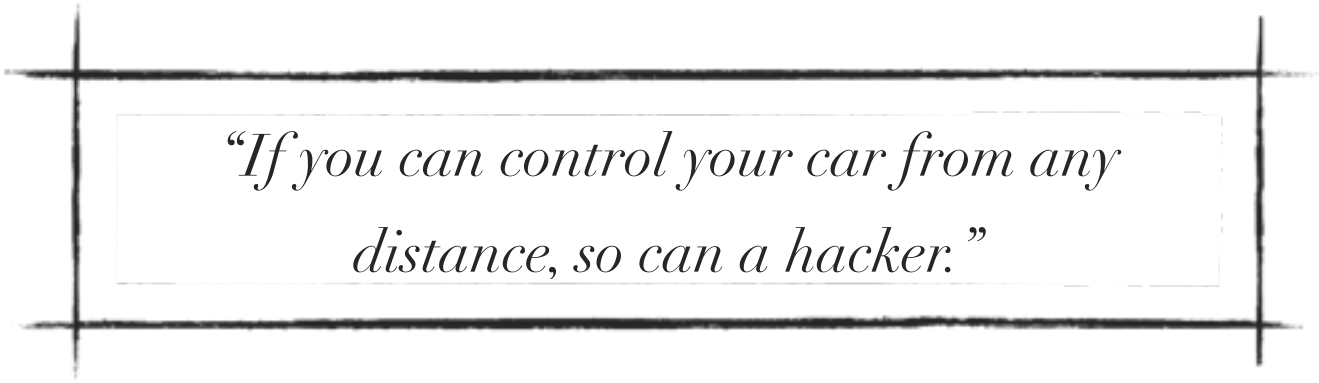
[6] "KDDI and AT&T to Connect Toyota and Lexus Vehicles," Toyota, Jan. 2019: https://corporatenews.pressroom.toyota.com/releases/kddi+att+connect+toyota+lexus+vehicles.htm

[7] "Why Ford's Cellular to Vehicle Matters," Nicholas Rossolillo, *The Motley Fool*, Jan 2019: https://finance.yahoo.com/news/why-ford-apos-cellular-vehicle-151600854.html

[8] "FCA Selects HARMAN (Samsung) and Google Technologies for New Global Connected Vehicle 'Ecosystem,'" Fiat Chrysler Automobiles, Apr 2019 https://www.fcagroup.com/en-US/media_center/fca_press_release/2019/april/Pages/fca_selects_harman_and_google_technologies_for_new_global_connected_vehicle_ecosystem.aspx

[9] "Nissan, Renault ready next-gen connected car platform," Hans Greimel, *Automotive News*, Mar. 2019 https://www.autonews.com/technology/nissan-renault-ready-next-gen-connected-car-platform

ten best-selling sedans in the U.S. are available with Internet connectivity. As of model year 2019, four of the ten best-selling sedans are only available with Internet capabilities. The connectivity is marketed under various names, but a common feature is the ability to control your car from an unlimited distance away using a smartphone app. If you can control your car from any distance, so can a hacker. Other "connected car" features may include voice assistant integration (e.g., Amazon "Alexa"), and the ability for the automaker to update the car's software "over the air".



Many automakers are touting the ability to start your car's climate control system from your smartphone, so the cabin is a comfortable temperature before you get in. This capability requires the car to have cellular or other wide-area connectivity, and internal communication linking that connectivity to the most critical parts of the vehicle. In many cases, these capabilities are optional, and require you to pay a recurring service charge. However, whether you subscribe to the service or not, as long as the equipment is present in your car, the car could be vulnerable to hackers.

The chart below shows the availability of dangerous connectivity features in a sampling of popular model year 2019 cars[10]. Model year 2020 cars will be rolled out to consumers this fall. The list of affected vehicles will expand as automakers follow through on their promises to make these technologies standard across all vehicles. Every major automaker now offers connectivity. Some brands, like BMW, Mercedes, and Tesla, have already made connectivity standard in 100% of their vehicles, and other makes are rapidly approaching that goal.

[10] "America's 9 Best-Selling Cars of 2018 by Category," *CARFAX*: https://www.carfax.com/blog/2018-best-selling-cars-by-category

Figure II: Vulnerable Connectivity Features in Top Models

Vehicle	Commercial Name(s)	Models
Toyota Camry	Remote Connect, Safety Connect	*** All Models ***
Lexus ES	Enform	*** All Models ***
Honda Civic	HondaLink	All hatchbacks; coupes and sedans "Sport" model and above
Mercedes C-Class	me connect	*** All Models***
Subaru Outback	STARLINK	*** All Models ***
Tesla Model 3	*N/A -- connectivity is an integral feature in all Tesla vehicles*	*** All Models ***
Ford F-150	SYNC Connect	All but the lowest-end models
BMW 5-series	ConnectedDrive	*** All Models***

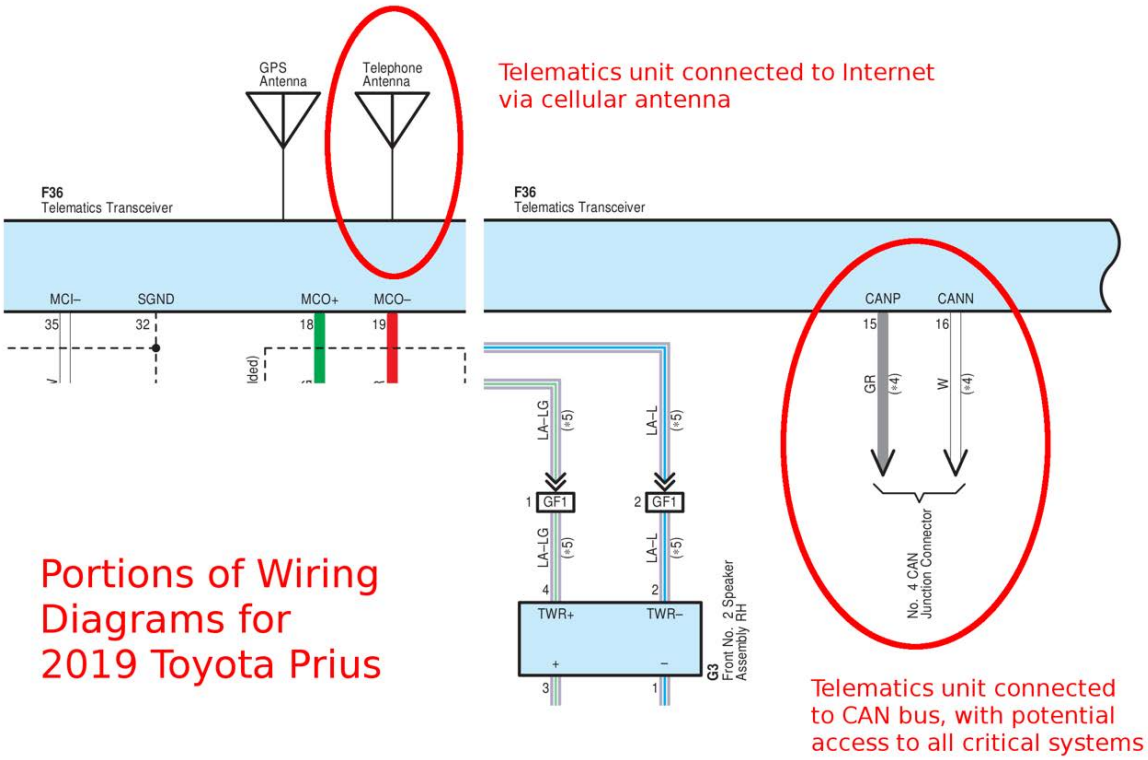
The Threat: Internet Connectivity to Safety-Critical Systems

Most connected vehicles share the same vulnerability. The head unit (sometimes called the infotainment system) is generally responsible for non-critical information and entertainment, such as music and in-car navigation. It is connected to the Internet through a cellular connection, and also to the vehicle's CAN (Controller Area Network) buses. CAN buses are a technology dating to the 1980s that links the vehicle's most critical systems, such as the engine and the brakes.

Like any complex electronic device on the Internet, a head unit is vulnerable to hackers. To date, nearly every documented car hack has used the head unit, which is complex and not designed for security, as a bridge from the Internet to the brakes and other safety-critical components.

Experts agree that connecting safety-critical components to the Internet through a complex information and entertainment device is a security flaw. This design allows hackers to control a vehicle's operations and take it over from across the Internet. This

security flaw is evident in the wiring diagram below, obtained from Toyota's own Technical Information System (TIS)[11]:



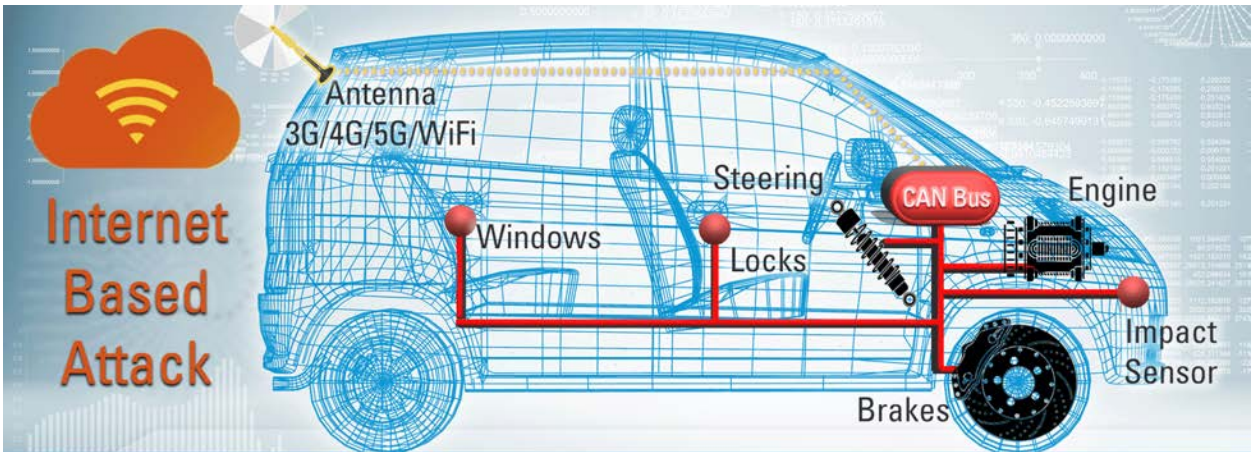
Some more sophisticated vehicles add a "gateway unit" between the head unit and the CAN bus. The gateway unit is responsible for ensuring only authorized communication can reach the safety-critical systems. While this would seem to solve the problem, it really only adds more complexity. A successful attack must pass through the gateway unit, requiring a more sophisticated attack. However, the additional hardware and software in the gateway unit also create more opportunity for hackers to find vulnerabilities.

Anatomy of a Remote Car Hack

A dangerous remote hack requires two components: a means of accessing the vehicle's internal systems from afar, and a means of taking control once inside. Neither component on its own is particularly dangerous.

[11] Technical Information System, Toyota: https://techinfo.toyota.com/techInfoPortal/appmanager/t3/ti

For more than 30 years, the most common electronic communication medium between components in cars has been the CAN bus[12]. Given that networking technology was in its infancy when CAN was developed, security was simply not a consideration in its design. A hacker can easily inject malicious messages onto a CAN bus to make a car potentially unsafe.[13] However, without a scalable way for hackers to access the CAN bus, this wasn't problematic when CAN was designed—attacks were only possible with physical access to the vehicle. That changed when cars were connected to the cellular network, providing potential outside access to the insecure, yet safety-critical systems[14]. Not only does this allow a hacker to attack a car without physical access to it, it allows a single hacker to attack many cars at once.



This is not simply a theoretical possibility. White-hat hackers have demonstrated these capabilities more than a dozen times in the past decade (see "Recent History of Car Hacking" below). For example, in 2015, when researchers Chris Valasek and Charlie Miller shut down a Jeep Cherokee's engine while it was on the highway[15], and later disabled its brakes, they did this from miles away, over the Internet, without physically touching the vehicle. This exploited a vulnerability in the radio to access safety-critical systems through the CAN bus. The vulnerability allowed them to issue commands to the Jeep's engines, brakes, and other systems from a laptop located miles away.

---

[12] "History of the CAN Technology," CiA https://www.can-cia.org/can-knowledge/can/can-history/

[13] "Automotive Security in a CAN," Bill Boldt, *Electronic Design*, Sep. 2017: http://www.electronicdesign.com/automotive/automotive-security-can

[14] "Why the Connected Car is One of this Generations Biggest Security Risks," Conner Forrest, *ZDnet*, Mar. 2016 https://www.zdnet.com/article/why-the-connected-car-is-one-of-this-generations-biggest-security-risks/

[15] "Hackers Remotely Kill Jeep on the Highway," Andy Greenberg, *Wired*, July 2015: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

A hackers' ability to control your car is not limited to the features officially supported by the car's smartphone app. Once the hacker has gained access to your car's electronics, all of the car's systems become vulnerable. In the hands of a hacker, a system designed to let you activate your car's air conditioning from your smartphone could be used to disable your car's brakes and airbags from anywhere in the world.

Consumers currently have no control over this aspect of their own vehicles: they do not have the option of disconnecting their car from the Internet. The software sitting between the Internet and the safety-critical systems, and therefore most critical to fending off cyber-attack, is a veritable black box. The automaker provides no information and no guarantees whatsoever about its reliability or testing, or even its authorship.

Even as automakers aggressively market the hot new connected car features to the public, the hacking risks are real enough that carmakers have warned the one group of people they are legally obligated to level with: investors.

> *"Despite extensive security measures, the risks in this area are classified as high."*
>
> — BMW Internal Report

CEOs Acknowledge Hacking Risks To Investors

A review of several of the automakers' annual reports and Securities Exchange Commission (SEC) statements finds that car companies including Daimler Chrysler, Honda, Toyota, Tesla, Ford, and BMW acknowledge to their shareholders that security and hacking concerns are real and growing.

Figure III: Investor Disclosures Acknowledge Hacking Risks[16] [17] [18] [19] [20]

Tesla	2019 SEC 10-K	"We have designed, implemented and tested security measures intended to prevent unauthorized access to our information technology networks, our products and their systems…**there can be no assurance that vulnerabilities will not be exploited in the future before they can be identified, or that our remediation efforts are or will be successful."**
Daimler Chrysler	2018 Annual Report	"Due in particular to the changed risk situation relating to cybercrime and hacker attacks, the possible impact of information-technology **risks has increased compared with the previous year from Medium to High."**

(continued)

[16] Tesla, 2018 Securities and Exchange Commission Form 10-K, Page 29: https://ir.tesla.com/node/19496/html

[17] Daimler Chrysler 2018 Annual Report, Page 151: https://www.daimler.com/documents/investors/reports/annual-report/daimler/daimler-ir-annual-report-2018.pdf

[18] Ford Motor Company, Form 10-K Securities and Exchange Commission 2018, Page 18: https://s22.q4cdn.com/857684434/files/doc_financials/2019/annual/ford-10k.pdf

[19] General Motors, Form 10-K Securities and Exchange Commission 2018, Page 14: https://www.sec.gov/Archives/edgar/data/1467858/000146785819000033/gm201810k.htm

[20] BMW, Annual Report 2018, Page 98: https://www.bmwgroup.com/content/dam/bmw-group-websites/bmwgroup_com/ir/downloads/en/2019/gb/BMW-GB18_en_Finanzbericht_190315_ONLINE.pdf

Investor Disclosures Acknowledge Hacking Risks		
Ford	2018 SEC 10-K	"Such cyber incidents could materially disrupt operational systems; result in loss of trade secrets or other proprietary or competitively sensitive information; compromise the privacy of personal information of customers, employees, or others; jeopardize the security of our facilities; **affect the performance of in-vehicle systems; and/or impact the safety of our vehicles. A cyber incident could be caused by malicious third parties using sophisticated, targeted methods to circumvent firewalls, encryption, and other security defenses, including hacking, fraud, trickery, or other forms of deception. We, our suppliers, and our dealers have been the target of these types of attacks in the past and such attacks are likely to occur in the future. The techniques used for attacks by third parties change frequently and may become more sophisticated, which may cause cyber incidents to be difficult to detect for long periods of time**. Our networks and in-vehicle systems may also be affected by computer viruses or breaches due to the negligence or misconduct of employees, contractors, and/or others who have access to our networks and systems."

Investor Disclosures Acknowledge Hacking Risks		
General Motors	2018 Annual Report	**"Security breaches and other disruptions of our in-vehicle systems could impact the safety of our customers and reduce confidence in GM and our products**. Our vehicles contain complex information technology systems. These systems control various vehicle functions including engine, transmission, safety, steering, navigation, acceleration, braking, window and door lock functions. We have designed, implemented and tested security measures intended to prevent unauthorized access to these systems. However, hackers have reportedly attempted, and may attempt in the future, to gain unauthorized access to modify, alter and use such systems to gain control of, or to change, our vehicles' functionality, user interface and performance characteristics, or to gain access to data stored in or generated by the vehicle."
BMW	2018 Annual Report	"If risks relating to information security, data protection and IT were to materialize, they could have a high earnings impact over the two-year assessment period. **Despite extensive security measures, the risks in this area are classified as high**."

Carmakers have acknowledged to their investors the risk that their cars will be hacked is high now that safety-critical systems are being connected to the Internet. The question that baffles technologists is why automakers continue to invest in unsafe, poorly-architected technologies even though the risks have been known to automakers for almost a decade.

The military industrial complex and aviation industries have addressed the threat of cyberattack by not connecting critical systems to the Internet. In cases where Internet connectivity is required, they invest in proprietary software that is simple and effective, focused on security rather than features, often using mathematical proofs to show that these systems are immune to attack. By contrast, automakers are utilizing smartphone technology and open source operating systems that run them—systems that have been proven time and again to be vulnerable—as the basis for motor vehicle safety, on which hundreds of millions of Americans' lives depend.

Even The Automakers Don't Know Who Writes Automotive Software

While practices vary by automaker, the bulk of software running in modern cars is not written by the automakers. Much of it comes from suppliers, such as Samsung-owned Harman, best known for its stereos. Harman developed the flawed infotainment system that allowed Valasek and Miller to gain remote access to the Jeep Cherokee in 2015. But frequently, even first-tier suppliers like Harman are not the original authors.

"More training and certification is legally mandated to style someone's hair or give someone a massage than to write safety-critical software for cars."

To minimize costs, the auto industry makes extensive use of free "open source" software, such as Linux and Android. Open source software is "crowdsourced", in the sense that hundreds or thousands of unpaid hobbyists from around the world may have contributed to its design and implementation. While open source software use is common in the software industry, and can avoid some up-front expenses, it comes with serious safety and reliability pitfalls, most notably that there is rarely any accountability for the quality or support of the software. Most open-source software includes a boilerplate legal disclaimer, that begins (capitalized as shown): "THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED..." Android and Linux have a long and ever-changing list of security vulnerabilities.[21]

Two anonymous ex-Tesla employees independently reported that the "gateway unit" in Tesla cars, responsible for protecting the most sensitive systems in the car from Internet traffic, runs an open-source operating system called FreeRTOS, common in "Internet of Things" (IoT) devices. In October

[21] *CVE Details,* https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html

2018, security researchers discovered more than a dozen vulnerabilities in FreeRTOS[22], potentially making all aspects of Internet-connected Tesla vehicles susceptible to hackers. Tesla made no public statement about this safety-related defect in their cars, nor is there record of the problem being reported to regulatory bodies that track automotive safety, such as the National Highway Traffic Safety Administration (NHTSA). There is no public information about how long the vulnerability was present, and how (or even if) it was ultimately fixed.

The world's most widely used open source operating system is Linux. The Linux kernel is also the basis of the Android mobile device operating system. Linux's creator, Linus Torvalds, has said that Linux should not be responsible for protecting human lives. In a November 2015 *Washington Post* interview, Torvalds said the following regarding a hypothetical scenario in which hackers exploit a flaw in Linux to cause a meltdown at a nuclear power plant: "There is no way in hell the problem there is the [Linux] kernel. If you run a nuclear power plant that can kill millions of people, you don't connect it to the Internet." Yet, Linux and Android have found widespread use in Internet-connected cars.

While some automakers are up-front about their use of open-source software in specific systems within their vehicles, the origins and authorship of most automotive software remain beyond public view. Consumers are expected to trust that automakers will use software that is safe, well-maintained, and secure, when all evidence points to the opposite being true.

Figure IV: Known Current and Future Open Source Operating Systems

Linux	Tesla, Audi, Mercedes-Benz, Hyundai, Toyota, BMW, Chevrolet, Honda
Android	Fiat-Chrysler, Volvo, Renault, Nissan, Mitsubishi
FreeRTOS	Tesla

The complex supply chain and large number of unknown authors make it very difficult for automakers to maintain the software that runs our cars, let alone to design the security of the software in a coherent and effective way. Whereas training, licensing, and design quality standards apply in practically every engineering discipline that deals with human safety, the same is not true for automotive software. More training and certification is legally mandated to style someone's hair or give someone a massage than to write safety-critical software for cars. Writing software that could affect the safety of millions of motor

[22] CVE Details, CVE-2018-16528, Dec 2018 https://www.cvedetails.com/cve/CVE-2018-16528/

vehicles requires little more than getting hired by a third-tier supplier or participating, possibly anonymously, in one of any number of open source software projects.

Breeding Software Bugs That Can Be Exploited

A bug is an instance of software failing to behave as it was designed, usually caused by mistakes made during the process of writing the software. Bugs can cause software-based systems to be unreliable, make mistakes, or provide access and control to unauthorized parties.

The larger and more complex the body of code, the more bugs it is likely to contain.[23] This is particularly worrisome given the staggering quantity of software in a typical modern car:

> *"Today's cars can contain over 100 million lines of code. For perspective, an F-35 joint strike fighter jet contains about 9 million," said Neil Steinkamp, a managing director in Stout's automotive practice who has led the firm's research and analysis of automotive recalls. "When you have that much software in a car—and particularly when much of that software is relatively new—there are going to be some issues."* [24]

Why the disparity between the amount of code in a car versus a plane? There are several likely reasons. Each line of code is a technical liability—a potential failure point. For this reason, aircraft manufacturers try to minimize the amount of code in planes, making the software easier to maintain and less buggy.[25] The auto industry clearly hasn't adopted this habit yet.

Software used in aircraft must meet stringent government safety standards that don't apply to the auto industry. On the contrary, the auto industry has repeatedly fought regulation, such as with 2018's AV START Act, which attempted to block state and local agencies from regulating autonomous vehicle safety so nascent technologies could be rushed to market. In addition to uncovering bugs before the software goes into

---

[23] "The Danger Of Complexity: More Code, More Bugs." Chad Perrin, *Tech Republic*, February 2010 https://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs/

[24] Report reveals spike in software-related recalls; explores emerging risks such as hacking, data breaches, *Stout*, Apr 2016: https://www.stoutadvisory.com/news/srr-2016-automotive-warranty-recall-report-reveals-spike-software-related-recalls-explores-emer

[25] "Ford's new GT has more lines of code than a Boeing jet airliner," Stephan Edelstein, *Digital Trends*, May 2015: https://www.digitaltrends.com/cars/the-ford-gt-uses-more-lines-of-code-than-a-boeing-787/ and. "How important is it to reduce the number of lines in code" *Ars Technica*, Apr 2013 https://arstechnica.com/information-technology/2013/04/how-important-is-it-to-reduce-the-number-of-lines-in-code/

production, the certification process for aircraft software substantially increases the cost per line of code, providing additional incentive to keep the software simple.[26]

One sign that software bugs are a serious and growing concern for all consumer vehicles is the increasing number of software-related recalls. The percentage of auto recalls due to software failures tripled between 2011 and 2016.[27] The 2017 Stout Automotive Warranty and Recall Report shows an increasing trend of software-related recalls both as measured in unique recall campaigns and in the number of vehicles affected.[28] The report offers the following explanation for the increase:

> *"One reason for the likelihood of sustained elevated recalls in the coming years is an increased number of defects related to software and integrated electronic components. The continued development of new technologies to assist drivers, differentiate vehicles, and improve vehicle safety also poses recall risk. The widespread use of such innovations as adaptive cruise control, rear backup cameras, forward-collision detection, emergency braking, and brake assist improve vehicle safety, yet add complexity to safety-critical systems."* [29]

Automakers have a financial incentive to focus on these software-heavy features. Since software does not involve physical parts, once it is developed, it can be mass-produced at practically zero cost. These same software-based features can increase a vehicle's price to consumers by hundreds or thousands of dollars.

The more software a car contains, the greater the chance of software bugs that hackers can exploit to take control of vehicles. Automaker "bug bounty" programs have demonstrated that vulnerabilities can be purchased for a few tens of thousands of dollars. To someone interested in causing harm, this is much cheaper than conventional weapons. A clever hacker could even make it look like a third party was responsible.

Below is a list of the public auto industry "bug bounty" programs, which have already collectively uncovered hundreds of bugs in carmakers software. Most automakers have no public bug bounty programs at all. Some automakers claim to have bug bounty programs,

---

[26] "Toyota's Expensive Software," Jack Gannsle, *Embedded*, Mar 2014: https://www.embedded.com/electronics-blogs/break-points/4429601/Toyota-s-Expensive-Software

[27] "Report: Software Issues Have Tripled Auto Recalls in Past Five Years," Andy Szal, Manufacturing.net, Jun 2016: https://www.manufacturing.net/news/2016/06/report-software-issues-have-tripled-auto-recalls-past-five-years

[28] 2017 Automotive Warranty and Recall Report, Stout, Figs. 17,18: https://www.stoutadvisory.com/insights/report/2017-automotive-warranty-recall-report

[29] 2017 Automotive Warranty and Recall Report, Stout, p. 12: https://www.stoutadvisory.com/insights/report/2017-automotive-warranty-recall-report

but the programs are highly limited or ineffectual. For example, GM's bug bounty program is only available to a tiny group of researchers[30]. The hundreds of bugs known to be found through these bug bounty programs are clearly just a fraction of the number of software bugs that exist in cars on American roads and that can be exploited through Internet connections to safety critical systems by hackers.

Figure V: List of Bug Bounties

Fiat-Chrysler	• 93 vulnerabilities rewarded • 300+ "hall-of-famers" who reported vulnerabilites • $4,760 payout per bug on average over the last 3 months • Disclosing details of the vulnerability to the public explicitly prohibited	https://bugcrowd.com/fca
Tesla	• 348 vulnerabilities rewarded • 426 "hall-of-famers" • $2k average payout	https://www.tesla.com/about/security https://bugcrowd.com/tesla https://techcrunch.com/2018/09/06/teslas-new-bug-bounty-protects-hackers-and-your-warranty/
BMW	Note: does not appear to offer any reward Note: no statistics available	https://www.bmwgroup.com/en/general/Security.html

The Mythological "White Hat" Hacker

Bug bounty programs are intended to attract the efforts of "white hat" hackers. Unlike "black hat" hackers who are out for personal gain at others' expense, "white hat" hackers

[30] "GM offers bounty software bugs," Nora Naughton, *Detroit News*, Aug. 2018: https://www.detroitnews.com/story/business/autos/general-motors/2018/08/03/gm-offers-bounty-software-bugs/897057002/

develop sophisticated techniques for finding vulnerabilities with the goal of helping software developers make their products more resilient. While white hat hackers generally have good intentions, their efforts are often counterproductive to improving security in safety-critical systems.

The biggest flaw in the "white hat" model is that it encourages automakers to repeatedly patch a system that was never fundamentally secure. History has shown that, while this can make incremental improvements, the process never ends, so it does not result in a secure product. Internet-connected cars were unsafe a decade ago and are still unsafe today. With our safety at stake, we cannot wait another decade hoping that this process will eventually find the last remaining security vulnerability.

Despite the ineffectiveness of white hat hackers' efforts at producing a secure car, their work is extremely valuable to automakers. The continuous churn of finding and fixing bugs presents the illusion that automakers are "working hard" to create a safe product. Paying bug bounties to white hat hackers is generally much less expensive than hiring employees to do the same work, in that automakers need only pay for positive results. Further, the "hacker mystique" contributes to the positive publicity created when a white hat reveals a new vulnerability. Perhaps the most brazen example occurred in May 2018 when, after Keen Security Lab demonstrated more than a dozen vulnerabilities in Internet-connected BMW vehicles, BMW responded by giving them an award[31], cleverly deflecting the public shame of selling consumers an unsafe product. This may be why automakers are so enamored of white hat hackers, and why the *Detroit Free Press* called hackers "the hottest job in the [auto] industry."[32]

At the same time, the auto industry manipulates white hat hackers with threats of prosecution under anti-hacking laws, such as the Digital Millennium Copyright Act (DMCA). Most bug bounty programs require white hat hackers to abide by "responsible disclosure" rules, which include keeping details of the vulnerability secret.[33] This is ostensibly to prevent anyone from trying to exploit the vulnerability before it can be fixed. However, it also allows the automaker to control the public message, covering up an

---

[31] "First-ever BMW Group Digitalization and IT Research Award goes to Tencent Keen Security Lab for their connectivity and cybersecurity research. The two companies plan to expand their cooperation and joint research work," BMW Group, May 2018: https://www.press.bmwgroup.com/global/article/detail/T0281245EN/first-ever-bmw-group-digitalization-and-it-research-award-goes-to-tencent-keen-security-lab-for-their-connectivity-and-cybersecurity-research-the-two-companies-plan-to-expand-their-cooperation-and-joint-research-work?language=en

[32] "Carmakers struggle to hire hackers, the hottest job in the industry," Jamie LaReau, *Detroit Free Press*, Aug. 20, 2018 https://www.freep.com/story/money/cars/general-motors/2018/08/20/hottest-auto-job-town-hacking/986636002/

[33] Product Security, Tesla: https://www.tesla.com/about/security

inadequate solution, and ensuring a positive spin on what should be a public embarrassment.

Because vulnerabilities in automobile software are a public safety hazard, we must treat them like other public safety hazards. Consumers don't quietly tell polluters to clean up their acts in return for cash rewards. We inform the EPA. We report reckless drivers to the police. We do not let them hide behind "anti-reckless-driver-reporting laws." Why do we treat automakers whose products threaten public safety any differently? So-called "responsible disclosure" is irresponsible when public safety is at stake.

Over-The-Air Updates: Blessing or Curse?

A likely motivation for the proliferation of connected cars is the desire to address the increasing number of software defects with over-the-air (OTA) updates, which are much less expensive and less embarrassing than recalls. Several of the major automakers, including General Motors, have announced their intention to add or expand support of over-the-air (OTA) updates of vehicle software in upcoming model years.[34] While this mode of software release may be acceptable in cell phones and home PCs, it is potentially very dangerous in systems with safety-critical components, such as cars.

"Because vulnerabilities in automobile software are a public safety hazard, we must treat them like other public safety hazards."

"We're talking billions of dollars a year that could be saved," said Sam Abuelsamid, an automotive analyst at the consulting and research firm Navigant. He says software updates are "an increasingly large part of the warranty work that the dealers have to do because there's so much more that's software-driven."[35]

A 2015 IHS report estimated the savings to the auto industry from OTA updates will reach $35 billion by 2022.[36] While OTA

---

[34] "GM says most new vehicles to get over-the-air upgrade tech by 2023," Joe White, Reuters, May 2019 https://www.reuters.com/article/us-gm-technology/gm-says-most-new-vehicles-to-get-over-the-air-upgrade-tech-by-2023-idUSKCN1SQ1R7

[35] "Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?" Keith Barry, *Consumer Reports*, Apr. 2018: https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/

[36] "Over-the-air Software Updates to Create Boon for Automotive Market," IHS, Sept. 2015: https://news.ihsmarkit.com/press-release/automotive/over-air-software-updates-create-boon-automotive-market-ihs-says

"The ability to perform OTA software updates has serious security implications. Performing an OTA update requires the vehicle's software systems to be remotely accessible."

updates might seem like a reasonable way to combat software failures, they carry hidden dangers. Keith Berry, an automotive writer and editor explained by saying, "Modern vehicles run on millions of lines of code that control everything from brakes to steering. When automakers start updating that software remotely, any failure could be just as dangerous as if a mechanic made a faulty repair—and it might affect thousands of vehicles at the same time."[37]

The ability to perform OTA software updates has serious security implications. Performing an OTA update requires the vehicle's software systems to be remotely accessible. Put another way, if the vehicle's systems were not remotely accessible, there would be no way for the OTA update to reach the vehicle.

In their paper "A Survey of Remote Automotive Attack Surfaces," Valasek and Miller surveyed several popular vehicle makes and models, looking for the combination of vulnerabilities that could enable a dangerous remote hack. In the paper, they rated each vehicle by "Attack Surface" (ease of gaining remote access), "Cyber Physical" (ability to control the vehicle electronically once access is gained), and "Network Architecture" (ease of gaining access to the Cyber Physical components once the Attack Surface is breached.)

The paper includes a table of the vulnerabilities in several makes/models/years, rating each on a scale of pluses and minuses, from "--" (least hackable) to "++" (most hackable) in Attack Surface, Network Architecture, and Cyber Physical. Note that the trend shows vehicles becoming more vulnerable over time. For example, the 2006 Toyota Prius rates as (-, --, --), whereas the 2010 and 2014 redesigns of the Toyota Prius are rated (+, +, ++). The Ford Fusion saw a similar degradation in security from 2006 to 2014.[38]

The latest model year represented in the chart is 2015, so the information presented predates the publicity of the 2015 Jeep hack. We would expect that automotive security

---

[37] "Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?" Keith Barry, *Consumer Reports*, Apr. 2018: https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/

[38] "A Survey of Remote Automotive Attack Surfaces," Valasek and Miller, http://illmatics.com/remote%20attack%20surfaces.pdf

would have improved since then, but that appears not to be the case. While security may have progressed in some areas, it has clearly regressed in others.

In the terms of Valasek and Miller's "Car Ratings" table, allowing access to vehicles remotely through OTA updates translates to a most hackable "Attack Surface" rating. Further, if the OTA updates apply to safety-critical systems, such as those that control the steering and braking, then the safety-critical systems must be electronically connected to the systems receiving the OTA updates.This translates to a worse "Network Architecture" rating. So, the ability to perform OTA updates means that vehicle security is reduced as measured by two of the three metrics Valasek and Miller used to evaluate vulnerability.

"OTA updates are a huge money-saver, but to hackers, they are a wide-open door into the most sensitive software of a vehicle."

Over-the-air updates are already causing trouble. In February 2018, a Chrysler OTA update caused some cars' infotainment systems to become unusable.[39] At any reputable repair shop, a technician would verify that the repair was effective and had been performed correctly, but that is not possible when cars are modified en masse with an OTA update. Thankfully, this particular problem did not cause a safety-critical component of the vehicle to malfunction, though such a failure is certainly possible. It did, however, render a safety feature, the rear-view camera, unusable— along with the heat, radio, and navigation.[40] In September 2018, Tesla owners reported a similar OTA update causing the Autopilot feature to stop working.[41]

OTA updates may also have a negative effect on the quality of critical software by reducing the incentive for automakers to test the software fully before release. In May 2018, *Consumer Reports* announced they would not recommend the Tesla Model 3 due in

---

[39] "Chrysler's over-the-air update fiasco is limited to the Northeast, but customers are still waiting for a fix," Sean O'Kane, *The Verge*, Feb 2018: https://www.theverge.com/2018/2/14/17013016/fiat-chrysler-ota-update-problem-jeep

[40] "Chrysler's over-the-air update fiasco is limited to the Northeast, but customers are still waiting for a fix," Sean O'Kane, *The Verge*, Feb 2018: https://www.theverge.com/2018/2/14/17013016/fiat-chrysler-ota-update-problem-jeep

[41] "Tesla's Autopilot Not Working After Latest Over The Air Update," Ryan Felton, *Jalopnik*, Sept 2018: https://jalopnik.com/tesla-autopilot-not-working-after-latest-over-the-air-u-1829018937

part to inconsistent braking behavior.[42] About a week later, Tesla updated all Model 3 cars over-the-air. When *Consumer Reports* re-tested the same car, the average braking distance was reduced by nearly 20 feet, and they reversed their earlier decision, recommending the car.[43] "The fact that Tesla engineers were able to slash nearly 20 feet of stopping distance in a couple of days is a sign that there was something fundamentally broken in what they were doing," said Abuelsamid.[44] Further, if the software fix was developed in the days between *Consumer Reports*' two tests, it could not have undergone very much road testing before its release to consumers.

The ability to perform OTA updates creates a perverse incentive: by dramatically reducing the price of patching buggy software, it incentivizes rushing unfinished and poorly-tested products to market. Beating the competition to market with the latest features, even if they do not yet work fully, provides a significant competitive advantage. This poses a serious risk to consumers if the software affects braking, steering, or other critical components of the vehicle. This is exactly what is alleged in a suit brought against Tesla, a pioneer of automotive OTA updates, by a group of its customers. In the suit, the customers claim they paid extra for the privilege of becoming "beta testers of half-baked software that renders Tesla vehicles dangerous if engaged."[45] Indeed, the Autopilot software at the center of the suit may have been at fault in at least one deadly crash.[46]

Further, OTA updates allow automakers to cover up sloppy manufacturing and testing outside the scrutiny of the public or regulators. NHTSA, the U.S. federal body that governs recalls and other aspects of vehicle safety, requires automakers to report safety-related defects discovered in cars. Public disclosure of these defects, and the cost of recalls, helps motivate automakers to ensure their vehicles are safe before they reach consumers. Since NHTSA cannot monitor modifications made to vehicles over the air,

---

[42] "Tesla Model 3 Falls Short of a CR Recommendation," Patrick Olsen, *Consumer Reports*, May 2018: https://www.consumerreports.org/hybrids-evs/tesla-model-3-review-falls-short-of-consumer-reports-recommendation/

[43] "Tesla Model 3 Gets CR Recommendation After Braking Update" Patrick Olsen, *Consumer Reports*, May 2018 https://www.consumerreports.org/car-safety/tesla-model-3-gets-cr-recommendation-after-braking-update/

[44] "Tesla's Over-the-Air Brake Upgrade Was Amazing" Timothy Lee, *Ars Technica*, May 2018: https://arstechnica.com/cars/2018/05/how-a-software-brake-upgrade-won-tesla-a-consumer-reports-endorsement/

[45] "Tesla Customers Sue Over 'Dangerous' And Non-Functioning Autopilot Software" Alan Ohnsman, *Forbes*, April 2017 https://www.forbes.com/sites/alanohnsman/2017/04/19/tesla-customers-sue-over-dangerous-and-non-functioning-autopilot-software/

[46] "Tesla Autopilot Was On During Deadly Mountain View Crash" Jason Green, *San Jose Mercury News*, Mar. 2018 https://www.mercurynews.com/2018/03/30/tesla-autopilot-was-on-during-deadly-mountain-view-crash/

automakers can easily bypass the requirement to report safety-related software updates to regulators.

Tesla's use of an OTA update to fix the brakes also raises the question: if the brakes can be fixed through a remote software update, can they be disabled by the same mechanism? To automakers**,** OTA updates are a huge money-saver, but to hackers, they are a wide-open door into the most sensitive software of a vehicle.

In 2017, researchers at Keen Security Lab demonstrated a way to bypass the code signing mechanism in a Tesla Model X, which is supposed to guarantee that only the manufacturer can patch the vehicle's software, suggesting a hacker could use the OTA update mechanism to disable the brakes in Tesla cars.[47] It might also be possible for a saboteur within Tesla to achieve the same effect. In June, 2018, in response to sabotage in Tesla's manufacturing process, Elon Musk admitted to "a long list of organizations that want Tesla to die" including oil companies and rival automakers.[48] Again, none of these failures is possible if the update is carried out with a qualified technician present.

Anatomy and Scenarios of a Fleet-Wide Hack

Individual cars have been hackable for many years. With physical access to a car, there's little to stop a hacker from taking control of any of its systems. However, the risks associated with such an attack are relatively minor because it only affects a single car.

Connecting cars—to each other, to the Internet, or to other insecure devices like smartphones—multiplies the danger. Suddenly, with just a little more effort, an attack that can affect one car can affect entire fleets. This creates a very effective target for terrorists, hostile nation states, or anyone else wishing to inflict a lot of damage.

Tesla CEO Elon Musk, speaking at the National Governor's Association meeting in 2017, said, "I think one of the biggest risks for autonomous vehicles is somebody achieving a fleet-wide hack."

Here are the top scenarios of a fleet-wide hack:

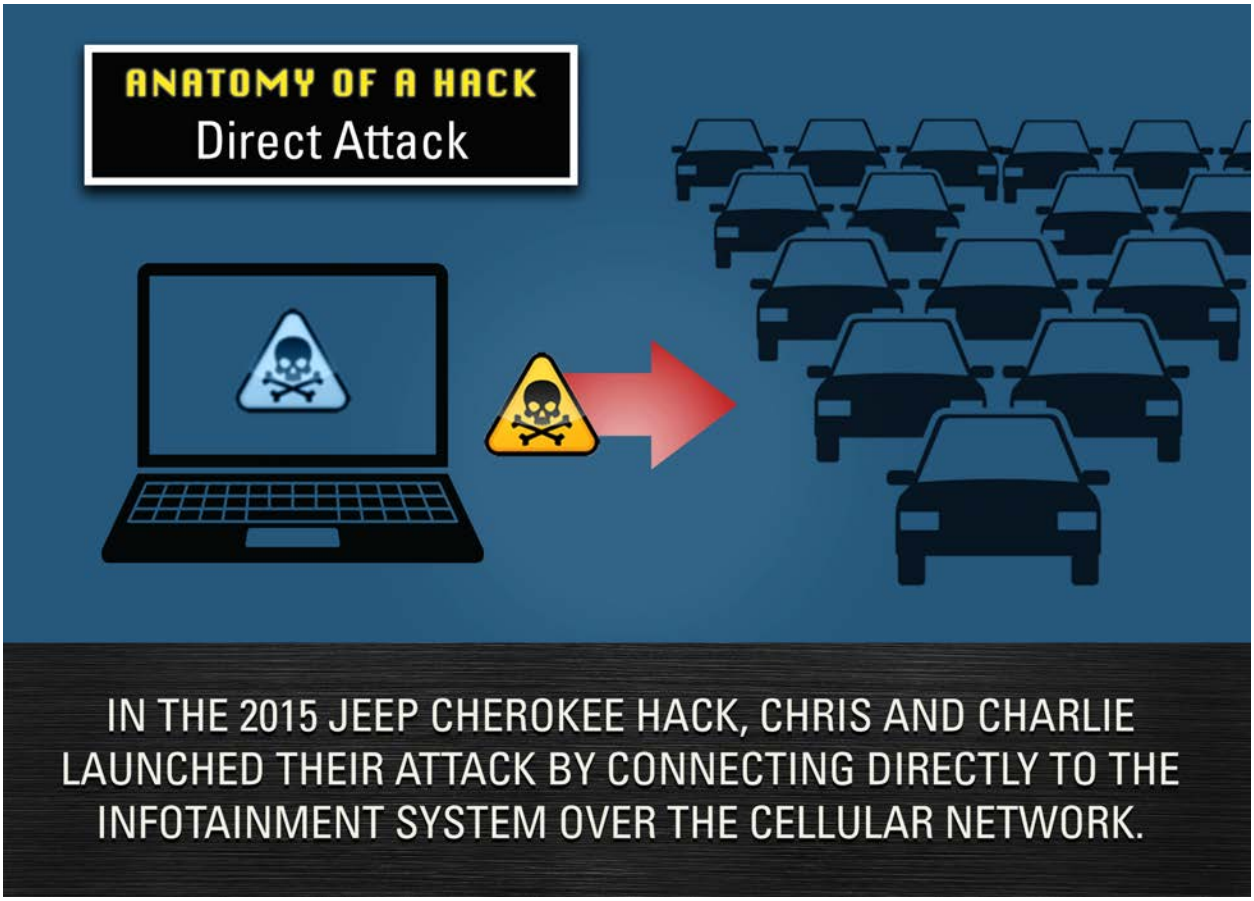
---

[47] "New Car Hacking Research: 2017, Remote Attack Tesla Motors Again," Keen Security Lab Blog, Jul 2017: https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/

[48] "Elon Musk Emails Employees About Extensive and Damaging Sabotage Conducted By Employee," Lora Kolodny, CNBC, Jun. 2018: https://www.cnbc.com/2018/06/18/elon-musk-email-employee-conducted-extensive-and-damaging-sabotage.html

Direct Attack

In the 2015 Jeep Cherokee hack, Chris Valasek and Charlie Miller launched their attack by connecting directly to the infotainment system over the cellular network from a laptop. In addition to targeting their own Jeep Cherokee for demonstration purposes, they scanned the network for other vulnerable cars.[49] During one such scanning session, in a short period of time, they found 2,695 vehicles with a similar vulnerability to the one they exploited in the Jeep. Since they had already automated their attack (by programming the steps into their computer), hacking all of those vehicles directly from the same laptop would have been a trivial exercise.



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

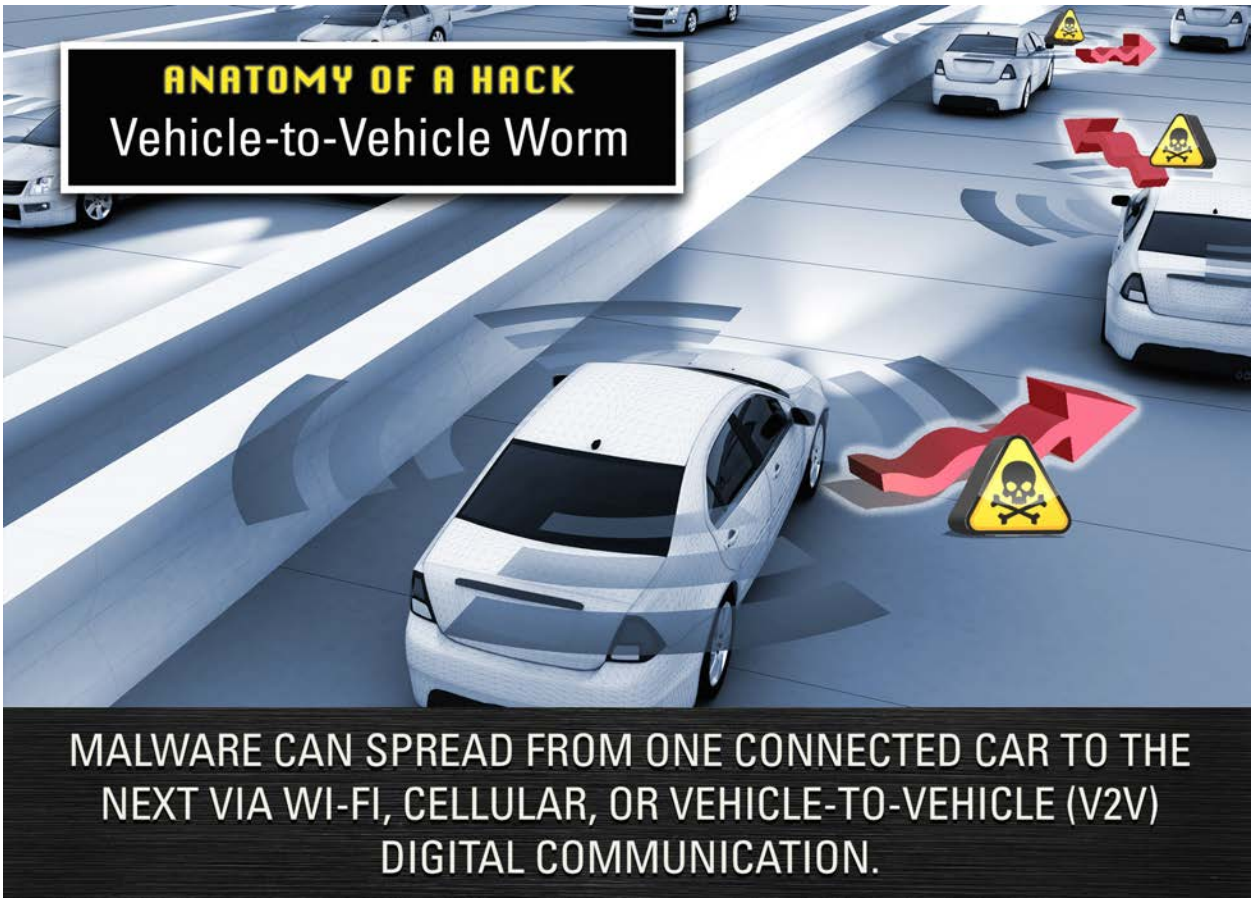
Vehicle-to-Vehicle Worm

In the paper describing their Jeep hack, Valasek and Miller hypothesized that malware could be designed to pass from vehicle to vehicle:

> *"Since a vehicle can scan for other vulnerable vehicles and the exploit doesn't require any user interaction, it would be possible to write a worm. This worm would scan for vulnerable vehicles, exploit them with their payload which would scan for other vulnerable vehicles, etc. This is really interesting and scary. Please don't do this. Please."*[50]

Instead of directly attacking each vehicle, such an attack would only involve infecting a small number of vehicles, and allowing the malware to spread, much as a virus spreads from human to human.

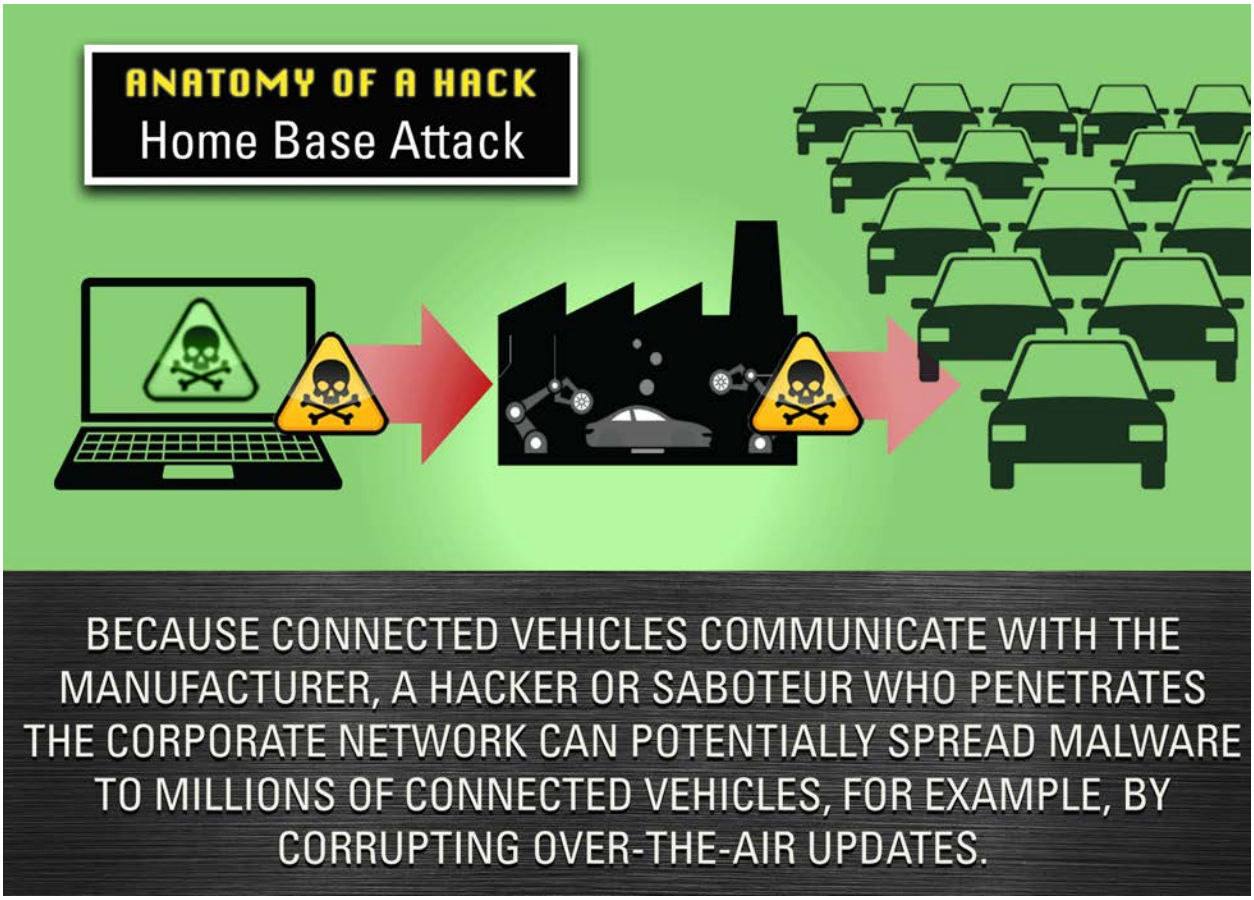
Such an attack could propagate over any number of wireless media, including cellular, wifi, or using vehicle-to-vehicle (v2v) technology, which is currently under development.



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

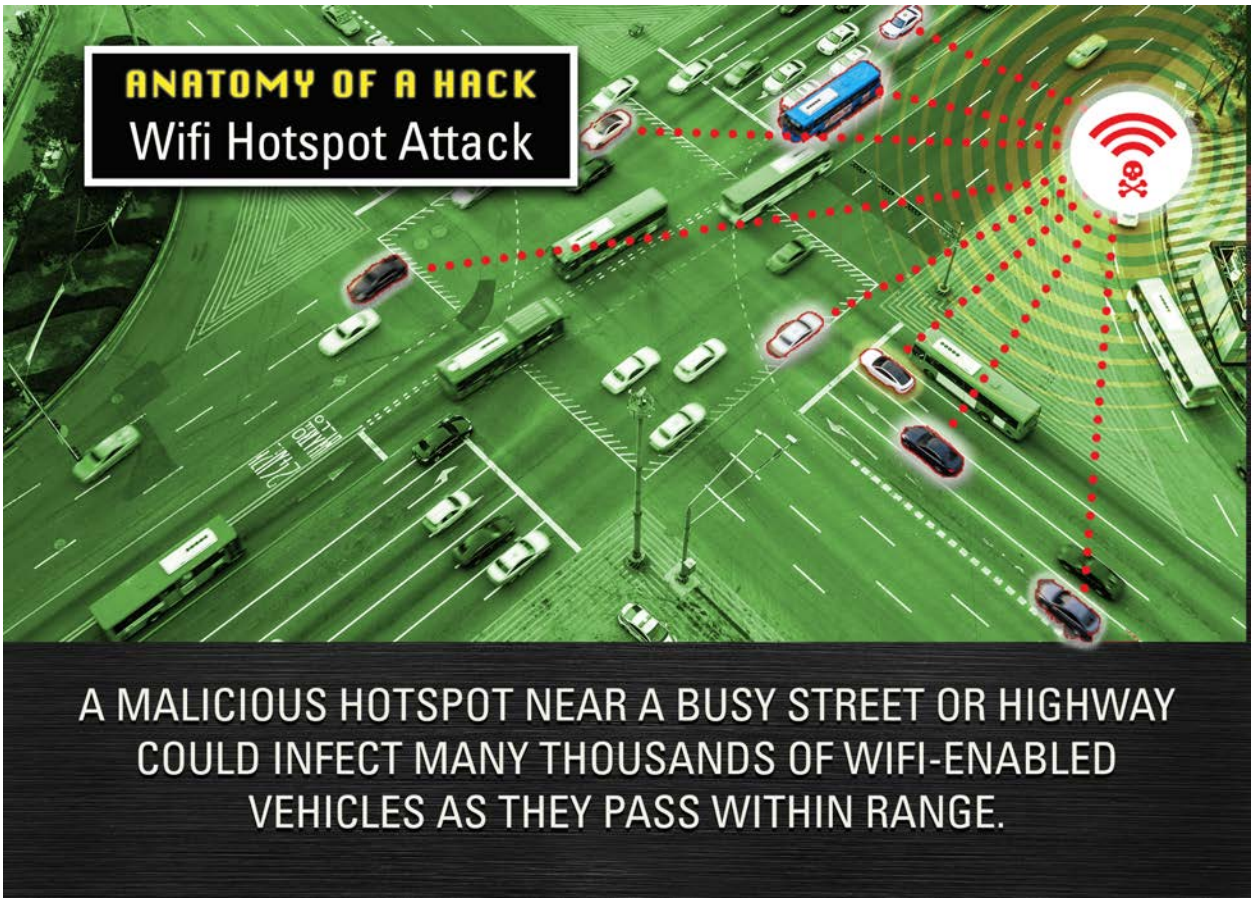
Home Base Attack

Connected vehicles exchange data with the manufacturer's computers, including software updates, which are an effective way to get malware into vehicles. This means the safety of the fleet is only as good as the security of the manufacturer's corporate servers. If the same attacks successfully carried out regularly against retailers, banks, and websites are used on automobile manufacturers, it could put the manufacturer's entire fleet in jeopardy.



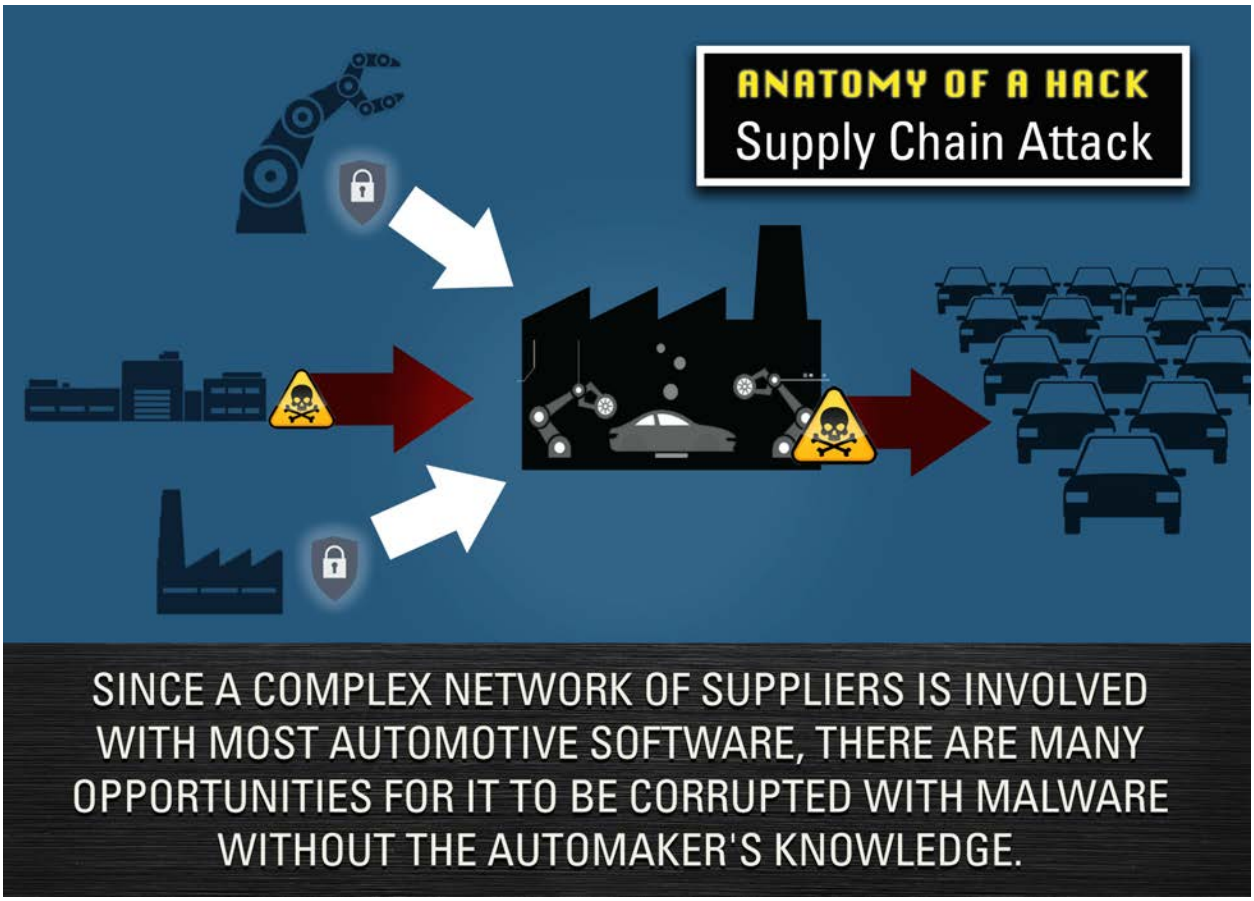
Wifi Hotspot Attack

Many connected cars are equipped with wifi, and automatically connect to nearby hotspots with familiar names. For example, if you've ever previously connected to a hotspot with the name "free-wifi," then your car will likely connect to any hotspot with the same name automatically. By setting up a malicious hotspot with a common name, a hacker may be able to get cars within range to connect to it automatically, at which point the hotspot can upload malware to the car. Such an attack could be made viral by turning the wifi in infected cars into additional malicious hotspots. As cars pass each other on the highway, malware can be transferred from car to car, much as a biological virus is transmitted from human-to-human.



Supply Chain Attack

Most cars are built from parts from manufacturers around the world, including some countries that may be hostile to the U.S. This provides ample opportunity for malicious software to enter the production process. Such malware could sit dormant until an external stimulus, such as a signal arriving over the car's Internet connection, causes it to unleash its deadly effects.

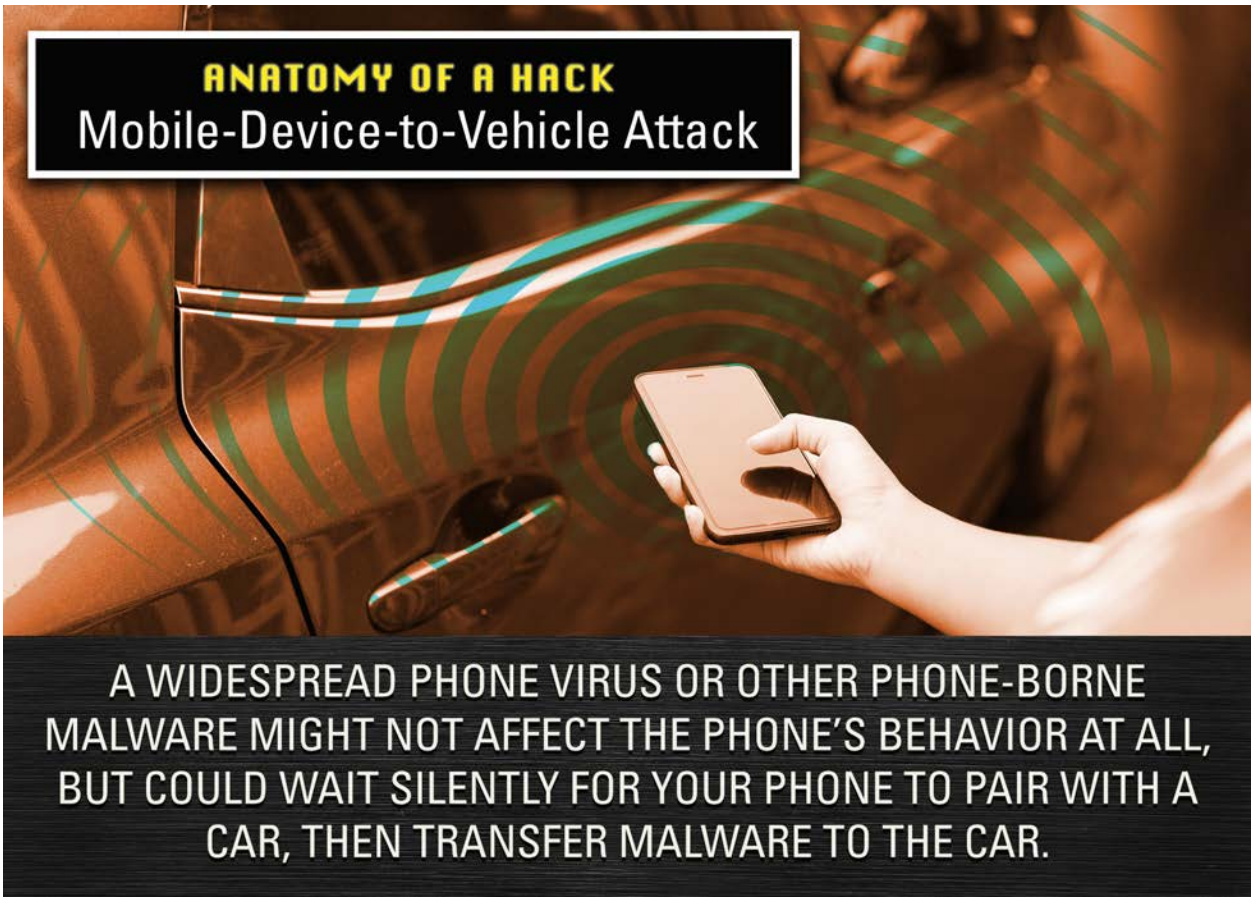


Digital Application Attack

Any digital "app" you run on your car is a potential vector for malware. Security holes in the app—whether accidental or malicious—could give attackers remote access to any vehicles with the app installed. This will become increasingly common as third-party apps in cars become commonplace. We expect this to be the natural evolution of car infotainment systems as mobile operating systems like Android are more widely deployed in cars.

Mobile-Device-to-Vehicle Attack

It has become commonplace to connect your smartphone to your car, usually by Bluetooth. This connection allows hands-free calling while you're driving, playing audio from your phone on the car's speaker system, and other conveniences. It is also a potential vector for malware. A widespread phone virus or other phone-borne malware might not affect the phone's behavior at all, but could wait silently for your phone to pair with a car, then transfer malware to the car.



Recent History of Car Hackings

In August 2019, at the annual Black Hat hacker conference in Las Vegas, a group of researchers from the Chinese company Keen Security Lab are scheduled to present technical details of vulnerabilities they discovered allowing hackers remote access to key systems in multiple BMW models.[51] BMW and other automakers want us to believe these vulnerabilities are harmless because they have now been fixed. The concern is not any individual vulnerability, but the pattern of vulnerabilities stretching back nearly a decade. This shows that, despite the auto industry's efforts and assurances, fundamental architectural problems have not been addressed, and consumers are still at risk.

"While individual bugs are being fixed, the architectural flaws allowing these dangerous exploits remain."

In 2010 and 2011, researchers from University of California, San Diego and University of Washington published a pair of papers describing the vulnerability of some vehicles to remote attack.[52] [53] The vulnerabilities remained unfixed for years. In February 2015, the attacks were demonstrated on the CBS show *60 Minutes*.

Later that year, in July 2015, two researchers, Chris Valasek and Charlie Miller, demonstrated that they could remotely attack and control a Jeep Cherokee.[54] Valasek and Miller published their methods in extensive detail.[55] Their exploit took advantage of two distinct security vulnerabilities: one allowing them remote access to the vehicle, and a second allowing remote control of the vehicle once their malicious code was "inside". The publication of their work and the surrounding media attention forced Fiat Chrysler

---

[51] "Zero days and mitigations: roadways to exploit and secure connected BMW cars" Keen Lab & BMW https://www.blackhat.com/us-19/briefings/schedule/index.html#-days--mitigations-roadways-to-exploit-and-secure-connected-bmw-cars-15313

[52] "Experimental Security Analysis of a Modern Automobile" Koscher et. All, University of Washington & UC San Diego, 2010 http://www.autosec.org/pubs/cars-oakland2010.pdf

[53] "Comprehensive Experimental Analyses of Automotive Attack Surfaces" Checkoway et al, UC San Diego & University of Washington http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[54] "Hackers Remotely Kill Jeep on the Highway" Andy Greenberg, *Wired*, July 2015: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

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

Automobiles (FCA) to recall not just the 2014 Jeep Cherokee used in the demonstration, but a broad range of models, totaling approximately 1.4 million vehicles.[56]

It is not surprising the security holes that allowed the exploit were not limited to one model. There is a strong economic incentive for automakers and their suppliers to reuse software to the greatest extent possible. The result is a monoculture that makes the fleet of cars more susceptible to cyber-attack, just as an ecological monoculture makes a biological population more susceptible to disease.

The FCA recall demonstrated that a single vulnerability can affect in excess of one million vehicles. The vulnerability that gave the researchers control of the vehicle was an architectural flaw, that would have been extremely costly for FCA to fix. Evidence suggests that it was not addressed in the recall, which only applied to vehicles with a particular version of the "Uconnect" system, the infotainment system containing the first vulnerability, through which Valasek and Miller gained access to the Jeep[57]. As one anonymous industry expert explained, "It's cheaper to use chewing gum and duct tape to plug holes than to really fix the problem."

Other vehicles that likely had the architectural flaw were not recalled, and it is very unlikely the flaw was fixed in any vehicle. As a result, a year after the recall, Valasek and Miller were still finding and demonstrating increasingly dangerous vulnerabilities.[58] In Miller's words, "There's no reason to think the bug we found and got patched last year is the only bug of its kind. There are definitely more vulnerabilities in other cars, and probably more in the Jeep, too."[59]

Recent events support Miller's assertion. Keen Security Lab demonstrated similar vulnerabilities in Tesla vehicles in 2016, and then again a year later, according to a July 2017 press release.[60] This is the same organization that will present its BMW vulnerability findings later this year.

---

[56] "After Jeep hack, Chrysler recalls 1.4 million vehicles for bug fix," Andy Greenberg, *Wired* Magazine, July 2015: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

[57] "Protect Yourt Chrysler, Dodge, or Jeep From Hacking," Linkov and Yu, *Consumer Reports*, July 2015: https://www.consumerreports.org/cro/news/2015/07/protect-your-chrysler-dodge-or-jeep-from-hacking/

[58] "Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse," Andy Greenberg, *Wired*, Aug. 2016: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[59] "Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse," Andy Greenberg, *Wired*, Aug. 2016: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[60] "New Car Hacking Research: 2017 Remote Attack Tesla Motors Again," Keen Security Lab of Tencent, July 2017: https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/

The steady pace of these demonstrations over the course of a decade is evidence that the industry is not substantially improving security. While individual bugs are being fixed, the architectural flaws allowing these dangerous exploits remain.

See the timeline below for a sampling of significant events in the recent history of car hacking.

Timeline of Notable Car Hacks

MAY 2010 — Researchers from UCSD and UW publish "Experimental Security Analysis of a Modern Automobile" in which they describe their research taking control of vehicles through their electronics. They do not identify the make of the vehicle in the paper ("We believe the risks identified in this paper arise from the architecture of the modern automobile and not simply from design decisions made by any single manufacturer. For this reason, we have chosen not to identify the particular make and model used in our tests.") However, it has since been revealed as a 2009 Chevy Impala.[61]

AUGUST 2011 — The same researchers from UCSD and UW publish "Comprehensive Experimental Analyses of Automotive Attack Surfaces" in which they extend their past work to cover remote attacks, and describe the possibility of such attacks against several makes. Their experimental research was performed on a Chevy Impala. GM did not fix the vulnerabilities until 2015.[62]

JULY 2013 — Researchers Charlie Miller and Chris Valasek demonstrate vulnerabilities in a Toyota Prius and a Ford Escape, including the ability to electronically disable the brakes. The demonstration requires physical access to the vehicle, but lays the groundwork for their later work.[63]

FEBRUARY 2015 — Remote car-hacking demonstration on CBS' "60 Minutes". The target vehicle is a Chevy Impala, attacked through its OnStar telematics system, though that was not disclosed in the video.[64]

JULY 2015 — Charlie Miller and Chris Valasek demonstrate remote takeover of an unmodified Jeep Cherokee over the Internet for *Wired* Magazine, leading to the

---

[61] http://www.autosec.org/pubs/cars-oakland2010.pdf

[62] http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[63] https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

[64] https://www.cbsnews.com/news/car-hacked-on-60-minutes/

recall of 1.4 million vehicles.[65]

JULY 2015 — At the DEF CON security conference, hacker Samy Kamkar demonstrates a small, inexpensive box he designed that allows taking control of GM vehicles.[66]

AUGUST 2015 — Kevin Mahaffey and Marc Rogers publish numerous vulnerabilities in a Tesla Model S.[67]

AUGUST 2015 — Researchers from UCSD demonstrate activating and disabling a Corvette's brakes using a common insurance company dongle.[68]

OCTOBER 2015 — Researcher Craig Smith, author of "The Car Hacker's Handbook," demonstrates a vulnerability affecting almost any make of car, in which the attack affects tools used by dealers and repair shops.[69]

MARCH 2016 — **FBI issues public service announcement warning about cyberattacks against connected cars.[70]**

AUGUST 2016 — Charlie Miller and Chris Valasek demonstrate additional, and potentially more deadly vulnerabilities in the same Jeep Cherokee they hacked a year earlier, even though it had been patched.[71]

SEPTEMBER 2016 — Keen Security Lab, a subsidiary of Chinese conglomerate Tencent, demonstrates remote takeover of a Tesla Model S, including remote control of the brakes.[72]

---

65 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

66 https://samy.pl/defcon2015/

67 https://blog.lookout.com/hacking-a-tesla

68 https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

69 https://www.wired.com/2015/10/car-hacking-tool-turns-repair-shops-malware-brothels/

70 https://www.ic3.gov/media/2016/160317.aspx

71 https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

72 https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

JULY 2017 — Keen Security Lab remotely takes over a Tesla Model X. [73]

FEBRUARY 2018 — Researchers at University of Michigan, Dearborn publish "State-of-the-Art Survey on In-Vehicle Network Communication "CAN-Bus" Security and Vulnerabilities."[74]

APRIL 2018 — Researchers Daan Keuper and Thijs Alkemade find flaws in the VW Golf GTE and Audi A3 e-tron allowing attackers to track the vehicle, listen to conversations taking place in the vehicle, and access the address book and communication history. The researchers stopped short of attempting to manipulate safety-critical systems, citing fear of prosecution under anti-hacking laws.[75]

MAY 2018 — Keen Security Lab publishes a whitepaper describing over a dozen vulnerabilities affecting BMWs.[76]

DECEMBER 2018 — Upstream, an automotive cybersecurity company, releases "Global Automotive Cybersecurity Report 2019." As of May 28, 2019, the repository of smart mobility cyberattacks on their website documented 276 cases.[77]

JANUARY 2019 — *Consumer Reports*: "As cars get more connected, the industry is trying to stay ahead of multiplying threats."[78]

FEBRUARY 2019 — Researchers Vivek, Yanni, and Yunker from Georgia Institute of Technology publish a paper in which they determine the percentage of cars that would need to be hacked to create gridlock in New York City. Their research shows that hacking cars of a single make during rush hour would probably cause a "city-wide disruption" of traffic.[79]

---

73 https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-Remote-Attack-Tesla-Motors-Again/

74 https://arxiv.org/abs/1802.01725

75 https://threatpost.com/volkswagen-cars-open-to-remote-hacking-researchers-warn/131571/

76 https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

77 https://www.upstream.auto/news/press-release-global-automotive-cybersecurity-report-2019/

78 https://www.consumerreports.org/automotive-technology/companies-target-the-next-car-hack-attack/

79 https://arxiv.org/abs/1903.00059

MARCH 2019 — Hackers Richard Zhu & Amat Cama demonstrate a security hole in a Tesla Model 3 at the annual "pwn2own" hacking competition in Vancouver, BC.[80]

MARCH 2019 — Keen Security Lab publishes a paper describing exploitation of a Model S Autopilot unit to take wireless control of the car. In the same paper, they demonstrate placing reflective stickers on the road to fool Autopilot into swerving into oncoming traffic.[81]

APRIL 2019 — Researcher Scott Gayou demonstrates breaking into the StarLink head unit, used in multiple Subaru models, including publishing details and source code online.[82]

AUGUST 2019 — Researchers from Keen Security Lab will reveal details of the vulnerabilities they found in BMWs at the annual Black Hat hacker conference in Las Vegas.[83]

Profits Over Security and Safety

One might assume that the automotive industry's unwillingness to invest in cyber-safety is the result of a failure to realize that secure software is now critical to automotive safety. While that is possible, there are other ways to explain the industry's behavior.

One possibility is that the automotive industry is in a state of Nash Equilibrium, in which all of the major automakers recognize the danger, but none has the motivation to make a unilateral change. Investing in security improvements can cause an automaker to lose ground in the marketplace, as security improvements divert valuable engineering resources away from the development of customer-visible features. If a cyber-attack occurs, while it could affect multiple models, it is likely to affect only a single vehicle make. Hardware and software is different enough from one automaker to the next that an attack affecting one make would likely be ineffective against others. Since even the most successful automaker controls less than 20% of the U.S. market, it is each automaker's

---

80 https://www.zdnet.com/article/tesla-car-hacked-at-pwn2own-contest/

81 https://www.forbes.com/sites/thomasbrewster/2019/04/01/hackers-use-little-stickers-to-trick-tesla-autopilot-into-the-wrong-lane/

82 https://hackaday.com/2019/04/16/jailbreaking-a-subaru-qnx/

83 https://www.blackhat.com/us-19/briefings/schedule/#0-days--mitigations-roadways-to-exploit-and-secure-connected-bmw-cars-15313

best strategy to wait until an attack occurs.[84] For any given automaker, such an attack would more likely than not affect part of the 80+% of the market controlled by their competitors. At that point, the government would likely impose regulations on the whole industry, without any individual automaker suffering a competitive disadvantage. Thus, it is to each automaker's advantage to avoid making any large investments towards fixing security until their hand is forced by regulation, consumer outcry, or some other external inducement.

"It is to each automaker's advantage to avoid making any large investments towards fixing security until their hand is forced by regulation, consumer outcry, or some other external inducement."

Another factor influencing automakers' adoption of connected technology is the allure of surveillance capitalism. With the auto industry concerned about layoffs and a global drop in demand for cars[85], they are understandably looking for other sources of revenue. Monetizing the information your car knows about you[86] is an obvious way to do that.

"We live in an era of constant total commercial surveillance," said Alastair Mactaggart, proponent of a ballot measure that inspired the toughest online privacy law in America—the California Consumer Privacy Act. "You need a cell phone just to survive in today's world, and yet your phone tracks you more thoroughly than any ankle monitor since your phone knows your thoughts and your interests. Your car knows how much you weigh, how often you speed, when you eat at a fast food restaurant, and how long you stay at the gym."[87]

Surveillance capitalism has made the richest and most powerful corporations in the world —Facebook, Google, Amazon—who and what they are. Carmakers, like every industry, have taken note of the money to be made from selling our private information to the

---

84 "Selected Automakers U.S. YTD Market Share in 1st quarter of 2019." *Statista*: https://www.statista.com/statistics/343162/market-share-of-major-car-manufacturers-in-the-united-states/

85 "'The pain is just beginning': After 38,000 layoffs, Wall Street wakes up to 'peak car'," Jim Edwards, *Business Insider*, Jun. 2019: https://www.businessinsider.com/peak-car-38000-layoffs-job-losses-sales-at-auto-makers-2019-5

86 "What your car knows about you," Christina Rogers, *Wall Street Journal*, Aug. 2018: https://www.wsj.com/articles/what-your-car-knows-about-you-1534564861

87 Alastair Mactaggart receiving Consumer Watchdog's Citizen Activist of the Year Award at The Rage for Justice Awards, May 18, 2019, Beverly Wilshire Hotel. https://www.youtube.com/watch?v=Ow879bRUkv4&t=18s

highest bidders. GM ran a pilot program in late 2017 in which they harvested data from 90,000 connected cars, looking for ways to monetize it.[88] In a 2018 interview, Ford CEO Jim Hackett suggested his company could make money cross-referencing what your car knows about you with auto loan data:

> *"We already know and have data on our customers. By the way, we protect this securely; they trust us. We know what people make. How do we know that? It's because they borrow money from us. And when you ask somebody what they make, we know where they work; we know if they're married. We know how long they've lived in their house, because these are all on the credit applications. We've never ever been challenged on how we use that. And that's the leverage we've got here with the data."* [89]

The desire for larger, easier profits from data-mining our cars is clear motive for automakers to connect all vehicles to the Internet in spite of the risks to consumers. The commercial value of where, when, and how we drive, and to what media we're exposed along the way is a gold mine. Car executives are well aware that the revenue associated with data collection from surveillance capitalism could exceed the margins to be made from making and selling the cars themselves.

Automakers' focus on profits also calls into question their commitment to maintaining automotive software into the future. Carmakers' solution to keeping connected cars secure is frequent software patches. Even if such an approach were effective, the average lifespan of a new car is about 11 years, and cars frequently remain in use for 20 years or more.[90] What will happen to your Internet-connected car when it no longer makes economic sense for the automaker to keep patching the software? This could result in the same "planned obsolescence" that we've seen with smartphones, PCs, and other consumer electronics. By reducing the lifespan of cars, this could boost auto sales at consumers' expense.

In 2016, Ashkan Soltani, while chief technologist for the Federal Trade Commission wrote, "If consumers are already exposed to security updates and end-of-life issues in more mature markets for routers and smartphones, one has to wonder what the security

---

[88] "GM's data mining is just the beginning of the in-car advertising blitz," Andrew Hawkins, *The Verge*, Oct 2018: https://www.theverge.com/2018/10/17/17990052/gm-radio-listen-tracking-habits-advertising-future

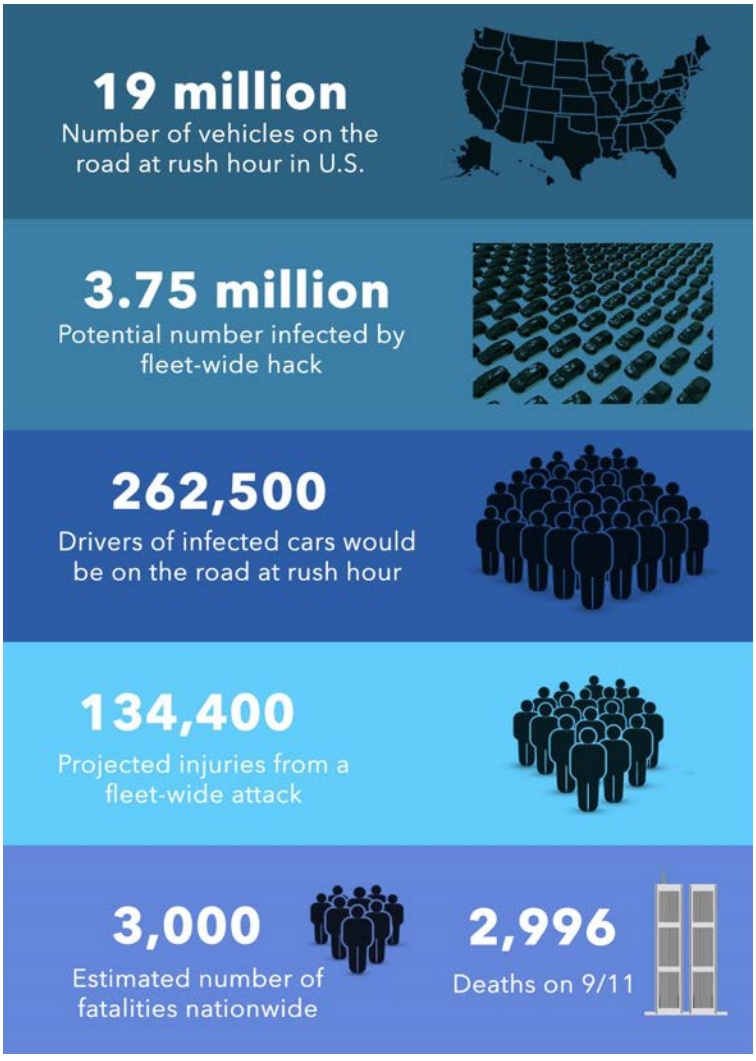
[89] "Can an Industrial Giant Become a Tech Darling? (Ep. 357)" Stephen Dubner, *Freakonomics*, Nov.2018: http://freakonomics.com/podcast/ford/

[90] "America's Cars and Trucks are Getting Older," Wolf Richter, *Business Insider*, Aug 2018 https://www.businessinsider.com/americas-cars-and-trucks-are-getting-older-2018-8

implication will be like of this new and rapidly emerging market of IoT."[91] Indeed, people will undoubtedly continue to drive connected cars after the maker stops supporting the software. Technologists contend that while it is practically impossible to secure a car manufactured today from today's hackers, it is ludicrous to expect a car manufactured today to be safe from hackers two decades from now. Without a way to disconnect the cars from the Internet, they will be vulnerable, creating a public safety risk. To date, the auto industry has not offered any viable solution to this problem.

Potential Damage from a Large-Scale Hack

Consider a hypothetical attacker who wants to cause as many casualties as possible. The attacker would most likely attempt a coordinated attack on as many vehicles as possible, to ensure a minimum of warning. Since infecting millions of vehicles simultaneously is probably not feasible, the attacker would more likely infect the vehicles over a period of weeks or months prior to the attack with malware that is programmed to activate at a specific day and time, or in response to an external signal. Such an infection could be achieved through the OTA update mechanism, using a virus or worm[92], or by any number of other means. Some vehicles may escape infection, so we will assume an 80% infection rate.



Only a fraction of infected vehicles would be on the road at

---

[91] "What's the Security Shelf Life of IoT?" Ashkan Soltani, Federal Trade Commission, Feb. 2015 https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot

[92] "Remote Exploitation of an unaltered passenger vechicle," Valasek and Miller, page 48, August 2015 http://illmatics.com/Remote%20Car%20Hacking.pdf

"It could affect the evening 'rush hour' across all four continental U.S. time zones, when the number of vehicles on the road peaks at around 19 million, or approximately 7% of the entire U.S. fleet."

any one time, so the attacker would pick a time of maximum traffic. If the attack occurred at 4pm Pacific Time on a weekday, it could affect the evening "rush hour" across all four continental U.S. time zones, when the number of vehicles on the road peaks at around 19 million, or approximately 7% of the entire U.S. fleet[93].

A hypothetical attack could disable the brakes and airbags in affected vehicles. Both are feasible once the CAN bus is compromised. Even mechanical brakes can be overridden by tricking the anti-lock mechanism into activating, or by "bleeding" the brakes while the vehicle is moving. Bleeding eliminates air bubbles from the brake hydraulics, with the side effect of making the brakes ineffective for a period. Valasek and Miller used the latter technique in their 2015 hacking demonstration.[94] A method of disabling the airbags was publicized in 2017 that is both impossible to patch and difficult for intrusion detection systems to detect.[95] The attack could also affect steering and acceleration in vehicles in which they are electronically controlled.

The attack is not guaranteed to cause an accident in every car, but might result in 80% of infected vehicles on the road involved in a collision. Statistically, in the U.S., there is one fatality per approximately 200 auto accidents.[96] Based on these numbers alone, we can expect one fatality per approximately 4500 vulnerable vehicles. While that does not sound very scary, with millions of vulnerable connected cars on the road, the death toll could feasibly be in the thousands.

Further, this estimate does not consider malicious intent. The number of fatalities could be much higher with airbags electronically disabled, and vehicles intentionally

---

93 "Summary of Travel Trends, 2009 National Household Travel Survey," U.S. Department of Transportation https://nhts.ornl.gov/2009/pub/stt.pdf (page 52)

94 "Remote Exploitation of an Unaltered Passenger Vehicle," Valasek and Miller, August 2015: http://illmatics.com/Remote%20Car%20Hacking.pdf

95 "How secure is your car? Unpatchable flaw lets attackers disable safety features," Liam Tung, *ZDnet*, Aug 2017: https://www.zdnet.com/article/how-secure-is-your-car-unpatchable-flaw-lets-attackers-disable-safety-features/

96 "Traffic Safety Facts 2016 Data," National Highway Traffic and Safety Administration, Sept 2018: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812580

manipulated to cause maximum damage. Emergency services could be overwhelmed by a large-scale attack, resulting in slower response to the critically injured.

It's hard to predict how these factors would affect the fatality rate, but it's reasonable to assume it could rise as high as 1 fatality per 1000 affected vehicles. Each of the top automakers sells around three million cars in the U.S. each year. If only one model year is affected by the hack, we can still expect about 3,000 deaths—about the same as 9/11.[97] If multiple model years are involved, which is quite possible as major model upgrades only happen every 4-6 years, the number of deaths could be several times 9/11.

The Future of Auto Safety: The Kill Switch & Beyond

The best fix is to ensure there is no electronic connection between the cellular-accessible components and the safety-critical components in the vehicles. This "air gap" method is time-tested and very effective, as no matter how buggy the software, a hacker cannot cross the air gap from the remotely-accessible components to the components that control the car's motion.[98]

In most cars, the biggest downside of such a change is that it would be impossible to OTA update the software controlling safety-critical systems. As explained above, these safety-critical software updates are better done under a mechanic's supervision anyway, and disallowing OTA updates of safety-critical systems creates an economic incentive for carmakers to engineer their software more carefully. Unfortunately, if all automakers began redesigning their cars today to air-gap the safety-critical components, it would take 4-5 years for the new, safer vehicles to show up in the showroom. This means it would take approximately 18 years before even half the vehicles on the road had the new air-gap security architecture.[99]

An even simpler, safer fix is to remove all vehicles from the cellular network until the air-gapped security architecture described above can be rolled out. There are very few features for which cars require access to the outside world, and most of them have viable (albeit sometimes less convenient) alternatives. For example, in-dash navigation systems might use a network connection to access live traffic data, but dash-mounted smartphones can provide an equivalent capability without posing an undue risk to the car's cyber-safety.

---

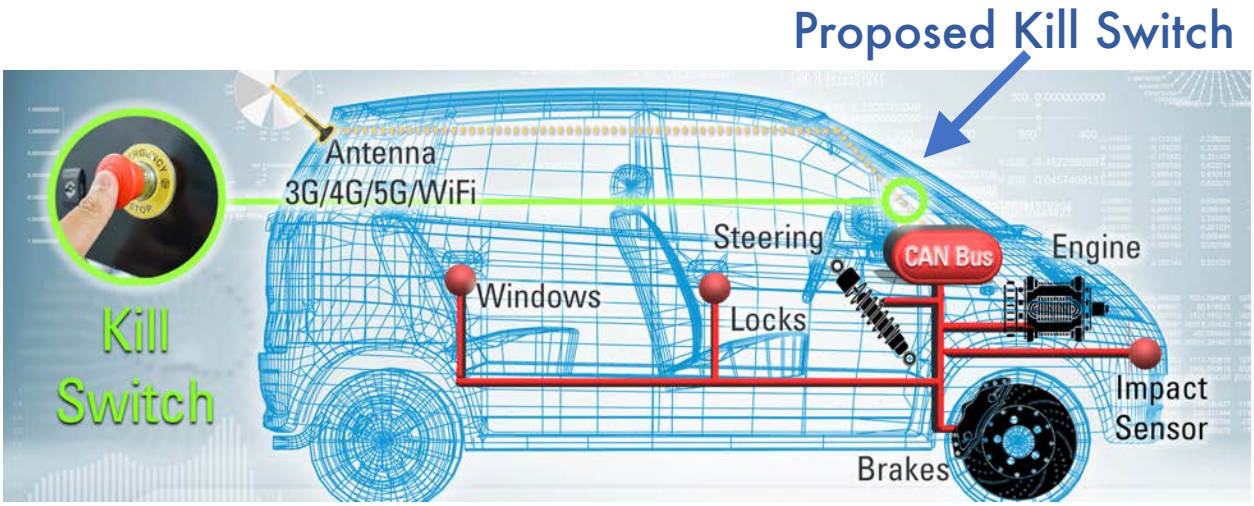
[97] "September 11 Terror Attack Fast Facts" CNN, Sept 2018: https://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/

[98] "Air Gap (Networking)" Wikipedia, https://en.wikipedia.org/wiki/Air_gap_(networking)

[99] "How long does it take for 50% of cars to comply with a new law?" *Fleetcarma*, Dec 2015 https://www.fleetcarma.com/cars-new-law-timeline/

The auto industry has existed for more than a century. Only in the last few years have we begun making cars remotely accessible via computer networks. It is therefore very unlikely that the features made possible by the "connected car" are things we cannot live without, at least until we can develop a safer way to implement them.

The most cost effective and practical approach to cybersecurity is the inclusion in every connected car of a "kill switch"—a low tech device that allows every driver to disconnect their vehicle from the Internet. The approximate cost of such a device is 50 cents or less. Automakers should commit to include a kill switch in every car they produce until they develop long term security solutions needed to combat this threat. If carmakers don't make such a commitment by the end of this year it should be mandated by Congress and safety regulators.



The greatest value of the kill switch would be to help restart the transportation infrastructure after a massive cyberattack. After 9/11, air traffic in the U.S. was shut down for several days while we implemented new security and verified that we could resume flying safely. In the aftermath of an automotive cyberattack, ensuring the safety of hundreds of millions of connected cars with "always-on" Internet connections could take months, during which time our economy and our ability to move necessities such as food across the country would be crippled. However, if cars were required to have the ability to disconnect from the Internet, we could restore our transportation infrastructure with the flip of a switch.

In addition to equipping every connected car in America with a "kill switch" that disconnects the safety-critical systems from the Internet and wide-area connections, the car industry should respond immediately with more transparency and consumer control.

If carmakers will not commit to equipping every vehicle with a kill switch by December 31, 2019, legislators and regulators should mandate these protections.

Given the auto industry's reluctance to submit to regulations and disclosure, federal and state regulators will likely have to take actions to force automakers to be transparent about their safety protocols.

In the short term, regulators should require automakers to publicly disclose the authorship, safety certifications, and testing methodology used for all safety- and security-critical software, allowing for analysis by independent regulatory and testing agencies.

CEOs of auto manufacturers should be required to sign personal statements and accept personal legal liability for the cyber-security status of their cars.

A precept that governs the industry standards should be that cars should not be connected to wide-area networks until they can be proven immune to hackers. If voluntary standards are not in the service of this imperative, then government at every level must act to insure this is the social more and legal standard that automakers live up to.

New car designs take three to five years to reach consumers. At the earliest possible implementation date, future designs should completely separate safety-critical systems from any device communicating with the Internet or other networks. Connecting safety-critical systems to the Internet is inherently dangerous design. Automakers must submit to this premise if safety on American roads is to be preeminent.

APPENDIX: Key Answers From Top Engineers

If cars are at risk, why haven't we seen reports of hackers taking control of cars "in the wild"?

Most hackers are motivated by money, and in recent years, we have indeed seen a startling rise in "electronic" car theft, usually involving keyless entry systems. Attacks that take control of a car's movement cause physical harm and property damage, but generally aren't profitable, so are less interesting to most hackers. Such attacks are mainly of interest to terrorists and hostile nation states, and, while much less common, are likely to come at large scale and without warning.

If the chance of a massive coordinated attack are low, why should we be concerned?

It only takes one large-scale attack to cost thousands of lives, disrupt our economy, and start wars. Given simple steps to prevent such an attack, it would be irresponsible not to take them. As an analogy, the chance of your home burning down may be small, but carrying homeowner's insurance is still a good idea.

Why would a hostile entity attack us through our cars? Aren't conventional weapons, such as bombs, more reliable?

An Internet-based attack has several potential advantages. Automaker "bug bounty" programs have demonstrated that vulnerabilities can be bought for a few tens of thousands of dollars, which is much cheaper than conventional weapons. Internet-based attacks also do not require physical presence on foreign soil, and can be nearly impossible to trace back to their source. A clever hacker could even make it look like a third party was responsible.

Is it possible to prove a car to be immune from cyber-attack?

The auto industry has existed for more than a century, and for most of that history, cars have been provably immune to cyber-attack because they weren't connected to the Internet. Maintaining physical separation (an "air gap") between Internet-connected components and safety-critical components is a way to allow most of the benefits of connectivity (live traffic reports, Internet-based communication and entertainment, etc.) without putting the movement of the car at risk. These are low-tech, low-cost options that work when implemented correctly.

Doesn't an Internet connection improve security by allowing manufacturers to keep our cars up-to-date with the latest security patches?

Yes, keeping software up-to-date is a good thing, and Internet connectivity makes it simpler, easier, and more reliable to do that. However, every software update you receive on your smartphone or other connected gadget means the previous version of the software wasn't finished. That's fine when novelty is more important than safety, such as on a tablet or smartphone. But when you buy a new car, do you really want the brakes operating on unfinished software?

It is the automakers' responsibility to ensure the most critical automotive software is working correctly before it leaves the factory, or else consumer safety is at risk. If critical software requires an update, the automakers' safety and quality control processes have failed. Allowing automakers to update critical software frequently, easily, and away from public and regulatory attention only serves to cover up a serious public safety hazard.