The New York Times | http://nyti.ms/1iRWBBw

BUSINESS DAY

Complex Car Software Becomes the Weak Spot Under the Hood

By DAVID GELLES, HIROKO TABUCHI and MATTHEW DOLAN SEPT. 26, 2015

Shwetak N. Patel looked over the 2013 Mercedes C300 and saw not a sporty all-wheel-drive sedan, but a bundle of technology.

There were the obvious features, like a roadside assistance service that communicates to a satellite. But Dr. Patel, a computer science professor at the University of Washington in Seattle, flipped up the hood to show the real brains of the operation: the engine control unit, a computer attached to the side of the motor that governs performance, fuel efficiency and emissions.

To most car owners, this is an impregnable black box. But to Dr. Patel, it is the entry point for the modern car tinkerer — the gateway to the code.

“If you look at all the code in this car,” Dr. Patel said, “it’s easily as much as a smartphone if not more.”

New high-end cars are among the most sophisticated machines on the planet, containing 100 million or more lines of code. Compare that with about 60 million lines of code in all of Facebook or 50 million in the Large Hadron Collider.

“Cars these days are reaching biological levels of complexity,” said Chris Gerdes, a professor of mechanical engineering at Stanford University.

The sophistication of new cars brings numerous benefits — forward-collision warning systems and automatic emergency braking that keep drivers safer are just

two examples. But with new technology comes new risks — and new opportunities for malevolence.

The unfolding scandal at Volkswagen — in which 11 million vehicles were outfitted with software that gave false emissions results — showed how a carmaker could take advantage of complex systems to flout regulations.

Carmakers and consumers are also at risk. Dr. Patel has worked with security researchers who have shown it is possible to disable a car's brakes with an infected MP3 file inserted into a car's CD player. A hacking demonstration by security researchers exposed how vulnerable new Jeep Cherokees can be. A series of software-related recalls has raised safety concerns and cost automakers millions of dollars.

Cars have become "sealed-hood entities with complicated computers and modules," said Eben Moglen, a Columbia University law professor and technologist. "All of this is deeply nontransparent. And all of this is grounds for cheating of all sorts."

The increasing reliance on code raises questions about how these hybrids of digital and mechanical engineering are being regulated. Even officials at the National Highway Traffic Safety Administration acknowledge that the agency doesn't have the capacity to scrutinize the millions of lines of code that now control automobiles.

One option for making auto software safer is to open it to public scrutiny. While this might sound counterintuitive, some experts say that if automakers were forced to open up their source code, many interested people — including coding experts and academics — could search for bugs and vulnerabilities. Automakers, not surprisingly, have resisted this idea.

"There's no requirement that anyone except the car companies looks at the code," says Philip Koopman, an associate professor at the department of electrical and computer engineering at Carnegie Mellon University. "Computers can now exert almost complete control over your car. But if that software misbehaves, there's nothing you can do."

Fear of Hacking

Andy Greenberg steered a 2014 white Jeep Cherokee down a highway in St. Louis, cruising along at 70 miles per hour. Miles away, two local hackers, Charlie Miller and Chris Valasek, sat on a leather couch at Mr. Miller's house, laptops open, ready to wreak havoc.

As Mr. Greenberg sped along, both hands on the wheel, his ride began to go awry. First, the air-conditioning began blasting. Then an image of the hackers in tracksuits appeared on the digital display screen. Rap music began blaring at full volume, and Mr. Greenberg could not adjust the sound. The windshield wipers started and cleaning fluid sprayed, obstructing his view. Finally, the engine quit.

Mr. Greenberg was on a highway with no shoulder. A big rig blew past, blaring its horn.

"I'm going to pull over," Mr. Greenberg said. " 'Cause I have PTSD."

The episode was in fact a stunt orchestrated by the hackers and Mr. Greenberg, a writer for Wired magazine, to demonstrate the Jeep's very real vulnerabilities. The article appeared on July 21.

Days later, Fiat Chrysler, the maker of Jeep, announced a recall of 1.4 million vehicles to fix the flaws the hackers had identified — the first known recall intended to address a possible hacking threat.

Though automakers say they know of no malicious hacking incidents so far, the risks are real. Stefan Savage, a computer security professor at the University of California, San Diego, said that automakers were "in a state of panic" over the prospect. "They are trying to figure out what to do, quickly," he said.

"Cars already have very complex computer systems across the board," said Elliot Garbus, vice president for transportation at Intel, the computer chip maker, which has a fast-growing autos division. "We're at the beginning of this evolution, and there's a question of how do we do a better job of securing the vehicle from cyberthreats, and those threats are significant."

Aware of the threats, most major carmakers have started to explore the idea of sharing critical information about security. General Motors last year appointed a chief product cybersecurity officer, the first automaker to create such a position.

Tesla has hired a new security chief from Google, who previously oversaw security for the Chrome web browser. And in early August, the company began offering $10,000 to outsiders who find security problems. (It had been giving $1,000.) “We are hiring!” the automaker wrote on a whiteboard at Def Con, a premier computer hackers’ conference in Las Vegas, in announcing the prize.

At the same conference, Tesla’s chief technology officer awarded the company’s commemorative “challenge coins” to two computer researchers. The researchers had revealed how to plug into the Tesla S computer system, unlock the sedan and stop the car under certain conditions — vulnerabilities that the company says are now patched.

Congress has moved to pressure automakers to more urgently address such risks. In July, Senator Edward J. Markey, Democrat of Massachusetts, and Richard Blumenthal, Democrat of Connecticut, introduced new legislation that would require cars sold in the United States to meet tough standards of protection against computer attacks.

While a future of malevolent hackers taking over steering wheels across the land still feels a bit like science fiction, more mundane issues are already turning up. Recalls over software are mounting. In July, Ford said that it would recall 432,000 Focus, C-Max and Escape vehicles because of a software bug that could keep the cars’ engines running even after drivers tried to shut them off. Ford dealers will update the software to fix the flaw, the automaker has said.

And last month, Toyota recalled 625,000 hybrid cars over a software malfunction that could bring the cars to a sudden stop; it recalled 1.9 million Prius hybrid cars last year for a similar problem.

Of course, software isn’t always the cause of flaws. One of the deadliest defects discovered in the last few years did not arise in chips or code: It was a mechanical problem with the ignition switch in some General Motors cars.

Hidden in Code

Software has made cars better. In fact, without software innovations, automakers could not meet tightening emissions standards in the United States, said Mr. Gerdes, the Stanford professor.

When a new car is stopped at a light, or in gridlock, for example, its engine might rev without prompting from the driver. That might feel like unintended acceleration to the driver, but inside what Mr. Gerdes called “the chemical plant” in your car, tightly controlled reactions are taking place. The internal emissions system has realized that the catalyst is getting cool, and if it gets cool, it won’t be as effective at reducing emissions. So the brains of the car command the engine to rev, creating hotter exhaust that keeps the catalyst warm.

And as the Volkswagen case has shown, these complexities create openings for automakers to game the system. Software in many of the German carmaker’s diesel engines was rigged to fool emissions tests. The cars equipped with the manipulated software spewed as much as 40 times the pollution allowed under the Clean Air Act during normal driving situations. Volkswagen executives admitted to officials in the United States that diesel cars sold in the country had been programmed to sense when emissions were being tested, and to turn on equipment that reduced them.

The German automaker got away with this trick for years because it was hidden in lines of code. It was only after investigations by environmental groups and independent researchers that Volkswagen’s deception came to light.

Errors in software, too, can be notoriously difficult to identify.

Jean Bookout was driving a 2005 Camry eight years ago on an Oklahoma highway when the car accelerated through an intersection and slammed into an embankment. Ms. Bookout, then 76, was injured, and her passenger, the 70-year-old Barbara Schwarz, died.

Experts who reviewed the source code for Toyota’s electronic throttle system — and testified in a lawsuit arising from the Oklahoma case — found that it contained bugs.

They also testified that Toyota had failed to follow proper coding rules and protocols. The resulting code, as one expert described it, was “spaghetti.”

An Oklahoma jury awarded $3 million in compensation to the plaintiffs. Toyota settled before the jury could consider awarding additional damages; to this day, the carmaker disputes that its electronic throttle system is flawed.

Enlisting the Public

Nat Beuse heads the office of vehicle safety research at N.H.T.S.A., the nation’s auto safety regulator. At a sprawling research lab in East Liberty, Ohio, a team of engineers from Mr. Beuse’s office are hacking into vehicles, tracking down safety defects as well as vulnerabilities that might allow an outsider to manipulate the critical functions of a car, like its brakes or steering.

It was in Ohio that the agency confirmed that a patch meant to fix the Jeep hacking would actually work. Now, N.H.T.S.A. investigators at the test facility are looking for vulnerabilities in other systems.

The agency is also testing a standard for writing code recently developed by the automakers. And it is studying whether black boxes in cars that record data, like a vehicle’s speed in a crash, can be programmed to record electronic faults.

But Mr. Beuse acknowledges that checking the millions of lines of code in automobiles is too gargantuan a task for regulators. In some cases, automakers can use two or three different versions of code in the same model year, he said.

“Whether you can actually police every little piece of software and electronics in a vehicle — I think the scope of that question is too large almost to answer,” he said. “What we’re focused on are very, very critical systems that affect safety — steering, throttle, braking and anything to do with battery systems.”

One model that N.H.T.S.A. has studied is the one now used by the Federal Aviation Administration, which regulates commercial aircraft. The F.A.A. dispatches representatives to plane manufacturers to directly oversee the software design process for the critical systems that control flying.

"They go in periodically, and say, 'Show me what you're doing and convince me that you're doing a good job — or else I'm not signing off, and it's not going in an airplane,' " Mr. Koopman of Carnegie Mellon said. "Can you tailor this so that it works for the car business? That's a question I don't have an answer for. But it's clearly an option."

If it were to carry out those inspections, N.H.T.S.A. would need skilled people. The agency estimates that it has 0.3 staff members for every 100 fatalities in automobile crashes; the F.A.A. has at its disposal over 10,000 staff members for every 100 fatalities on commercial aircraft, according to N.H.T.S.A.

"Companies are trying to use state-of-the-art software," said Mr. Gerdes of Stanford. "If you are going to attempt to regulate that, you need to have similar expertise in-house, and that can be challenging from a recruiting and compensation and talent perspective."

Given the challenges of regulating complex software, some experts are calling for automakers to put their code in the public domain, a practice that has become increasingly commonplace in the tech world. Then, they say, automakers can tap the vast skills and resources of coding and security experts everywhere to identify potential problems.

"We should be allowed to know how the things we buy work," Mr. Moglen of Columbia University said. "Let's say everybody who bought a Volkswagen were guaranteed the right to read the source code of everything in the car," he said.

"Ninety-nine percent of the buyers would never read anything. But out of the 11 million people whose car was cheating, one of them would have found it," he said. "And Volkswagen would have been caught in 2009, not 2015."

Automakers aren't buying the idea.

Fiat Chrysler's security chief, Scott G. Kunselman, told the hackers in the Jeep incident that it would be inappropriate and irresponsible for them to publish technical details about the breach because it would amount to a how-to guide for criminals to remotely attack a vehicle, according to a summary of the

correspondence provided by the company. The company declined to make Mr. Kunselman available for an interview.

Volkswagen, through its trade association, has been one of the most vocal and forceful opponents of an exemption to a copyright rule that would allow independent researchers to look at a car's source code, said Kit Walsh, staff attorney at the Electronic Frontier Foundation, a nonprofit advocacy group for user privacy and free expression.

"If copyright law were not an impediment," he said, "then we could have independent researchers go in and look at the code and find this kind of intentional wrongdoing, just as we have independent watchdogs that check vehicle safety with crash-test dummies."

"Keeping source code secret does not prevent attacks," Mr. Koopman of Carnegie Mellon said. "Either the code is vulnerable or it's not."

In the past, the Environmental Protection Agency has sided with automakers and opposed making automotive code public. There is a community of computer car tinkerers who tweak code to improve performance. The E.P.A.'s logic was that car owners might try to reprogram their cars to beat emissions rules.

The Volkswagen trickery has turned that argument on its head. The agency declined to comment on the copyright issue, and on Friday it announced it would conduct additional emissions testing on carmakers.

"Is the problem of individuals modifying their cars individually more serious than the risk of large-scale cheating by manufacturers?" said Mr. Moglen of Columbia.

Senator Blumenthal, a co-sponsor of the computer security bill, said that he would approach the E.P.A. about opening access to vehicle source code so that deceit could be prevented. Automakers "should not prevent the government or consumers from fixing their software," Mr. Blumenthal said.

"The reality is that more and more decisions, including decisions about life and death, are being made by software," Thomas Dullien, a well-known security

researcher and reverse engineer who goes by the Twitter handle Halvar Flake, said in an email. “But for the vast majority of software you interact with, you are not allowed to examine how it functions,” he said.

“The misbehavior of Volkswagen’s cars would have been easily spotted,” he said, “if someone had looked at the code.”

Nick Wingfield contributed reporting.

A version of this article appears in print on September 27, 2015, on page BU1 of the New York edition with the headline: The Weak Spot Under the Hood.
