DRIVERLESS DANGERS

Experts work to ensure autonomous vehicles are as safe from cyberattacks as they are from collisions

By Matt Alderton

THE IDEA OF CRUISING in the driver’s seat of a car that you don’t have to control is neat. But autonomous driving can also seem unnerving. Anyone whose vehicle has adaptive cruise control knows this firsthand. With the press of a button, the car assumes control. At up to 75 miles per hour, it traverses a crowded highway, automatically braking and accelerating as other vehicles enter and exit its path. As the driver, your only job is steering. And soon, you’ll relinquish even that responsibility, according to automakers like Ford and BMW, both of which plan to release fully autonomous vehicles by 2021.

Such a helpless feeling is one reason many people are skeptical of self-driving cars, according to a 2017 survey by the Massachusetts Institute of Technology (MIT), which found that nearly half of consumers (48 percent) say they’ll never purchase an autonomous vehicle. Their top reasons, MIT reported, are “loss of control” (37 percent), “I don’t trust it” (29 percent), “it will never work perfectly” (25 percent) and “it’s unsafe” (21 percent).

In reality, driverless cars may be the safest kind, according to the National Highway Traffic Safety Administration (NHTSA), which noted that human error causes 94 percent of serious car crashes. Case in point: As of December 2016, Waymo, formerly Google’s self-driving car, had driven more than 2 million miles on U.S. streets but caused only one accident; its at-fault crash rate, HuffPost reported earlier this year, is 10 times lower than that of the most experienced drivers.

The real cause for concern might not be autonomous vehicles’ safety — it might be their security. Their cybersecurity, to be exact.

“Folks need to think about cars — especially autonomous vehicles — as complex computer systems and treat them as such,” said Chase Garwood, cyber physical systems security program manager in the Homeland Security Advanced Research Projects Agency, within the Department of Homeland Security’s Science and Technology Directorate.

Government and industry are doing exactly that, he said. Ahead of their release, they’re thinking about autonomous vehicles’ vulnerabilities and working diligently to address them.

A RISKY RIDE

Understanding what makes autonomous vehicles vulnerable requires looking under the hood. There, engines cohabitate with central processing computers known as engine control units, or ECUs.

“Cars today ... are no longer just analog with a carburetor and mechanical systems,” said Garwood, whose office conducts scientific research that supports the development of commercial cybersecurity solutions. “They have onboard software that controls everything from airbag deployment, seatbelt performance and braking to entertainment systems, steering and parking.”

Unfortunately, all software has the same Achilles’ heel, whether it’s installed on a computer, smartphone or car: bugs.

“The software for premium connected and autonomous vehicles’ ECUs contains up to 60,000 bugs — including 5,000 security defects. These bugs potentially allow malicious hackers to take over the ECU, which is connected to the internet and external networks,” explained David Barzilai, co-founder and chairman of Karamba Security, an Israeli start-up that develops cybersecurity solutions for driverless vehicles. “Autonomous cars must be connected to the internet, to other cars and to infrastructure in order to enable complete autonomy. Each of those communication channels represents an

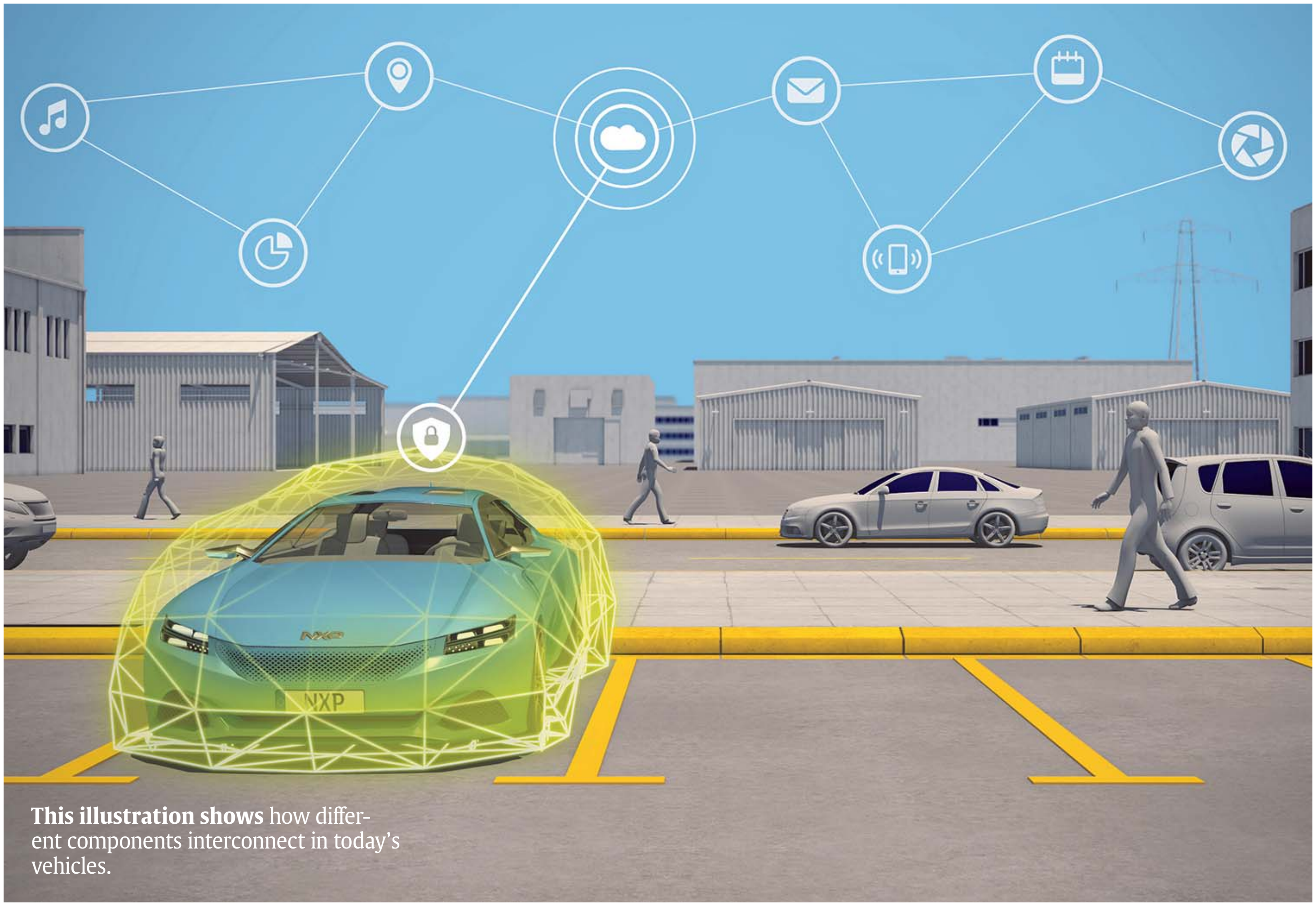
CONTINUED »

Waymo's self-driving cars, including a Chrysler Pacifica Hybrid minivan, left, and the Firefly, right, feature a panel of controls for riders to operate the vehicles.

WAYMO

Uber is testing self-driving vehicles in San Francisco, Pittsburgh and Tempe, Ariz.

GETTY IMAGES; UBER



This illustration shows how different components interconnect in today's vehicles.

NXP

attack surface through which hackers can infiltrate the car and take control."

In 2015, researchers Charlie Miller and Chris Valasek demonstrated that capability when they hacked the internet-connected entertainment system of a Jeep Cherokee to bring it to a standstill on a St. Louis highway. Fiat Chrysler subsequently recalled 1.4 million Cherokees, all of which shared the same security vulnerability.

"One of the big concerns is that you can potentially take control of not just one vehicle, but, in theory, hundreds, thousands or maybe even millions of vehicles at once," said Charles Covel, senior analyst in the Office of Cyber and Infrastructure Analysis (OCIA), within DHS's National Protection and Programs Directorate.

In August, OCIA published an analysis of the national security risks posed by autonomous vehicles and concluded that hackers could not only seize control of self-driving cars — and potentially weaponize them by causing fatal collisions — but also use them to violate privacy and steal data.

"If connections aren't secure, somebody who is able to access your vehicle can also access all your personal information," Covel said.

> "Rather than having a big open network, you now have isolated domains and a context-aware firewall ... that controls which information can flow from one domain into another. "
>
> **— Timo van Roermund**

BOTTOM–UP SECURITY

Before dismissing autonomous driving as ominous driving, one should know that self-driving cars are being designed to withstand their inherent risks. Like cruise control and air conditioning, cybersecurity comes standard.

"Autonomous vehicles are some of the most secure vehicles around because of what's at stake," said Hudson Thrift, security operations lead at Uber, which is currently testing autonomous driving in San Francisco, Pittsburgh and Tempe, Ariz. "We're building these things from the ground up with security in mind."

To understand the benefits of a ground-up design, consider BlackBerry. Although its popularity has plummeted, its mobile phones have long set the standard for security, according to CEO John Chen.

"Have you ever heard of a BlackBerry being hacked?" he asked. "The answer is no, and the reason for that is the way we build our devices."

With the same layered-security approach it uses with its devices in mind, BlackBerry is pivoting from smartphones to autonomous vehicles. It's hoping manufacturers will power their products with QNX, an operating system for automotive infotainment systems that BlackBerry acquired in 2010 and is currently modifying for use in driverless cars.

Starting at the foundation with a security system also makes it easier to segregate threats, which limits their impact.

"If you look at the majority of new vehicles, there's a change in the vehicle network architecture," said Timo van Roermund, security architect at NXP Semiconductors, which supplies computer chips to the automotive industry. "Rather than having a big open network, you now have isolated domains and a context-aware firewall, or filter, that controls which information can flow from one domain into another."

Simply put: A threat that enters an autonomous vehicle through its infotainment system is contained there.

TEAMWORK YIELDS TRUST

Ultimately, security hinges as much on teamwork as technology.

"The automotive industry traditionally has been rather closed, but that's starting to change," said van Roermund, who noted that in the past, automakers have been reluctant to share knowledge for fear of losing their intellectual property. With cybersecurity, however, there's a recognition that automakers are better off united than divided. Manufacturers are therefore establishing groups like the Automotive Information Sharing and Analysis Center, a consortium of global automakers and suppliers whose purpose is enhancing cybersecurity awareness and collaboration.

"The top companies in this space get together and we talk about what we're doing and how we can help one another," said Uber's Thrift, who chairs the Technical Steering Committee for Future of Automotive Security Technology Research, a similar group established in 2016 by Aeris, Intel and Uber. "One of us being bad at security doesn't help the others; we're all better off if we're all better at security."

Government has a role, too. Along with DHS, those studying autonomous vehicle security include the U.S. Department of Transportation and Congress, both chambers of which have introduced legislation requiring automakers to create and execute a written plan for detecting and responding to cyberattacks. Although the House passed its bill in September, the Senate is still mulling its version.

Meanwhile, automakers are keenly focused on developing driverless cars that are simultaneously high-tech and high-trust."Autonomous features have huge safety advantages that are hopefully going to save a lot of lives," Garwood said. "By talking about the risks, we're trying to be preventive instead of reactive."