Are Your Customers' Cars Safe From Hackers?

Imagine your favorite customer is in her brand new, networked vehicle and suddenly, it comes to a halt in the middle of an intersection. She looks around and notices all the other cars around her have stopped and can't start back up again. Guess what? She and her fellow motorists are part of a cyberattack.

That fictional scenario hasn't happened, but that doesn't mean it can't or won't. As the complexity of vehicles has been ratcheted up due to ever-increasing technological enhancements and innovation, so has the risk a hacker could acquire control of the various functions and systems of your vehicle — or your customers' vehicles.

This was demonstrated convincingly in 2014 when two hackers, Chris Valasek and Charlie Miller, remotely disabled a Jeep Cherokee driving at 70 miles per hour on a major highway, outside of St. Louis. The driver, Andy Greenberg, wrote about the experience for *Wired*. The article made auto industry professionals and others sit up and take notice about the potential of cyberattacks on drivers and their vehicles.

"There is definitely a risk," said Daniel Miessler, director of advisory services for security service firm, IOActive. "It was our research that led to the *WIRED* article. The hack [Chris] and Charlie performed was done remotely over the internet, which made it significant."

Miessler explained the complexity of systems in today's vehicles leads to vulnerabilities.

"As our cars continue to increase in terms of complexity due to technological advances and innovation, the risk becomes greater," Miessler said.

With each step up in terms of networked capabilities, cross-car communication and the ability to functionally interact with other devices, so increases the risk someone with less than benign intentions can take control of a vehicle's various systems.

Actually, this was demonstrated convincingly prior to higher profile media examples, as far back as 2011. That's when academic researchers at the University of Washington and the University of California at San Diego wirelessly took control of a car's braking system and its steering via remote attacks. They were also able to gain access to the vehicle's cellular communications, the Wi-Fi network and even the Bluetooth connection to an Android phone. You know how much more complex cars have become over the past five years; you've been the one servicing them.

"Cars have become, essentially, computers on wheels," said Kathleen Fisher, a Tufts University computer science professor and security researcher. "At the same time, car companies still see themselves in a more traditional sense as engineering and production-driven, when in essence, they've really become technology companies."

While safety has become an industry watchword and standard across the board, driving a great deal of the technological innovation found in newer models, Fisher sees the need for the auto industry to do a lot more in terms of making sure their cars are cybersafe. At the same time, Fisher is not certain the industry is capable of carrying that responsibility alone.

"The margins are pretty tight for auto manufacturers. Additionally, with increased complexity, the investment to ensure security continues to grow," Fisher said.

So, does the role of cybersecurity end up with government or even an industry coalition? Could companies pass some of the costs off to consumers by way of offering a premium for advanced safety features relative to preventing an attack?

There's also the issue of the Internet. Today's connected cars will be one of the key elements in the ecosystem called the Internet of Things. As cars become ever more connected to the Internet, collecting and making sense of massive amounts of data from an array of sources — basically, cars talking to other cars, exchanging data and alerting drivers to potential collisions — this makes them particularly vulnerable to the relative insecurity of the Internet itself. That insecurity makes it difficult to add effective safety measures on the back-end. Those previous flaws compound issues of cybersecurity related to automobiles that are increasingly connected to the web.

Does that mean your customers are now at the mercy of hacktivists, hackers, hobbyists and state actors bent on our destruction? Not necessarily. Actually, Miessler said he's optimistic the issue can be and is being addressed by the auto industry itself. He noted General Motors hired its first product cybersecurity chief in 2014, recognizing the need to be proactive in response to rising levels of technological complexity in the vehicles it manufactures.

On the government side, the National Highway Traffic Safety Administration has asked car makers to develop a common way to share information about efforts to hack vehicle data systems.

Miessler sees auto manufacturers pushing cybersecurity in terms of marketing, much the way they've promoted safety in vehicles across the board.

"Since safety is the driving force with so much of the industry, they could offer up their vehicles as being cybersecurity-certified, maybe based on an industry standard or a government mandate," Miessler said.

Miessler said he believes cybersecure-certified cars could realistically happen within the next couple of years.

"It's possible we'll be looking at cars with this security stamp (or something like it) as soon as the 2019 model year," Miessler said.

That doesn't mean we're home free in terms of safety from attacks upon vehicles and their drivers. There's still a great deal that needs to be done in terms of hardening vehicles against malicious intent, or simply the desire for hackers to put a notch or two on their belt — proving they could remotely take control of a vehicle, or something worse. In fact, Miessler doesn't think damage and disruption have to take on the Hollywood-style script of mayhem and death to be effective from a hacker's perspective.

"You could have 4 million cars slowly come to a stop without colliding and not be able to start up again. If this happened in a couple of major American cities, can you imagine the monetary cost of the disruption," Miessler questioned.

While vehicle security may be distinct from vehicle safety in some ways, vehicle security is essential to delivering vehicle safety. Some of the same organizational disciplines that led to safe and reliable cars also apply to security. Security must be part of the design phase, along with safety and reliability. To ensure a secure design, threat models could be created, anticipating different kinds of threats, while seeking to eliminate, or at the very least, mitigate them.

Automakers also need to consider creating a secure system for disseminating over-the-air updates, much like we have with our smartphones and other consumer and business electronics. With proper controls and safety precautions, these are vital to updating systems quickly whenever there's a breach or any vulnerability is discovered. This will also help in reducing the cost of recalls.

Hackers are more sophisticated and often part of criminal or nation-state groups with significant skills and funding. In addition, specifications for most chips and operating systems are readily available on the Internet, due to increased technology standardization and proliferation.

"There are resources all over the internet for hackers," Fisher said. "Once someone figures out how to hack a system, the information is out there for others to access and use."

Whether the catalyst is industry itself, or involves a collaboration between automakers, government and security firms, hardening vehicles against cyberattacks needs to become a priority. In much the same way that vehicle owners have come to trust the auto industry to manufacture vehicles that are functionally safe and structurally sound, technological innovation now demands cybersecurity becomes a front-burner issue, especially in terms of ensuring consumers remain confident their vehicles won't be unnecessarily vulnerable to being hacked.

Next time you see a customer with a connected car, you may have a new subject to discuss — vehicle cybersecurity.