Why you should keep your car keys in metal coffee can (& a metal lid)

By Phoebe Wall Howard
Detroit Free Press

Top cybersecurity experts would never hang car keys on a hook near the back door or leave them sitting on a kitchen counter. The best strategy to prevent theft? Store the key fob in an old-fashioned metal coffee can.

"Really, some cyber experts don't go to sleep without putting their key into a metal container," said Moshe Shlisel, a veteran of the Israeli Air Force and now CEO of GuardKnox Cyber Technologies. "It's called a Faraday Cage. You block the electromagnetic field."

Copying code from vehicle key fobs is easy. Tech thieves can do it from outside your home or a motel. Then they can steal a vehicle or just gain access without owners realizing they've been violated.

Cybersecurity companies, including the team at GuardKnox, are working with the Detroit Three and automakers globally to create protections that deter hackers who covet new cars and the data stored in them.

Within the past 90 days, GuardKnox has been granted three U.S. patents including a "Communication Lockdown Methodology" that prevents attackers from entering a vehicle's ecosystem. The patent covers trucks, buses, ships, planes, drones and even spaceships. The methodology has been implemented in fighter jets and missile defense systems.

"Vulnerability is everywhere. The fob is a symptom," Shlisel said in a phone interview from his office just south of Tel Aviv. "You're exposed to many attack vectors. Remember your computer 20 years ago? There weren't firewalls. What happens if someone takes control of your car while you're on the highway with two kids inside and you can't do anything? You're doomed. And that can be done today."

This is not sci-fi. This is real life. This is the reality of a wireless, connected world where car doors lock with a click and a chirp, where children in the backseat stream videos, where back-up cameras make parking easy, where driver assist prevents accidents and companies can update software technology remotely.

"Connectivity introduces cyber risk," said Faye Francy, executive director of the non-profit Automotive Information Sharing and Analysis Center, which specializes in cybersecurity strategies.

While auto industry engineers know a lot about traditional safety, quality, compliance and reliability challenges, cyber is an "adaptive adversary," she said.

"It's an ever-changing, emerging threat that requires diligence in every aspect of design through operations – it's not a simple engineering fix," Francy said. "And as we move into smart cities and autonomy, the interconnectedness provides greater efficiencies and safety but also introduces potential risk into the broader global ecosystem."

Needed: A cyber-Club

Remember the heavy steel devices _

continues on pp 2

Read below column last

Meanwhile, Ford puts out the most news releases in the mobility industry relating to smart cities and connected vehicles. It is a favorite topic for CEO Jim Hackett.

While Ford spokeswoman Karen Hampton didn't offer specifics on cybersecurity, she did say the company takes security and data privacy very seriously. "We will continue to evolve our processes and policies to ensure transparency, security and privacy as we expand our offering of connected products and services that improve our customers' lives and the communities in which we operate."

Meanwhile, Fiat Chrysler and Tesla pointed to their bounty programs that help identify and reduce cybersecurity threats.

A Tesla spokesperson said, "We have staffers dedicated to constantly stress-testing, validating and updating our safeguards. They focus on this daily. Meaning, we don't put the onus solely on bounty program participants to identify threats, but they are important in helping Tesla ensure we are always safeguarding our products."

Cybersecurity experts said they often have at least two vehicles, one that's older and one that offers the luxuries of cameras and new technology "because it's safer."

Read above last

End of pp 2

some called them Kryptonite Clubs _ that drivers attached to their steering wheels back in the 1980s and '90s? Well, now industry must find this on their networks to protect against hackers.

"Today we're in an interconnected society, from our computer to our phones to our cars to our homes. We need Kryptonite bars on the network," Francy said. "Automakers are starting to implement security features in every stage of design and manufacturing. This includes the key fob. Cybersecurity diligence is the cost of doing business in the digital age today."

In 2015, the Detroit Three and 11 other automakers formed the group that shares, tracks and analyzes potential cyber threats, vulnerabilities and incidents related to the connected vehicle in North America, Europe and Asia. One company's detection of a potential attack may mean another company's prevention of a security breach, Francy noted.

Shlisel, whose board of directors includes executives who served on the board at GM, said digital firewalls are essential. "If you don't have a mechanism that can protect his communication from someone replicating them, then it's a no-brainer. Companies sell things legitimately on Amazon to clone transmission from a vehicle. This is called 'the man in the middle attack' or 'the relay attack.'"

So while consumers love the convenience that connectivity offers and are willing to pay more for enhanced technology, connectivity has a price.

"People call it the internet of things or, as I like to say, 'The internet of threats,'" Francy said. "You can't read the newspaper without reading about another cyberattack."

Companies that specialize in hacking protection won't reveal how frequently they're able to hack vehicles or how easily. Said one cybersecurity researcher, "Our job isn't to embarrass the industry." Some automakers said they didn't want to discuss the topic for fear of being perceived as challenging hackers.

Vehicles with easy remote access definitely offer benefits.

In 2017, Tesla remotely and temporarily enhanced the battery capacity, and therefore driving range, of its Tesla vehicles for owners in Florida who were trying to escape Hurricane Irma.

But too often, these tactics can be used for evil, industry observers say.

Real and growing threat

Dan Sahar, vice president of product for Upstream, a cybersecurity startup based in Silicon Valley, said the risk of a widespread cyberattacks on vehicles is real and growing.

Vehicles are vulnerable in part because of the complexity of the software, with hundreds of millions of lines of code, said Sahar, whose company focuses on cybersecurity for the cloud, watching for and stopping anomalies.

With so many lines of code, bugs are bound to exist, he said, and "if there's a bug, the hacker can utilize the bug."

But it's not clear how quickly, or even if, the public would learn about a mass hack on a group of vehicles.

"Some companies don't ever admit it. You know Uber got hacked. When did you learn about it? You learned about it (more than a year) after it happened," Sahar said.

"In that case, hackers stole the data of 57 million Uber users. Rather than report the incident, Uber paid the hackers $100,000 to delete the stolen data and keep it secret."

The consequences of a cyberattack on moving vehicles are especially frightening.

The most famous, or infamous, incident involved a Jeep Cherokee in 2015. Hackers were able to interfere with the Jeep as it drove on a St. Louis-area highway in traffic. The cybersecurity researchers were able to disable the car's transmission and brakes, and, while the vehicle was in reverse, take over the steering wheel.

That incident damaged the reputation of Fiat Chrysler Automobiles, though it was not the only company hurt; the connection that allowed the hack in the first place came through a cellular network, Sahar said, noting that because automakers rely on so many suppliers, many more potential vulnerabilities exist.

Of course, the Jeep hack is just one example.

In 2017, Chinese security researchers had hacked a Tesla Model X for the second time, "turning on the brakes remotely and getting the doors and trunk to open and close while blinking the lights in time to music streamed from the car's radio," according to USA TODAY.

In response to inquiries from the Free Press, a number of automakers including the Detroit Three acknowledged ongoing efforts to address cybersecurity.

As vehicle connectivity continues to evolve, GM continues to strengthen cybersecurity protections, said spokesman Tom Wilkinson. "GM's three-pillar approach employs defense-in-depth, monitoring and detection, and incident response capabilities to protect our customers, their vehicles, and their data."

Fiat Chrysler, which established a bug bounty program in 2016, emphasized it has a group dedicated to preventing, detecting and responding to cybersecurity risks. The company "is deploying both hardware and software technologies to protect against cyberintrusions," and partnering with others, said Sandra Hosler, senior manager of vehicle cyber security.

Last column is on page one