How vulnerable is your car to cyberattacks?

December 17 2019

The emergence of smart cars has opened the door to limitless possibilities for technology and innovation -- but also to threats beyond the car itself. Credit: Free via Px Here: pxhere.com/en/photo/655303

The emergence of smart cars has opened the door to limitless possibilities for technology and innovation—but also to threats beyond the car itself. New research from Michigan State University is the first

to apply criminal justice theory to smart vehicles, revealing cracks in the current system leading to potential cyber risks.

"Automotive cybersecurity is an area we don't understand well in the social sciences. While there are groups of computer scientists and engineers digging into some of the issues, the social aspects are extremely relevant and under-examined," said Thomas Holt, professor of criminal justice at MSU. "As the technology gets greater market share, it's critical to get ahead of the curve before there are issues we can't rein in."

As vehicles become smarter and more connected to WiFi networks, hackers will have more opportunities to breach vehicle systems. Connecting your smartphone through a USB port can give a hacker backdoor access to data from both your phone and your car. Additionally, Google Android users who can download apps from unverified sites are even more at-risk.

The research, published in the *Journal of Crime and Justice* applied Routine Activities Theory, used a popular criminal justice framework, to current forms of vehicle security and provided recommendations for manufacturers and owners to improve safety.

"The risk with vehicles isn't just personal data—though that is still a real concern," Holt said. "Say the car is compromised and a hacker alters certain alert systems that tell a driver when tire pressure is low or so the emergency brake sensory systems don't kick in. That could lead to loss of life."

The theory Holt applied says that in order for a criminal to act three things need to come together: a motivated offender, a suitable target and a lack of guardian. In the context of vehicle security, he said that motivators and targets are clear, but the presence of a guardian was

where vehicles fell short.

"Where we found holes was surprising: there's no one technically responsible for these vehicles' central computer systems," Holt said. "The automotive and equipment manufacturers need to recognize that as it stands, they serve as the guardians in the space, and the onus is on them. They need to take the lead in thinking more critically about data flows, software vendors and how to communicate security with dealerships."

Holt explained that in a traditional automotive context, an equipment failure would lead to a recall of the vehicle to fix the problem. However, cyber security is entirely different.

"It's critical to think beyond thresholds and recalls because cybersecurity isn't a recoverable problem, but rather one that requires constant system patching updates, installations and new codes written," Holt said. "This is more complicated but needs to be an active guardian process."

Similar to how smart phone manufacturers release security updates, the only way to disrupt the current problem is to have guardians that are consistently, actively updating system software.

"Not everyone updates their smartphones when they're supposed to, but customers need to realize that to a certain extent, manufacturers can only do so much. The customer must have a role in protecting their cars as well," Holt said. "We can't expect every vehicle owner to go to a dealership every time there's a security update. But once the guardians find a way to make it more accessible, they'll be the ones responsible for protecting their vehicles—and themselves."

Holt says that it won't be long before all vehicles have smart capabilities. He fears that it will take too many tragic stories of accidents or breaches

to get people to act.

"We need to improve the presence of software guardians and better resources; we also need to think about developing policies to protect users, vehicles and customers," Holt said. "There are real benefits to smart cars and autonomous features, but we need to get ahead of the risks before those benefits are lost."

More information: Jay Kennedy et al. Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking, *Journal of Crime and Justice* (2019). DOI: 10.1080/0735648X.2019.1692425

Provided by Michigan State University

Citation: How vulnerable is your car to cyberattacks? (2019, December 17) retrieved 23 April 2024 from https://techxplore.com/news/2019-12-vulnerable-car-cyberattacks.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.