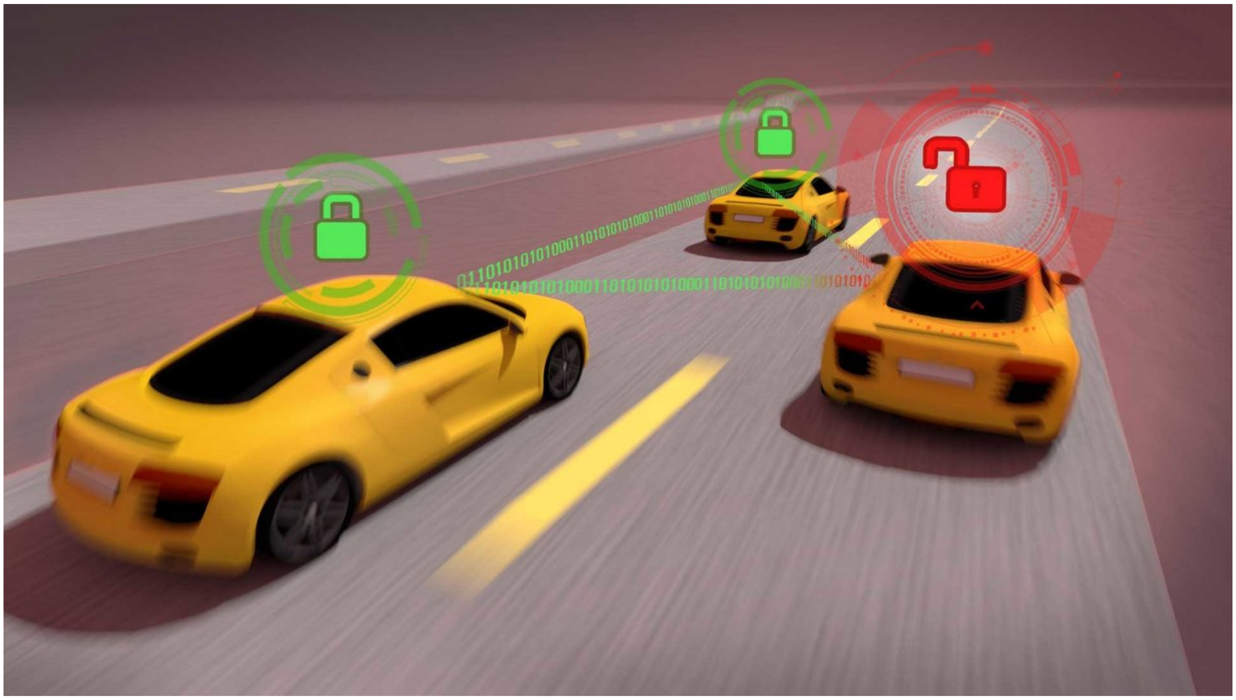
PHYS.ORG

Threat identification tool for cybersecurity in self-driving cars

January 5 2018, by Susan Carney



While every new generation of auto tech brings new security risks, the vulnerabilities that come along with advanced mobility are both unprecedented and under-studied, new research from the University of Michigan shows. A new white paper could help academic and industry researchers analyze the likelihood and severity of potential cyberthreats to autonomous and connected vehicles. Credit: Steve Alvey, Michigan Engineering

Instead of taking you home from work, your self-driving car delivers you to a desolate road, where it pulls off on the shoulder and stops.

You call your vehicle to pick you up from a store and instead you get a text message: Send $100 worth of Bitcoin to this account and it'll be right over.

You buckle your seatbelt and set your destination to a doctor's appointment, but your car won't leave your driveway. It senses it's been hacked and your home is its pre-programmed safe destination.

These three hypothetical scenarios—posited in a new white paper by University of Michigan researchers working with Mcity—illustrate the breadth of the cybersecurity challenges that must be overcome before autonomous and connected vehicles can be widely adopted. While every new generation of auto tech brings new security risks, the vulnerabilities that come along with advanced mobility are both unprecedented and under-studied, the paper states.

The white paper introduces a tool called the Mcity Threat Identification Model, which could help academic and industry researchers analyze the likelihood and severity of potential threats. The new model outlines a framework for considering: the attacker's skill level and motivation; the vulnerable vehicle system components; the ways in which an attack could be achieved; and the repercussions, including for privacy, safety and financial loss.

The tool is believed to be the first of its kind focused on automated vehicles. Mcity, led by U-M, is the nation's largest public-private partnership working to advance connected and automated mobility.

Understanding the threats

"Cybersecurity is an overlooked area of research in the development of autonomous vehicles," said Andre Weimerskirch, lead author of the paper, who leads Mcity's cybersecurity working group and is also vice president of cybersecurity for Lear Corp. "Our tool marks not only an important early step in solving these problems, but also presents a blueprint to effectively identify and analyze cybersecurity threats and create effective approaches to make autonomous vehicle systems safe and secure."

Connected and automated vehicles are what researchers call a cyber-physical system, with components in the "real" and virtual worlds. The safety stakes are as high as these systems are hard to protect. Connected and automated vehicles will face familiar threats, and new ones, the report describes.

They will be vulnerable to those that regularly disrupt computer networks, like data thieves of personal and financial information, spoofers who present incorrect information to a vehicle, and denial-of-service attacks that move from shutting down computers to shutting down cars.

In addition, new threats unique to automated vehicles themselves emerge—hackers who would take control over or shut-down a vehicle, criminals who could ransom a vehicle or its passengers, and thieves who direct a self-driving car to relocate itself to the local chop-shop, for example.

Finally, there are security threats to the wide-ranging networks that will connect with autonomous vehicles—the financial networks that process tolls and parking payments, the roadway sensors, cameras and traffic signals, the electricity grid, and even our personal home networks.

"It might seem convenient for an autonomous car that gets within 15 minutes of your home to automatically turn on your furnace or air conditioner, open the garage and unlock your front door," the researchers write. "But any hacker who can breach that vehicle system would be able to walk right in and burglarize your home."

The new threat identification model

To demonstrate the insights the new model can provide, the researchers used it to examine vulnerabilities in automated parking—both parking assist technology and the more advanced remote, self-parking. They determined that the most likely attacks are: a mechanic disabling the range sensors in park-assist or remote parking in order to require additional maintenance, and an expert hacker sending a false signal to your vehicle's receiver to turn off remote parking. Both received sixes on the researchers' 10-point scale, with 0 being lowest probability.

At the same time, the type of attack that would have the most impact would be a knowledgeable thief spoofing your remote parking signal in order to steal your car. This type of attack received a 7 on the researchers' scale of impact.

"Without robust, fool-proof cybersecurity for autonomous vehicles, systems and infrastructure, a viable, mass market for these vehicles simply won't come into being," said Huei Peng, Mcity director and the Roger L. McCarthy Professor of Mechanical Engineering. "Funding this kind of research is a critical part of Mcity's mission to help break down barriers to widespread deployment of connected and automated vehicle technology."

The white paper is titled "Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles." The thread model is also detailed in a paper, "Risk Assessment for Cooperative Automated Driving," published in the Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy.

More information: "Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles." mcity.umich.edu/wp-content/upl … er_cybersecurity.pdf

"Risk Assessment for Cooperative Automated Driving," dl.acm.org/citation.cfm?id=2994499

Provided by University of Michigan

Citation: Threat identification tool for cybersecurity in self-driving cars (2018, January 5) retrieved 25 April 2024 from https://phys.org/news/2018-01-threat-identification-tool-cybersecurity-self-driving.html