Researchers create framework to stop cyber attacks on internet-connected cars

May 29 2018

Credit: CC0 Public Domain

A new study by Maanak Gupta, doctoral candidate at The University of Texas at San Antonio, and Ravi Sandhu, Lutcher Brown Endowed Professor of computer science and founding executive director of the

UTSA Institute for Cyber Security (ICS), examines the cybersecurity risks for new generations of smart which includes both autonomous and internet connected cars.

"Driverless and connected cars are increasingly becoming a part of our world, where cybersecurity threats are already a reality," Sandhu said. "It's imperative that we support research that addresses these concerns and presents a strong, innovative solution."

Cars with internet connectivity, also known as "connected cars," offer potential for many conveniences and innovations. They could allow for real-time and location-sensitive communication between drivers or even pedestrians, which could help make the roads safer for both. The connectivity could also allow the cars to capture safety and environmental conditions around the vehicle, including road obstructions, accidents, which also enables real-time vehicle-to-vehicle interaction on road.

"Connected cars have almost infinite possibilities for creative technological applications," Gupta said. "Companies could even take advantage of the connectivity to implement location-based marketing tactics, providing drivers with nearby sales and offers."

However, the researchers caution that as soon as cars are exposed to internet supported functionality, they are also open to the same cybersecurity threats that loom over other electronic devices, such as computers and cell phones. For this reason, Gupta and Sandhu created an authorization framework for connected cars which provides a conceptual overview of various access control decision and enforcement points needed for dynamic and short-lived interaction in smart cars ecosystem.

"There are vulnerabilities in every machine," said Gupta. "We're working to make sure someone doesn't take advantage of those

vulnerabilities and turn them into threats. The questions of 'who do I trust?' and 'how do I trust?' are still to be answered in smart cars."

Gupta and Sandhu framework discussed an access control oriented architecture for connected cars and proposed authorization framework, which is a key to determine what and where vulnerabilities can be exploited. They further discuss several approaches to mitigate cyber threats in this ecosystem.

Using this framework, the team at ICS is trying to create and use security authorization policies in different access control decision points to prevent cyber attacks and unauthorized access to sensors and data in smart cars.

"There are infinite opportunities in this new IoT domain but at the same time cyber threats will have serious implications in smart cars. Can you imagine if someone controls your car steering remotely, or shuts down the engine in the middle of the road?" Gupta said. "There should not be absolutely any open end to orchestrate attacks on these cars."

According to Gupta, the authorization framework can also be applied to driverless cars, noting that these vehicles may be even more vulnerable to cyber threats.

"If we're going to open the world to cars driven by machines, we must be absolutely certain that they aren't able to be compromised by a malicious attack," he said. "That it what this framework is for."

More information: Paper: DOI: 10.1145/3205977.3205994

Provided by University of Texas at San Antonio