CyLab researchers discover novel class of vehicle cyberattacks

8 June 2021, by Daniel Tkacik

Credit: CC0 Public Domain

Vehicles are becoming more and more connected to the Internet, and malicious hackers are licking their lips.

A team led by Carnegie Mellon University CyLab researchers have discovered a new class of cybersecurity vulnerabilities in modern day vehicles. If exploited, an attacker could sneak past a vehicle's intrusion detection system (IDS) and shut down various components, including the engine, by executing some crafty computer code from a remote location. No hardware manipulations nor physical access to the vehicle are necessary.

The new class of vulnerabilities was disclosed in a new study presented at last month's IEEE Symposium on Security & Privacy, held virtually.

"In response to the first generation of automotive attacks, new guidelines urge automakers to build an IDS into their next vehicles. As they do, they need to consider these more advanced attack strategies," says CyLab's Sekar Kulandaivel, a Ph.D. student in Electrical and Computer Engineering and lead author of the study. "It's not as simple as pushing a software update. To really defend yourself against this type of attack, you have to update the hardware."

The team confirmed the feasibility of the vulnerabilities by launching proof-of-concept attacks on them in two vehicles: a 2009 Toyota Prius and a 2017 Ford Focus. The researchers posit that many modern cars are likely vulnerable to these kinds of attacks, but an attacker would have to compromise the vehicle's network first before launching these types of attacks.

"Without compromise of additional elements, this particular example cannot be used to directly attack current commercial vehicles," says Shalabh Jain, senior research scientist at Bosch Research and a co-author on the study. "However, this class of vulnerabilities can provide new directions for lateral movement in a larger attack chain."

The "lateral movement" that Jain mentions refers to the fact that once an attacker has control over a particular component in the vehicle, they could then impact the operations of another component while undetected.

The new class of vulnerabilities stem from some architectural choices that automakers have made—such as energy-saving modifications—in recent years. Essentially, most modern car functions are controlled by one or more ECUs or Electronic Control Units. To reduce the amount of power the ECUs consume, designers implemented a feature called "peripheral clock gating" into vehicles' microcontrollers which enables ECUs that aren't actively being used to shut down to conserve energy.

"We uncovered a new attack strategy that could turn off this signal," says Kulandaivel. "Eventually we were able to craft raw data onto the vehicle's network and shut down any ECU we wanted."

While some of these shutdown attacks were shown in prior work, they required either physical access to cars or hardware modifications or can be easily detected. The novel part of the attack here is that it can be launched remotely, without requiring hardware modifications, and it bypasses several state-of-art defenses.

This points out a larger issue: a systemic problem in how vehicles are designed.

"Security hasn't been a real threat yet to automakers, so they're focusing on cost reduction," says Kulandaivel. "The automotive world is decades behind personal computer security."

Moving forward, study co-author Jorge Guajardo, lead expert and senior manager for Bosch Research's Security and Privacy Group, says that automakers need to encourage more work like this.

"Automakers need to continue to proactively investigate attacks and in fact encourage this type of adversarial, white-hat research which is possible in collaboration with academic partners such as CMU," says Guajardo. "Also, they need to develop security solutions that have been carefully analyzed and vetted by the security community."

More information: CANnon: Reliable and Stealthy Remote Shutdown Attacks via Unaltered Automotive Microcontrollers: users.ece.cmu.edu/~vsekar/asse … oakland21_cannon.pdf

Provided by Carnegie Mellon University