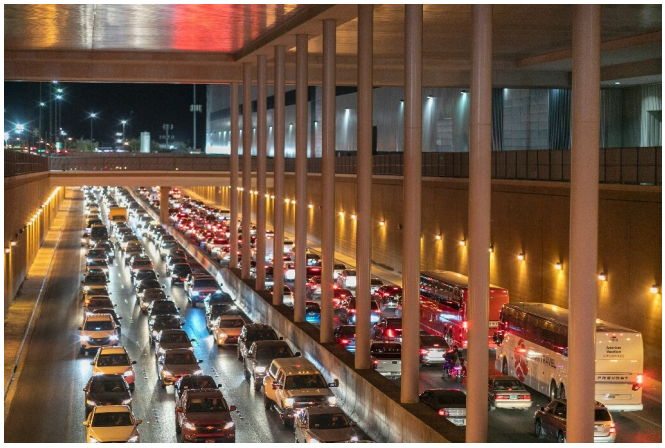
Connected cars moving targets for hackers

10 January 2020, by Julie Jammot



Traffic becomes heavy as people leave the 2020 Consumer Electronics Show (CES) in Las Vegas, Nevada

As cars evolve into rolling mobile computers, the potential for disastrous cyber attacks has become a new road hazard.

Israeli cybersecurity firm GuardKnox demonstrated the threat in a Formula 1 driving simulation at the Consumer Electronics show this week in Las Vegas.

Moments into the virtual drive, a GuardKnox engineer playing the role of hacker struck and the steering wheel no longer controlled the speeding car.

The faux race was over for the driver, stuck on the side of the road in a scenario that cybersecurity specialists say could become very real.

New car models are packed with computer chips, sensors and mobile technology that hackers could exploit to sabotage systems or commandeer controls.

Opportunities for attacks are being revved up by the trend of self-driving, electric cars communicating in real-time with the cloud, smart city infrastructures, and one another.

GuardKnox chief executive Moshe Shlisel gave an example of a hacker remotely taking control of a fuel tanker truck, sending it to crash into a building.

"It's September 11 on wheels," Shlisel said in an interview at CES.

Cybersecurity has become as integral to vehicle engineering as crash safety and fuel efficiency, according to Henry Bzeih, a former member of the Council for Automobile Cybersecurity, who spoke at the Las Vegas event.

"Connectivity is the reason why this is happening," Bzeih said.

"Now, all elements have to be designed with cybersecurity in mind."

'Anything is possible'

Israeli startup Upstream logged more than 150 cybersecurity incidents involving automobiles last year, twice as many as in 2018.

The majority of those hacks involve remotely car door locks, but an increasing number targeted software applications or connections to the cloud.

Last year in Chicago, dozens of luxury cars were stolen by hacking Daimler's Car2Go app.

"The ultimate worst-case scenario would be if somebody applies one of the car functions when it's not supposed to do that, and does that across multiple vehicles," said Upstream vice president Dan Sahar.

"For example, someone hits the brakes on all vehicles of a specific model at the same time. That would be catastrophic."

Since cars in model lines share engineering

specifications, they share system vulnerabilities by design.

"If you can design an attack and execute it on a computer, and that computer is attached to a car, anything is possible," said Ralph Echemendia, expert in cybersecurity and self-described "ethical hacker."

Five years ago, a pair of cybersecurity researches remotely commandeered the controls of a Jeep Cherokee by taking advantage of a vulnerability in its infotainment system, triggering a recall of vehicles.

Never-ending battle

Carmakers have responded to the menace by offering bounties for vulnerabilities found by researchers and paying partners to build security into components.

Upstream collects data shared to the cloud by vehicles, scouring it in real time for strange activity that could signal hackers are up to no good.

GuardKnox engineers drew on their experience in the Israeli air force to design a processor that protects computers in vehicles and also serves as a secure operating system.

As in the world of smartphones and desktop computing, hackers relentlessly seek ways to infiltrate new software or features in automobiles in an ever-escalating battle with defenders.