No autonomous cars without cybersecurity

12 December 2017

Autonomous cars aim to reduce traffic congestion and optimize the flow of vehicles. But in an environment where cars will constantly be connected to their neighbors and to infrastructures, these vehicles' autonomy will be dependent on their cybersecurity.

-
-
-

-
- Save

Protecting cars from cyber-attacks is an increasingly important concern in developing smart vehicles. As these vehicles become more complex, the number of potential hacks and constraints on protection algorithms is growing. Following the example of the “Connected cars and cybersecurity” chair launched by Télécom ParisTech on October 5, research is being carried out to address this problem. Scientists intend to take on these challenges, which are crucial to the development of autonomous cars.

Connected cars already exist. From smartphones connected to the dashboard, to computer-aided maintenance operations, cars are packed with communicating embedded systems. And yet, they still seem to be a long way from the futuristic vehicles we’ve been dreaming up in our imagination. They do not (yet) all communicate with one another or with road infrastructures to provide warnings about dangerous situations for example. Cars are struggling to make the leap from “connected” to “intelligent”. And without intelligence, they will never become autonomous. Guillaume Duc, a research professor in electronics at Télécom ParisTech who specializes in embedded systems, perfectly sums up one of the hurdles to this development, “*Autonomous cars will not exist until we are able to guarantee that cyber-attacks will not put a smart vehicle, its passengers or its environment in danger*.”

Cybersecurity for connected cars is indeed crucial to their development. Whether rightly or wrongly, no authority will authorize the sale of increasingly intelligent vehicles without first guaranteeing that they will not be out of control on the roads. The topic is of such importance in the industry that researchers and manufacturers have teamed up to find solutions. A “Connected Cars and Cybersecurity” chair bringing together Télécom ParisTech, Fondation Mines-Télécom, Renault, Thalès, Nokia, Valéo and

Wavestone was launched on October 5. According to Guillaume Duc, the specific features of connected cars make this is a unique research topic.

"*The security objectives are obviously the same as in many other systems*," he says, pointing to the problems of information confidentiality or certifying that information has really been sent by one sensor instead of another. "*But cars have a growing number of components, sensors, actuators and communication interfaces, making them easier to hack*," he goes on to say. The more devices there are in a car, the more communication points it has with the outside world. And it is precisely these entry points which are the most vulnerable. However, these are not necessarily the instruments that first come to mind, like radio terminals or 4G.

Certain tire pressure sensors use wireless communication to display a possible flat tire on the dashboard. But wireless communication means that without an authentication system to ensure that the received information has truly been sent by this sensor, anyone can pretend to be this sensor from outside the car. And if you think sending incorrect information about tire pressure seems insignificant, think again. "*If the central computer expects a value of between 0 and 10 from the sensor and you send it a negative number, for example, you have no idea how it will react*," explains the researcher. This could crash the computer, potentially leading to more serious problems for the car's controls.

Adapting cybersecurity mechanisms for cars

The stakes are high for research on how to protect each of these communicating elements. These components have only limited computing power while algorithms to protect against attacks usually require high computing power. "*One of the chair's aims is to successfully adapt algorithms to guarantee security while requiring less computer resources*," says Guillaume Duc. This challenge goes hand in hand with another one, limiting latency in the car's execution of critical decisions. Adding algorithms to embedded systems leads to increased computing time when an action is transmitted. But cars cannot afford to take longer to brake. Researchers therefore have their work cut out for them.

In order to address these challenges, they are looking to the avionics sector, which has been facing problems associated with the proliferation of sensors for years. But unlike planes, fleets of cars are not operated in an ultra-controlled environment. And in contrast to aircraft pilots, drivers are masters of their own cars and may handle them as they like. Cars are also serviced less regularly. It is therefore crucial to guarantee that cybersecurity tools installed in cars cannot be altered by their owners' tinkering.

And since absolute security does not exist and "*algorithms may eventually be broken, whether due to unforeseen vulnerabilities or improved attack techniques*," as the researcher explains, these algorithms must also be agile, meaning that they can be adapted, upgraded and improved without automakers having to recall an entire series of cars.

Resilience when faced with an attack

But if absolute security does not exist, where does this leave the 100% security guarantee against attacks, which is the critical factor in developing autonomous cars? In reality, researchers do not seek to protect against all possible attacks on connected cars. Their goal rather to ensure that even if an attack is successful, it will not prevent the driver or the car itself from remaining safe. And of course, this must be possible without having to brake suddenly on the highway.

To reach these objectives, researchers are using their expertise to develop resilience in embedded systems. The problem recalls that of critical infrastructures, such as nuclear power plants, which cannot simply shut down when under attack. In the case of cars, a malicious intrusion in the system must first be detected when it occurs. To do so, the vehicle's behavior is constantly compared to previously-recorded behaviors which are considered normal. If an action is suspicious, it is identified as such. In the event of a real attack, it is crucial to guarantee that the car's main functions (steering, brakes etc.) will be maintained and isolated from the rest of the system.

Ensuring a car's resilience from its design phase, resilience by design, is also the most important condition for cars to continually become more autonomous. Automakers can provide valuable insight for researchers in this area, by contributing to discussions about a solution's technical acceptability or weighing in on economic issues. While it is clear that autonomous cars cannot exist without security, it is equally clear that they will not be rolled out if the cost of security makes them too expensive to find a market.