Security in Connected Cars

Imagination's Marc Canel, Vice President of Security, talks to New Electronics about connected vehicle security

Having recently joined Imagination to head up its security efforts, Marc Canel, VP of Security, spoke with New Electronics to discuss why, as more cars become connected and are fast turning into 'computers on wheels', the issues of security and privacy are now taking centre stage.

"There have been multiple advances in connected cars, and we will see more progress in the years to come as the driving experience changes even more," said Canel. "The car has moved from being a standalone device with limited electronics to a system that has Bluetooth, Wi-Fi and cellular connectivity. Most cars now integrate a GPS receiver and a satellite radio and with Apple CarPlay and Android Auto, the smartphone has become an integral part of the automotive experience."

According to Canel the smartphone is not just an 'adjunct device' that people have with them.

"It's fully integrated into the driving experience, with entertainment and navigation functions and it has its own independent communications capabilities. Multiple systems in the car have self-diagnostic functions that report their status over-the-air to a cloud-based operator, while some cars are able to automatically report an accident."

The advent of 5G will also bring in advanced autonomous driving functions with its very high speed and low latency capabilities and, as a result, the connectivity systems of the car will play an active role in vehicle to vehicle and vehicle to infrastructure communications.

"5G will become the fundamental enabler of autonomous driving," suggested Canel.

But, as cars become more connected, what new security issues does this introduce?

The more connections a car manages the greater the attack surface. The greater the number of applications processors and cyber tasks performed by the car, the more opportunities for weaknesses and vulnerabilities. The car is made up of multiple systems that cooperate in a network for the operations of the vehicle. Millions of lines of code are executed in a car and multiple connectivity systems interface with the outside world.

"Security issues range from basic safety problems such as the one demonstrated in the Jeep hack of 2015, to loss of privacy with smartphone applications tracking the activities and location of the user, to theft of the car through an interface," explained Canel. "As vehicles become autonomous, the security challenges increase with safety considerations, theft of the vehicle, privacy and theft of entertainment and guidance content."

Privacy issues

How about privacy issues - what should users be aware of?

"Loss of privacy can come from multiple angles. Location with built-in navigation systems, that have connectivity beyond a GPS receiver, could become vulnerable to sophisticated hackers. Upcoming systems in cars will track the user, their skills at operating the car, how they respects road laws, their level of attention and alertness, even a driver's mood.

"Regulators in some countries are looking into the automatic detection of alcohol consumption. All this information is personal data that can be legitimately used by the car system for safety purposes, or by insurance companies to offer discounts to good drivers and safe drivers.

"Cars will integrate payment systems for highways, entertainment content, traffic information, guidance systems as services on demand gain in popularity. Identity and payment materials on the users will all be available in the car," said Canel.

Private materials in a car can certainly be the object of attacks but at the same time, given the importance of the transportation industry and its intersection with other services such as payment, it is expected that regulators will define the framework for privacy of data.

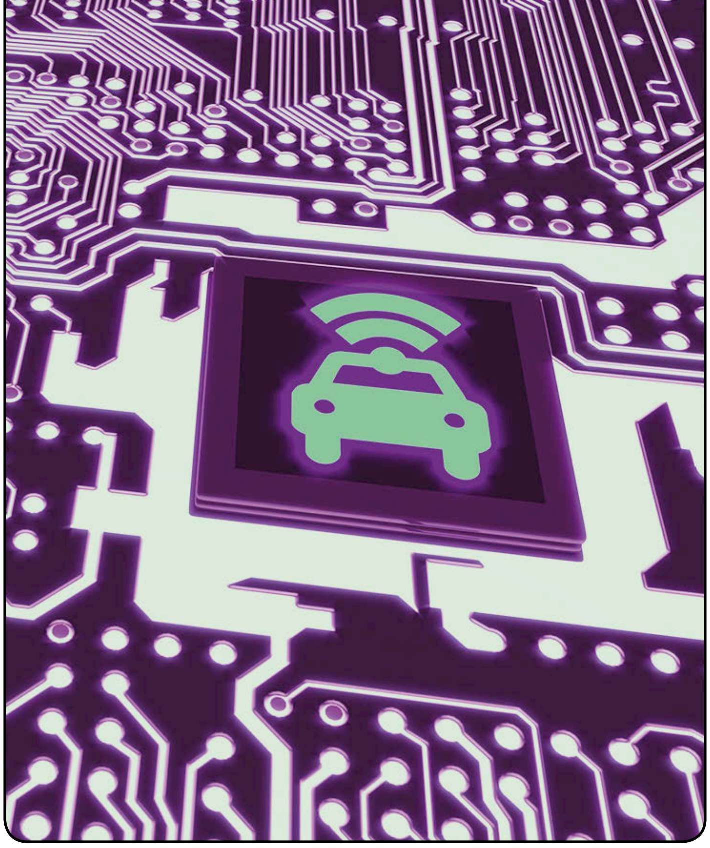
"Personal information that is closely tied to the user or to regulated services, such as payments, will have to be protected with levels of robustness that will be defined in legislation," explained Canel.

In this increasingly connected world, how will GDPR affect the automotive sector?

"The automotive sector will be very much the object of GDPR. Driving skills, driving patterns, location information, payment and entertainment choices are all information that represent the profile of an individual. This information is protected by GDPR regulations. The usage of some of the information by services providers such as insurance companies and others will be regulated. The data will have to be protected by the actors that use it and its analysis will have to be accepted by the user."

When it comes to manufacturers how are they dealing with these issues? What aren't they doing that you think they perhaps should be?

"Manufacturers will adjust their products and how they handle the metadata generated by the products on a local basis. As described earlier, privacy regulations play an important role in how personal



MARC CANEL

Marc Canel has extensive experience in both the IoT and mobile markets and at Imagination Technologies he is now working on the next generation of security architectures. Prior to joining Imagination, he drove Arm's security strategy for IoT security systems. He was also VP of software and security systems at Qualcomm, where he also worked on software ecosystem management. Before joining Qualcomm he worked at IBM for 12 years, where he held various product development and management roles in data networking products.

data gets protected and processed. Manufacturers will create architectures that meet the requirements of the local regulators, region by region, country by country.

"Some services will require loss of privacy and they will require a trade-off that the user will have to decide upon. For example, letting the insurer adjusts rates based upon driving patterns, behaviour and location may be an acceptable trade-off for some people.

"In other situations, the car will send metadata about its operations at the engine level. This will be very useful information to the manufacturer to prevent failures and warn the user of necessary maintenance."

One security issue is the risk when a car is sold and the new driver is able to access all of the same apps the previous owner used.

"The risk, in this case, is no different than when loaning a smartphone to a stranger. The seller of the car will need to go through a hard reset of all his applications and private data.

"Manufacturers should offer hard reset functions, removing the applications and the private data of a user when a car is being transferred from one individual to the next."

The impact of 5G

What will be the implications on privacy and security when autonomous vehicles with 5G capability become more mainstream?

"I expect that 5G will create opportunities for the car industry, most notably in the area of autonomous driving systems. 5G delivers the high-speed communications and the low latency that cars will need to operate as autonomous entities on busy roads.

"Whereas a car today is an anonymous entity in a large fleet of vehicles on a highway, cars with autonomous systems that take advantage of 5G will broadcast information about themselves to other cars and to the infrastructure. The car is no longer an anonymous entity, it operates as a living and moving entity within a network and it is connected to its neighbours and the infrastructure. In other cars, the car will always be tracked. Its precise location is an information in the system. It is correct that today, a driver can be tracked by smartphone, but there is always the possibility of shutting the phone off and escaping its tracking capabilities," according to Canel. "This will not be possible in an autonomous car as it will be required to broadcast its location at all times. Communications with the car through the 5G network, either for navigation purposes or other functions, will have to be protected by fast and robust cryptography and session level protocols between applications."

As for the future of connected cars and the role privacy will play in their development, Canel said that regulators will need to play a role in defining privacy frameworks.

"To a certain extent, they already do when they set up rules for payment data, privacy rules around the tracking of users watching entertainment content, the protection and usage of regulated airwaves. The car industry will inherit some of these, but new rules will be needed to protect the information on the usage of the vehicle when it comes to autonomous driving systems."