Who is responsible for securing the connected car?

The number of intelligent cars on the road is growing. In the event of a cyber attack on a vehicle, who is responsible – the driver, the manufacturer or the suppliers of car parts?

As vehicles get smarter, cybersecurity in the automotive industry is a growing concern for vehicle manufacturers, OEMs and drivers. The array of technology embedded into connected and autonomous vehicles (CAVs) promises accident prevention, safer driving, lower emissions and an enhanced driver experience. However, this enabling technology also creates a growing attack surface that allows hackers to exploit vulnerabilities to access car systems, where drivers' personal information and their physical safety could be compromised. Attackers no longer need physical access to a vehicle to take control, and the industry now has to focus efforts on more than just the physical security of the vehicle.

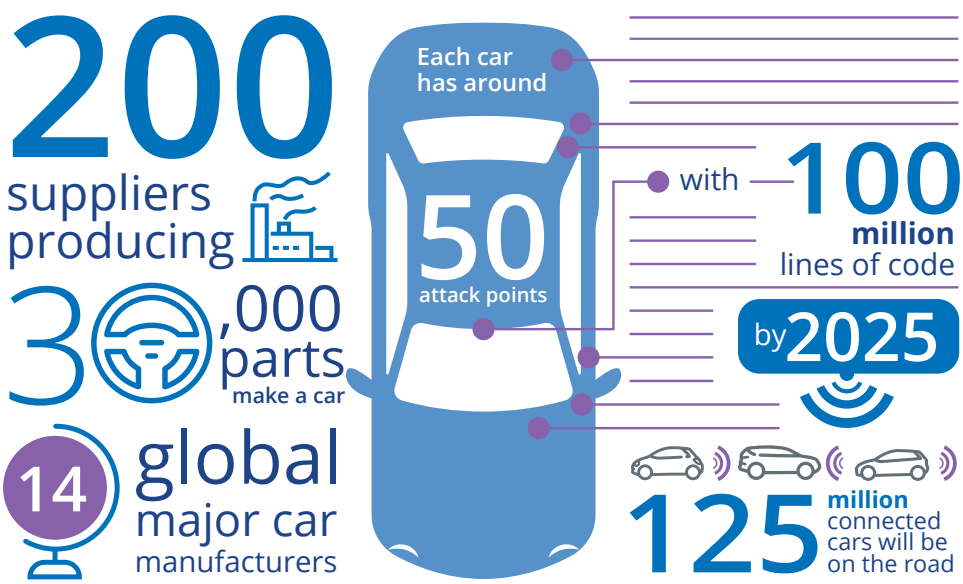
Connected insurance

As vehicles become increasingly connected, manufacturers will need to work harder to convince drivers that connected and autonomous vehicles are safe to drive and difficult to hack. And insurance companies will need similar reassurances if they are to underwrite policies for CAVs.

For insurers, a huge advantage of driverless vehicles in particular, is road safety, and the insurance industry is preparing itself for the day when the majority of vehicles on the road will be autonomous. There's a long transition period however, where mixed fleets of driven and driverless cars will be sharing the roads, and in some countries, the UK for example, the Automated and Electric Vehicles Act 2018 legislates that all vehicles on public roads must be fully insured, with or without a driver. If there's an accident, the legislation ensures that the compensation route for the individual is via the insurer, rather than via a product liability complaint against the manufacturer. This ensures that victims all have access to compensation, but the legislation also highlights that an insurer involved in any claim would have the right to make a subsequent claim against the manufacturer if the car was the cause of the accident. That sounds simple enough, but there are still significant issues around liability and manufacturers will be keen to ensure that vehicle owners are

52% of organizations globally believe that transport networks could be vulnerable to cybercriminals.
Risk:Value

Figure 1 The connected car supply chain is complex and insurance companies need to know who is responsible for security – the supplier, the manufacturer or the driver



obligated to prove they have continuously undated the vehicle's software.

The issue that is challenging insurance companies more, is the safety of CAVs with respect to cybercrime. We've seen numerous high-profile hacks of cars in recent years, resulting in safety recalls and reputational damage for the manufacturers. Insurance providers now need to understand and prepare for a new range of risks such as ransomware, where a hacker could disable a car unless a ransom was paid by the driver; or malicious attempts to take over the controls of a car to cause damage to the vehicle, the driver or other road users.

Who though will reassure the insurance industry that a car is secure? Is it possible to underwrite policies when there is little historical data? And who is ultimately responsible for securing a car against cyber attack – the manufacturer, suppliers of component parts, or the driver himself?

"Cyber insurance for cars will be growing market, but there are still many security complexities and challenges across the entire supply chain."

Kai Grunwitz, NTT Security

Car or computer?

Both connected and autonomous vehicles rely on millions of lines of code – over 100 million lines in fact – which is more than a commercial aircraft, a fighter jet and Facebook combined. Add this to over 30,000 component parts, 30-100 electronic control units (ECUs) and around 25 gigabytes of data created every hour by a connected car, and we can see that today's car is a sophisticated computer than needs securing, patching and updating regularly.

It's inevitable therefore that cars will increasingly become the target of attacks, and when that happens who will the insurer hold responsible for the breach?

Security by design

Insurance providers will look first to the manufacturer to ensure that the car is secure, and that might mean a closer look at the risk profile of the organization, its production plants and the design of the car itself. Today's production plants operate in an Industry 4.0 environment, where growing levels of connectivity increase the risk of cyber attacks and the opportunity therefore to damage the integrity of the end product. And Society 5.0 is now on the horizon with a vision for a fully connected society. But it's the security of the connected car itself that would likely become the battleground between the insurance company and the manufacturer, in the event of an insurance claim. It is here that a hacker could infiltrate the car's network and gain access to the ECUs that control every aspect of the car from the radio to the brakes and steering.

The automotive industry has a unique set of challenges: connected cars are highly complex and impossible to produce with some vulnerabilities; the supply chain is highly fragmented with hundreds of suppliers each producing component parts and ECUs to their own standards and patch specifications; and even if the individual component is robust, poor integration can lead to vulnerabilities.

Insurers will likely want to look at the design stage of the car where security should be embedded into the design of each hardware and software component. Adding security fixes on top of an unsecure product will never create a secure car, only add complexity and vulnerability. It's the responsibility therefore of the manufacturer to develop strategic solutions to the ongoing challenge of cybersecurity, and to design the vehicle with security in mind.

Insurers may also insist that vehicles are eventually all monitored by Vehicle Security Operation Centers (V-SOCs), where vehicle data is continuously transmitted back to a V-SOC for live monitoring and analysis. Here, it could be established if an attack is taking place, and for remedial action to be taken swiftly. Again, it would be the responsibility of the manufacturer to design such an infrastructure.

A sum of its parts

The manufacturer however will look to its supplier ecosystem to share the responsibility for security. Traditionally, the manufacturer will specify exactly what they expect the suppliers to produce, but they will only vaguely specify cybersecurity requirements and are unlikely to mandate the use of specific standards or frameworks. And suppliers have been reluctant to invest in creating their own standards in case the manufacturer mandates a different one.

In 2015 hackers took over a moving Jeep Cherokee from a laptop miles away, to prove that they could infiltrate the car, and control the brakes, steering and transmission. Chrysler recalled 1.4 million vehicles.

In 2016, insecure APIs meant that hackers could take control of Nissan Leaf vehicles and control some of the car's systems.

It's a stalemate situation that can't continue if security is ever to be part of the design stage of a vehicle and the manufacturer, as the final assembler of all component parts, needs to take responsibility for ensuring that third-party systems are also secure by design, and that systems do not become vulnerable when connected.

Don't forget the end user

Insurance companies already set premiums based on the safe driving record of the driver and usage-based insurance policies take this a step further, using telematics to continuously monitor the way in which a driver handles and drives their vehicle, in order to assess driver risk.

One area however, where driver risk is harder to assess is cybersecurity risk.

Despite the growing understanding in the industry that cybersecurity needs to be taken seriously, driver-awareness of the cyber risk to cars is relatively low and this will trouble the insurance sector. User awareness often peaks after high profile attacks and then quickly drops away and drivers typically don't give a second thought to how a vehicle functions. This needs to change and insurers will need to be reassured that end users are sufficiently aware of the fact that a vehicle's software systems need to be up to date or that it's unsafe to install software on a phone that will connect a car and expose it to threats.

Understanding the threat landscape

Critical to the success of building security into the design and maintenance of vehicles is understanding the threat landscape, openly sharing information across the supply chain and engaging with independent third parties to share their global threat intelligence. This is common practice in sectors like financial services and makes it easier for participating companies to benefit from collective threat insight.

The main challenge though is that responsibility for security needs to be owned by somebody in the automotive supply chain before the insurance industry can start to look at underwriting policies. And before this can happen, the industry needs to fully understand security, threat intelligence and what prevention and response measures are possible. It's time to get all interested parties into a room, government advisers, insurers, manufacturers, suppliers and independent security advisers, to talk through the challenges and build a model for security best practice for connected vehicles. Until that happens, responsibility sits with everybody – and nobody – at the same time.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **http://www.ntt.co.jp/index_e.html** to learn more about NTT Group.