The connected car industry needs a road map for cybersecurity

The connected car has been with us for some time, from the early years of telematics in the late 1990s when features were primarily for notification of crashes; to today's vehicles with remote parking control, summon features, vehicle servicing alerts and V2I technology. It is now likely that by 2040, there will also be 33 million autonomous vehicles added into the mix[1], with connectivity levels we can only imagine today.

We're all now used to the increasing amount of technology in our cars, and manufacturers continue to innovate to shape the car of the future. Today's tech giants, ambitious start-ups, traditional suppliers and industry Original Equipment Manufacturers (OEMs) are all looking for a slice of the action, recruiting talent and investing heavily in a rapidly- changing industry.

But much as we're all enjoying an increasing number of ways to stay safe, connected and informed in our vehicles, there's a growing amount of data generated, exchanged, processed and stored in our cars. And this means the number of attack vectors is on the rise, leaving financial, personal and vehicle information vulnerable and attractive to hackers. The problem isn't so much about accessing the vehicle to drive it away; it's about remotely accessing the critical infrastructure of a highly connected vehicle and compromising the safety of the vehicle and its passengers.

The question is, when will we have a common, binding information security standard for vehicles? And how can manufacturers work now to ensure that cybersecurity is a priority in our cars?

Vulnerabilities

There are some serious challenges associated with increasing connectivity and embedded computing functionality inside our cars. Today's vehicles are crammed full of technology to improve the driving experience. But at the same time as offering the driver new and improved functionality, they also expose the connected car and users to online threats.

82% of consumers would be wary of buying a car from an automaker if they had been hacked.

KPMG Cyber Consumer Loss Barometer

[1] *IHS Markit, Autonomous Vehicle Sales Forecast, January 2018*

One of the first major pieces of research released on this came from Charlie Miller and Chris Valasek in 2015 when they remotely hacked a moving vehicle, from a computer 10 miles away, controlling brakes, radio, accelerator and windscreen wipers. They exploited several vulnerabilities and weaknesses from the connectivity element to the lack of secure separation between various on-board systems.

At the time, remote patching was not an option, and today it would still be impossible to remotely patch 100% of the code in a car. In the same year, 51 million vehicle recalls were conducted by OEMs leading to a spike in lawsuits due to security vulnerabilities misused by attackers.

Car hacking remains a key area of concern for security experts who warn that allowing lateral movement could enable a hacker to infiltrate the car's weakest point and then pivot from, say, entertainment systems to the control bus in charge of steering. In a 2017 survey of 1,519 people in the U.S. and Germany, Gartner 'found that 55% of respondents will not consider riding in a fully autonomous vehicle, while 71% may consider riding in a partially autonomous vehicle.'[2]

Car manufacturers have accepted that connected cars are as vulnerable to attack as anything else connected to the internet. But while awareness is great, protection is extremely complex, as demonstrated in 2017 at the DIVMA security conference in Bonn, Germany. Researchers pointed to a security issue in the Controlled Area Network (CAN) protocol that car components use to communicate with one another within the car's network. This vulnerability would allow a hacker to shut off key automated components including safety mechanisms – more a denial of service attack that turns off components, rather than hijacking them to take over basic driving functions.

Product lifecycle too is creating problems for the industry and, right now, there are more questions than answers. With cars on the road for up to 20 years and having multiple owners, it's hard to see how suppliers and manufactures can provide security updates for the lifecycle of the vehicle. Does the customer visit a dealership for security updates? Can they be managed remotely by the customer? What happens when there's a breach and cars need to be recalled? And who's responsible for the cost of vehicle security over the lifetime of a car?

Rapid learning curve for automotive industry

Whatever the answers, a connected car will only ever be secure if it's built with security in mind from day one. That's easier said than done in an industry with a complex and fragmented supply chain.

But it's imperative that the connected car is designed as secure as possible and that automotive manufacturers overcome a number of technical and organizational challenges to make that happen. Any lack of confidence in the industry's ability to tackle the issue head on can lead to customer mistrust and onerous regulatory requirements, which could increase the cost of building connected cars, and nobody wants that.

Connected cars are made up from many different digital systems, any one of which could be vulnerable to attack. And today's cars are built by the OEMs, traditional suppliers and myriad new software and tech companies in the market. The supply chain is more fragmented; no single company is responsible for securing the connected car; it's organizationally difficult to manage a growing number of suppliers and the result is that we're still some way from having a unified industry position for baseline security in cars. Meantime the attack surface gets wider.

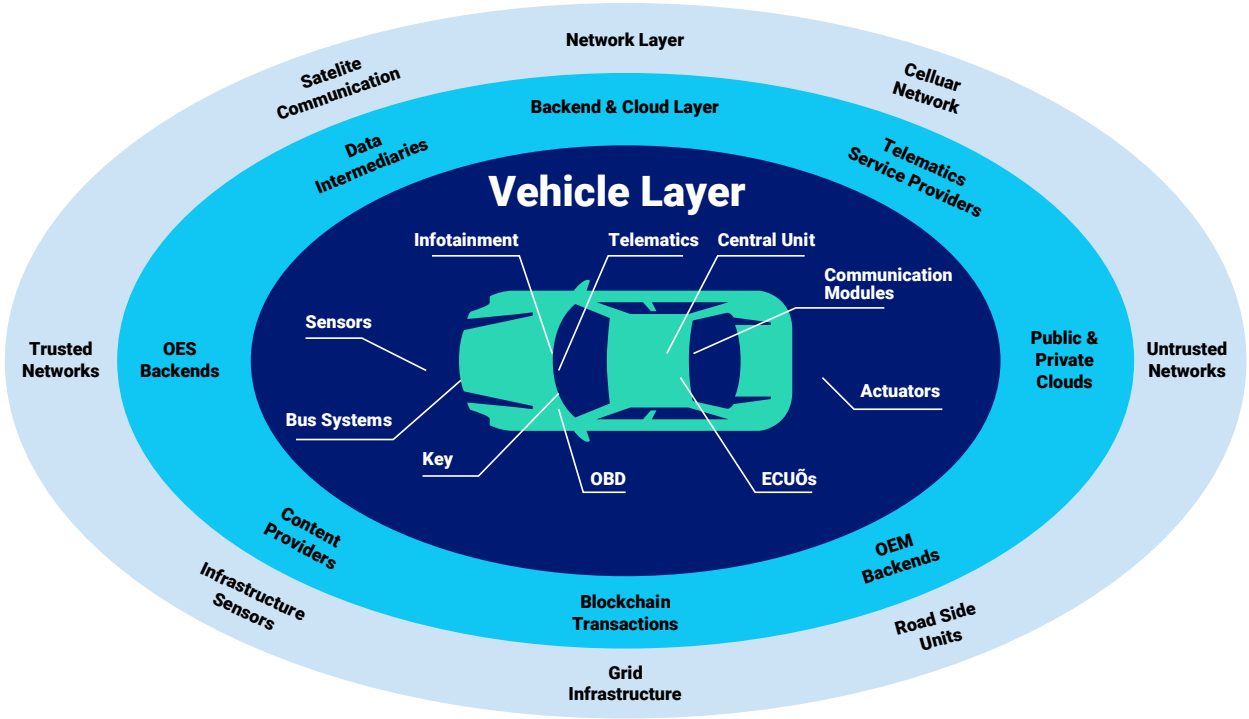

Figure: The multiple digital systems making connected cars vulnerable to attack

[2]*Gartner, Smarter with Gartner: 4 Areas Driving Autonomous Vehicle Adoption, Amy Forni, September 2017*

Securing the layers – where do you start?

Preventing attacks in the connected car ecosystem is a complex task. The illustration above shows the multiple layers that offer serious cyber-risk.

Vehicle layer challenges

At the vehicle layer, the interconnectivity between different systems means that an attacker could potentially exploit vulnerability in one of the in-car systems before pivoting to compromise the vehicle's safety or control systems.

Manufacturers and OEMs are challenged to guarantee that security enhancements can be maintained over the life of the car. Achieving this will require them to review their security architecture to ensure that it is fit for purpose over the next 10 to 20 years. Current cost-optimization hardware architectures lack sufficient RAM and computing power to fulfil critical cybersecurity requirements. Therefore, instead of looking for the least expensive way to implement hardware, the industry needs to focus on creating the optimum environment to support the security measures needed to keep connected cars safe.

Furthermore, a large number of components are manufactured by multiple suppliers, with no one supplier taking overall responsibility for detailed security testing processes and procedures.

Best practice would be for OEMs to take responsibility for security; to put in place strict security standards when onboarding applications, evaluate security of third-party vendors and conduct security testing when integrating in-vehicle applications that have been developed for practicality rather than safety.

Backend and cloud layer challenges

In the cloud and backend layer, attacks are likely to be more complex and the potential damage to the organization's reliability and reputation is high.

It's vital to ensure that the right controls are in place to secure the infrastructure of not only the OEM, but the partners and suppliers that integrate their products into the vehicle or have a direct connection to the vehicle itself.

That means taking a holistic approach to secure the cloud, hybrid cloud, virtual environments, the data center and servers.

It will never be enough to focus on the secure connections between OEM and OES systems, instead manufacturers need to assess the safety levels of every supplier to ensure that vehicles are safe.

Data privacy too is something that more connected car drivers will start to ask questions about. At the moment there's widespread ignorance about the personally identifiable information (PII) that a car is storing. Not only will this data become gold dust for OEMs who will bundle and sell it, it's also valuable in the hands of a hacker. Customers will start to demand more information about privacy and security policies that come with connected cars, and manufacturers and OEMs will need to address this.

Network layer challenges

Connected cars rely on multiple communications links with external networks to provide services such as over the air updates, streaming, car2car communication, car2infrastructure communication and navigation features. Valasek's control of a vehicle brought this into sharp focus and highlighted the importance of securing this network layer. Traditional architectures inherently have a lack of encryption in order to ensure lightweight and seamless data transmission and connectivity, but that's no longer sufficient to protect the car.

Certificate-based authentication and encryption is now essential to establish trust in the device identity and for sending data from the car to the manufacturer and other third parties. This will prevent hackers from packet sniffing, capturing and manipulating data in order to take control of the vehicle.

Make security a differentiator

It's unlikely that any car manufacturer will market its vehicles as the most secure – claims such as these will be a magnet for cyberattackers. But manufacturers need to be assured that suppliers are taking security seriously, and suppliers should now be working hard to ensure that their products are built from the ground up with security in mind. Suppliers should realize that security will likely become a decision factor in partnerships with automakers in the future. As more connected cars are designed, it's time to see security as an enabler for car innovation rather than a perceived hindrance. Time therefore to seek the right advice from security experts to ensure that the industry will continue to drive innovation and competitive edge and at the same time ensure that cybersecurity controls are firmly in place.

An understanding of regulatory standards is required

As the market in connected cars continues to grow, governments are now providing guidelines for car manufacturers and suppliers. Having an understanding of key industry standards will provide a benchmark of the security standards that manufacturers need to meet. It will also inform decisions around security by design for the industry as a whole.

> While OEMs can use data collected through connected vehicles to optimize performance, **reliability and safety of vehicles they produce, failure to get cybersecurity right could have a lasting impact on brand.**
>
> Gary Silberg, KPMG

In the UK, the government has introduced new guidelines[3] to improve the cybersecurity of connected and autonomous vehicles, to ensure that all parties involved in the manufacturing supply chain are provided with a consistent set of guidelines.

[3]*Gov.uk, The key principles of vehicle cyber security for connected and automated vehicles, August 2017*

Organizations may well need support to implement

the correct processes and controls, and engaging with a third-party security provider would ensure the creation of combined overarching standards that are aligned with the commercial objectives of the business and that compliance considerations are not overlooked. The eight key principles are:

- Organizational security is owned, governed and promoted at board level.
- Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.
- Organizations need product aftercare and incident response to ensure systems are secure over their lifetime.
- All organizations, including sub-contractors, suppliers and potential third parties, work together to enhance the security of the system.
- Systems are designed using a defense-in-depth approach.
- The security of all software is managed throughout its lifetime.
- The storage and transmission of data is secure and can be controlled.
- The system is designed to be resilient to attacks and respond appropriately when its defenses or sensors fail.

Within these guiding principles are recommendations that all new designs embrace security by design; organizations embed a culture of security; security risk assessments are in place; incident response plans are in place; organizations can recover forensically robust data; all parties in the supply chain must be able to provide assurances of their security processes and products; organizations will jointly plan for how systems will securely interact with external devices; the security architecture applies defense-in-depth techniques to mitigate risks, and data must be sufficiently secure when store and transmitted.

Although not yet enshrined in law, these are a comprehensive list of requirements deemed necessary as cars become more vulnerable than ever to hacking and data theft. It should be noted however that, like any other standard, simply carrying out these actions may not be enough.

OEMs will need a proactive program and should evaluate security and risk continuously. To approach this as another compliance tick-box exercise will not account for the unique risk posture and appetite of that manufacturer.

In the US, the Security and Privacy in Your Car (SPY Car) Act of 2017 was reintroduced by senators keen to improve baseline privacy and security in the automotive industry. The SPY Act calls for all cars to be equipped with the ability to detect, report and stop a breach. Manufacturers failing to include this capability would be fined USD 5,000 for every car that doesn't have the technology built in. The new act goes a step further calling for technology such as a cyberdashboard to show the driver how far the manufacturer has gone to secure the car's on-board systems. It also requires that every car notifies the driver as to what driving data is being collected, with the facility for the driver to opt out of data collection if required.

Connected cars need a secure architecture

It's going to take some time before cybersecurity frameworks are widely embraced by the automotive industry, and a paradigm shift in vehicle design is required before connected cars can be successfully protected from cyberattacks. *Security by design* needs to be the mantra for the industry and managing security must become part of the entire lifecycle of the vehicle – an integral part of the vehicle's design, rather than an afterthought.

NTT recommends the following for the industry to consider when assessing the risk associated with compromised systems:

- Build cybersecurity into the design. Develop an appropriate lifecycle process from concept through production, operation, and decommissioning.
- Apply a defense in depth strategy – have multiple layers of security in place to mitigate the risk of one component being compromised.
- Embed cybersecurity in enterprise- wide risk governance.
- Conduct cybersecurity gap assessments - identify high risk areas when building in security by design – use risk assessments and follow mandatory development procedures and policies to mitigate these risks.
- Prepare for emerging security threats by continuously monitoring the threat landscape and applying actionable threat intelligence.
- Conduct vulnerability assessments and routine pen testing to regularly assess the security of component parts – from the backend IT infrastructure to in-car systems – and verify third-party providers have carried out full-lifecycle testing.
- Systematically execute cybersecurity plans and regularly maintain the security architecture.
- Work with a security partner who understands the very specific challenges facing the automotive industry and the risks from the whole car perspective.

Conclusion

The car is no longer a simple mode of transport. It's becoming an information technology system on wheels – an information and entertainment hub equipped with hundreds of sensors to improve convenience, comfort, efficiency and safety. Car buyers will become increasingly aware of the privacy and security limitations of connected cars and will need to be continually reassured that manufacturers are now investing in cybersecurity alongside design and car safety. Other means of transport critical infrastructure (planes and trains) have integrated cybersecurity concerns into early stages of development, and it's time for the automotive industry to do the same.

What is needed now is a sense of urgency and the right level of collaboration between manufacturers, suppliers, governments, regulators and cybersecurity experts to strike the right balance between security and design of highly connected vehicles.


NTT