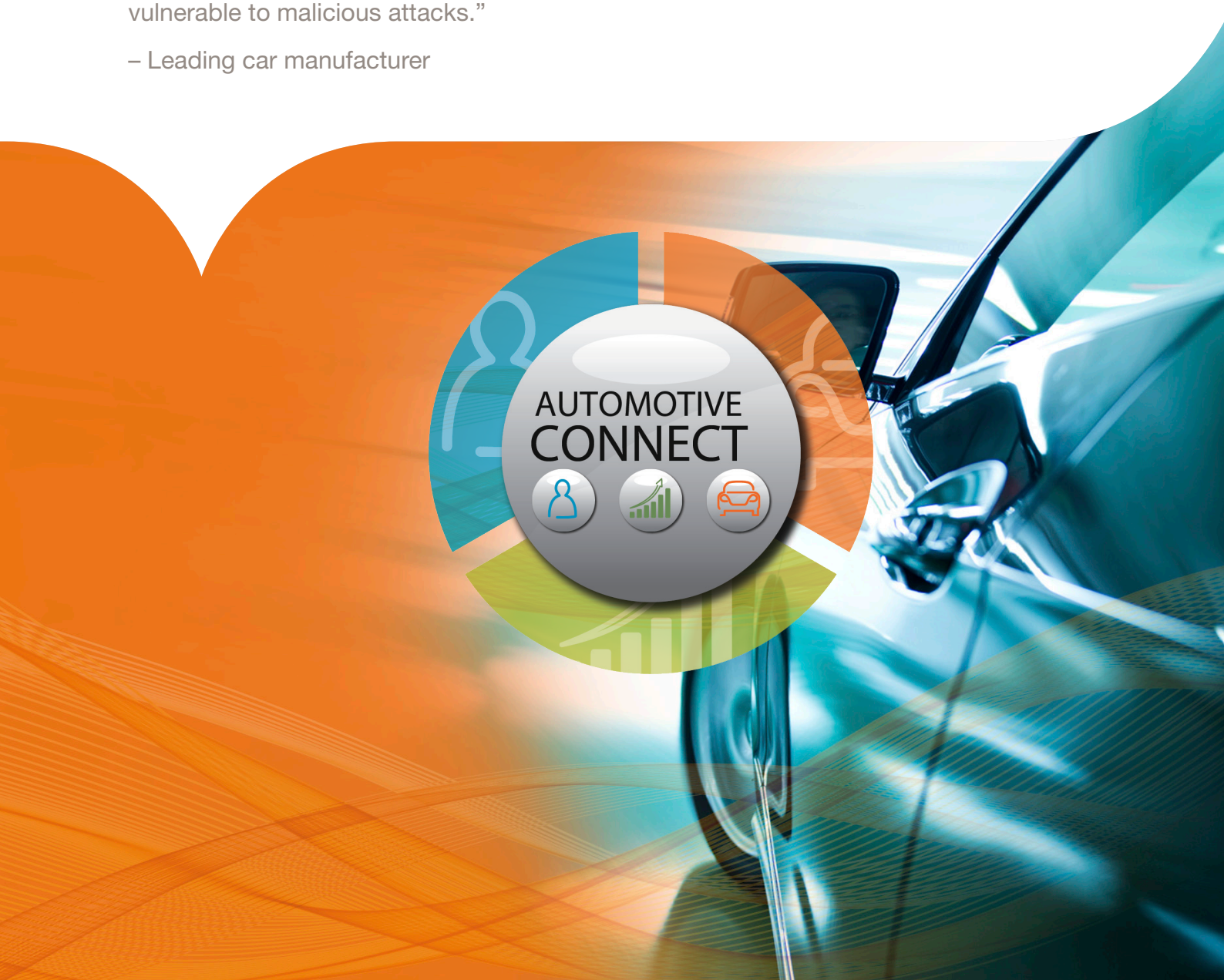
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Cybersecurity for the Connected Vehicle

> "While car manufacturers are currently focusing mainly on infotainment-related connectivity, in the coming years we will see many more developments in the field of car-to-car communication and remote diagnostics. But this also means that we will be more and more vulnerable to malicious attacks."
>
> – Leading car manufacturer



The concept of the connected vehicle[1] responds to consumers' expectations by making the vehicle into "just another node on the network"– an extension of their home, office or club that streamlines their lives. However, the connectivity that makes it all possible also introduces new and disturbing security risks.

Security is not something that can be delegated to suppliers. OEMs need to take overall responsibility for security and make it central to their business. They must view the vehicle as part of a wider system and, in that context, take steps to secure both the existing fleet and new vehicles. OEMs that gain and fulfill the trust of their customers will also win a competitive advantage, and will be able to grow securely and confidently as digital enterprises.

The connected vehicle introduces a new security paradigm, which opens up the possibility of various disturbing scenarios in future. For example, it's becoming possible to manipulate the vehicle directly. Attackers such as political activists could immobilize an entire fleet of a type of vehicle favored by prominent individuals, or launch a Denial of Service attack on a vehicle or group of vehicles. These scenarios are not limited to vehicles – a toll bridge could be prevented from letting people through or a traffic light system could be thrown into chaos.

What has changed to make all these things conceivable? Until recently, vehicles were designed to be self-sufficient, rather than part of a network. Their connectivity was limited and based on wired, peer-to-peer connections. For example, a mechanic in a workshop might connect a computer to the OBD II port to run diagnostics. The security risks associated with this type of connection required physical access to the car, and therefore only basic security measures were in place.

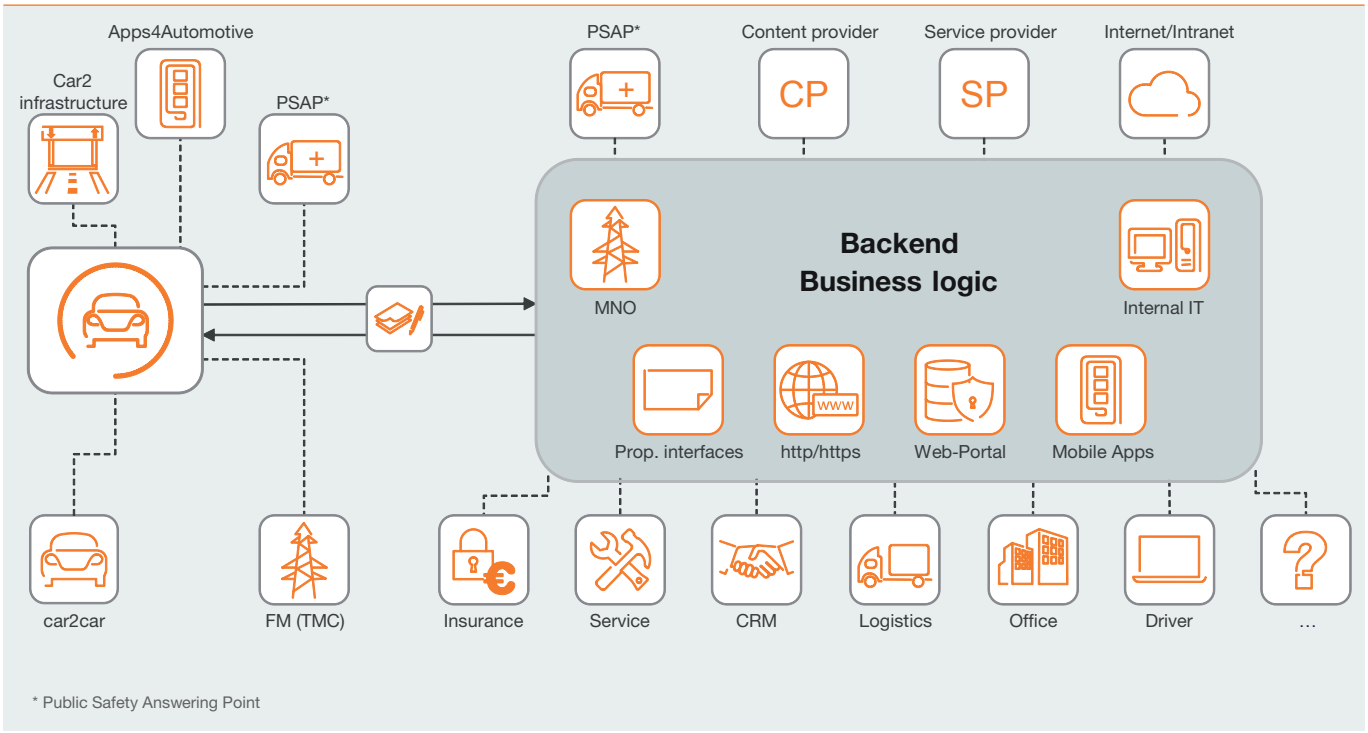
Now the vehicle's connectivity has been extended in several ways.

- Firstly, the existing connectivity within the vehicle opened up by the introduction of telematics services, and services provided over the Internet such as infotainment. In addition, OBD II port can be accessed via Bluetooth or Wi-Fi dongles, like the ones that insurance companies hand out so that drivers can prove they are driving safely and get a reduction on their insurance premiums. All of a sudden, what used to be a closed system has become an open one, but security measures have not always caught up.
- There are also new types of connectivity within the vehicle. Previously separate groups of computing devices are now closely interconnected, with telematics and infotainment modules linked to other services in the vehicle, including safety-relevant ones. Tire pressure is transmitted wirelessly to the dashboard. Hands-free connections link entertainment systems to mobile phones. A modern vehicle is effectively a data center containing as many as 100+ interconnected servers – control units, sensors, actuators – and many of the connections are wireless.
- In addition, back-end systems within the OEM's organization can communicate with vehicles remotely. The back-end systems might, for example, transmit firmware updates to the vehicle periodically. When a vehicle breaks down, a workshop might connect to it remotely to diagnose and fix the problem in lieu of roadside assistance. Increasingly these types of connection are made over the internet rather than a dedicated network.

In this new connected world, the attack surface extends across the entire ecosystem (see figure on page 3). As more connected services are offered and taken up, information will be increasingly exposed as it travels to and from, and is used in, the vehicle. Autonomous driving will increase the attack surface even further because of increasing connectivity with infrastructure, other vehicles, and back-end services.

[1] Capgemini, AutomotiveConnect: Driving Digital *and* Capgemini, Connected Vehicle: Making the vehicle a node on the network

Figure 1: Connected Vehicle, High-Level Architecture



Source: Capgemini

The vehicle's connectivity puts all types of **assets** at risk of various types of attack by several types of **threat agents** with different **motivations.**

Types of attack

Let's take a closer look at each of the three aspects of an attack – assets, threat agents, and motivations – since it will make it easier to understand the actions required to manage the risks.

Assets. An asset can be anything worth stealing, damaging or destroying, and can be either tangible or intangible. As well as the vehicle and its contents (such as freight or personal belongings), we define tangible assets to include the safety of people and compliance with safety regulations. Intangible assets are mostly information-based: for example, drivers' and owners' personal data, or service usage data such as subscriptions and payments, but also extend to the OEM's brand reputation.

Threat agents. Several types of individuals and organizations have an interest in exploiting these assets. They have varying levels of skills and resources at their disposal.

Motivations. Attacks can be classified according to whether the threat agent's motive is challenge, profit or activism. Although many attacks would primarily affect an OEM's customers, the OEM's brand reputation would also be affected and the OEM might be exposed to litigation.

- **Nation states:** national security, surveillance, political gain, or manipulation.
- **Organized crime:** financial gain and political influence.
- **Political activists:** political aims and sometimes damage to a brand name.
- **Terrorists:** political aims, manipulation, assassinations.
- **Ordinary thieves:** profit.
- **Exploratory hackers researching for academia, security companies or government organizations:** prestige, research funds, and government contracts.
- **Hobbyists trying out hacks found on the internet:** fun and maybe a reputation as a knowledgeable individual.

Updating security strategy to address the connected vehicle ecosystem

OEMs as IT providers: the cybersecurity implications

As the endpoint in a new IT landscape, the connected vehicle requires security features that previously only applied to conventional computers. Antivirus, firewalls and anomaly detection are not yet implemented in the connected vehicle, largely because of the complexity of updating policies and software regularly and frequently. Units inside vehicles have limited resources, which are often already fully utilized by the vehicle's functions.

OEMs are increasingly providers of IT services rather than just vehicles. It follows that IT security should be viewed as part of their core business, and should become an integral part of all their activities.

To secure the vehicles that are being built now, the way the industry approaches security needs to evolve to reflect industry change. A number of elements of the current approach have been called into question by the advent of the connected vehicle:

- Back-end systems may originally have had reasonable levels of security built into them – but those back-end systems are now part of an ecosystem, and it's the security of that whole ecosystem that matters.
- On-board systems were designed to be wired and peer-to-peer, and as such were reasonably secure – but now they have been opened up by the use of wireless dongles, which may not even include authentication mechanisms.
- OEMs may be relying on outdated approaches like "security by obscurity". Hiding a software specification or a shared key is no guarantee of security; tools and knowledge of how to locate and extract keys, or hack software, are now readily available.
- Development is often thought of as a one-time effort, but by its nature software contains flaws that are detected late, possibly after the software has been deployed in vehicles. That might have been less of a problem when the vehicle was a standalone entity, but today's remote access capability makes it a serious concern.

Another, very important, issue with the traditional approach to security is that OEMs are used to expecting suppliers to take care of the safety and security of their products. However, it is much harder to secure software than to test a bearing, and many suppliers lack the resources and expertise to get involved with encryption keys and the like.

The truth is that only the OEM is in a position to address the overall security of the vehicle and ecosystem – for example, it would be possible for them to introduce a hardware security module to authenticate the driver to all the systems inside the vehicle (not something an individual supplier can do). OEMs need to start considering connected vehicles as part of a larger system that includes vehicles, networks, telco infrastructure, OEM IT, and all kinds of services from third-party providers, and to take overall responsibility for the security of the entire ecosystem.

In addition, OEMs need to start viewing security in terms of the vehicle's entire life and not just the initial sale. The vehicle and all the supporting back-end services must continue to operate safely and securely until the last vehicle in a particular range is taken out of use – or, if not, services must be capable of being decommissioned in a secure way, without leaving any security holes.

Core requirements

As information and instructions are shared between elements of the connected vehicle system, it's vital that we always know who we're talking to and can be sure that any information received is legitimate. The vehicle, as a "thing" in the Internet of Things (IoT), needs to be able to authenticate itself in order to achieve accountability (that is, to tie actions to individual entities) – and so does everything in its environment. This is the only way updates, protection of intellectual property, driver identification, etc., can be carried out securely.

Authenticity, integrity and accountability are vital to every stakeholder in the system. As a vehicle owner, you want to be sure that your doors can be unlocked only by you or someone else you have authorized. As an OEM, you want to be sure that only the online updates that you have tested and provided are accepted by the vehicle, and that only eligible vehicles receive updates or upgrades.

Information security therefore needs to be established and designed early in the construction of the units, to ensure that there will be the resources and capability to handle the security functions needed. This will involve working out how to use cryptography in a secure way – which, contrary to what many people think, is not so much about the ciphers themselves as about key management. OEMs also need to put in place well-functioning and omnipresent identity management to support authentication and authorization across the new ecosystem.

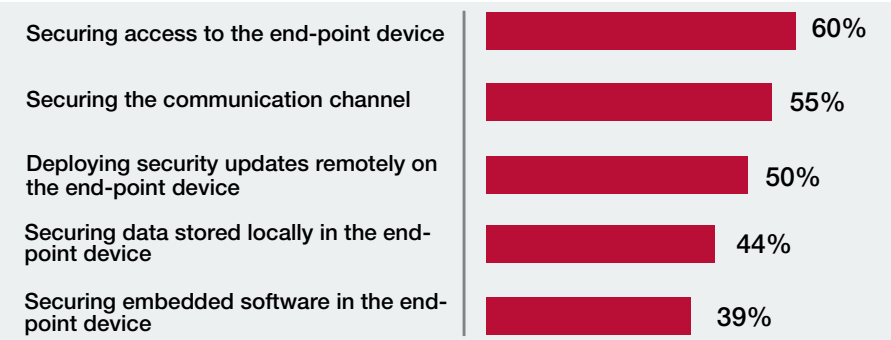
In tackling these requirements, we can draw on other disciplines such as security measures that are currently being adopted for mobile computing and the IoT, though the connected vehicle has specific requirements.

- **Connected vehicles and the IoT:** The connected vehicle raises some of the same issues as the IoT generally, including the need for integrity and authentication. However, vehicles are atypical in terms of their high value and long lifecycle (five to 10 years for a TV compared with 15 or more years for a vehicle). In addition, a vehicle is harder to update (it may involve a workshop visit) and the cost of failure in terms of both money and human life is potentially much higher than average.
- **Connected vehicles and mobile computing:** The connected vehicle concept also shares many of the security issues that surround mobile computing, but raises issues of its own. Vehicles have much less computing power, a much longer lifecycle, a very heterogeneous hardware landscape, various (including real-time) operating systems, no file systems, no privilege distinction, and in general a very constrained execution environment.

The industry is recognizing the Internet of Things challenge

Capgemini Consulting and Sogeti High Tech – a subsidiary of the Capgemini Group that specializes in product engineering – recently conducted a study of cybersecurity threats for the IoT[2]. Among automotive sector respondents, 65% agreed that security concerns will impact customers' purchase decisions for IoT products. Just 35% of automotive respondents rated the IoT products in their industry high on resilience to cyber attacks, however.

Figure 2: Key Challenges to Securing IoT Products



Source: Capgemini Consulting and Sogeti High Tech, "Security in the Internet of Things Survey", November 2014 N=109

[2] Capgemini Consulting and Sogeti High Tech, Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT

Steps OEMs should take now

OEMs need to adjust their thinking on cybersecurity sooner rather than later – particularly given the long life expectancy of vehicles. The attacks that are currently hitting the headlines may be limited in their immediate impact, but they indicate increasing risk. We must expect to see serious attacks on connected vehicles in the near future.

It's time for OEMs to take action, and we recommend the following steps.

Develop a whole-system view

OEMs should start to build their understanding of connected vehicles as a part of a system that includes sensors, in-vehicle IT, networks of all kinds, and OEM-controlled IT systems, as well as third-party services.

Security needs to be considered in relation to this whole connected vehicle system, not just the vehicle. Consider the security requirements implied by this context, and align your organization with these requirements, bringing together parts of the organization that are traditionally separate such as IT and electric and electronic development. Identify which of your development units cooperate when you develop a new service or capability, whether it's electronic control unit (ECU) development or IT (back-end) development. Decide who has responsibility for each aspect of security, and overall responsibility for the security of the service or capability.

In addition, every project should have a security follow-up, just like every other functional attribute of the vehicle. Otherwise, the security aspects will be seen as having lower priority, and the end product will be less secure as a result.

Protect existing fleets

Compensate for security flaws in existing fleets by adding adequate measures to the back end wherever possible. Try to ensure that you could use the back end to detect an anomaly in your connected vehicle fleet communication, and to protect the fleet from an intrusion attempt. Perform regular penetration tests on both existing and new vehicles. Electric car manufacturer Tesla Motors uses "white hat" hackers to challenge its defenses against cyber attacks[3].

Ensure vehicles in development are secure from the start

Information security must be considered throughout the complete lifecycle of the vehicle, from the earliest stages right through to decommissioning. Security must be built into the requirements definition. For example, the requirements must take account of the need for regular patching and updates.

The most important aspects of information security are:

- **Authenticity, accountability** and **auditability,** so that you can tell if information is genuine and can prove who sent it to whom.
- **Integrity,** so that you can determine that the information is accurate and consistent.
- **Availability,** to ensure that the vehicle functions as desired when it is needed.
- **Confidentiality,** to protect personal or sensitive information from eavesdropping (please see panel "Protecting personal information").

To provide authenticity, **authentication** and **authorization** should be integral to both on-board and off-board systems.

Ensure that information security continues to be central throughout the lifecycle. Sign-off milestones must check that security is appropriately addressed at each stage, starting with requirements specification. If you don't already have a secure software development lifecycle framework such as Microsoft SDL in place and working, implement one.

In the recent Capgemini/Sogeti IoT study, 35% of respondents cited the shortage of specialized security experts in their organizations as a key challenge to securing IoT products.

[3] Wall Street Journal, "Tesla Invites Hackers for a Spin", August 2014

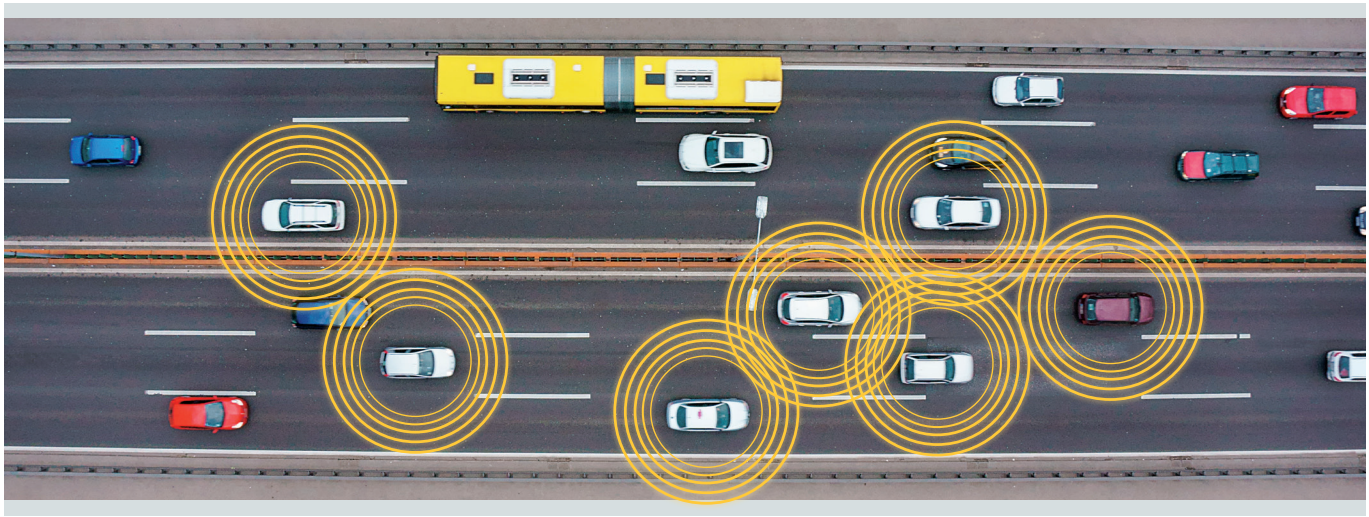
Protecting personal information

Vehicles create increasing amounts of sensitive data – current location, who drives, where and at which times, where home is, typical times when a driver leaves home, what kind of driver they are, and so on.
Much of this data is transmitted without the knowledge of the driver, and often without the option to deactivate the transmission process. This will have to change.
Drivers need to be empowered to make the decision about what identifiable personal information they are willing to share, and then the OEM needs to ensure that the data is used in accordance with the drivers' wishes and in compliance with privacy legislation and best user experience. This is a complex task, first because of country-specific data protection laws, and second because of the challenge of providing user-friendly, intelligent interfaces that allow the driver to give consent at a detailed and specific level without too much effort or concentration.

Make sure that best practice for secure software development is adopted throughout your organization. A governance framework for software product security, such as OpenSAMM or BSIMM, will help you make best use of your security skills.

Start now to gain competitive advantage

Only by grappling with the security issues now can OEMs pursue the connected vehicle vision securely. By taking the steps recommended above, they can meet customers' expectations about connectivity while also securing their trust, and hence gain competitive advantage. They may reduce potential financial damage posed by lawsuits like the one recently initiated in the US against major automotive manufacturers, alleging that they have failed to secure their products against hackers[4].
The challenge may look daunting but to a great extent it is about adopting established good practice from software development (including mobile and IoT) and applying it to the broader requirements of the automotive industry. Working in conjunction with our automotive security specialists, Capgemini's Cybersecurity Service line has the resources you need to do just this. We can strengthen your defenses, optimize your investments, and control your risks.



[4] Computerworld, "Lawsuit seeks damages against automakers and their hackable cars" March 10, 2015

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

For more information please contact:

Dr. Magnus Gerisch
Business Technology, Automotive
magnus.gerisch@capgemini.com

Hans Lohmander
Capgemini Sweden
hans.lohmander@capgemini.com

Vaibhav Mahajan
Capgemini India, CHROME (Automotive Center of Excellence)
vaibhav.mahajan@capgemini.com

Didier Appell
Sogeti High Tech
didier.appell@capgemini.com

Alexander Heßeler
Business Technology, Automotive
alexander.hesseler@capgemini.com

About Capgemini

With almost 145,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2014 global revenues of EUR 10.573 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cybersecurity, combining world-class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, the USA and India. Sogeti is a wholly owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 2,500 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT, industrial systems, and Internet of Things (IoT) products and systems. We have the resources to strengthen your defenses, optimize your investments, and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, five multi-tenant security operation centers (SOCs) around the world, an Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

About Capgemini's Automotive practice

Capgemini's Automotive practice serves 14 of the world's 15 largest vehicle manufacturers and 12 of the 15 largest suppliers. More than 5,000 specialists generate value for automotive companies every day through global delivery capabilities and industry-specific service offerings across the value chain, with a particular focus on Connected Customer, Connected Vehicle, and Connected Insights.

For more information:

www.capgemini.com/automotive

Learn more about us at
www.capgemini.com