Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Automotive | the way we see it

Automotive Suppliers and Cybersecurity

People matter, results count.

OEMs sometimes specify their security requirements in an incomplete or vague way, but that certainly doesn't mean that Tier 1 automotive suppliers (Tier 1s) should neglect responsibility for cybersecurity. By adopting a proactive approach to the topic, it becomes possible to add value for the consumer, the OEM, and the Tier 1, as well as mitigate risk. It's better for everyone if automotive suppliers take action to ensure that security is built into products, collaborating as far as possible with both OEMs and other suppliers.

Cybersecurity is a key to strengthening relationships with OEMs

A great way to strengthen a company's position as an automotive supplier is to become more proactive about security, and indirectly meet OEM expectations about privacy and security in the connected vehicle.

There are a number of benefits to tackling security in this way:

- **Increase value.** Building in security can reduce the total cost of ownership for OEMs, if risk is calculated as a potential cost. This benefit is something OEMs should be willing to pay for once they understand the proposition properly, because consumers are very interested in security. In a recent Capgemini survey[1] on Internet of Things (IoT) security, 65% of respondents from the automotive industry expected security concerns to influence purchase decisions.
- **Reduce risk.** Suppliers can avoid the danger of security breaches that could result in litigation and reputational damage. Security flaws can imply safety flaws with a very high damage potential.
- **Build stronger relationships.** By being seen as a source of expertise, a Tier 1 can become a partner to OEMs, instead of just a supplier.

Major reasons for reluctance to use connected vehicles included lack of trust over data privacy plus risk of cyberattacks.

Capgemini, Cars Online 2015 – The Selfie Experience
www.capgemini.com/cars-online-2015

Privacy features create competitive advantage

Tier 1s should consider designing appropriate means for secure data selection, storage and destruction of sensitive data, as well as for handling consent. These means support OEMs in providing drivers and owners with transparent choices to selectively suppress storage and submission of person-related data.

Challenges for automotive suppliers

In our recent IoT survey, we asked organizations globally which types of exposure concerned them most. A variety of threats emerged (figure 1).

These attacks threaten fundamental security requirements such as authenticity, authority, confidentiality, integrity and availability. Tier 1 suppliers therefore should create products that provide capabilities regarding authentication, authorization, cryptography and resilience. These capabilities provide answers to the challenges that were named by most of the respondents to the IoT survey (figure 2).

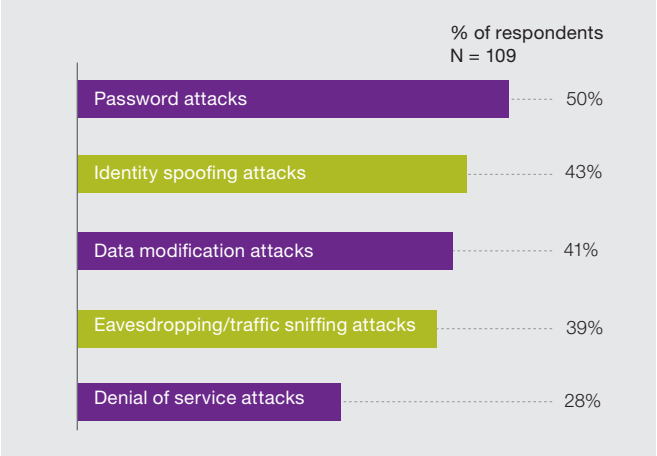
So how do these key challenges relate to the security requirements mentioned above? The two first challenges – securing access and the communication channel – call for authenticity, authority, confidentiality and integrity. For remote security updates, authenticity, authority and in some cases confidentiality are among the requirements. Secure storage mainly needs confidentiality and integrity. All in all, the requirement for an effective, rich and secure cryptographic capability is a central part in offering a secure platform to the OEMs.

1 Capgemini Consulting and Sogeti High Tech, "Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT", 2014

In order to create such a secure platform, Tier 1s may use base components from other suppliers. These Tier 2 components must support the desired security capabilities.

Last but not least, OEM purchasing departments are well aware of safety. But they may not consider security as an underlying requirement for safety.

Figure 1: Top security threats to IoT products



Source: Capgemini Consulting, Sogeti High Tech, "Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT", 2014

Collaboration with Tier 2 suppliers (Tier 2s)

Car electronic control units (ECU) – just like any other kind of computers – are commonly based on components from other suppliers. It's important for Tier 1s to give careful consideration to the selection of appropriate base components, from silicon to software. The Tier 2s' systems development lifecycle (SDLC) should be incorporated into the Tier 1's own.

Tier 1s should derive security requirements from those of OEMs, and pass them on to Tier 2 suppliers. Where base components are custom made, appropriate quality assurance should be part of the sign-off process. For off-the-shelf products, the choice should be guided by the security requirements.

Existing security capabilities of base components should be used by default. This may seem obvious but doesn't always happen.

Relationships with OEMs

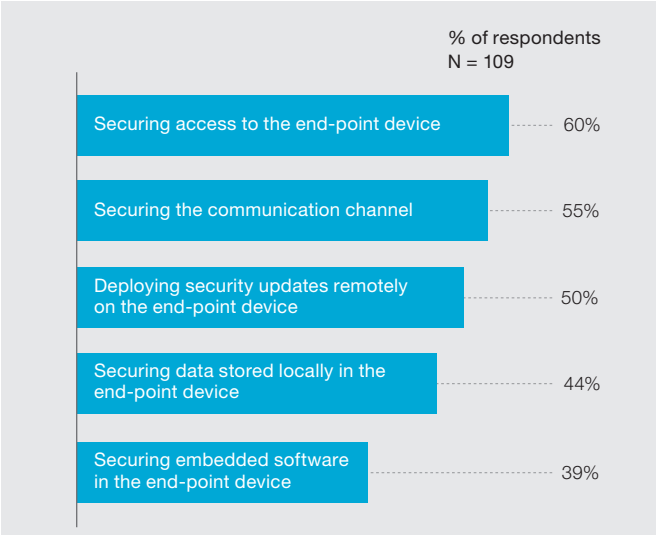
We firmly believe OEMs should take responsibility for security, and that, in the future, they will make increasingly explicit demands on their suppliers for security provisions. Today, however, OEMs often don't formulate security requirements in sufficient detail, and may be implicitly passing security responsibilities on to their suppliers.

At present, OEMs' purchasing departments tend to be focused on getting the best price. This approach may work well for materials, where OEMs have a good understanding of quality assurance. However, when it comes to quality assurance of software – particularly with regard to non-functional requirements like security – OEMs tend to rely on their suppliers. They may neither check specifications thoroughly, nor perform security analysis of code. They may not even assess the software development lifecycle of their suppliers. At first glance this may look like a reasonable approach, but it means that OEMs do not have control over security issues, which could cause major problems for them in the future.

For now, anyway, OEMs' emphasis on price, together with the lack of well-defined security requirements, means that if a supplier offers anything but a minimal solution, there is a risk that the proposal will be thrown out.

This poses a dilemma for suppliers, but one that we believe can be overcome by making security into a fundamental part of the way the company does business, and demonstrating its value.

Figure 2: Key challenges to securing IoT products



Source: Capgemini Consulting, Sogeti High Tech, "Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT", 2014

The solution: proactively ensure security is built into products

Adopt a "consulting attitude"

We recommend that suppliers work closely with OEMs to develop a joint approach to security. If security requirements in a request for proposal (RfP) are unclear, then it's best to point it out early on and show how clarity about goals will reduce risk.

By adopting a consultancy-style approach, the Tier 1 can start to provide advice on what's missing or inadequate and recommend actions to improve matters.

Build an internal security capability

To be a credible advisor to OEMs, it's vital that Tier 1s invest in internal security capabilities, and start to make use of them as soon as possible. To begin with, it may be hard to recoup the cost from OEMs, but the capabilities can still be a differentiator. In due course, OEMs should start to appreciate that security provides additional value, and become willing to pay for it.

There are a number of steps that can help automotive suppliers to build and embed a security capability:

- Bring in or develop security expertise for a quick start – not just technical experts but people who understand risk as the core element of security. In the IoT security survey mentioned earlier, 35% of respondents cite the shortage of specialized security experts in their organizations as a key challenge in securing products.
- Make sure everyone understands that security is not a feature – it has to be an integral part of everything a supplier does: a state of mind.
- Ensure security decisions are made by business departments that carry risk, not by engineering. Engineers may or may not understand the business implications of risk – but more importantly, it's not their risk.
- Adopt a secure development practice along with a maturity model for security: BSIMM-V or OpenSAMM combined with Microsoft SDL or OSSTMM, for example.

Maturity models like OpenSAMM can guide companies through an incremental improvement program. This should include the following measures:

- Pursue a consistent cybersecurity policy and governance model throughout the organization.
- Strive to develop new products in a secure-by-design fashion.
- Be proactive in watching for security vulnerabilities in existing products, and be transparent with OEMs about any non-public vulnerabilities known to be in the products.
- Offer a security-patching policy to OEMs. Selling products with vulnerabilities is unavoidable, but not offering a way to correct known vulnerabilities is inexcusable.

In addition, there are specific steps that can secure the supply chain:

- Tier 1s should formulate derived security requirements for Tier 2 suppliers – and make the most of their capabilities.
- In choosing base software, look for products with a security model and good security features in place. Adhere to the model and use the features when building new software.
- Just as OEMs will increasingly ask suppliers to vouch for the security of software they supply, Tier 1s should seek similar assurances from software suppliers.

Recommended implementation approach

We recommend an incremental approach. A full-scale security practice can't be adopted overnight, nor does it makes sense to invest a lot before establishing what OEMs will pay for.

Choose the right focus area. Adopt a risk-based approach to identifying the items to tackle first. A gateway or a feature common to a number of products might be a good choice. So might a product that has a large attack surface, such as an element of an infotainment system. Their compromise may have less severe consequences for suppliers than, say, attacks on locks, but they have been an entry point for recent hacks[2].

Align the approach with business risk management. The quality and security of solutions is an aspect of business exposure. In the event of a major breach, the business

2 Miller, C. and Valasek, C., Remote Exploitation of an Unaltered Passenger Vehicle, 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf

would take a hit in terms of lawsuits, penalties and liability. Awareness of these risks should shape the implementation approach, and, as already mentioned, decisions relating to risk should be made by the business rather than by engineers.

Build specific capability in the chosen area. Use suppliers' capabilities where appropriate, too, to address the security aspects of a given product or feature.

Show that security and privacy adds value and that consumers are willing to pay for it. Use an approach based on risks and benefits to interest OEMs and colleagues in security. Consider engaging directly with the consumers in order to raise their awareness of security issues, and also collect evidence to demonstrate to OEMs how interested their customers are in security. This consumer engagement can be achieved via indirect marketing, social media listening, etc.

For more information please contact:

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

Hans Lohmander
Cybersecurity Expert, Automotive
hans.lohmander@capgemini.com

Nick Gill
Chairman, Automotive Council
nick.gill@capgemini.com

About Capgemini

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

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 our AutomotiveConnect propositions for OEMs and suppliers.

For more information: **www.capgemini.com/automotive**

Learn more about us at
www.capgemini.com

MCOS_GI_PT_2016.02.22

People matter, results count.