Connected Car Business Brief Series | 02

Bild: shutterstock.de

PROTECTING PEOPLE AND PRIVACY IN THE ERA OF CONNECTED CARS

The connected car era will create a wealth of new opportunities – and just as many new risks.
To succeed, automotive OEMs must prioritize security.

In July 2015, security experts Charlie Miller and Chris Valasek made headlines around the world by successfully hacking into a moving vehicle, and taking control of everything from the windscreen wipers to the accelerator pedal. The potential consequences are as obvious as they can be deadly. Moreover, as cars become more connected and software-centric, the risk of such attacks increases significantly. That's because as the proportion of vehicle functions that rely on software to control them rises, so does the number of potential entry points for hackers. However, while these kind of 'in motion' attacks will grab most of the media attention when it comes to the security of connected and driverless cars, there are also many other potential risks to consider.

For example, criminals may attempt to hack into vehicles, not to control them, but to steal proprietary or sensitive data from manufacturers, application providers or corporate vehicle operators such as haulage and delivery vehicle drivers. This should provide serious food for thought for automotive OEMs, especially within the context of the 53% rise in annual industrial espionage cases reported by the FBI in July 2015.[1]

Another potentially damaging scenario involves the theft of personally identifiable data from individual vehicle owners or users. For instance, many drivers have their smart phones connected to in-car infotainment systems via Wi-Fi or Bluetooth connections. Increasingly, these devices are being used to make purchases and can therefore be a rich source of financial data such as credit card details. They also continuously transmit location data, which could be used to prove or disprove a driver's movements and driving behavior by employers, insurance companies or private investigators. All of which creates significant data privacy issues that automotive OEMs need to be aware of, in order to protect themselves against litigation and damage to brand reputation. Moreover, regulations and attitudes to data privacy vary significantly between countries, adding another layer of complexity.

In the worst case scenario, the failure to deal effectively with these issues could reduce or even eliminate consumer demand for vehicles, applications or services that are viewed as insecure. The potential consequences range from missed sales targets, to the market failure of new services or models.

In an ideal world, all of these risks should be preempted through a comprehensive strategy for connected car security covering the entire vehicle lifecycle, from design and manufacturing, through sales, usage and eventual retirement. And so the question arises, what is the optimal approach to connected car security?

VMware's experience in and innovative approach to security in the data center, vehicle head unit and across wireless networks, positions it perfectly to answer that question for organizations across the connected car value chain.

[1] FBI press briefing, July 2015

KEEPING THE HACKERS OUT – FROM THREAT TO OPPORTUNITY

It's every driver's (and manufacturer's) worst nightmare – losing control of a vehicle and suffering damage or injury due to a mechanical failure. Fortunately, modern vehicles are so well built and reliable that these instances are rare. But what if an apparent failure was instigated and controlled deliberately from outside the car?

The recent 'in-motion' hack attack staged by two security experts in the US (see previous page) proved that such an attack is possible, although they had actually already achieved a similar feat two years previously. The difference between the two events? In 2013, they were sitting in the vehicle with a computer physically connected to the head unit. In 2015, they hacked into the head unit remotely by exploiting an open port available for connecting to a cellular network via an embedded SIM card. The potential consequences of such an attack in a real world scenario are clear – serious injury or worse for vehicle occupants, and a catastrophic effect on the vehicle vendor's reputation. This provides proof, if any were needed, of the potential dangers associated with increasingly software-driven vehicles. What's more, these kind of 'traditional' hack attacks are not the only threat.

For example, a research fellow at the University of Cork has demonstrated how, by combining a laser device (similar to that used in mass market laser pens) and a pulse generator that can be created on any computer, the lidar sensors guiding a driverless car can be fooled into seeing objects on the road that are not actually there. In the researcher's test, the car slowed down automatically to avoid hitting these phantom objects and, had enough of them been projected onto the road, the vehicle would have stopped completely.[2] Just like the first example, this kind of incident is a great headline maker. But hackers can also inflict damage in many other ways. Potential threats include:

- Vehicle theft or electronic damage / disablement
- Falsifying vehicle information such as mileage data
- Accessing personal information such as phone numbers, address books, credit card details, location information etc., all of which could potentially be misused either directly, or for blackmail purposes
- Intercepting voice or data communications
- Accessing proprietary manufacturer, service provider or app vendor data from vehicle head units

Automotive OEMs must give this issue a very high priority, because failing to address it effectively could have a significant impact on interest in and demand for connected cars, driverless cars and the benefits they bring. However, there is also a more positive angle for manufacturers to focus on.

Vendors that can solve the challenges of securing connected cars in a thorough and scalable way, have a potential speed-to-market advantage over their competitors. In addition, if they can prove the superiority of their security solutions, they will have a powerful differentiator that can help them gain customer trust and build market share.

VMware is a pioneer in the fields of containerization and micro-segmentation, both of which improve security by separating computing resources, networks and data, minimizing the potential impact of hack attacks. Not only that, VMware understands how to leverage this technology in the data center and in the vehicle, in order to give automotive OEMs a competitive advantage in the connected car era.

[2] Reported in IEEE Spectrum, September 2015

BUILDING TRUST IN THE CONNECTED CAR

One of the biggest threats to the future success of connected and driverless cars is customer inertia and mistrust. Even 'digital natives' that generally care less about online privacy will think twice about taking advantage of connected car functionality, if they think it could put their personal information, or that of family and friends, at risk.

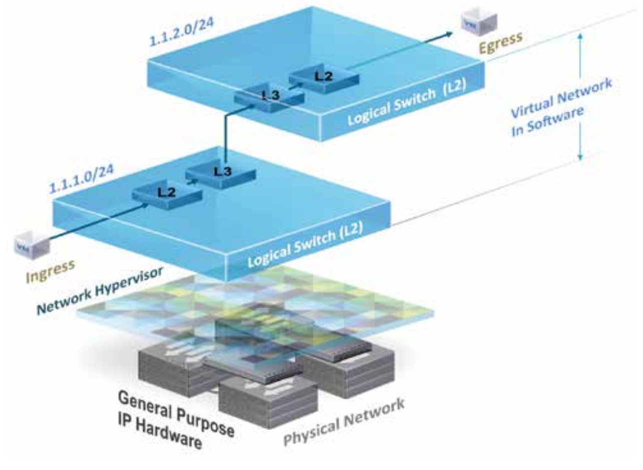
In this context, an important element in delivering a more personalized and connected automotive experience through new apps or services is ensuring that the personal data involved stays private. At the same time, manufacturers must also protect their own infrastructure and data from actions taken by customers or vehicle users. This could involve preventing drivers from using potentially insecure third-party applications within a secure vehicle software or network environment. But it could also be about preventing them from deliberately modifying a vehicle in ways that would invalidate warranties or insurance policies, or at least discovering they have done so, even if they have attempted to cover their tracks.

Finally, as car sharing increases, connected car manufacturers and fleet owners may want to be able to track driving behavior and journeys, and attribute them to specific individuals in the event of extreme driving behavior causing damage to a vehicle or otherwise invalidating a legal agreement.

It is clear that in the connected car era, every vendor in the value chain must perform a continuous and difficult balancing act between protecting customer privacy on the one hand, and ensuring the integrity and traceability of their own data and processes on the other. Finding that balance will be essential in ensuring disputes can be resolved and compliance obligations upheld, and a customizable approach to managing the type and frequency of data collected will be required. For example, some of the data needed for predictive analysis cannot be displayed or made available to third parties, in case it enables the unauthorized / illegal profiling of a driver's behavior.

AirWatch by VMware uses industry-standard algorithms and a strong privacy engine to enable the required customization of collected and stored data types in this scenario. Not only that, the head unit's IoT agent can store data in an encrypted container and transmit it to the data center over secure channels. Containerization, a technology well-established in the enterprise mobility management industry for the separation of corporate and private data, can also be used to address security and privacy challenges across the entire value chain.

VMware's NSX solution enables the three key functions of micro-segmentation: the isolation of networks, segmentation of communications, and support for multiple third-party security products. The same principles could potentially also be leveraged in the vehicle to provide even greater protection.



And, as a pioneer in micro-segmentation (see diagram), VMware can also ensure that if one vehicle application or system is compromised, other systems and services remain unaffected. All of which makes VMware the vendor best positioned to help manufacturers minimize the security risks and privacy / compliance issues that the connected car era will inevitably generate.

Bilder: shutterstock.de

CONNECTED CAR BUSINESS BRIEF SERIES

The VMware Connected Car Business Brief Series explains how VMware helps automotive OEMs build a highly scalable and secure infrastructure for the connected car and driverless vehicle era. The brochures cover the following topics:

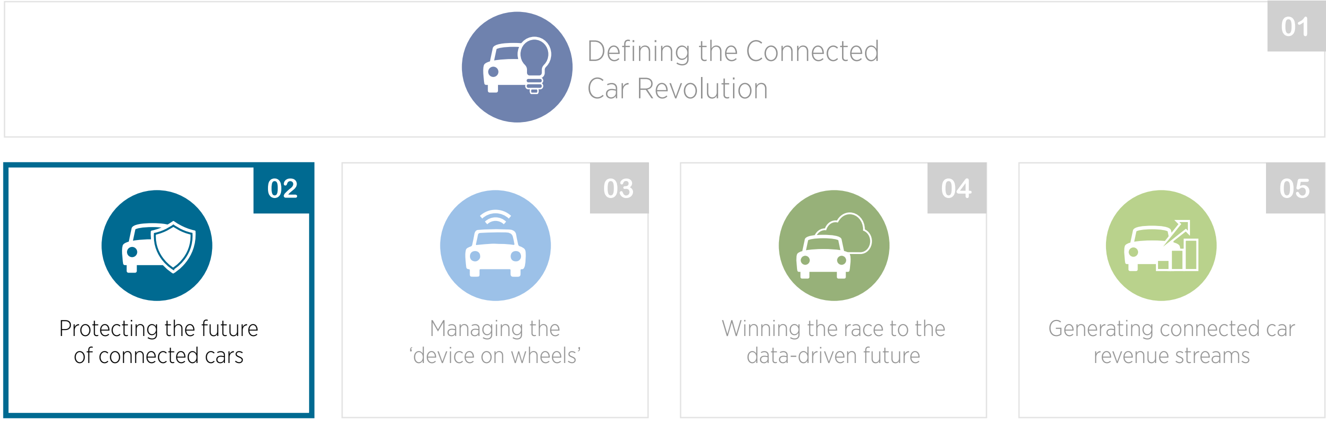
01 Vision: Powering new automotive business models through the secure and efficient sharing of data and intelligence between vehicles, users and vendors via the cloud.

02 Security: Innovative segmentation-based approaches to security in data centers, vehicle head units and wireless networks that minimize business risk and protect drivers.

03 Software over-the-air: Secure collection, analysis, management and delivery of real-time data transmitted over-the-air between drivers, vehicle head units and vendors.

04 Data collection & analysis: Maximum value from connected car data supported by the software-defined data center, secure public cloud infrastructure, cloud-based data management and intelligent in-vehicle device agents.

05 New business models: Driving new revenue streams through data recycling, shaping the in-vehicle user experience on demand, driverless transport services, and more.



01 Defining the Connected Car Revolution

02 Protecting the future of connected cars

03 Managing the 'device on wheels'

04 Winning the race to the data-driven future

05 Generating connected car revenue streams

Your Contact

Matthias Schorer
Lead Business Development Manager – IoT, EMEA

Since 2017 Matthias Schorer leads the Business Development for IoT in EMEA. Before he was Head of Strategy Consulting and responsible for the VMware Accelerate Advisory Services Team in Central and Eastern Europe. He has extensive expertise in IT architecture, legacy system migration, cloud computing and virtualization across multiple industries, with a focus on the automotive sector and connected car innovations.

mschorer@vmware.com
Tel. +49 89 / 3706 17108

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with its Cross-Cloud Architecture™ and solutions for the data center, mobility, and security. With 2016 revenue of $7.09 billion, VMware is headquartered in Palo Alto, CA and has over 500,000 customers and 75,000 partners worldwide.

vmware®

VMware Global, Inc.
Zweigniederlassung Deutschland

Freisinger Str. 3
85716 Unterschleißheim

www.vmware.com/de