Bodyguards of the road

Even cars have long been under attack from the Internet. In the worst case, a passenger's life is at risk. It is time for a cyber bodyguard to protect against hacking in real time.

COPY —— Yvonne Schmitz

Kevin Costner knows how to protect people: In the movie "The Bodyguard", the actor wrests pop singer Rachel played by Whitney Houston from a raging mob of fans and flees with her in a limousine whose driver had previously completed an advanced driving course.

This blockbuster was released in 1992, today the scene would probably look quite different. To protect against attacks, a skilled chauffeur and high-traction tires are no longer enough. Digital defenses are also needed. After all, 10 to 30 percent depending on which study you use of all cars are now connected to the Internet, and the trend is growing. This means not only more convenience from digital services like a mobile hotspot, but also more attention from hackers. Without airtight safeguards, cybercriminals can access a vehicle online from anywhere in the world – a foe from which not even Kevin Costner could drive away.

The most recent example shows that cars are not immune to security flaws: Around September 2018, Belgian experts publicized a weakness in the key fob for Tesla's Model S with which they were able to clone the key in seconds, then unlock and start the car itself. Great for car thieves, disastrous for car owners.

SECURITY FROM THE START

The automotive industry has acknowledged the risk and is making cyber upgrades. The law firm Foley & Lardner surveyed automobile and technology managers from the U.S. and Asia on the development of connected and self-driving cars: Nearly two-thirds indicated concerns about cyberattacks. Additionally, the 15 carmakers in the European Automobile Manufacturers Association (ACEA) have signaled their willingness to discuss new cybersecurity risks with government agencies, industry players, and other third parties. But is that enough? "Regardless of how carefully cars are developed in terms of IT security, a security flaw can always be left behind or develop with time," warned Christian Olt, senior security manager for automotive and manufacturing at T-Systems. This is why cars need a digital bodyguard that detects cyberattacks throughout its entire service life and immediately intervenes in an emergency: an automotive security operations center (SOC).

KEEN WATCHDOG ON BOARD

An automotive SOC is where all security-related data from the car and its surroundings would converge. One important source of data would be an intrusion detection system (IDS) inside the car. The automotive industry is already working intensely on integrating such systems. However, abnormalities in mobile networks and the manufacturer's backend are also relevant. For example, unexpected messages in the onboard network do not necessarily need to originate from an intruder. However, if unusual processes ran in the auto manufacturer's database shortly beforehand, the probability of a hack increases.

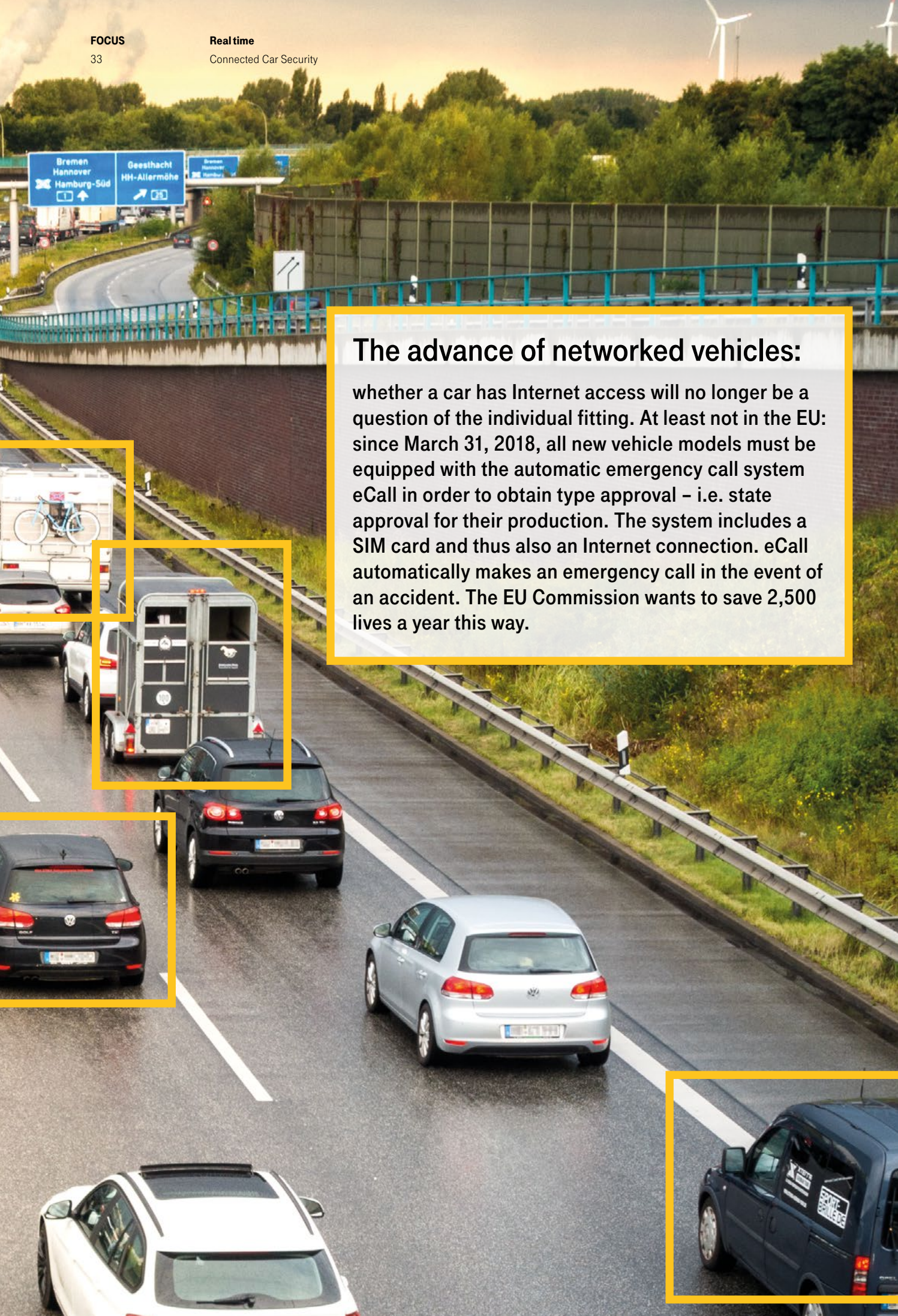
External information also helps identify cyberattacks. Threat intelligence, for example, uses a list of malicious IP addresses, tips from well-meaning security experts, and other SOCs, or even special future honeypots: car simulations that specifically attract hackers in order to discover new attack patterns.

RAPID RESISTANCE WITH A SIEM SYSTEM

A special system called a security information and event management (SIEM) system analyzes and correlates all data. If the system finds indications of a cyberattack, it alerts the security analysts in the automotive SOC through a dashboard. These analysts then take on the event, checking messages for false alarms and conducting their own research. The tough cases are handed to digital detectives at the security center: the IT forensic investigators, who comb through compromised systems and attempt to reconstruct the perpetrator's process. If necessary, they secure data from the affected vehicles directly on site.

Yet how do the specialists at the automotive SOC scare off attackers in an emergency? This procedure has been

Photo: iStockphoto



The advance of networked vehicles:

whether a car has Internet access will no longer be a question of the individual fitting. At least not in the EU: since March 31, 2018, all new vehicle models must be equipped with the automatic emergency call system eCall in order to obtain type approval – i.e. state approval for their production. The system includes a SIM card and thus also an Internet connection. eCall automatically makes an emergency call in the event of an accident. The EU Commission wants to save 2,500 lives a year this way.

3,300

data sources provide data for Deutsche Telekom's Security Operation Center.

The honeypot sensors in the Telekom network register

12 million attacks

every day.

Deutsche Telekom's Security Operation Center analyzes

1.5 billion

security-relevant events per day.

defined down to the last detail: An incident response plan establishes what steps the security analysts need to take for what alert. "Malicious software, for example, can spread through a network in minutes or even seconds," explained Olt. "There is no time for discussion. The faster the response, the less damage is done." Ideally, the carmaker would then also determine how quickly an analyst needs to respond to an alert.

Especially in extremely critical cases or when the countermeasure will not remain unnoticed, the automotive SOC team needs clear, coordinated instructions or has to get in contact with decision-makers, such as when a compromised vehicle SIM card continuously calls expensive hotlines and the SOC team wants to disable the mobile network module, but doing so would also turn off services like real time navigation.

PLAYING IT SAFE WITH DATA PROTECTION

One important aspect of working with data for an automotive SOC is data protection. For example, the German Association of the Automotive Industry (VDA: Verband der Automobilindustrie), along with state and federal data protection officers, assume all data associated with a license plate or vehicle identification number (VIN) is personal and thus relevant to data protection. This can apply to GPS data or vehicle speed. The problem with this is that, even without direct reference to a person, some data can be used to point to a specific passenger, such as revolutions per minute, which depends on an operator's driving style. "If carmakers want to be on the safe side," said Olt, "we recommend declaring that all data for an automotive SOC is personal."

However, for its analysis, the SOC itself does not need to even know the specific vehicle or person to which the data belongs. For this reason, car manufacturers should anonymize or pseudonymize this information before it is transmitted to the cyber defense center. The latter is always useful when the manufacturer wants to reestablish reference to the person at a later time to contact the owner, for example. This is not possible with anonymization.

EXPERTS WITH DOUBLE KNOW-HOW

Security operations centers themselves are nothing new. They exist in numerous sectors, including the automobile industry, to protect the IT of a company. The classical IT SOCs, however, are unfamiliar with both automotive technology and vehicle-specific threats. This is why cyber defense for connected cars needs its own specialized security center that combines the expertise from both fields: IT security and vehicle IT. However, a hotline between the two SOCs is advisable, since an attack that starts in the work space could spread to the vehicle domain.

Since the fall of 2017, Deutsche Telekom has been running one of the largest and most advanced security operations centers in Europe. A total of 200 experts monitor the systems of Deutsche Telekom and those of its clients around the clock both here and at connected sites all over the globe. They detect attacks virtually in real time, fend them off, and then analyze how the cybercriminals did it in order to optimize their own security. This effort is supported by important information obtained from the 2,200 worldwide honeypots in Deutsche Telekom's network.

The automobile know-how that is essential for an automotive SOC is also embedded in the corporation's DNA: The Deutsche Telekom subsidiary T-Systems helps many major manufacturers, suppliers, and dealers develop connected and self-driving cars. "With our experience in the areas of security and automobiles, we can help car manufacturers organize specialized cyber defense for the connected car," emphasized Olt. "Depending on need, we can also take over selected roles in operations, such as offering a standardized initial analysis of security alerts."

In a remake of "The Bodyguard", Kevin Costner could then ward off a hacker's attack that has remotely taken over control of Whitney Houston's limousine by reaching for his phone and simply asking his cyber colleagues to interrupt the car's mobile network connection.

Christian.Olt@telekom.de