ESCRYPT GmbH

Am Hain 5,
44789 Bochum, Germany
Phone: +49 234 43870-200

Press and Public Relations:
Martin Delle

martin.delle@escrypt.com
www.escrypt.com

Press Release

New security solution detects, analyzes, and parries cyberattacks on vehicles in the field

At CES 2018, ESCRYPT is presenting its intrusion detection and prevention solution. With the complete system combining an embedded solution and a cyber security backend, automotive manufacturers can detect and defend against cyberattacks on individual vehicles or entire fleets.

Bochum, December 8, 2017 – When car thieves try to break into a vehicle, their efforts should ideally, set off its alarm. And even if the alarm does not sound, there are still visible signs of the break-in. Contrast that with the hitherto invisible signs of unauthorized and criminal attacks on the IT systems of connected vehicles. The consequences can be dramatic: for example, when a hacker takes control of the car radio and suddenly turns it up to full volume, or siphons off personal data from a docked smartphone. And that is not to mention attacks on ECUs, which govern a vehicle's behavior, or illegal manipulation of the powertrain system.

Automotive security specialist ESCRYPT has now developed a solution that detects, analyzes, and defends against cyberattacks. Available since 2017, the Intrusion Detection and Prevention Solution (IDPS) for vehicles detects and documents attempted attacks and can automatically forward the data to a cyber security backend for evaluation. There, teams of experts apply the data in conducting forensic analysis of the events, so that they can define and implement appropriate countermeasures – for example, over-the-air security updates.

With these methods of detecting and defending against attacks, automotive security is becoming a continuous process that covers prevention (e.g. a firewall), the monitoring, reporting, and analysis of attacks, and the constant rollout of specific countermeasures. Not content with static defensive measures in individual vehicles, IDPS incorporates constantly updated data from the entire vehicle fleet. This means it can immediately provide effective responses to new – and always changing – risks and attack strategies.

A holistic approach – implemented with reliable technology

There is an urgent need for this comprehensive and integrated security approach. Forecasts indicate that in just four years, more than 380 million vehicles will be connected. Vehicle systems that have thus far been closed will rapidly open up to the outside world; interfaces to smartphones and the possibility of car-to-x communication are accompanied by new risks. At the same time, ECUs and their software are relieving the driver of more and more responsibility: automated driving is becoming a reality. This new connected world calls for integrated security strategies in which functional safety and automotive security are inextricably linked throughout the vehicle's entire lifecycle. This linkage starts right when development does, then continues with secure parameterization of ECUs in production, ensures safe vehicle operation at all times, and does not end until the cryptographic key has been deleted and vehicle identity invalidated before the vehicle is scrapped.

ESCRYPT has been employing this kind of integrated protection concept for almost 14 years. In addition to integrity testing of ECU software, authenticated onboard communication, and the securing of various vehicle domains using firewalls, IDPS has become an essential part of the ESCRYPT solution portfolio. Now that IDPS ensures the security of IT systems in connected vehicles during operation, the focus is now shifting to risks that are unknown or do not even exist at the time the vehicle is being developed and manufactured.

Intrusion detection and prevention for vehicles – IDPS

Intelligent intrusion detection and prevention systems are nothing new in traditional IT, having been tested and proven over the past several years to protect IT infrastructure. What *is* new is the transfer of this technology to the connected vehicle. Special security software in the vehicle's central ECUs or gateways detects and documents anomalies in vehicle network communication.

In the event of an attack, IDPS launches a five-step defense. If the attack follows a known pattern, the embedded firewall CycurGATE immediately blocks access to ECUs. But to parry future attacks as well, the established rule sets (black- and whitelists) have to be continuously updated – and this is precisely the essence of IDPS. In the second step, anomalies and signs of a previously unknown type of attack are identified by the new intrusion detection software CycurIDS. Designed to run on CAN-based and future Ethernet-based EE architectures, it monitors data traffic. Step three stores any anomalies logged in the vehicle and uploads them later, or automatically transmits them to a cloud-based event database to enable faster response times. In this database, reports from all the manufacturer's connected vehicles can be compiled and the reported anomalies can be compared with the fingerprints of known attacks.

From the analysis of the data, OEMs receive a comprehensive and always up-to-date overview of the strategies hackers are employing, what vulnerabilities they are targeting, and if the attacks are increasing. Evaluating this extensive event database in the backend is step four of the defense strategy: CycurGUARD. Based on big data analysis technologies, this automated software solution analyzes the attack patterns and presorts them, the results of which can be used by the security and data forensic experts in the Cyber Defense Center in deciding on countermeasures. These may include specific adjustments to the firewall, updates to the CycurIDS rule sets, or even closing loopholes in the software in close cooperation with the manufacturers of the ECUs affected (step five).

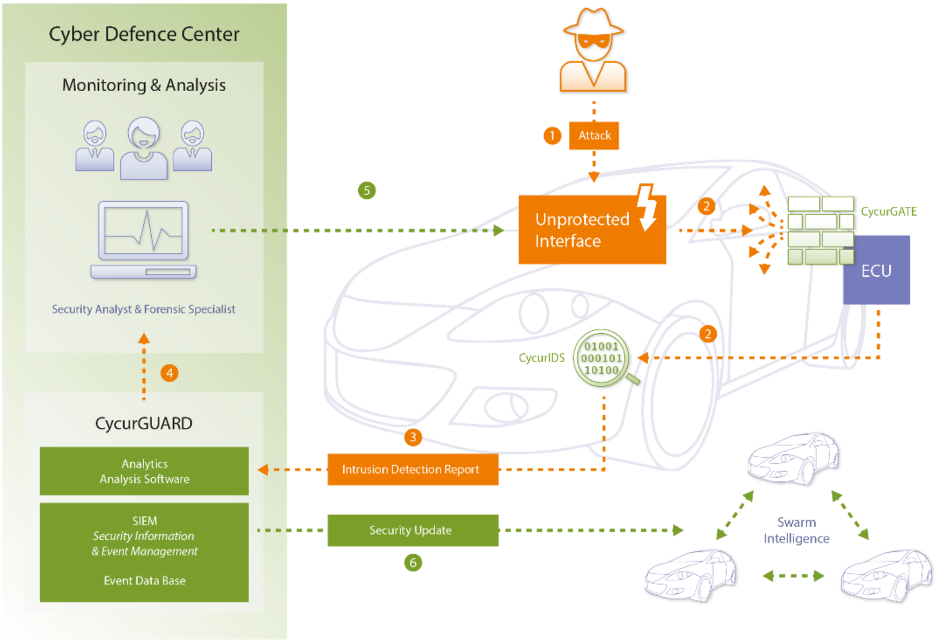
As one possible countermeasure, security updates can then be transmitted over the air to all connected vehicles in the fleet; naturally, these transmissions are sent only over a secure communication channel. In addition, the updates themselves are protected with digital signatures against unauthorized modifications. A complete key management solution (CycurKEYS) for such use cases, is also part of the ESCRYPT portfolio.

Intelligent security is based on a broad, continually updated database

With its five-step defense strategy, IDPS represents a future-proof, scalable solution. But it's more than that: every vehicle added to the system boosts its ability to analyze and detect attacks, thus improving the options for defense. Each hitherto invisible attack – possibly blocked by firewalls – helps to tailor security measures more closely to current risks. Instead of languishing in data storage until the vehicle's next trip to the repair shop, logged anomaly reports are sent directly to the cyber security backend, where they can immediately help improve protection. In other words, IDPS is the connected car's "immune system": it grows stronger with every attack and is becoming steadily smarter, thanks to a constantly expanding database.

As a pioneer in automotive security, ESCRYPT leverages its years of expertise to prepare vehicles for the profound changes brought about by a connected world. IDPS puts customers in a position to adapt their defense systems to modified attack strategies and new cyber risks at any time, instead of getting stuck on the defensive using passive protection. Thanks to its wide-ranging experience gained in numerous large-scale industry projects, ESCRYPT can seamlessly integrate its holistic security solutions into the development and verification of ECU hardware and software. In this way, IDPS and over-the-air updates are incorporated into production models via secure and established paths. The traces of digital break-in attempts are therefore no longer invisible – in fact, they can even be used to improve defensive countermeasures.

Intrusion Detection and Prevention – IDPS at a glance



ESCRYPT GmbH - Embedded Security

Martin Delle

+49 234 43870-290

martin.delle@escrypt.com

ESCRYPT GmbH – Embedded Security

ESCRYPT - Embedded Security is the leading system provider for embedded security world-wide. With locations in Germany, UK, Sweden, USA, Canada, India, China, Korea, and Japan we have security specialists available to help with current security topics such as secure M2M-communication, IT-security in the Internet of Things, protection of e-business models and automotive security and they develop highly secure, worldwide valued products and solutions which are tailored to the specific requirements of embedded systems and the relevant IT-infrastructure and are tested and proven a million times in automotive series production.

For further information: www.escrypt.com