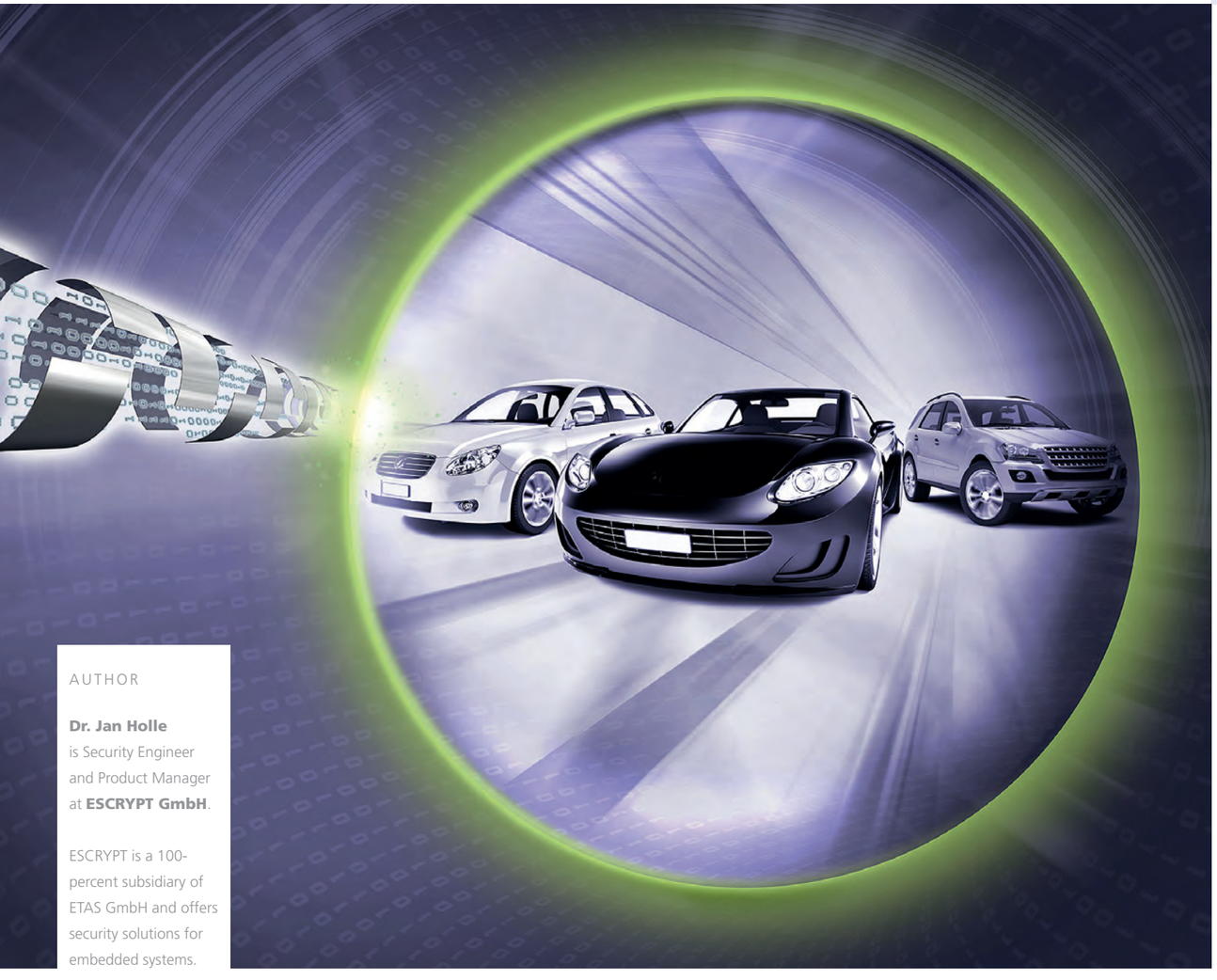
Immune System for the Connected Vehicle

Intrusion detection and prevention system (IDPS)

Increased safety and comfort. Optimized service and more enjoyable driving experiences. There is a long list of advantages to connected vehicles. However, integration into the Internet of Things also involves risks. It increases the danger of cyber attacks, and attackers are forever finding new weaknesses to exploit. Therefore, connected vehicles need learning defense systems which detect attacks even when the pattern is still unknown and are able to swiftly pass on new experiences to other vehicles in the field.



AUTHOR

Dr. Jan Holle
is Security Engineer and Product Manager at **ESCRYPT GmbH**.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Once vehicles are in the possession of customers, then manufacturers have only occasional access to their systems. Nevertheless, buyers rightly expect their vehicles to be protected at all times. At a time when vehicles are becoming increasingly connected, this throws up new challenges. Although it does mean manufacturers obtaining better access possibilities, entering the Internet of Things also increases the risk of unauthorized access and malicious cyber attacks. Functional safety alone is no longer enough. Manufacturers also have to guarantee comprehensive automotive IT security, if hundreds of millions of connected vehicles are to be on our roads around the world. In addition to this, we must also consider the coming trend of automated driving, which will increase the safety and security requirements of IT systems even further.

Holistic protection throughout the entire life cycle

The required security level presupposes well-thought-out and effectively implemented measures. Automotive security is not retrofittable – or at least only at horrendous costs. What is needed instead are holistic strategies in which safety and security are considered together from day one of development. Part of the solution is standardized processes in the development of embedded software, such as reliable protective measures. Modern chip architectures with hardware security add-ons – including Hardware Security Modules and secure hardware extensions – physically shield safety-relevant system domains against unauthorized access. Around these security cores, further measures are required: secure boot functions that recognize any manipulations of the ECU firmware, and protected network gateways or cryptographic solutions for safeguarding all communication. No less important are organizational protective measures in development and manufacturing, from access-restricted security areas to the restriction of access rights for crypto keys and unlock codes to a few responsible individuals.

The measures described reduce the probability of random errors. And they thwart the efforts of hackers to get into vehicle systems. However, they still do not answer the question of how to guarantee the protection of connected systems once the vehicle is in the customer's possession. In this core phase of the life cycle, manufacturers have only limited opportunities to access the vehicle. Theoretically, they have to pre-arm vehicle systems during the development stage to deal with attacks that can lie more than a decade in the future. A look back at the state of information technology ten years ago should be enough to appreciate how improbable that is.

The challenge: protection against unknown dangers

The logical conclusion is that IT security measures must be dynamic and ongoing in order to reliably protect the systems even when they are in customers' possession. However, whereas the boundary conditions of functional safety are based predominantly on the laws of nature and statistical predictions, which continue to apply during the usage phase, the assumptions and boundary conditions of IT security are volatile. Attackers continuously seek out new weak points in the system. It is in the nature of things that manufacturers are generally not aware of the existence of these weak points. Equally, it is not possible for security experts to foresee all attack strategies that may eventuate many years in the future. Traditional IT is also

faced with the challenge of protecting IT infrastructures against attacks using unknown patterns. Here, too, attackers try to get around security mechanisms that are thought to offer full protection. Increasingly in this area, protection means providing intelligent intrusion detection and prevention systems (IDPS). On closer observation, these systems are predestined to protect connected vehicles also.

Immunization via IDPS

The unique advantage of IDPS technology is that it uses the connectivity of vehicles to be able to respond quickly to new attack scenarios and immediately pass on the resulting defense strategies to the entire vehicle fleet. This creates a sort of immune system that reacts dynamically to attacks – and in which each new attack strengthens the defenses of the fleet.

The core of ESCRYPT's IDPS is special security software which keeps watch in ECUs or gateways and constantly analyzes all on-board electrical communication in its entirety. If anomalies arise, it documents them – and instigates defensive measures when there is a serious threat. If the detected attack pattern is of a known kind, firewall mechanisms block communication between the various data buses. This is already routine and – like the entire IDPS – can be used on the mainstream CAN networks of today as well as future Ethernet networks.

Where IDPS technology really shines, however, is in its ability to recognize and repel unknown patterns and attack strategies. To do this, it possesses a repository of rule sets (blacklists and whitelists) that are constantly updated. This is one of the strengths of the approach: anomalies and clues for currently unknown attacks are detected by the "CycurIDS" attack recognition software. This software is able to store anomalies in the vehicle so that they can be reviewed later. Even more effective, however, is a function that automatically transmits all anomalies to a cloud-based event database, where all anomalies from all the manufacturer's connected vehicles are stored together with the fingerprints of known attackers, facilitating effective comparisons.

Whole fleet as basis for a dynamic protection strategy

From the analysis of the data, OEMs receive a comprehensive, always current overview of which strategies hackers are pursuing, which weak points they are targeting, and whether attacks are clustering in a particular area. To evaluate this comprehensive event database in a backend, the next stage of the dynamic defense system kicks in: the automated CycurGUARD software solution, which is based on big data methods. This software analyzes the attack patterns and carries out a presorting process, on the basis of which security analysts and forensics experts located in a Cyber Defense Center decide whether countermeasures are required and which ones should be initiated. These measures might be targeted adjustments to the firewall, or updates of the CycurIDS rule set, or removing weaknesses in the software of affected ECUs in close consultation with their manufacturers.

The measures undertaken can then be transmitted over-the-air to all connected vehicles in the fleet – cryptographically protected of course. In addition, the updates are protected against unnoticed changes by virtue of digital signatures.

Summary

Because all detected anomalies from all vehicles in the field converge in the central, cloud-based event database, new attack patterns are identified quickly. With each additional vehicle that connects to this network, IDPS becomes more intelligent and better equipped to defend against threats. This is so because previously invisible attacks – e.g., ones that have been blocked by firewalls – feed into a continuous situation evaluation, meaning that security measures can be adapted in a faster, more targeted manner to current risks. In a network, this then creates an immune system for the connected vehicle, which becomes stronger and better able to defend itself with every new attempted attack. The constantly growing database and immediate relaying of defense strategies to all vehicles in the fleet ensure all-around protection that grows ever more comprehensive all the time.

Security for the entire vehicle life cycle, from the initial idea through to decommissioning.

Five steps to an "immunized" fleet.