INTERVIEW
Dr. Thomas Wollinger discusses the safest route to smart mobility

CONNECTED MOBILITY
Holistic IT security helps combat automotive ransomware

CONNECTED INDUSTRY
End-to-end protection against cyber attacks – a must in connected manufacturing

ESCRYPT
Security Special

www.escrypt.com
Dr. Wollinger, is the automotive industry starting to pay more attention to security issues?

Dr. Thomas Wollinger:
It’s really exciting to see how things are taking shape. The industry is facing a fundamental shift, including completely new business models based less on selling cars and more on data-driven services. As digitalization and connectivity extend their reach, we are continuing to witness the death knell of traditional vehicle platforms with static control units and the advent of Ethernet-based platforms with distributed and connected ECUs. Individual embedded security functions just don’t cut it anymore. We must think and act beyond the vehicle and take a holistic approach.

What do you mean by that?

Dr. Thomas Wollinger:
When we talk about the future, we’re talking about connected and automated driving. And this is based on exchanging data in real time, which provides a bigger target for attacks and means that threats take on a whole new dimension. When vehicles become rolling computers in a network, IT security becomes a question of personal safety.

So the car as a system needs to be completely protected, as does the communication among vehicles and between vehicles and roadside equipment, as well as the traffic infrastructure itself. And we must do this throughout the entire life cycle. We need to protect vehicles that will be on the road for 15 years or more from cyber attack methods we haven’t even experienced yet. Achieving that means having the right processes and organization in place right from the start. Holistic automotive security, as we at ESCRYPT understand it, requires effective protection for the entire system and its infrastructure. We need to apply that to the entire life cycle and provide the corresponding organizational support.

So that’s the theory – but how does it translate into practice?

Dr. Thomas Wollinger:
A prime example is our intrusion detection and prevention solution: Security software in the vehicle monitors the central ECUs and gateways. Anomalies in the electrical system communications are detected, documented, and forwarded to a security operations center in the backend. There, tools analyze the aggregated data and, in the event of a cyber attack, security updates are carried out for the whole fleet in line with defined incident response procedures. The major advantage is that new attack patterns are detected as soon as one vehicle is targeted, so immediate steps can be taken to protect the entire fleet. What you get is a kind of immune system in which IT security mechanisms are sustainably maintained over the entire life cycle and supported by the organization.

In other words, the IT security of an automaker’s fleet hinges less on the security measures themselves and much more on how these are coordinated and managed.

Dr. Thomas Wollinger:
Absolutely. For OEMs, protecting their vehicle fleets will be a constant, complex, and crucial task. They will require predictive concepts, concrete security structures, and sufficient resources. And they will need a central security management function that
ensures the harmonious interplay of all the security measures, providing guidance to everyone involved at the OEM as well as to external service providers, suppliers, and workshop participants – similar to how a conductor leads and develops an orchestra.

Just as automakers already orchestrate the processes and requirements of their core business, in the future they will have to orchestrate automotive security. The only route to smart mobility is through effective IT security.

“When vehicles become rolling computers in a network, IT security becomes a question of personal safety.”
Dashboard demand for ransom payment

WannaDrive? Holistic IT security helps combat automotive ransomware

Commercial vehicles and vehicle fleets are high on the list of targets for online extortionists. Potential victims include trucks transporting perishable goods on tight delivery schedules, bus companies, rental car fleets, car-sharing pools, expensive construction machinery, and special-purpose vehicles, to name just a few examples. If cyber attackers succeed in taking these vehicles as digital hostages using ransomware, their chances of coming away with the cash are pretty high.

Ransomware attacks take little effort to orchestrate

Although there are no known cases of ransomware attacks on vehicles to date, a look at real-world examples from other sectors make it easy to conceive a likely attack scenario. Cyber criminals usually rely on a ready-to-use ransomware kit or ransomware-as-a-service solutions, which include bot masters and bitcoin payment systems. Ransomware kits have thus far primarily targeted conventional desktop PCs and servers. But with the number of vehicles open to such attacks and fleet operators’ vulnerability to extortion in the connected network increasing, ransomware variants for Automotive Linux or AUTOSAR will inevitably start to appear. There are already numerous potential access points for ransomware. Examples include infotainment systems that retrieve online content; in-vehicle reception of communications (such as emails, text messages, instant messenger services, digital radio); smartphones or navigation systems that are connected to a port in the vehicle; firmware updates over-the-air.
Security engineers from ESCRYPT were able to simulate a ransomware attack using a test model. They took a Raspberry Pi computer running Linux OS and a touchscreen as the automotive infotainment system. The next step was to connect these to a genuine speedometer control unit with OEM firmware using a gateway ECU and a proprietary bus network – as would be the case in a normal vehicle. They subsequently exploited a USB port to “infect” the Raspberry Pi, or host ECU, with Python-based ransomware. As intended, the ransomware client then locked the speedometer and set it to display the top speed at all times. At the same time, a demand for a ransom payment to an anonymous bitcoin account flashed up on the infotainment system’s touchscreen (see Figure). The ESCRYPT experts concluded that ransomware attacks on vehicles are easy to execute and pose a real threat – if IT security is not continuously upgraded to address the increasing connectivity of motor vehicles.

Holistic security approach prevents attacks from the outset

Despite their numerous vulnerabilities to attacks, vehicles on the road today often fail to provide backup for important data and functionalities. Nor do they receive regular security updates. What’s more, most of today’s vehicles have only very basic (gateway) firewalls and rarely feature automatic intrusion detection and prevention systems (IDPS) that provide proper protection. Upgrading these vehicles is usually difficult and costly. The most effective way to protect vehicle IT systems against ransomware and other forms of cyber attack lies in automotive manufacturers integrating comprehensive and effective information security into the development of their vehicle platforms from the outset. An all-encompassing security approach should address the entire vehicle system from end to end – including its IT infrastructure and the entire life cycle of the vehicle until it is scrapped. It should also cover the complete spectrum of organizational aspects such as defined security processes and security governance.

The comprehensive protection of vehicles therefore necessitates a series of interconnected security measures. In vehicles themselves, embedded security components can help defend against hacker attacks and malware with known signatures. Moreover, an intrusion detection and prevention system (IDPS) can detect and shut down critical anomalies in onboard network communications – including ransomware attacks. This can be achieved within the vehicle itself. Alternatively, a connected cyber security operations center (SOC) in the backend can distribute security updates to an entire fleet of vehicles to counteract a newly detected hacking pattern. But what if a ransomware attack succeeds? In such a case, the victim needs to respond quickly and effectively. A pre-defined incident response procedure, for example, can be used to specify countermeasures, one of which might even be payment of the ransom demand as a last resort in an emergency.

One thing is for sure: the potential threat that ransomware poses to vehicles calls for effective, end-to-end security – and this should not be seen as a costly burden, but rather as a key factor for success. After all, this security gives fleet operators and vehicle manufacturers the protection they need to ward off online blackmailers, and prevent product recalls and claims for damages.

If ransomware successfully hijacks the system, it proves extremely difficult to free the car, a digital hostage, from the hands of the cyber criminals

Author

Dr.-Ing. Marko Wolf is Head of Consulting & Engineering at ESCRYPT.
Time is of the essence. Picture a facility in which production processes run at full capacity 24 hours a day. Suddenly, the touchscreens on several machines fail. When the personnel check to see what is wrong, they realize that access to the central process data is blocked. It is not long before they receive a blackmail threat by email.

This is not a made-up scenario. Since 2016, Germany has been hit by six major waves of cyber attacks. According to the Federal Office for Information Security (BSI), some of the companies affected saw their operations grind to a standstill for several weeks and reported losses amounting to millions of euros. The BSI reports that attacks on plant control systems and industrial computers are on the rise. This upward trend is attributable to increasing numbers of connected processes which create new targets for cyber criminals. BSI president Arne Schönbohm is understandably worried: “We’re seeing an ongoing surge in IT security incidents; they are occurring with increasing frequency and reaching new levels of sophistication.”

At the dawn of Industry 4.0, this is clearly an unsettling message.

Industry 4.0 promises to bring enhanced efficiency, transparency, and flexibility to production processes – but also comes with a greater number of risks. Connected environments see the field-buses used in the past replaced by Industrial Ethernet, while production systems can be accessed via internet protocol (IP). Opening the systems to the outside world in this way increases the risk of unauthorized access to the control software and to sensitive data. The recent spate of attacks – many of them successful – shows that even global corporations with highly advanced IT infrastructure underestimate the risks.

Small and medium enterprises do not always make the necessary investments in cyber security, either. Many falsely assume that hackers would have no interest in their production facility. They run their production IT systems non-stop and often miss updates as a result, which is precisely what makes these companies so vulnerable to both manual and automated attacks. Even machines not connected to the smart factory are at risk from attack during maintenance, for example, or via unauthorized USB interfaces. Blackmailers can moreover target production operations as part of wider supply chains. And if that is not reason enough to take precautions against cyber criminality, new regulations such as Germany’s IT Security Act stipulate that companies must implement industrial IT security measures by law.

A job for the experts

The only way to reliably protect connected production facilities from the dangers of cyber criminality is to put holistic security solutions in place. It takes a deep understanding of heterogeneous
IT systems in the production environment to perform the detailed status quo analyses required to systematically identify and evaluate risks, and to define security objectives. Security concepts must allow for maintenance and updates in facilities where machines run around the clock, and account for multiple operators accessing individual systems – which makes password protection a highly impractical solution. In-house IT departments – perhaps more accustomed to dealing with office IT – are rarely in a position to develop holistic security solutions for their production systems alone. This is where the experts come in.

After all, security needs to be addressed at all levels and appropriate governance developed in order to firmly embed IT security in organizational structures, in processes, and in people’s minds. Verification of the solution’s effectiveness using the PDCA cycle (plan, do, check, act) is equally as important as having an information security management system in place (ISMS). Cornerstones of holistic protection include prevention of risks, identification of critical incidents, and initiation of quick responses to defend against such incidents. End-to-end security solutions must also enable conclusions to be drawn about future threats. Only in this way can companies ensure the integrity, availability, and authenticity of all IT components and systems in their connected production facilities, and protect the confidentiality of the associated data.

Concrete security measures

Given the heterogeneous nature of IT systems, existing production lines are difficult to protect. For this reason, it is advisable to transfer protection measures for individual machines or security zones to upstream systems. That, first of all, shields process communication from the outside world and filters out any suspicious network traffic. It moreover enables antivirus software, defense functions, application recognition, and user identification to be updated without stopping production activities. Zone models also provide protection whereby firewalls monitor communication between individual production zones. Based on source and target information, they filter out unauthorized network traffic. Setting up these zones calls for IT experts to work closely with production experts. And, if a secure environment is divided up in this way, it is important to ensure that tasks such as implementing updates or changes, or legally compliant reporting, remain easy to manage.

Best practice: end-to-end security by design

The situation is different in new smart factories, however, because industrial cyber security can be integrated directly into the software and hardware control systems for the production lines in the planning stage. Security organization, continuous IT security management, and protection of components and systems can be harmonized from the outset and designed to cover the entire lifecycle of the plant and machines. This end-to-end security by design approach means that production facilities become connected IT systems in themselves, which puts security at the very heart of Industry 4.0.

Author

Norman Wenk is Group Manager Enterprise IT Security Consulting at ESCRYPT.

*) Source: BSI-Magazin 2018/1
Solution Portfolio

Design Security

Security Consulting and Design

Strategic Security Consulting
- Strategic security development, security vision and roadmap
- Security standardization, lobbying, and strategic cooperation

Enable Security

Security Products and Solutions

Production Key Server
Crypto server for secure key injection in mass production

ECU Production

Managed PKI Service
allows OEMs to maintain internal control over vital aspects of security such as certificate issuance, suspension, and revocation.

CycurHSM
Automotive-qualified security stack for HSM

Security Operations Center (SOC)
acts as mission control, tracking anomalies and events in any aspect of a vehicle’s operation.

Secure Product Design
- Secure Product Design
- Secure Connected Products
- Automotive Security

Enable Security

Security Basics
- Security Risk Analysis
- Secure Product Design
- Secure Connected Products
- Automotive Security

Secure Operations
Center (SOC)
acts as mission control, tracking anomalies and events in any aspect of a vehicle’s operation.
Product Security Consulting
- Security Risk & Threat Analyses, Protection Requirements
- Security Concepts & Design
- Security Roles & Processes
- Custom Consulting

Product Security Engineering
- Security Specifications
- Security Implementations
- Security Integration
- Security Production
- Security Management

Security Testing
- Functional Security Testing
- Vulnerability Scans & Fuzzing
- Penetration Testing
- Code Security Audits
- Security Certifications
- Security Test Management

Threat Intelligence and Forensics deliver evidence-based knowledge about existing or emerging menaces to induce informed decisions and responses.

Vulnerability Management helps uncover flaws and enables OEMs to implement a proactive threat-prevention strategy.

CycurV2X-SCMS V2X security credentials management system

CycurKEYS Secure management of cryptographic keys and certificates

CycurTLS Transport Layer Security (TLS) for embedded platforms

CycurGUARD Intrusion monitoring and analysis

CycurACCESS Vehicle access and key sharing

CycurV2X Secure V2X Communication SDK

CycurGATE Automotive firewall

CycurIDS Intrusion detection

CycurLIB Cryptographic library

Credential Management

Cyber Defense Center

Backend
Homogenous security for hybrid V2X communication

Standard solution enables versatile data transfer during connected driving

Connected driving is one of the most promising concepts in the future of mobility. Achieving it requires a Cooperative Intelligent Transport System (C-ITS) – a solution that enables the real-time exchange of data in both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. In the future, experts expect this vehicle-to-everything communication to work on the basis of multiple technological standards simultaneously. Yet maintaining security will still be paramount.

Up to now, direct V2X communication has been based primarily on ITS-G5, a dedicated short-range communication (DSRC) standard. That means the vehicles and roadside equipment essentially exchange data through direct wireless LAN communication. But this situation is set to change. Efforts are already underway to implement parallel use of another standard for V2X data exchange, namely the LTE-V standard for high-speed wireless communication (currently 4G, soon to be 5G). With new kinds of wireless chips installed in devices, that will make it possible to include other road users (e.g., pedestrians or cyclists) in the communication process in the form of direct, ad hoc data exchange between devices (C-V2X autonomous). A number of other standardized concepts will also be added to the mix, including mobile edge computing (MEC), which distributes messages via a cellular network at close range (e.g., for tailback warnings), and traditional wireless communication via cell towers for communication with cloud and backend services (see Figure 1).
That raises the question of how to secure this kind of hybrid V2X communication in the most efficient manner.

The solution lies in ensuring the protocol stacks used for V2X communication between all V2X devices and entities have a consistent, intelligent structure (see Figure 2). V2X messages are generated on the application or device level and relayed to the transport and transmission level. This is where the security header is added to each V2X message via the security components interface. The header includes the message signature and the associated certificate; if necessary, the message can be symmetrically encrypted in a second step. Information relating to the symmetric key is included in the header to enable recipients to decrypt the V2X message. To ensure data protection for the entities communica-

Protocol stacks with a consistent, intelligent structure

The likelihood is that we will see various types of V2X communication designed to serve different channels and standards depending on the particular use case and entity. That raises the question of how to secure this kind of hybrid V2X communication in the most efficient manner. It would be entirely wrong to think that each of the different transmission channels should have its own security solution. Instead, what is called for is a security concept that is effective across the full spectrum of V2X communication with all its different use cases.

Road testing with the CONCORDA project

Hybrid communication for vehicles is a sensible and useful development for connected driving. It paves the way for integrating more systems, road users, and services into V2X data exchange. At the same time, IT security is and will remain a necessary and fundamental condition for V2X. Establishing an intelligent concept means providing consistent, homogeneous, and efficient IT security across the various V2X communication channels and standards.

A trial run is currently underway on test routes in the Netherlands, Belgium, Germany, France, and Spain in the shape of the CONCORDA (Connected Corridor for Driving Automation) project, which is funded in part by the European Union and carried out in collaboration with companies including ESCRYPT, Deutsche Telekom, Nokia, Bosch, and Volkswagen. By mid-2020, CONCORDA will have shown how a hybrid V2X communication system with ITS-G5, LTE connectivity, and a consistent IT security architecture performs in practice.

Authors

Dr. Norbert Bißmeyer is Project Manager at ESCRYPT. Jan-Felix van Dam is Security Engineer at ESCRYPT.
Automotive security from the inside out

Hardware security module (HSM) offers protection inside ECU’s main processor

Electronic control units (ECUs) are the backbone of in-vehicle communication and function control – and that means they need reliable protection against unauthorized access. Hardware security modules (HSMs) meet this challenge by embedding security functions within the ECU’s main processor. Combined with security software stacks, they are the key pillar of any effective vehicle security system.
When chip tuners access powertrain ECUs to modify system parameters, noise and emissions restrictions are the last thing on their mind. Yet perhaps even more unsettling is the very idea that they can access electronically controlled vehicle systems in the first place.

The problems that a malicious hacker could cause in a powertrain or chassis ECU simply do not bear thinking about. Every ECU in a vehicle’s electrical system is a potential target, especially when it comes to connected vehicles. To prevent unauthorized software manipulation and access to critical key material, modern vehicles need robust IT security mechanisms to shield them from the outside world. That’s exactly what hardware security modules (HSMs) do by implanting security functions right at the heart of ECUs.

**Automotive-specific HSMs**

HSMs are a form of hardware that physically encapsulates security functions. Specifically designed for IT security applications, these integrated chips typically have their own processor core, various types of memory (e.g., RAM, ROM, flash), and hardware crypto accelerators. HSMs must also meet specific standards for use in vehicles, and highly efficient integration is essential to keep costs down. Key requirements include secure interfaces between the ECU application and the HSM as well as debugging and testing interfaces for analyzing malfunctions. HSMs must be able to process cryptographic information with minimal latency and exhibit adequate resistance to the typical temperatures found in automotive environments.

Several leading chip manufacturers already offer hardware security modules with automotive-grade architecture, including Infineon, ST Microelectronics, Renesas, and NXP. Essentially, the HSM uses its own processor core to provide all the IT security functions required for automotive use cases. These include a 128-bit AES hardware accelerator, a true random number generator (TRNG) to generate key material, hardware-protected storage of cryptographic keys, flash and debugging functions, and the HSM’s own RAM that is separate from system memory (see Figure 1).

**Tailored security software and real-time communication**

An automotive HSM only really comes into its own in combination with a secure software stack. If the HSM is the nucleus of vehicle IT security, then HSM security software is its genetic code. ESCRYP'T provides this in the form of its CycurHSM security firmware, which is specifically tailored to automotive HSMs from a range of manufacturers. CycurHSM links the existing hardware security peripherals to the relevant HSM and host controller applications. The firmware also implements a comprehensive cryptographic library on the HSM including symmetric and asymmetric encryption mechanisms and additional HSM-based security functions. CycurHSM also includes the AUTOSAR-compliant and non-AUTOSAR-compliant interfaces required to integrate HSMs in standard vehicle ECUs.

The core element of the software architecture is a real-time operating system. This ISO 26262-certified system is specifically
tailored to automotive ECUs and supports real-time HSM functions such as secure in-vehicle real-time communication. The operating system works with minimal runtime overhead and is MISRA-C-compliant. CycurHSM includes a session manager that implements priority-based task scheduling. For example, the validation of new messages on the vehicle bus takes priority over non-time-critical operations. It also incorporates a keystore manager that governs both access to and generation, storage, and deletion of key material in the HSM and supports symmetric and asymmetric keys of different lengths. The cryptographic library (CycurLIB) provides the cryptographic primitives (ECC, RSA) using the HSM’s crypto accelerator. Where required, a SHE emulation can also be run on the HSM while accessing the cryptographic library in order to meet enhanced automotive-specific requirements (SHE+). In addition, dedicated HSM drivers secure communication between the HSM and host processor: an AUTOSAR-compliant crypto service manager (CSM) at the interface to the HSM ensures that AUTOSAR applications can access the module at any time (see Figure 2).

This feature set enables the HSM software stack to support a broad array of security use cases. It provides a standardized interface that can be used to implement a variety of IT security functions either on the HSM itself or in concert with the host processor, in all cases based on strong cryptography. These functions start with secure boot – in other words checking the code stored in the flash memory each time the ECU is activated – and also include runtime manipulation detection and secure flashing as well as authentication of software download providers and a secure log function for reliably documenting security-critical events. The core principle in all these cases is mutual authentication of the requesting instance and the HSM. This also applies to secure debugging.

New HSM firmware generation

The development of HSM hardware and software is progressing rapidly, and an increasing number of microcontrollers for ECUs now come with an automotive-specific hardware security module as standard. ECRYPT is keeping pace with these developments which protects the ECU against unauthorized access to the debug port while simultaneously allowing authorized access for software debugging purposes. In this case, too, the HSM exercises control over communication and authentication.

Figure 2: Software architecture of the hardware security module (HSM).

Multifunctional and easy to implement

Hardware security modules offer far more powerful features than purely software-based solutions. Since the HSM security functions are physically encapsulated, the ECU host controller can focus entirely on its own tasks. Combined with the HSM security software, this approach yields a turnkey solution with numerous advantages:

- Enables simple customer integration through standardized interfaces to HSM
- Fully programmable – can be configured to meet specific needs thanks to its modular structure
- Multicore support

This feature set enables the HSM software stack to support a broad array of security use cases. It provides a standardized interface that can be used to implement a variety of IT security functions either on the HSM itself or in concert with the host processor, in all cases based on strong cryptography. These functions start with secure boot – in other words checking the code stored in the flash memory each time the ECU is activated – and also include runtime manipulation detection and secure flashing as well as authentication of software download providers and a secure log function for reliably documenting security-critical events. The core principle in all these cases is mutual authentication of the requesting instance and the HSM. This also applies to secure debugging,
by steadily improving its HSM software stack, CycurHSM. The latest generation of CycurHSM offers even more user-friendly and differentiated options for implementing customized IT security functions in ECUs. The new HSM firmware enables easy configuration via the applet manager plus activation of individual security features using the variant management system. The ASPICE-compliant software also comes with a flexible keystore architecture.

End-to-end protection is the name of the game when it comes to securing connected vehicles and their increasingly automated driving technologies in the future. Developers need to secure all the critical points in the connected environment by integrating technology such as intrusion detection systems, automotive firewalls, secure over-the-air software updates and secure V2X. End-to-end protection means embedding IT security functions right down at the most fundamental component levels of digital vehicle functions – in other words within the microprocessors of individual ECUs. That’s exactly what hardware security modules can offer. They lie at the heart of today’s developments in automotive security – and their future looks equally bright (see Figure 3).

### Figure 3: Hardware security modules (HSMs) lie at the heart of automotive security

**ESCRYPT** honored as “Innovator 2018”

Renowned German business publishing house *brand eins* recently released its annual ranking of the most innovative German companies – and ESCRYPT was one of the top performers. The company took a leading position among SMEs in the Technology and Telecommunication category, earning the accolade “Innovator of the year 2018.”

Guided by specific selection criteria, more than 25,000 experts were asked to name innovation leaders from a pool of over 3,400 companies. ESCRYPT received an above-average number of recommendations in all three predefined innovation areas: products and services, process innovations, and corporate culture. “We are delighted to have received this award,” says Division Head Uwe Müller. “More than ever, it’s an incentive to ensure innovation continues to be the driving force at our company.”

**Author**

Dr. Frederic Stumpf is Head of Product Management at ESCRYPT.

Dr. Uwe Müller, Head of Application Field Cyber Security Solutions, ESCRYPT (Bosch Group)
Heroic deeds for your security needs

Good triumphs thanks to security
ESCRYPT has been setting new standards in automotive security for years now. Our comprehensive solutions relentlessly protect your vehicle data against manipulation and theft.

www.escrypt.com