www.itk-engineering.com

itk ENGINEERING

SERVICE OVERVIEW

» CYBERSECURITY ENGINEERING

" Security is like the brakes of your car. It slows you down but it also enables you to go a lot faster. "

Contents

Our motivation – cybersecurity is necessary

The dark side of "connected products"

The trend of connected products is ubiquitous in most industry sectors. While connectivity enables a lot of innovative features, it also increases the potential for malicious attacks. To attack a non-connected system, physical access is required. Attacking connected systems does not necessarily require physical access and, thus, potentially enables attackers to remotely compromise many devices at the same time [1] [2] [3].

Connected products are often not developed from scratch, but re-use legacy components – components that were never designed for secure use in a connected scenario. Examples for this include industrial control systems (ICS) that were connected to the internet [4], vehicles that are connected by aftermarket dongles [5], and infusion pumps that are connected to the hospital network [6].

The resulting security incidents can threaten company business models due to reputational damage, data privacy fines and compensation payments to end-customers as well as B2B customers. Furthermore, scalable attacks put social values at risk, which motivates legislators to take action in terms of cybersecurity legislation.

The developing attack landscape

While a decade ago, attackers were mostly targeting IT systems, a shift of their focus to embedded systems can be observed [5] [6] [7]. Reasons for this are manifold:

- Embedded systems are easier targets, as they do not apply security mechanisms that are already common in IT systems and user awareness is mostly non-existent.
- Successfully attacking embedded systems often has a direct impact on the physical world (e.g. safety goals), which leads to more publicity.
- Attacking embedded systems enables attractive business models that go beyond online banking fraud and identity theft (e.g. "What is it worth to you that the vehicles of your fleet are still able to drive tomorrow?").

More and more academic papers on vulnerabilities and attacks are being published [8] [9] and the first attacks have already happened in the real world [10] [11] [12]. This can be compared to the security situation in the realm of IT during the late 80s and early 90s, just before malicious players started exploiting these findings to massively spread viruses and trojans. If the historical development of attacks in the IT world is of any indication, we will be confronted with drastic situations and should make it a priority to learn from the past. The amount of observable real-world attacks when it comes to embedded products is not at its peak yet, but the attacker side of the security game does not rest and is currently developing technologies and methodologies that make attacking connected products more convenient. As a consequence, the effort involved in attacking embedded systems becomes increasingly less of a problem. The future risk for companies, individuals, and society also dramatically increases if products that are developed today are not hardened with appropriate countermeasures.

The ongoing standardization & legislation

The necessity to harden embedded products against attacks and keep up with the current developments in the attacker world is recognized by major companies, standardization bodies, and lawmakers. This is shown by current standardization efforts such as ISO/SAE 21434 [13], IEC 62443 [14] or the NIST Cybersecurity framework [15] and new regulations regarding cybersecurity in specific domains [16] [17] [18] [19] [20].

In many industry sectors, applying adequate security mechanisms and security engineering processes will no longer be a choice of each company, but a requirement – either made by lawmakers or by B2B customers who have to demand security for supplied products in order to make their own products secure.

The complexity of security

While standards and legislation demand secure products, it is easier to demand cybersecurity than it is to achieve. Security is a complex topic due to several aspects that have shown to be challenging for companies.

- An ever-changing attack landscape: security has to protect against intelligent attackers that continuously develop their abilities further and adapt to the countermeasures that are in place. Security has to be thought of like an "arms race" rather than a "one and done" kind of challenge.
- Required mindset change: The security topic is new to most companies and not yet part of the employees' mindset – and that is true both for management and engineers. The security topic is easy to grasp, but hard to master. For instance, creating checklists to tackle the problem is often the first reaction, but this evidentially over-simplifies the problem and leads to unsecure systems. Thus, security engineering cannot be introduced into a company overnight but requires careful preparation, management support, and the participation of all employees and management hierarchies.
- Technical challenges: Applying security mechanisms does not come for free. They consume memory and computing resources that might not be available and they potentially conflict with other functional or non-functional requirements like safety. As these goal conflicts have to be carefully balanced, security cannot be considered in isolation. Thus, security engineers need to have the capability to understand the bigger picture and the restrictions of the technologies involved.
- Business goal conflicts: On the one hand, systems have to be secure; on the other hand, they have to make it to market in time and costs have to be acceptable. Often this constitutes a goal conflict. Security has to be considered from the beginning of an engineering project to avoid unnecessary delays and costly architectural changes late in the engineering process. In reality, however, security is often thought of much later when design decisions have already been made and boundary conditions are established – which makes achieving adequate cybersecurity even more challenging than it already is.

The fact that security is complex and cannot be thought of in a unidimensional way is also recognized by existing standards, which require the application of "adequate" security mechanisms, yet do not explicitly define which security mechanisms have to be applied. For companies, this makes security much more complex than ticking boxes in a checklist. To avoid costly and unnecessary investments in security mechanisms that are not needed after all, they first have to prepare and determine what "adequate" means within their unique setup.

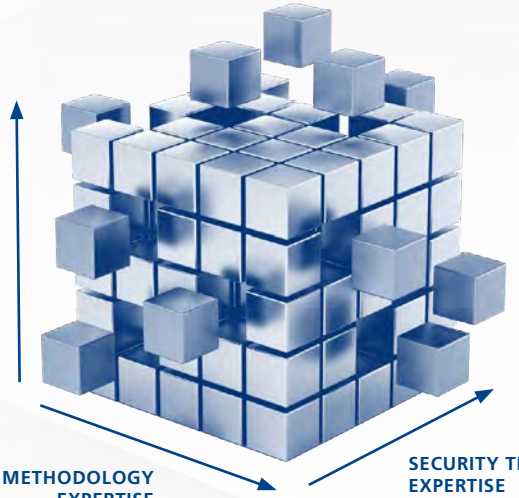
The consequence

Cybersecurity is often considered a rather unpleasant side topic. However, in light of recent developments – both the ongoing standardization and legislation as well as the evolution of the real attack landscape – adequate cybersecurity is becoming a strict requirement instead of simply nice to have. Companies cannot establish security processes and a security culture overnight. This constitutes a market differentiation opportunity: investing in building up cybersecurity capabilities now enables companies to develop innovative features quickly and efficiently in the future. This constitutes a market advantage.

Our business model – benefits of collaboration

Enabling our customers to build secure systems

In the center of our work is the enablement of the customer to build secure products by means of engineering support, consulting services or workshops. Based on broad engineering knowledge and cross-domain cybersecurity expertise, the customer receives a tailored and standards-compliant solution including all rights of IP and source code (whitebox model). Focusing on the specific customer needs, product independence is given.



Cybersecurity is only one piece of the puzzle: leveraging engineering expertise

The ongoing digitalization indeed increases the importance of cybersecurity, yet it is only one piece of the puzzle. Industry domain-specific technologies and concepts, safety experience and product development methodologies are only a few examples of other areas with which cybersecurity has to interface in practice. Cybersecurity cannot be approached in isolation. Only when considering the full system and boundary conditions will the result be a secure system or a feasible technical solution that will work in practice and will make it to the market. This is why methodological security expertise and a good understanding of industry-specific technologies are required to build secure systems. Based on past engineering projects, ITK Engineering, ITK for short, has a huge experience pool from which our security engineers can draw. Thus, we never look at cybersecurity in isolation and proactively sense challenges that may arise when implementing security mechanisms.

No reinvention of the wheel: domain-spanning security expertise

Cybersecurity is necessary for all industry sectors that cope with digitalization. Many sectors develop their own standards, technical solutions, and methodologies. Thus, "state-of-the-art" differs between industry sectors: a pressing problem in one sector might have already been solved in another.

From automotive and industrial to healthcare – ITK performs cybersecurity projects in many domains, and thus has a broad overview of state-of-the-art security technology and methodology. This knowledge enables us to fit well-established solutions from similar scenarios and problems which were already solved in another context. This often results in sped up engineering at a lower cost.

Whitebox solutions instead of vendor lock-in

Openness and transparency are the foundation of modern security (Kerckhoffs principle). The security of a system must not depend on the fact that its inner workings are proprietary and secret. Non-proprietary solutions are also favorable for customers from a business perspective, as they prevent vendor lock-in.

ITK provides whitebox solutions, for example, our customers retain both intellectual property rights and knowledge of the inner workings of our work products (e.g. source code). Apart from strengthening the security of the system by enabling independent assessments of our work products, this underlines our aim to enable our customers by providing extraordinary quality, timely deliveries, and flexible solutions instead of shackling the client with vendor lock-in.

Product-independent consulting and engineering services

A good balance between quality and cost can be achieved if consulting and engineering services are unbiased and independent. Security products induce costs and should thus only be applied when they are needed and fit the problem at hand. Our portfolio does not contain own products but offers consulting services and customer-specific solutions independent of products or platforms. Based on our motto, "what we advise, we can also provide", we look beyond concepts, sense potential conflicts that may arise during implementation, and address them in the concept phase. The result: truly unbiased cybersecurity consulting and streamlined engineering services that fit the customer's needs.

Our customers – helping to leverage cross-industry knowledge

Migrating security knowledge between industry domains since 2010

Cybersecurity is relevant for most industries that work with embedded systems. Our cross-domain knowledge enables our experts to migrate security solutions and methodologies between domains and often leads to a quick solution, especially when problems were already solved by other industries.

AUTOMOTIVE

Connected car and autonomous driving are challenging trends in the automotive domain. Both trends already have had an impact on different aspects of the traditional vehicle technology and underline the need for cybersecurity: secure diagnostics, secure over-the-air (OTA) updates, secure onboard communication (SecOC) and secure boot are just a few examples. Furthermore, security standardization progressed with ISO/SAE 21434 and AUTOSAR. Cybersecurity technologies and methodologies affect OEMs as well as Tier1 and Tier2 suppliers.

ITK works actively for all of them, making sure that no information gets lost on the way and addressing potential security pitfalls for our customers before they become a difficult challenge. To be as close to these upcoming technologies as possible, ITK is a premium partner of the Adaptive AUTOSAR consortium and is actively contributing both in safety and security working groups.

AGRICULTURE

While the agricultural industry is closely looking at the developments in the automotive domain for some technologies, it is way ahead in others. A huge variety of use cases and special requirements are very specific to the agriculture industry because of the nature of the industry itself (e.g. interfacing with third-party equipment on a very low level) or new trends like smart farming. Based on our cross-domain knowledge, we are able to transfer security technologies and customize solutions if necessary – not only conceptually but also in code.

ITK is actively participating in the Agricultural Industry Electronics Foundation (AEF) and develops concepts as well as libraries for secure Tractor Implement Management (TIM).

HEALTHCARE

Medical devices have to become increasingly connected to provide patients with optimal care. At the same time, the healthcare infrastructure is increasingly targeted by attackers (e.g. via ransomware [25]). This is also recognized by national and international regulatory bodies that demand to take cybersecurity into account when developing healthcare products [17] [19] [20].

Since 1994, ITK has been providing engineering services to medical device manufacturers, so our engineers are very familiar with the relevant regulations and standards as well as the complex regulatory framework of the healthcare domain (e.g. MDR, FDA, and ISO 13485).

INDUSTRY 4.0

The industry domain faces many trends that inadvertently lead to security challenges. Production processes are optimized for efficiency by connecting equipment to enable predictive maintenance and to automate factories. Collaborative robots (Cobots) are integrated into manufacturing environments. Information technology (IT) and operational technology (OT) increasingly converge. Digital twin technologies allow for the tracing of the manufacturing process and the components of products. All these trends have to be enabled by connecting a previously closed system to company networks or even to the outside world. This leads to attack possibilities, which is also recognized by upcoming standardization, such as IEC 62443 [14].

ITK assists in making use of the industry 4.0 trends with contributions to general software and process consulting services. The technical and process expertise that we gathered in these projects helps to design tailored solutions that also merge well with existing systems and the according boundary conditions.

RAIL

The railway industry faces connectivity trends, including electronically connected grade-crossing, digitally connected railway stations, European Rail Traffic Management System (ERTMS), European Train Control System (ETCS), GSM Rail (GSM-R), electronic interlocking (ESTW), and predicted maintenance. This induces cybersecurity requirements which are also captured by upcoming standards (e.g. DIN VDE 0831-100 [26] and IEC 62443 [14]). Introducing cybersecurity mechanisms is especially challenging for the railway domain, which is a complex ecosystem of technologies that already exist, and new technology has to be compatible to the legacy systems. Also, the lifetime of these systems is much longer than in other industries. Laying out security mechanisms that are also secure in 30+ years constitutes a big challenge.

ITK has been actively contributing software to the railway industry since 2015. We are used to designing security under boundary conditions, tailoring existing solutions, or building new solutions from scratch, if required.

Our services – developing secure products

ITK as a security partner from requirement elicitation to testing

Our security portfolio is closely aligned with existing standardization activities such as ISO/SAE 21434 and IEC 62443. In this section, we show the generic security services that are relevant in all industry sectors.

FROM REQUIREMENTS ENGINEERING TO TESTING

(aligned with IEC 62443 & ISO/SAE 21434 draft)

Ignition-phase security services:

Cybersecurity CheckUp

How secure is my product/company?

(e.g., assessment of current product/concept/process security state)

Baseline Cybersecurity Concept

How to make my architecture „security-ready“?

(e.g., identification of hardware requirements, crypto benchmarking, security-by-design)

Product security services:

Cybersecurity Risk Assessment

What does „secure“ mean in my system?

(e.g., damage-scenario identification, attack-tree modeling, risk analysis)

Security Goals

Review & Validation

Cybersecurity Concept Consulting

Which security mechanisms have to be put in place?

(e.g., secure onboard communication, secure boot)

Security Concept

Review & Validation

Cybersecurity Software Development

How to implement security mechanisms securely?

(e.g., cryptographic library integration, HSM integration, source code hardening)

System

Cybersecurity Testing

Are there attack vectors that were missed?

(e.g., penetration testing, fuzz testing)

Enabler services:

Cybersecurity Trainings

How to enable my company to deal with security?

Training course: Basics of Security Engineering
Training course: Secure Coding in C

Cybersecurity Process Consulting

How to establish a security process in my company?

(e.g., ISO/SAE 21434, safety-security interaction)

CYBERSECURITY CHECKUP

In many cases, our customers are not sure where their products stand in terms of security. It is obvious that security is important, but it is unclear how much to invest, where to start, or how to proceed. To prevent over-investing, a decision basis is required that often cannot be established in-house because the customer's core business is far from cybersecurity.

Our answer is: two security experts, two weeks and a security check-up report as a result. Our experts will determine whether actions are required to strengthen the security of your products and make recommendations on what these actions should look like. As the state of security processes and documentation can widely differ for different companies, we leverage the whole ITK security portfolio and adaptively apply the methodologies that fit the scenario best. For instance, if security concepts already exist, our security engineers can review them. If no documentation is available, our security engineers can interview developers and architects to assess whether actions are required. If nobody is available to answer questions, our engineers can even apply penetration testing techniques. There is a custom solution for each customer – based on their fixed budgets.

BASELINE CYBERSECURITY CONCEPT

Timelines are often tight, and decisions have to be made quickly to reduce time-to-market. At the beginning of designing a system, initial architecture and hardware decisions need to be made. These decisions are required as an input for cybersecurity risk analysis and concept development. But at the same time, fixed hardware and architecture decisions can also make it impossible to apply adequate security mechanisms. For instance, if the result of a risk analysis demands a secure boot concept, but the hardware does not include an adequate trust anchor, the hardware decision has to be revised mid-project. To solve this "chicken or the egg" dilemma, the security-by-design principle has to be applied; in other words, security has to be considered from the first step of the project.

The goal of a baseline cybersecurity concept project is to first identify hardware and software requirements that address the most common risks before the hardware or architecture is decided. A baseline security concept does not replace a thorough risk analysis and concept development, but it anticipates the results to make the system "security-ready". Furthermore, a forecast on the final requirements that arise from the detailed concepts is often possible.

CYBERSECURITY RISK ASSESSMENT

"What does 'secure' mean?" – a question that needs to be answered in every security engineering project. 'Security' is context-specific: while confidentiality is an important protection goal for passwords, it certainly is not needed for public news. The goal of a risk analysis project is to identify protection goals as well as potential vulnerabilities of a system that can be exploited to compromise these goals and estimate the implied risk.

Our risk assessment report provides a prioritized list of vulnerabilities and risk assessments as a decision basis to determine which vulnerabilities should be addressed by a security concept. Thus, it acts as both a source for security requirements that have to be satisfied by the system and a tool to get management support for the security topic. Depending on the customer's needs, we apply common risk analysis methodologies that are aligned with standards like ISO/SAE 21434 and IEC 62443 or with the customer's own established method. ITK provides the risk analysis results as well as the right tooling to view and adapt these results to the ever-changing reality.

CYBERSECURITY CONCEPT CONSULTING

"Which security mechanisms have to be applied to make the system 'secure'?" – this is the question that has to be answered once the meaning of 'secure' has been defined for the target system. A security concept provides a security architecture. It also identifies implementation requirements that satisfy the security requirements while considering industry-specific boundary conditions of the system, for example, safety and performance requirements. Once the security concept is available, implementation-ready requirements can be formulated in a security specification. ▸

ITK builds on industry-specific expertise, gathered through project experience since 1994, and combines it with security expertise to build security concepts. In particular, we create software-, platform- and communication security concepts, depending on the customer's requirements. Based on a security concept, hardware and software requirements can be identified and written down in a specification. On top of that, ITK provides guidance on the next steps for implementation and common pitfalls based on experience gained in security implementation projects.

CYBERSECURITY CONCEPT REVIEW

Testing the security of a system is challenging. It is not about testing whether the product "works", but testing whether imaginable attacks fail. Testing the security of the final product via penetration testing is an option, but potentially leads to huge costs if conceptual vulnerabilities are revealed and changes have to be made to the system architecture. A concept review aims to rule out such vulnerabilities before implementation. Security concepts should be reviewed by unbiased parties, as they are better suited to scrutinize conceptual decisions.

As a product-independent security partner, ITK is able to provide unbiased reviews. Concept reviews can be conducted both for the customer's products and products that are developed and delivered by a customer's supplier. The deliverable is a document that summarizes the identified vulnerabilities in a security concept, prioritizes them and offers mitigation options. To minimize cost on the customer's side, ITK aims to find the least intrusive mitigation option. Our security concept review service provides customers with the confidence that their security concept is a secure foundation and suitable for further development, avoiding design flaws that could cost a lot to change in the future.

CYBERSECURITY SOFTWARE DEVELOPMENT

Software vulnerabilities can easily jeopardize the security of the system, even if its security concept and specification is bulletproof. In the embedded world, even highly skilled developers can make security-relevant mistakes and introduce unintended vulnerabilities. All programming languages are prone to software vulnerabilities - languages like C and also higher programming languages like C++ or Java [27] [28]. Furthermore, non-language-specific vulnerabilities such as algorithmic mistakes or exploitable side channels can be introduced when developing a system [29]. Thus, extraordinary care must be taken when developing software. That is not only true for the parts of the software that implements security mechanisms, but for the whole software as an attacker who can exploit a vulnerability in the non-security-related parts of the software might also be able to take over control over the rest of the system. Besides security aspects, boundary conditions (e.g. CPU performance, latency requirements, and memory consumption requirements) have to be considered and proactively handled to ensure that the developed system is useable in the end.

Our secure software development team provides software that satisfies the defined security requirements of the customer under the specified boundary conditions. ITK rigorously adheres to secure coding practices [30] and applies semi-automated code analysis techniques to ensure conformity of code. Furthermore, manual reviews are conducted to avoid vulnerabilities that are on the algorithmic level, rather than the programming language level. When developing cryptographic libraries, ITK typically uses well established cryptographic libraries (both closed- and open-source), performs upfront benchmarks, tailors the libraries to the customer's requirements and provides the customer with test code. Once the library is delivered, ITK offers maintenance packages that include monitoring the attack landscape to notify the customer of upcoming vulnerabilities and patch the libraries if required. The result of our software development service is typically a security-reviewed, turnkey security solution that is tailored to the customer's environment and can be integrated effortlessly. ▸

CYBERSECURITY CODE ANALYSIS

Software has to be tested to be reliable – the same applies to software security. A distinction can be made between functional security testing (ensuring that security mechanisms are invoked and do not prevent the system from working) and non-functional security testing (ensuring that there are no vulnerabilities that can be exploited by an attacker). Especially for non-functional security testing, it has become evident that experienced developers alone do not suffice and additional security expertise is required to spot vulnerabilities. Furthermore, to ensure the effectiveness of code reviews, source code ideally shall be reviewed by unbiased parties who were not involved during implementation.

The goal of code analysis is to minimize software vulnerabilities by reviewing the source code. The code should be analyzed by unbiased reviewers: one team provides an implementation and another team tries to find exploitable vulnerabilities in it. ITK applies different code analysis techniques based on individual project requirements of the customer. These techniques include tool-based, semi-automated static code analysis, dynamic code analysis based on binary instrumentation, and manual code analysis. The code analysis can be complemented with blackbox fuzzing if either software is too complex for whitebox code analysis or the source code is not available.

CYBERSECURITY FUZZ TESTING

Code analysis tools can only identify specific types of vulnerabilities and often software or entire systems are too complex to be manually reviewed. In such scenarios, fuzz testing is an option to test the security of the system. A security fuzz test sends randomized data to system interfaces and monitors the behavior of the system to identify irregular behavior that hints at security vulnerabilities. In contrast to a security code analysis, a fuzz test can also be conducted without the source code of the system, which makes it also applicable to proprietary third-party components. Challenges include the setup of the environment (e.g. simulation of the communication network) and evaluation of the fuzz testing results, i.e. identifying false-positive findings and finding the root cause for the remaining findings.

The depth and scope of fuzz testing depends on the customer's needs and budget. It is possible to perform network-level fuzzing (e.g. whole vehicle), component-level fuzzing (e.g. single ECU) and code-level fuzzing (e.g. software module). ITK uses existing Hardware-in-the-Loop (HIL) expertise and testing facilities to efficiently setup the required environment for fuzz testing targets. As a result, our experts provide a detailed report that highlights the identified vulnerabilities and proposes feasible countermeasures. Fuzz tests can be used to increase the confidence of the customer that a system/component that was produced in-house or by an external supplier does not contain any security-critical vulnerabilities.

CYBERSECURITY PENETRATION TESTING

Engineers are human beings who can make mistakes. These mistakes can happen in each development step but also during integration. That is why the security of the final product is often tested in a so-called penetration test. A penetration tester assumes the role of an attacker and examines the product for vulnerabilities. A good penetration test considers both known and zero-day attacks that exploit yet unknown vulnerabilities. Furthermore, it should be performed by an unbiased party who knows the relevant technologies in the domain, but who was not involved in the product development. As the amount of theoretically possible attacks is typically too big to cover, a penetration test cannot be "complete" and, thus, has to be performed in a time-boxed manner. This also means that penetration testing cannot replace solid security engineering during requirement elicitation, design, and implementation, and thus should only be considered as a supplement.

ITK offers unbiased experts to perform penetration testing. The choices include network-level penetration testing (e.g. a whole vehicle), component-level penetration testing (e.g. a single microcontroller) and code-level penetration testing (e.g. a software module). The depth and scope depend on the customer's needs. Thus, the attack paths to be tested are prioritized by experienced penetration testers and can be influenced by the customer. In the end, the customer gets a detailed report that highlights not only the identified vulnerabilities but also proposes feasible countermeasures.

CYBERSECURITY TRAININGS

Central to our work is the enablement of our customers. In addition to engineering projects and consulting tasks, we also build up the customer's security expertise and awareness. The two cybersecurity trainings provide insight into useful security methodologies and techniques:

- Basic Training for Cybersecurity Engineers
- Secure Coding in C

CYBERSECURITY PROCESS CONSULTING

While bringing security into products is the first step on the road to push cybersecurity into a company, establishing cybersecurity processes and methodologies are required to get reproducible results. This leads to several challenges. For instance, security processes typically have interdependencies and goal conflicts with other processes, such as safety. These interdependencies have to be reflected by interleafing the processes of both domains at the appropriate time. Furthermore, in most companies, employees have to undergo a mentality shift to establish security processes. This mentality shift can meet strong resistance from both developers and managing personnel, as security processes often lead to conflicts with existing goals (e.g. timeline and budget goals).

As ITK has an established security engineering process; we know first-hand about the technical and organizational challenges that arise from the transition to security processes. We are keen to let others learn from that. When supporting our customers in establishing new security processes/methodologies, our experts consider individual customer requirements, technical boundary conditions and existing processes. Improvements of existing processes and the development of methodologies from scratch can also be within the scope of a process consulting project. Examples for such projects include, but are not limited to: risk management methodologies, security testing methodologies, manufacturing process security, and security of supply chains.

Our technical expertise – enforcing security on a technical level

Matching security with business objectives every day

This chapter is about applying the aforementioned security engineering process and services. It shows an excerpt of specific technical security aspects that we typically work on and tailor to the technical as well as non-technical objectives of our customers.

RISK ANALYSIS TOOLING

Risk analysis is crucial to identifying the security mechanisms that are actually worth investing in. There are many risk assessment methods on the market that are structured around a trade-off between the effort that is required to model the system and the accuracy of results. Risk analysis methodologies that lead to accurate results are often favored by product developing companies but are rather complex to perform by hand or in Excel. Furthermore, risk analyses often have to be adapted due to changing boundary conditions during the development process or even during product life.

ITK has developed tooling that cuts costs for proper risk analysis by using templating methods and allowing for rapid change of the system modelling. The tool is compatible with existing standards and can be tailored to fit most risk assessment methodologies on the market. This enables us to seamlessly integrate the individual risk assessment method that is applied by our customer. The outcome: a static report as well as an interactive deliverable that allows the customer to change the risk analysis without assistance in the future. If required, we also use the experience we gained in developing our tooling to help customers build up their own individual risk analysis tooling.

SECURE BOOT

Attacks that survive a reboot of a control system can be used by attackers for a variety of purposes, including tuning and exploration of whether additional system components can be attacked. secure boot enforces that hardware systems only boot software that is authorized to be executed. To achieve this, close interaction with a hardware trust anchor is required. This can – but does not have to be – hardware security modules (HSMs) or trusted platform modules (TPMs).

Based on our knowledge of the internal workings and capabilities of different trust anchor technologies, ITK finds solutions that fit customer secure boot requirements. As we are not tied to a single product or concept, we can provide custom solutions for secure boot, even if the hardware has already been chosen and other off-shelf solutions are not feasible.

SECURE UPDATE

A system update feature is a double-edged sword. On the one hand, an update functionality is crucial to be able to patch newly identified vulnerabilities in a connected world. On the other hand, the update functionality can be potentially misused by an attacker to compromise the system. Misuses can happen in all stages of an update's lifecycle: in development, during the distribution from the backend, along the transmission channel, or within the target system itself. Thus, the update functionality has to be included in systems and adequate security mechanisms have to be implemented to prevent misuse.

ITK can support customers in designing and developing a solution and integrate existing or third-party components. Based on the cryptographic, architectural and implementation security expertise of our security engineers, we deliver solutions that work and ensure that the delivered solutions are secure.

SECURE DIAGNOSTICS

Diagnostic capabilities are an essential feature of any ECU, no matter if in the development or out in the field. Access to sensitive diagnostic information and the ability to even modify an ECU to a certain degree via this interface must be protected against misuse. This is why deploying a strong security mechanism for access to the ECU's diagnostic interface as well as protecting diagnostic messages themselves is essential. Furthermore, it is also necessary to secure any required cryptographic material in the diagnostic testers that connect to these interfaces on the ECU to prevent counterfeit testers from accessing the diagnostic capabilities.

ITK regularly designs security mechanisms for diagnostic ports, which are based on a variety of different interfaces (e.g. OBD, USB, JTAG or even wireless) and protocols (e.g. UDS, DoIP, and CAN/ISO-TP). We utilize state-of-the-art security protocols based on symmetric or asymmetric cryptography and also design custom-tailored solutions to customer's needs. ▸

Furthermore, we enhance our solutions by also providing key management concepts that ensure the best protection of the ECU.

SECURE COMMUNICATION

"Defense in depth" is an important paradigm of modern security architectures. In simple words, it means "security mechanisms can fail, so do not trust single mechanisms". To live up to that paradigm, not only do entry points (e.g. telematic systems) to a system of systems (e.g. a vehicle) have to be protected, but also the communication between different subsystems. Just because an attacker was able to overcome the entry point does not mean it should be possible for the attacker to spoof arbitrary messages on the internal network and control arbitrary system functions. Challenges when designing secure communication protocols in embedded domains include boundary conditions like network frame size, processing power, transmission overhead and storage restrictions.

With our strong cryptographic background, we are able to build and tailor secure communication protocols. This background is paired with our knowledge of different, domain-specific technologies and security solutions. It provides us with the ability to find the best fit for customer systems – by evaluating and leveraging already existing technologies (e.g. AUTOSAR SecOC [31], OPC-UA [32], and TLS [33]) or by customizing solutions based on customer requirements.

CUSTOMIZED CRYPTOGRAPHIC PROTOCOLS

Cryptographic communication protocols are omnipresent in the connected world of today. Examples include pairing of smart devices, over-the-air updates and diagnostic access. Many scenarios can be covered with existing, well-understood protocols. However, especially in embedded domains, well-established protocols are occasionally not feasible because of boundary conditions, such as hardware resources and legacy systems.

Our cryptographers design and tailor specialized protocols for customer scenarios in which nothing else fits. Also common in academia, the designed protocols undergo rigorous review rounds and validation steps before they are shipped as a whitebox solution to the customer. Some of the protocols even become patented – with the customer as the IP owner.

KEY MANAGEMENT

Key management is the foundation of most security concepts. Regardless of whether a secure boot concept has to be established or updates have to be secured, cryptographically strong keys are necessary and have to be managed. There are multiple ways to handle it, each with advantages and disadvantages when it comes to resource consumption, revocation of compromised keys and deployability in manufacturing infrastructures.

ITK helps the customer find the right fit for the specific scenario and makes unbiased recommendations for third-party products. If necessary, ITK also supports the customer during the integration of the chosen solutions – or even design a custom-made system from scratch if none of the available solutions fit. The result: unbiased product choice and unproblematic integration.

HARDWARE SECURITY MODULES

Hardware Security Modules (HSMs), ARM Trustzone and Trusted Platform Modules (TPMs) are hardware enclaves that are separated from the much more complex and potentially vulnerable main system. This property makes them ideal not only to store secret cryptographic keys but also as a trust anchor for the whole system. Such a trust anchor is often required to achieve adequate security in the face of physical attackers or to contain attackers who manage to exploit a software vulnerability. They enable security mechanisms like secure boot, secure updates and secure communication.

ITK participates both in the development of HSM solutions and the integration of existing solutions. This enables us to provide our customers with expertise of the inner HSM workings while being unbiased about products. In case a device lacks a full-fledged HSM or equivalent solution, it is also often possible to utilize other existing hardware features in order to implement a security mechanism that significantly reduces the likelihood of a successful attack.

VIRTUALIZATION

A common goal is to reduce the physical complexity of, for example, a car network and all its attached systems. In order to achieve that goal, fewer but more powerful processors must be utilized that, in turn, handle many different tasks at once. However, there is a vast amount of security challenges associated with the co-location of different applications on one system. For instance, a compromised application ▸

could undermine the security of all other co-located applications on such a system.

ITK works on cutting-edge projects that enable the secure co-location of applications. To achieve this, we utilize the best-fitting combination of software-based (e.g. Hypervisors and Containerization) and hardware-based (e.g. HSM, TrustZone, and TPM) technologies. Combining these technologies is especially important for building systems that are secure while ensuring scalability and maintainability. Sometimes it is even feasible to achieve some of the hardware-provided security properties solely by utilizing state of the art software-based isolation techniques.

INTRUSION DETECTION SYSTEMS

Intrusion detection systems (IDS) are the "immune system" of products that enable companies to detect and be able to react to attacks that are in progress. While IDS systems are already widely established in the IT domain, embedded IDS systems differ significantly due to resource boundary conditions, industry-specific technologies, and product architectures. Many security companies offer embedded IDS systems with different levels of maturity, detection features and detection rates.

ITK leverages its product independency to help customers find the product that best fits their scenario. If necessary, ITK helps to close remaining gaps by providing concept and implementation services.

COUNTERFEIT PROTECTION

Theft of intellectual property and product counterfeiting has continuously increased in recent years. As product counterfeits have a direct impact on revenue and constitutes a risk to return-on-investment calculations, preventing it is one of the top priorities with most of our customers. Counterfeiting can be prevented by multiple techniques on different layers (e.g. ECU layer, network layer or backend interaction layer).

ITK leverages the security knowledge that have been gained in security projects to also address the counterfeiting problem. In many cases, we can provide our customers with synergy effects between security mechanisms. For instance, security mechanisms that are used to secure network communication are useful against malicious attackers and also against counterfeit products if they are applied in the right way.

CLOUD INTEGRATION

In the Internet-of-Things, embedded systems are often connected with a backend that is hosted in the cloud. This leads to a system that includes embedded devices as well as a communication channel and an IT backend. While developing and integrating these subcomponents is challenging on its own, the security of the system typically cannot be broken down to sub-components without overlooking crucial vulnerabilities. Security has to be considered for the system as a whole.

ITK brings secure communication, access control and key management expertise together with dedicated cloud developers from non-security teams to deliver a turn-key solution to the customer.

AUTOSAR SECURITY

AUTOSAR is a standard for modern vehicle E/E architectures that can be applied to embedded control units (classic AUTOSAR) and vehicle computers (adaptive AUTOSAR). AUTOSAR can be applied in the automotive domain, to off-highway machines and sometimes even to medical equipment. Security services of AUTOSAR include secure onboard communication, key management, intrusion detection interfaces, update and configuration management and secured diagnostics. However, integrating them securely is often a challenge – especially if third-party components like hardware-security modules have to be integrated.

ITK actively participates in the security working group WP-SEC in the AUTOSAR consortium to maintain an edge on recent developments. Apart from that, ITK has experience implementing and integrating AUTOSAR code, including classic AUTOSAR software components, complex device drivers, Adaptive AUTOSAR stack components and Adaptive AUTOSAR applications.

Sources

[1] „Hackers can hijack Wi-Fi Hello Barbie to spy on your children," The Guardian, [Online]. Available: https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children.

[2] „Shodan search exposes insecure SCADA systems," zdnet.com, [Online]. Available: https://www.zdnet.com/article/shodan-search-exposes-insecure-scada-systems/.

[3] "Hackers Remotely Kill a Jeep on the Highway—With Me in It," wired.com, [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[4] zdnet.com, „Employees connect nuclear plant to the internet so they can mine cryptocurrency," [Online]. Available: https://www.zdnet.com/article/employees-connect-nuclear-plant-to-the-internet-so-they-can-mine-cryptocurrency/ .

[5] „Researchers remotely kill the engine of a moving car by hacking vulnerable car dongle," [Online]. Available: https://www.computerworld.com/article/3191519/researchers-remotely-kill-the-engine-of-a-moving-car-by-hacking-vulnerable-car-dongle.html.

[6] „Video Shows a Terrifying Drug Infusion Pump Hack in Action," [Online]. Available: https://www.wired.com/2015/08/video-shows-terrifying-drug-infusion-pump-hack-action/.

[7] „The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse," wired.com, [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

[8] J. Dürrwang, J. Braun, M. Rumez, R. Kriesten und A. Pretschner, „Enhancement of automotive penetration testing with threat analyses results," SAE International Journal of Transportation Cybersecurity and Privacy, 2018.

[9] E. Mahmoud Hashem und N. Qiang, „Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," IEEE Vehicular Technology Magazine, 2017.

[10] „BMW and Hyundai hacked by Vietnamese hackers, report claims," [Online]. Available: https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/.

[11] „Daimler and BMW's car-sharing service was reportedly hacked in Chicago and up to 100 luxury cars are missing or stolen," [Online]. Available: https://www.businessinsider.com/daimler-and-bmws-car-sharing-service-reportedly-hacked-in-chicago-2019-4?r=DE&IR=T.

[12] „Experts: North Korea Targeted U.S. Electric Power Companies," NBC News, [Online]. Available: https://www.nbcnews.com/news/north-korea/experts-north-korea-targeted-u-s-electric-power-companies-n808996.

[13] „ISO/SAE DIS 21434 Road vehicles - Cybersecurity engineering," [Online]. Available: https://www.iso.org/standard/70918.html.

[14] „IEC 62443 - Industrial Security," [Online]. Available: https://webstore.iec.ch/publication/64465.

[15] „NIST Cybersecurity Framework," National Institute of Standards and Technology (NIST), [Online]. Available: https://www.nist.gov/cyberframework.

[16] „Task Force on Cyber Security and (OTA) software updates (CS/OTA)," UNECE, [Online]. Available: https://wiki.unece.org/pages/viewpage.action?pageId=40829521.

[17] „BSI-Kritisverordnung (BSI-KritisV)," Bundesamt für Sicherheit in der Informationstechnik (BSI), [Online]. Available: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2016/kritis-vo.html.

[18] „Security and Privacy in Your Car Study Act," United States of America, [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/701.

[19] „Medical Device Regulation (MDR)," European Union, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745&from=DE.

[20] „Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," U.S. Food and Drug Administration, [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices.

[21] „Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus," Fortune, 2020. [Online]. Available: https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/.

[22] „VDE V 0831-100:2019-08," Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE), 2019. [Online]. Available: https://www.vde-verlag.de/standards/0800594/din-vde-v-0831-100-vde-v-0831-100-2019-08.html.

[23] „SEI Cert C++ Secure Coding Standard," [Online]. Available: https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682.

[24] „SEI CERT Oracle Secure Coding Standard for Java," [Online]. Available: https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java.

[25] F.-X. Standaert, T. G. Malkin und M. Yung, „A unified framework for the analysis of side-channel key recovery attacks," Annual international conference on the theory and applications of cryptographic techniques, 2009.

[26] „CERT Secure Coding Standards," SEI, [Online]. Available: https://wiki.sei.cmu.edu/confluence/display/seccode.

[27] AUTOSAR, „Secure Onboard Communication (SecOC)," [Online]. Available: https://www.autosar.org/standards.

[28] OPC, „OPC Unified Architecture (OPC-UA)," [Online]. Available: https://opcfoundation.org/about/opc-technologies/opc-ua/.

[29] IETF, „RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3," [Online]. Available: https://tools.ietf.org/html/rfc8446.

[30] J. Köhler, „Processes Are Only Half the Battle: Organizational and Technical Challenges of Security Engineering," International VDI Conference - Connected Off-Highway Machines, 2019. [Online].

[31] J. Köhler, „Secure Remote Diagnostics for Electronic Control Units in Off-Highway Machines," International VDI Conference - Connected Off-Highway Machines, 2017. [Online].

[32] S. Labitzke, „Cyber Security of Agricultural Machines is not even a Feature: How can we afford that?," John-Deere Electronics World Conference, 2017. [Online].

[33] H. Kühner und J. Koehler, „Security Engineering Prozess für den Schienenverkehr," safe.tech, 2018. [Online].

[34] S. Labitzke, „Security vernetzter Nutzfahrzeuge - Was wir aus anderen Domänen lernen können," CVC Jahrestagung, 2019. [Online].