Cybersecurity & privacy and Architecting

White Paper Resulting from Architecture Forum Meeting

November 14-15, 2018, Daimler, Sindelfingen, Germany

Edited by:

Teun Hendriks, ESI

Gerrit Muller, USN-NISE and ESI

Eirik Hole, Stevens Institute of Technology

Input was provided by the following participants in the Architecture Forum:

Name	Organization
Christoph Fischer	Roche Diabetics Care
Teun Hendriks	ESI
Eirik Hole	Stevens Institute
Bjørn Victor Larsen	Kongsberg Defense
Wouter Leibbrandt	ESI
Hugo van Leeuwen	Thermo Fischer Scientific
Alexander Lepple	Daimler AG
Jamie McCormack	Thermo Fisher Scientific
Gerrit Muller	USN-NISE and ESI
Jurgen Nicolai	Bosch Thermotechnik

Name	Organization
Chandu Potluri	Daimler AG
Solve Raaen	Kongsberg Maritime
Martin Simons	Daimler AG
Daniel Skiera	Bosch Thermotechnik
Marnix Tas	Sioux Embedded Systems
Alexandr Vasenev	ESI
Egil Vassend	Kongsberg Maritime
Bart Verdaasdonk	Bosch Thermotechnik
Paul Zenden	Sioux Embedded Systems

Published, December 2021

1 Introduction

Increasing "connectedness", data, and analytical power (AI, learning) enable new capabilities, now emerging from many systems. At the same time, these trends cause increased security and privacy threats. Consequently, (cyber-) security and privacy are qualities that require more architecting. In this forum meeting, members explored cybersecurity and privacy in relation to architecting.

The members of the architecting forum discussed this topic, using the following questions:

- How do you assess the maturity of the cybersecurity and privacy of your systems?
- What challenges does your architecture face to prepare itself for an increase in “connectedness”, data, and analytical power, especially related to cybersecurity and privacy?
- How do these challenges affect your way of architecting?
- What principles, guidance, thought frameworks, or patterns are useful for you to architect in cybersecurity and privacy?
- How to cope with a general lack of competency in the relative new disciplines of cybersecurity and privacy, and the distance of these disciplines with older dominating disciplines?

2 Security threats and mitigations in automotive

The forum explored security threats and mitigations in high-tech systems based on an automotive use case. The automotive industry is rapidly changing from a mechanical/mechatronic equipment industry to what can be aptly described as an “Internet-of-Things” industry.

Some challenges which the automotive industry is facing are the following:

- Customers have rapidly changing expectations on connectivity (e.g., via a smartphone and apps),
- Highly autonomous driving is pushed by high-tech competition, e.g., Tesla and Waymo,
- Vehicle ownership is partly replaced by mobility rental.

Increased connectivity offers convenience yet brings an increased threat to security of vehicles and privacy of their owners. In 2015, white hat hackers (security researchers) demonstrated that they remotely could take over control of a Jeep Cherokee via its internet connected entertainment system (Wired, 2015). In response, Fiat-Chrysler needed to recall 1.4 million cars (BBC, 2015). This hack exposed the risk that vehicle connectivity presents in terms of new ways in which hackers can compromise a vehicle's safety.

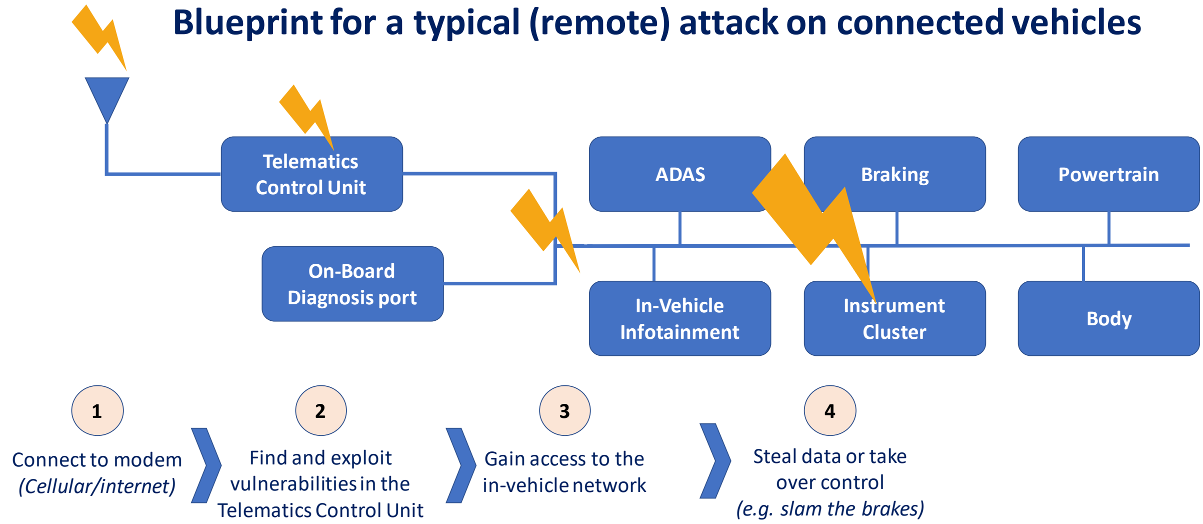

Blueprint for a typical (remote) attack on connected vehicles
Telematics Control Unit
On-Board Diagnosis port
ADAS
Braking
Powertrain
In-Vehicle Infotainment
Instrument Cluster
Body
1
Connect to modem (Cellular/internet)
2
Find and exploit vulnerabilities in the Telematics Control Unit
3
Gain access to the in-vehicle network
4
Steal data or take over control (e.g. slam the brakes)

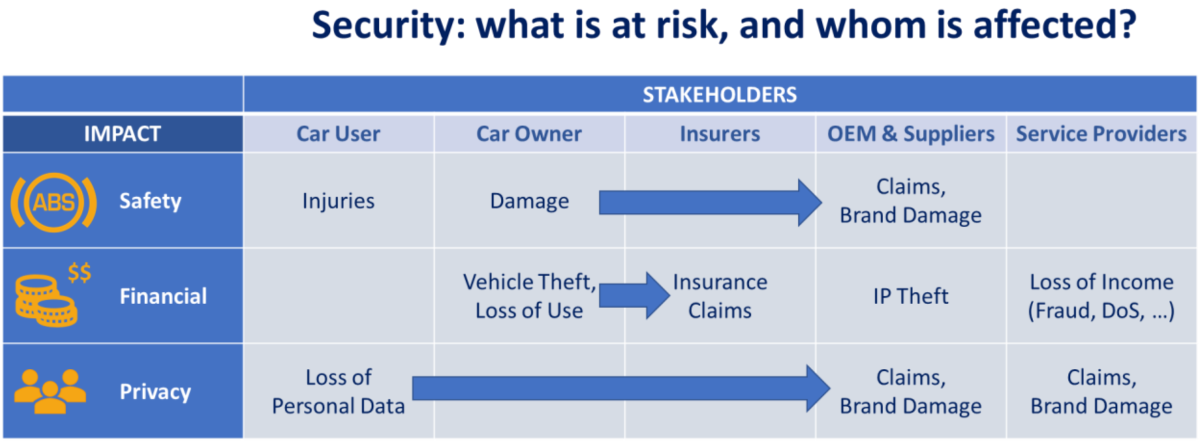
Figure 1 - Blueprint for a typical remote attack into a vehicle (van Roermund, 2017)

Offering remote connectivity opens a pathway for large scale, remote attacks. A typical blueprint for a remote attack pathway into the vehicle is sketched in Figure 1. By establishing a wireless connection to the vehicle's modem, hackers can exploit vulnerabilities in that modem to gain access to the vehicle's internal communication network. Once access to that in-vehicle network is achieved, then the vehicle control systems can be manipulated, e.g. by forcing braking or steering actions. Furthermore, vehicle or driver information can be stolen, or vehicle control systems be re-programmed. This can also effectively become a general criminal ransomware activity (i.e. loss of use of the vehicle until ransom paid with no guarantees after payment) if the fleet size makes this worthwhile to criminals.

Impact

As the Jeep Cherokee hack demonstrated, impact of security attacks can be large. Successful security hacks may cause various types of impact on various stakeholders such as the vehicle user, vehicle owner, insurers, OEMs and their suppliers, and service providers (see Figure 2).

Impact may vary from compromised safety (as in the Jeep Cherokee hack) to financial impact (vehicle theft), to privacy impact (loss of personal data). In 2018 in the UK, vehicle theft rose by 15%. Of those stolen vehicles, 80% were taken without using the owner's key (Motor1.com, 2018). For such keyless car theft, criminals employ a 'relay attack' method (i.e. relaying the electronic signal from a key fob stored in the victim's home to close to the vehicle, using a pair of radio transmitters). Using this method, vehicles can be opened and driven off in seconds (Motor1.com, 2018).



Security: what is at risk, and whom is affected?

	STAKEHOLDERS				
IMPACT	Car User	Car Owner	Insurers	OEM & Suppliers	Service Providers
Safety	Injuries	Damage →	→	Claims, Brand Damage	
Financial		Vehicle Theft, Loss of Use →	Insurance Claims	IP Theft	Loss of Income (Fraud, DoS, …)
Privacy	Loss of Personal Data →	→	→	Claims, Brand Damage	Claims, Brand Damage

Figure 2 - Impacts of security hacks for various stakeholders (van Roermund, 2017)

With the advent of connectivity, all safety critical subsystems in a vehicle are now also cybersecurity critical. Indeed, safety and security are interlinked in a vehicle system, and increasingly so due to the trend towards autonomous driving (where multiple sub-systems may have impact on safety critical functions, e.g. the steering function). Data privacy regulations force OEMs in addition to rethink data collection, usage, and retention practices.

OEM concerns

From an OEM perspective, cybersecurity and privacy concerns are now manifold:

- How to make the trade-off between security & privacy versus usability?
- What constitutes an "acceptable" residual risk? How to keep this uniform across a vehicle model and model lines?
- How to cope with BORE (Break Once, Run Everywhere) security exploits? Attacks at scale are big threats to mass produced vehicles and any (connected) mass market products in general.
- How to perform security analysis? Is it possible to scope such analysis, what assumptions can be made to base such analysis on?

- How to ensure that security stays OK from conception to vehicle launch as security threats change?
- After vehicle launch, what is the impact on lifecycle engineering? How to cope with as of yet unknown security exploits?

Emerging approach

Security and safety thinking thus needs to be an integral part of the design process, and design for resilience. The vehicle industry is developing concepts and approaches to handle cybersecurity and privacy. Key aspects of are the following:

A multi-layer security and safety concept. Each system or sub-system is responsible for its own safety & security. Multiple gateways in the vehicle isolate sub-systems and domains - the Jeep Cherokee hack clearly showed that a single fence and a single 'safe' area inside is not good enough. In other words: in security / safety critical systems one must assume that every fence can be broken, and one has to have a mechanism in place to minimize the impact of any single security breach. Key elements in a multi-layer security and safety concept are the following:

- secure access – to ensure authorized entry with assigned privileges only,
- secure gateways, safety barriers – to ensure domain isolation, intended interaction,
- secure communication – for communication confidentiality, integrity & availability,
- secure processing – for SW code & run-time integrity, and secure updating.

Risk assessment on safety & security. The automotive industry already has a strong safety and safety assessment approach based on ISO standards (ISO 26262). A similar approach and standardization for cybersecurity was in progress at time of the meeting (ISO/SAE 21434), now published in 2021. Recently, the international UNECE regulation UN R155 (UNECE, 2021) makes cybersecurity governance as well as cybersecurity architecture a mandatory part of a vehicle's certification process. Therefore, similar to e.g. Hazard and Risk Analysis methods used for safety, Threats and Risk Analysis is now becoming standard practice.

Security testing. Security testing is an important ingredient to ensure adequate security. Comprehensive security testing beyond infotainment systems is still in its infancy. Both black box and white box testing needs to be done, often using external partners in addition to internal hacker specialists. This poses its own problems as white box testing exposes IP, and those external partners could be sources of leaks.

Reflection

The deployment of security measures and a security mindset is still in its infancy in the automotive industry, certainly when compared to safety. Security standards are still evolving – OEM architects need to learn their application in product, process, and organization, where the organizational structure and system breakdown also influence the way of thinking about security & privacy. Finally, security testing is still immature. The activation of regulations such as UN R155 (UNECE, 2021) will spur a much more rapid learning curve compared to when the automotive industry introduced safety norms.

A lesson learned along the way is that Systems Engineering for security ("system security") requires for architects to have a *paranoid* mindset. They need to consider all that could potentially go wrong, even when ostensibly improbable (i.e., loss-driven thinking). This exposes an architecting dissonance, as normally architects are trained to look for opportunities (i.e., value-driven thinking).

Principle 22.1: System security requires architects to have a paranoid mindset: to consider all that could potentially go wrong, even when ostensibly improbable.

System security is a fast-developing field; much is yet unknown. The challenge for architects is how to keep innovating, yet learn fast — in a safe way — how to handle security.

Many issues are still being investigated:

- How to ensure that attacks do not scale?
- How to make intrusion detection reliable for deployment in in-vehicle networks?
- What to do when an intrusion is detected?
- How to manage such events in a supplier chain, and protect multi-vendor systems?
- How to patch security breaches, how to make it a continuous process with an agile workflow that can be integrated e.g. in the strict automotive development regime?

Solutions to address such system security issues must be balanced against the associated costs over the lifetime of a vehicle.

3 Security threats, mitigations, and approaches across the high-tech industry

Having looked at an automotive use case, the forum explored the wider landscape concerning security threats and mitigations across the high-tech industry. What are the typical security threats, and concepts / philosophies across these industries?

Table 1 - Actual state of security aspects, threats, and concepts across industries (an 'X' indicates consideration)

	Automotive	Medical	Oil & gas industry	Heating	Defense	Instrument industry
Aspects						
No safety without security	X	X	X		X	
Privacy	Regulated	Regulated	NOT regulated	NOT regulated		NOT regulated
Threats						
Remote access	X	X	X	X		
Third party access / maintenance	X					
Take over control	X			X	X	
Intentional tampering	allowed[1]	NOT allowed	NOT allowed		NOT allowed	
Denial of service	X	X	X		X	
Malfunctioning of components (internal attacks)	X		X			
Capture physical system / reverse engineering	X				X	
Compromise information / sabotage data integrity	X				X	X
Spoofing (manipulating sensor data)	X				X	
IP theft /data theft	X	X			X	X

[1] A vehicle owner is allowed to make modifications to a vehicle (with exceptions such as changing a vehicle's mileage reading, which is not allowed)

	Automotive	Medical	Oil & gas industry	Heating	Defense	Instrument industry
Concepts / philosophy						
Defense-in-depth	X	X	X	X	X	
Degraded-mode	Limp home	Indepen-dent operation	X		X	
Protect-and-detect	X		X	evidence trail		
Protect-and-prevent	X	X				
Zero-trust		X				
Death-pill (data destruction)					X	
Sensor fusion for data integrity	X				X	

In terms of the lifecycle process, industry reported various practices as deployed and anchored in the Engineering Process to improve security and privacy of the system and its operation. Forum members mentioned a number of security best practices as follows:

- Imposed audits,
- Awareness training,
- Due management attention, including defined policy on exposure,
- Paranoid mindset,
- Continuous process and upgradability,
- Installation of a Computer Emergency Response Team (CERT),
- Exchange with industry peers, e.g. ISAC Information Sharing for Analysis Centre (IT-ISAC, 2018),
- Adoption / deployment of community guidelines, e.g. from the Open Web Application Security Project® (OWASP, 2018).

Categorization of threat effort vs impact

So how difficult would hackers find it to compromise a system? The forum attempted to categorize the effort by hackers to breach a system's security versus the impact on the system (see Table 2). This table shows this attempt based on three levels of hacker effort (low, medium, high) versus three levels of impact to system operation, or business.

Table 2 - Attempt to categorize threat effort by hacker versus impact on system

	Impact		
Hacker effort	*Low*	*Medium*	*Critical*
High		• "Forbidden" tampering	• Blocking of a system safety function • Manipulating sensor data, or sensor / actuator HW • Take over control of the system
Medium		• Connection induced malfunction evidence • System bus (local) hack • IP theft • Instrument data leaks to competitor OEMs • Reverse engineering • Information security breach • Using interfaces for 3rd party assets • Malfunctioning of components (internal attackers)	• Denial of service • Change data to change behavior • Ransomware / blackmail • Reputation, brand image loss / business loss
Low	• Capture physical system (defense) • "intended" tampering	• Steal privacy / business sensitive data • Degrade performance / sabotage	• Compromise data • Remote access • 3rd party access / maintenance

This categorization proved to be difficult to perform. The needed hacker effort is rather difficult to gauge and may depend foremost on the type of exploit used. Also the impact may depend largely on specifics. Clear however is that whenever safety is compromised, then impact is critical. Finally, in case of a hack to multi-supplier systems, an unsolved question is how to prove which component and which supplier is liable.

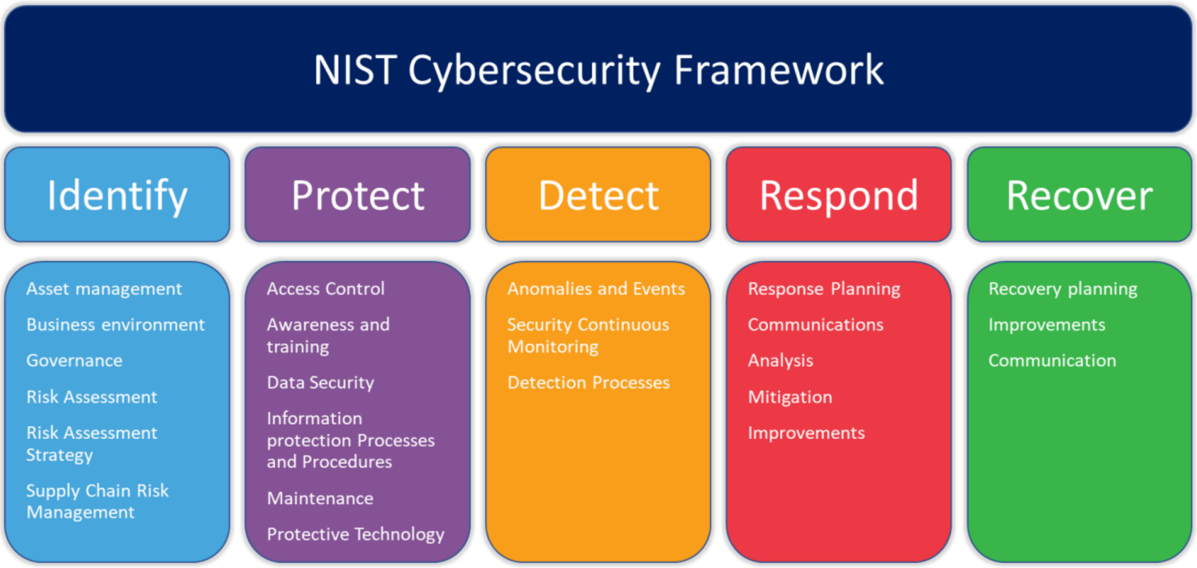


Figure 3 - Key functions and main categories in the NIST Cybersecurity framework

4 Architecting dilemmas

Architecting for security means facing a number of dilemmas in the context of an as of yet immature engineering state-of-practice. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (Barret, 2018) provides an insightful categorization of the key functions and main categories for presenting these dilemmas. The NIST framework (see Figure 3) defines the key functions as in the following Table 3.

Table 3: Definitions of key functions in the NIST Cybersecurity Framework

Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Architecting for security requires striking a balance between security and privacy on one hand, and functionality, usability, performance, cost, etc. on the other hand. Security also sometimes has a hate/love relation with privacy (especially when considering anti-terrorism measures). With elaborate, multi-vendor, supply chains and systems-of-systems constellations, topics such as governance and liability are complex to address when striking a balance between these concerns and product value and cost.

The forum discussed architecting dilemmas that are encountered in the various product domains. The identified dilemmas are categorized in Table 4.

Table 4: Architecting dilemmas categorized across the NIST Cybersecurity framework main functions

Architecting dilemmas across the NIST Cybersecurity framework	
Identify	• How to obtain management buy-in for security? No answers to questions, such as: ○ *"How much is your reputation worth to the business"* ○ *"Are we willing to take risks or be "fast followers"?* • How to calibrate what security level and residual risk level is acceptable or not? ○ *"We are not building nuclear weapons"* ○ *"What hassle do we accept"* ○ *"We do the bare minimum as required by law"* • How to deal with required culture changes in an organization? ○ *"Transition needed from a HW company to an IT culture"* • How to pitch security vs other features to management? ○ How to compare/contrast added value versus loss aversion • How to reconciliate different points-of-view in different countries? • How to consider lifecycle cost vs initial cost for security measures? • How to keep up with the security body-of-knowledge and its evolution?
Protect	• How do you build in security to enable for connectivity based functions? • How do you model security (e.g. UML, SysML block diagram)? • Who is the malicious actor? ○ White label hackers, in evenings hacking for real? ○ Security researchers achieving two minutes of fame, and a life-long well-paid ($$) career? ○ … with danger of followers interested to make a fast buck also? • How to avoid negative impact of security measures on the system?

Architecting dilemmas across the NIST Cybersecurity framework	
	○ Security aspects increase development time, ○ Security is computational resource hungry, will test cases be effective to signal such negative impact? • How to deal with legacy architectures and security? ○ Critical infrastructure typically has a decades-old installed base ○ Old technology often is too hard to fix • How to deal with systems-of-systems? • How to combine security concepts? • How to be ready for future threats?
Detect	• How to be able to detect security breaches? ○ No real solution for detection in "multi-vendor systems" security ○ How to deal with systems-of-systems and integration of multi-vendor (black-box) components?
Respond	• How to balance upgradeability versus modularization? • How to reconcile the needs for fast patching of security issues with safety and e.g. the need for clinical validation in the medical domain?
Recover	• How to ensure that we minimize impact, or can restore operation quickly? • How to ensure that we learn from a security incident? ○ An agile patch should not obviate analysis and learning.

The distribution of dilemmas in Table 4 shows that most forum participants are still very much concerned with embedding and anchoring security in their respective products and organizations. Legacy systems and architectures make such anchoring and embedding harder, as security cannot be simply designed-in, but must be retrofitted with great care.

5 Security in a cloud-based locker system

Next, the forum turned to a different security use case: a cloud-based locker system. In such locker systems, their increased usage convenience through cloud connectivity brings along significant cybersecurity concerns.

Locker systems are prevalent at many locations (e.g. offices, swimming pools, universities) to store personal belongings. In "classical" locker systems, each locker has not only its own lock, but also its own user interface to lock/unlock the storage space Although robust (and fully decentralized), these classical locker systems also have their disadvantages. Loss of keys or forgotten PIN codes present a hassle (both to students and school personnel). Lockers can be permanently (b)locked without being in use; locker managers have no insight in actual usage patterns and capacity needs.

The next level of locker systems incorporate a centralized UI (User Interface). This enables centralized key management and centralized lock/unlock capability, which have clear advantages. The next available locker can be allocated to a new user. Electronic readers for e.g. personnel badges can grant access to specific lockers; no more PIN codes, nor locker numbers, need to be remembered.

Figure 4 - A cloud-based locker system

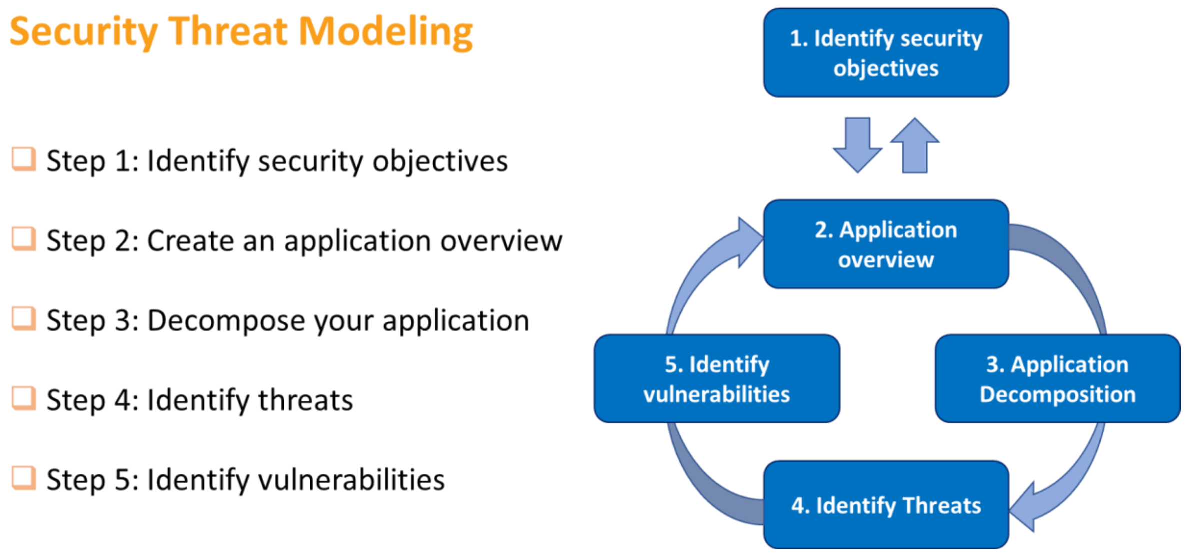
A cloud-based locker system (see Figure 4) adds the option to interact with users remotely via a smartphone APP. Also for locker management one can obtain easily, and remotely, real-time insight into actual locker usage, and remaining capacity. Lockers can be assigned to specific users, for potentially specific amounts of time (e.g. per school year). Unused lockers can be made to open only to specific cleaning personnel. All this results in less hassle, and optimized locker usage. Users can be informed when a locker is no longer used/allowed. Thus less lockers, and less locker space is needed. Combined with simplified locker management this yields significant cost savings, with greatly improved ease-of-use.

Challenges

The user benefits of a cloud-based locker system are manifold. However, how can an SME , which is selling such locker systems, ensure the (cyber-) security of such a cloud-based system as well the protection of (personal) data of its users? A host of new issues must be addressed to be able to sell a cloud-based system successfully, e.g.:

- Ensure the level of privacy of (locker) users,
- Prevent unauthorized access to APPs and data,
- Prevent tampering with data,
- Prevent loss or corruption of data,
- Provide trace-ability of important actions,
- Comply with legislation and regulations,
- Guarantee availability.

These “cyber” security concerns still are only part of the overall “system” security concern, which is to protect the end-user’s belongings. Whereas cybersecurity aims to prevent unauthorized access via cyber-means, also unauthorized access via physical means, e.g. physical tampering must be prevented. At the same time, end-users must not be prevented, nor locked-out, from their belongings (when e.g. the electronic communication has been tampered with, or the electrical power gets interrupted).



Security Threat Modeling

❑ Step 1: Identify security objectives

❑ Step 2: Create an application overview

❑ Step 3: Decompose your application

❑ Step 4: Identify threats

❑ Step 5: Identify vulnerabilities

1. Identify security objectives

2. Application overview

3. Application Decomposition

4. Identify Threats

5. Identify vulnerabilities

Figure 5 - Security threat modelling steps

Approach

Where to start with securing a cloud-based locker system? For the “cloud-based” part, i.e. the cybersecurity, one source of information is the Open Web Application Security Project (OWASP, 2018). OWASP is a nonprofit foundation that works to improve the security of software, and provides resources source for developers and technologists to secure cloud-based applications. OWASP publications and methods provide a basis to build and populate a security strategy.

Product security. Firstly, the security of the *product* needs to be ensured. This requires threat modeling and impact assessment. Figure 5 shows steps involved in the security threat modelling to identify the pertinent threats. Important in creating an application overview is not just to create a static decomposition of the application, but rather consider the *dynamic* decomposition, i.e. the dynamic flow of data through the application. Initiatives such as OWASP (OWASP, 2018), provide support for such endeavors, in particular, OWAPS maintains a top 10 of cloud-induced security risks (OWAS-top-10, 2018).

Table 5 - STRIDE-LM security threat types

STRIDE-LM security threat types		
S	**Spoofing**	Impersonating another user or system component to obtain its access to the system
T	**Tampering**	Altering the system or data in some way that makes it less useful to the intended users
R	**Repudiation**	Plausible deniability of actions taken under a given user or process
I	**Information Disclosure**	Release of information to unauthorized parties (e.g., a data breach)
D	**Denial of Service**	Making the system unavailable to the intended users
E	**Elevation of Privilege**	Granting a user or process additional access to the system without authorization
LM	**Lateral Movement**	Expanding control over the target network beyond the initial point of compromise.

After threat modeling, a second step is to perform risk assessment by security threat classification. Here the STRIDE-LM security type categories (Muckin & Fitz, 2014) provide guidance, see Table 5. These types are well combined with the DREAD severity categories (*Damage potential, Reproducibility, Exploitability, Affected users, Discoverability*) to assess threat impact severity to arrive at a risk classification.

Once security risk assessment has been performed, appropriate solutions for mitigating security risks have to be identified, implemented and tested. This requires extensive security pen(etration) testing, see e.g. (Engebretson, 2013).

Product compliance. Secondly, compliance with applicable regulations need to be demonstrated. GDPR (GDPR, 2016) specifies strict regulations for (personal) data protection. Although law in the European Union, GDPR has set a global benchmark and increasingly GDPR compliance is requested or required also outside the EU.

Assuring compliance with regulations as security of the product and privacy preservation is already a daunting task for smaller organizations and SMEs in particular. Nonetheless, also customers will have many questions and demands to be met.

The scope of customer security concerns

Thorough consideration of product security and compliance is only one part of addressing security. A major lesson learned was that customers bring up many additional concerns, and pose many demands on the company’s operations, its organization, and pertinent process and procedures.

Examples of customer questions are the following:

- Does the system comply with standards such as ISAE 3402, NIST SP 800-14, NIST SP 800-53, NIST SP 800-92?
- Is the organization certified (e.g. ISO 27001 certified)?
- Have assessments and audits been undertaken on data center facilities & services?
- What are the Key Performance Indicators (KPIs) for security of the infrastructure, at various levels (e.g. network, OS, database, application)?

Furthermore customers may pose many questions on the security implementation, e.g.:

- How is customer data encrypted (at rest, in transit)?
- How is the distribution of secret keys arranged, and secured?
- How do you maintain confidentiality and integrity of customer data?

- Are incident detection tools implemented?
- Do you have application logging, and at which granularity?
- What is your risk management strategy for subcontractors. How do you de-risk the services from third parties?
- Can you support my (customer's) Single Sign-On (SSO) process?
- What is your Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)?
- *And many more questions……*

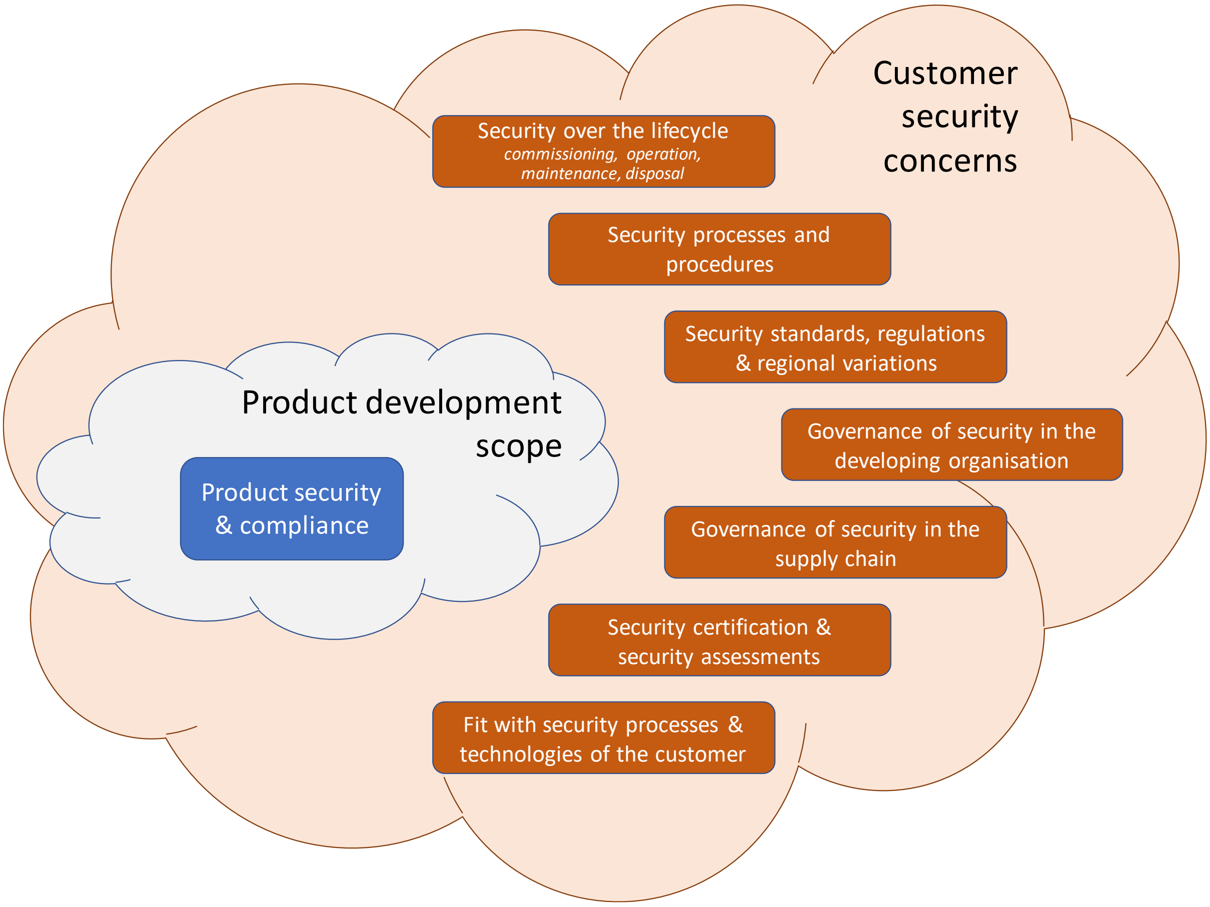

Customer security concerns
Security over the lifecycle
commissioning, operation, maintenance, disposal
Security processes and procedures
Security standards, regulations & regional variations
Governance of security in the developing organisation
Governance of security in the supply chain
Security certification & security assessments
Fit with security processes & technologies of the customer
Product development scope
Product security & compliance

Figure 6 - Customer security concerns greatly exceed the design scope of a product

Reflection

Surprisingly perhaps, a "simple" locker system exhibits a large complexity with respect to security, including coping with all the security issues following a system installation at a customer site. The system context (and integration into customer context) plays a large role, as are the many standards and regulations to be taken into account.

Security concerns increase complexity very rapidly: many aspects and even more considerations need to be addressed. The complexity of security lies in the amount of issues to be handled, where the devil is in the details. Adversaries on the other hand need only to exploit a single weak spot to hack your system. Furthermore, customers are very concerned with security, and will want to know how security is addressed in the product; in product operation; in the process and procedures used during product development, and also commissioning, maintenance etc.; whether security assessments have been done or certification obtained; how governance in the developing organization, and in the supply chain is arranged (see Figure 6).

On the other hand, the fact that customers start to ask for security presents also an opportunity to innovate and compete with security. Architects thus need to go back to the customer key drivers, to address the many questions which also show customer (in) security. Having a clear end goal in mind, in this case trust, may help to establish a healthy trade-off between fast innovation and adequate security, at system level.

6 Security as a Systems Engineering activity

Security discussions have become a regular part of the systems engineering process. The key systems engineering challenge with respect to security is how to keep innovating while providing an adequate level of security and privacy: now and over the lifetime of the system. Security concerns are often found to be at tension with other concerns such as usability, performance and cost. Consequently, system security, i.e., addressing the concern of security in Systems Engineering, entails much more than selecting the appropriate security technologies.

System security requires architects to take an “end-to-end” stakeholder perspective along the whole product lifecycle. System security also requires thinking about commissioning, maintenance, repair, disposal, including the social engineering aspects of security (humans and behavior). Security governance requires aligning organizational processes and procedures. This goes hand-in-hand with securing the supply chain; building organizational awareness and security mindset (“expect the unexpected”) in establishing an organizational competence around security.

Principle 22.2: System security requires architects take an “end-to-end” stakeholder perspective, while fostering organization-wide awareness and competence on security.

System security thus is a rather comprehensive undertaking. How to eat it in small steps? Work is ongoing to address security as a Systems Engineering undertaking. In the forum meeting, the then just started SECREDAS project (SECREDAS, 2018) gave a short research presentation. This European Union research project aimed to develop and validate multi-domain architecting methodologies, reference architectures & components for autonomous systems, combining high security and privacy protection while preserving functional-safety and operational performance (SECREDAS, 2018). One notable outcome of the project is a consolidated list of security and (personal) data protection principles (see appendix A), which may provide guidance to architects.

System security notably requires a counter-intuitive attitude from architects. While architects focus primarily on *value creation*, for security and privacy they rather should focus on *loss creation*, exactly to understand how to avoid such losses. Efforts are needed to combine reliability, safety, and security engineering approaches. While generic security patterns such as layered architectures have appeared, little architectural guidance appears yet available across industries, nor across the loss-related system qualities such as reliability, resilience, safety, and security[2].

[2] INCOSE INSIGHT magazine published —post-meeting— a theme issue on “Loss-driven Systems Engineering” (INCOSE,2020).

7 Conclusions

System security seems like a game that cannot be won. A single security weakness, when exploited by hackers, could negate all careful considerations and extensive efforts undertaken in the product creation process. Indeed, some highly publicized security incidents have occurred — raising the awareness for security across many domains. Consequently, security is now seriously considered across the industry. Some best practices, useful architectural security patterns, and (many!) standards are emerging.

Security in systems engineering goes well beyond securing technology. Architects need to take an end-to-end stakeholder perspective, and look beyond product development and technical issues. They need to work with a 'paranoid' mindset, and also consider human and behavioral weaknesses that could potentially cause security breaches. Organizations need to examine needed processes, their governance, and instill organization awareness and savviness with respect to security, guided in part by frameworks such as the NIST framework.

At the time of the forum meeting in the Fall of 2018, little architectural guidance was available. The trend towards increasing system connectedness, nonetheless created a much enlarged exposure ("attack surface") to security vulnerabilities. Architects are in need of more system security "tools": security-aware reference architectures; architectural methods and approaches to strike a balance between the "value-oriented" system qualities and the "loss-oriented" system qualities such as security and privacy.

The heightened awareness for security has caused that these gaps in architectural guidance and methods are recognized as important research topics. These are taken on by research projects such as the SECREDAS project, by (non-competitive) engineering communities, such as OWASP, and research organizations, such as ESI (ESI, 2021). Their (future) results are awaited to support architects in achieving an appropriate, balanced level of system security.

8 Literature

Barrett, M., Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, 2018 [online], https://www.nist.gov/cyberframework

BBC, Fiat Chrysler recalls 1.4 million cars after Jeep hack, 2015 https://www.bbc.com/news/technology-33650491

Engebretson, P., The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier, 2013. https://www.sciencedirect.com/book/9781597496551/the-basics-of-hacking-and-penetration-testing

ESI, Security and privacy aware design, 2021 [online], https://esi.nl/research/output/methods/secredas

GDPR: G. D. P. Regulation, "Regulation eu 2016/679 of the european parliament and of the council of 27 april 2016." Official Journal of the European Union, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

INCOSE, Theme Issue: Loss-Driven Systems Engineering. INSIGHT, 23(4). https://doi.org/10.1002/inst.12229 .

ISO, ISO/SAE 21434, Road vehicles — Cybersecurity engineering, ISO 2021. https://www.iso.org/standard/70918.html

IT-ISAC, The Information Technology – Information sharing and analysis center, 2018, https://www.it-isac.org.

Khashooei, B., Vasenev, A., Kocademir, H., & Mathijssen, R.: Architecting System of Systems Solutions with Security and Data-Protection Principles, In 16th International Conference of System of Systems Engineering (SoSE) (pp. 43-48), IEEE, 2021. https://doi.org/10.1109/SOSE52739.2021.9497461 .

Motor1.com, Keyless systems may make driving more convenient, but they also make stealing easier too, 2018, https://uk.motor1.com/news/266371/keyless-car-theft-rise/

Muckin, M., & Fitch, S. C., A threat-driven approach to cybersecurity. Lockheed Martin Corporation, 2014. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

National Highway Traffic Safety Administration. Cybersecurity best practices for modern vehicles. Report No. DOT HS 812.333 (2016), https://www.nhtsa.gov/document/cybersecurity-best-practices-modern-vehicles

Paar, C., and Pelzl, J.: Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

OWASP, The Open Web Application Security Project® (OWASP), 2018, https://owasp.org/

OWASP top-10, Top 10 Web Application Security Risks, 2018. https://owasp.org/www-project-top-ten/

van Roermund, T., Security for Self-Driving Cars, presentation at ESI symposium, 2017, https://esi.nl/ecosystem/networking/symposium/esi-symposium-archive/esi-symposium-2017

SECREDAS, Product Security for cross domain reliable, dependable automated systems, ECSEL Joint Undertaking project, 2018, https://secredas-project.eu/

Smith, R. E., A contemporary look at Saltzer and Schroeder's 1975 design principles. IEEE Security & Privacy, 10(6), 20-25, 2012, https://doi.org/10.1109/MSP.2012.85

UNECE, UN Regulation No. 155 - Cyber security and cyber security management system, 2021. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

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

Appendix A: Security and (personal) data protection principles

The SECREDAS Ecsel project (SECREDAS, 2018) consolidated and linked a number of relevant security and (personal) data protection principles for use in architecting system of system solutions (Khashooei et. al., 2021). In this consolidation, SECREDAS took the Saltzer and Schroeder design principles (Smith, 2012) as the basis for the security principles. The European Union's General Data Protection Regulation (GDPR, 2016) provided the basis for the (personal) data protection principles.

In the following, Table 6 shows the consolidated security principles, and Table 7 shows the consolidated (personal) data protection principles. These principles categorize a range of concerns, and can be helpful to provide guidance for selecting appropriate solutions to mitigate threats to security and data protection.

Table 6 - SECREDAS security principles

SECREDAS security principles	
🚫	**Least privilege** Only provide the minimum set of privileges necessary to complete a task. Function, not identity, should determine access controls.
✗	**Least common mechanism** Mechanisms used to access resources should not be shared between different services (or different sets of users) with different priorities and values.
🔓	**Open Design** The security of a mechanism should not depend on the secrecy of its design or implementation. *Information where secrecy is needed (password, cryptographic keys) still stays secret, e.g. white box technologies.*
🔍	**Economy of mechanism / Keep it simple** A design, implementation, operation of a security mechanism shall be as simple as possible, so that it can be thoroughly analyzed, verified, tested.

SECREDAS security principles	
	Fail-safe defaults A system shall remain secure in case a security mechanism was broken or is misbehaving.
	Complete Mediation Every access to every object must be validated. No path may violate this. *Usually done once, on first action.*
	Separation of privilege A system should not grant permission based on a single condition. *Multiple conditions (e.g. 2 factor authentication) should be required to grant privileges, and two or more system components should work together to enforce security (“defense in depth”).*
	Psychological Acceptability The resource should not be more difficult to access than if the security mechanism were not present. *In practice difficulty proportionate to the value of protected asset is accepted.*
	Compromise recording The system should keep attack records, even if attacks are not blocked.

Table 7: SECREDAS (personal) data protection principles

SECREDAS (personal) data protection principles	
	Transparency Data subjects should be informed for all risk, rules, safeguards, and rights concerning the processing in a concise, easily accessible, and easy to understand manner.

SECREDAS (personal) data protection principles	
	Lawfulness of data processing (Personal) data processing must meet criteria for at least one (1) of six (6) "lawful bases”[3] as identified in GDPR (GDPR, 2016).
	Fairness of data processing (Personal) data is processed in ways that do not produce any unreasonable negative consequences for data subjects.
	Data minimization Collecting the minimum amount of data required to carry out the stated purpose and no more.
	Storage limitation (Personal) data no longer needed should be deleted or anonymized.
	Accountability Be able to show that concrete measures have been taken within their capacity to meet their compliance obligations.
	Purpose limitation Describe why personal data is being collected, be transparent for which purposes the data is collected.
	Accuracy of personal data Keep personal data updated where reasonable and applicable. The data must not be incorrect or misleading, especially in a way that could be harmful to the data subject.
	Integrity and Confidentiality Process (personal) data in a way that ensures the presence of appropriate security countermeasures, which provide adequate protection.

[3] GDPR (chapter 6 in (GDPR, 2016)) considers six lawful bases for the use of personal data as follows: i) Consent, ii) Performance of a Contract, iii) Legitimate Interest, iv) Vital Interest, v) Legal Requirement, vi) Public Interest.