TRUSTONIC

Automotive Webinar 19th November 2020 – Questions

Q: What is the main function of cybersecurity in automotive?

A: The primary function must be to ensure the correct functioning of the vehicle, even if subject to cyberattack. Secondary functions may be to prevent other less critical attacks, for example malware that attempts to listen to vehicle occupants. There is also a broad range of areas where cybersecurity addresses other problems – for example, the use of counterfeit parts during vehicle repairs.

Q: How are the ideal approaches to integrate cybersecurity with end-to-end architecture to prevent vulnerability systematically? Do you have any examples, that refer to European WP29? How best to deal with rating and the intrusive test, is it something that Keysight and Ixia can cooperate with?

A: The best approach is to embrace a design for security approach from the start to the end of the development process. This is in essence what WP.29 and ISo21434 are seeking to bring about within the automotive industry. Typically, when embracing such an approach this includes a strong focus on designing code to be secure and enhancing the range of testing that systems are subjected to, in order to ensure that they offer the highest level of protection. It is typical, that a layered architecture is used to provide a wider range of protective measures against different attacked vectors and to ensure that a vulnerability in one part of the system is not automatically cascaded to other domains.

Q: Many automotive hacking events happen. Any proposal to Jeep, Nissan Leaf, Tesla and other cases?

A: Such events are normally white hat events, with the intent of finding vulnerabilities and helping the industry to improve overall. We view this overall, as a good thing to raise awareness within the industry. However, they will tend to focus on specific and generally high-profile areas, such as gaining entry or control over a vehicle, and tend to set ground rules that may not apply in the real world (such as the attacker being outside the vehicle). They have their place but are no substitute for secure design and rigorous testing from day one.

Q: Does the panel think that security certifications will become more important in light of the new UNECE regulations?

A: Absolutely. To show compliance with new regulations, and/or to defend against litigation, OEMs are going to have to show that they are taking security seriously and using best practices to protect vehicle users. Certifications are a clear means for demonstrating both.

Q: How are the cybersecurity ecosystem looks like worldwide? Local for local? Any concerns about trade war risks?

A: Automotive is a global industry, but the reality is that there are numerous local standards, both for physical and cyber components – whether encryption schemes or DRM standards. This is a complexity we just have to live with. UNECE WP.29 is introducing new regulation, that will become national law, that is attempting to harmonise multiple different country standards and laws and will provide a common framework for more than 60 countries around the world, including the whole of Europe, which definitely helps.

Q: Related to that, has enough been done to connect V2X? Especially connected to the micro-payments you mentioned. Local authorities planning on extracting these tolls - are they necessarily best placed to do this without support?

A: V2X is still in the early phase of deployment in most parts of the world. There are many use cases that it is expected to support with payments solutions being one of them, but this will vary by country. Many toll collection schemes use architectures originally designed for electronic train tickets, and there is lots of variation. In time this may move towards more global standards, such as EMVCO used for credit/debit payments. That would open the market up to others and allow for broader applications – but this is just one part of V2X. Digital signage is a whole different area, where mutual trust between vehicle is critical, and where more needs to be done.

Q: China authorities require cybersecurity application integrated SM2 algorithm

A: Correct. China has defined the SM2, SM3, SM4 standards for secure communication between devices. The SM2 standard is required for the generation and verification of digital signatures when used in V2X.

Q: Besides Automotive ISAC, what are other top forums for auto cybersecurity? Have OEMs and Tier1's participated in the IoT Cybersecurity Alliance (founded by Trustonic, AT&T, Nokia, Qualcomm, etc. a few years ago)?

A: There are multiple different consortia working to enhance the understanding, sharing and implementation of automotive cybersecurity. The AutoISAC is a good example of forum, that is aiming to bring together players from across the industry and around the world the share the latest learnings, identified threats and research in this domain. Other forums include Automotive Cybersecurity Industry Consortium (ACIC), and special focus projects within the Society of Automotive Engineers,
Alliance of Automobile Manufacturers, Alliance for Automotive Innovation are also focused on Cybersecurity. There are also a range of national associates such as the 5Stars initiative in the UK.

Q: How is Cybersecurity related to (functional) safety?

A: Very good question and one that is being asked on a regular basis. Today, they are often considered separate, and a technical answer is in how failure is treated. A functional safe system must degrade safely, whereas a secure system will typically stop if under attack. In practice we need functionally safe systems to also be secure, and that adds a lot of complexity. In time we anticipate that standards and certifications for the two areas will merge as there are already areas of commonality between ISOP 26262 and ISO 21434.

Q: How would you suggest changing the behaviours within a company who perhaps has not had cybersecurity at the heart of its decision making in the past?

A: Cybersecurity is a complex issue that spans all functions within a business. For many companies this can be a considerable undertaking requiring experiences and experience that may not reside within the company. Hence, it is important to think about having the right partners who can help develop a comprehensive cybersecurity strategy. Although cybersecurity is a relatively new topic in automotive, it is not a new discipline and there are companies, such as Trustonic, who have been addressing similar needs in other markets for many years. For an OEM, understanding how to phrase security needs on an RPF to Tier 1s, is one example where the right and timely advice from a partner can be invaluable.

With the upcoming UNECE WP.29 regulations and new standards such as ISO 21434, it is also important to elevate Cybersecurity from being an activity and in to being part of the company philosophy and broader strategy.

Q: Are Software or hardware like cryptography chips more important?

A: Increasingly software solutions, such as TEE based soft HSMs can meet the security needs without the cost/complexity of additional special purpose hardware – but that does not mean that hardware advances are not important. For example, vehicles contain hundreds of microcontrollers that generated, typically insecure, signals consumed by larger ECUs. Newer microcontrollers can support hardware security features to allow these signals to be encrypted and/or authenticated, adding to the overall security of the vehicle.

Q: Any latency concerns about cybersecurity data processing?

A: If the performance requirements are correctly taken into consideration at the start of the project and form an integral part of the overall architecture design phase then, latency should not be an issue. The overhead to decrypt or validate signatures is generally small and can easily be accounted for with the target performance criteria, provided the system is configured correctly.

Q: Does a vulnerabilities database helps? How does artificial intelligence research can improve cybersecurity?

A: There are a number of different areas where artificial intelligence can help to enhance cybersecurity. One area will be predictive modelling to help anticipate potential attack

vectors. Another area will be in the intrusion detection area where AI will be used to identify suspicious behaviour. AI is also likely to be used to help build more advanced driver behaviour models in order to identify when unauthorised drivers are attempting to use the vehicle. Over time, aspects of AI are likely to be included in many of the core vehicle systems to help keep the vehicle users as safe as possible.

Q: What are key differences (or similarities) for manufacturer Security Operation Centers (SOCs) in securing BOTH the business/enterprise and vehicle security? Should detections, investigations, remediation and response be performed by the same team or different teams?

A: The main difference between these two environments are the specific workflows that are modelled between and enterprise environment and a vehicle. While many of the techniques and approaches maybe similar the specific software, algorithms and domain knowledge required by the monitoring team will be different. As to if the same team should operate the SOC this is a question for each OEM to address on an individual basis based on their experience, resources and strategy.

Q: You are talking about software to address cybersecurity needs. But secure hardware is playing an important role, too. When do you think that hardware will be in a state when it is 100% reliable (if possible, at all?)

A: In automotive cybersecurity, as in many other technology drive industries, software is replacing specialized hardware over time, but being run on increasingly powerful and flexible 'general' hardware architectures. Let's take the example of an automotive HSM. This stores keys and signs/encrypts messages and does so perfectly well and stores the keys in a highly secure manner. The issue with an automotive HSM is cost. Specialist hardware is always more expensive than a software equivalent – and software HSMs running within a secure area of a general-purpose processor (i.e. on a Trusted Execution Environment) will be cheaper and easier to manufacture. Software is also more flexible. In a software environment you can distribute keys across the vehicle in ways that hardware HSMs don't support today. As we look towards autonomous vehicles, the need for hardware support in terms of 'AI processors' is increasing, but those are generally designed with flexibility in mind, so that the software algorithms can evolve far faster than the hardware they run on.

Q: How does each car know to trust each other? How do we know that someone isn't injecting signal data into the system?

A: This is an important area that the industry is starting to place a strong focus on. Up to now, a lot of emphasis has been placed on securing the individual vehicle. To meet the vision of fast flowing autonomous motorways we will have to address the wider security implications V2V and V2X. Enabling a vehicle to secure connect to another vehicle or a ride side unit will be key to ensuring a safe environment. A combination of different approaches, such as secure boot and validation of the software image, full attestation of the end points and use of encryption within the vehicle network and between other vehicles, and infrastructure will all play an important role. Knowing which vehicles to trust, will most likely come down to OEMs vouching for them and the advanced use of

secure certificates to support this. This will need to be back up by robust certification and enforcement of 'digital MOT' schemes.

Q: Will a web giant like Amazon invest automotive cybersecurity, since they have deep understanding of cybersecurity?

A: Only Amazon can know what they will invest in. However, as Amazon increases its involvement in the automotive industry, through the provision of cloud services and the availability of Alexa in vehicle, it is clearly in their interest to ensure that such services are safe, secure and will help to build trust with the vehicle user.

Given the complex nature of cybersecurity coupled with the complex value and delivery chain for connected services the ability to leverage the expertise of companies such as Amazon can only be a good thing for the industry, as it moves towards creating secure end to end chains of trust for its customers.

Q: EDR (Endpoint Detection & Response) is commonly used to secure enterprise assets from cyber-attacks. When does the panel think we will see widespread use of EDR to protect vehicles, particularly as the complexity and attack vectors increase?

A: We have already seen a number of OEMs deploy Intrusion Detection and Prevention (IDS / IPS) solutions to enhance the level of protection provided within a vehicle. Given the new regulations and standards coming in to force over the next few years, and the growing awareness of cybersecurity amongst consumers, it is reasonable to expect that by 2024/2025 the use of these solutions will start to become widespread.

Q: I've driven a Tesla for more than 5 years with no major security incidents. Are they leading OEMs in auto cyber safety? Does their OTA update model the leading standard? Are others following/challenging?

A: Tesla have clearly been very successful in leveraging OTA to not only provide updates to the vehicle, but also to enhance the overall engagement with the vehicle users. There are multiple standards for OTA and while individual companies such as Tesla may grab the headlines most Tier 1s and OEMs are leveraging 3rd party developed standards-based solutions. It is widely recognised in the automotive industry that Harman's OTA solution is the market leader in terms of deployments and vehicle backlog.

Q: OEM invest lots in software, like Volkswagen. May OEM become competitors of Tier 1? How can Harman manage the relationship with OEM.?

A: OEMs have indeed started to enhance their in-house software organizations, but this has been in response to the growing level of importance in the role software plays in the future of the

automotive industry. Further with new industry regulations coming into force this is also requiring OEMs to have a greater in-house knowledge of the vehicle's software and the related cloud services.

Given that modern vehicles already have more than 100M lines of code and fully autonomous vehicles are expected to have 300M plus it is highly likely that OEMs, will continue to work closely with their Tier 1 partners and the wider value chain to ensure that they can deliver the most advanced and secure vehicles, and related services, possible.

Q: TS16949 will integrate with cybersecurity requirements? How can cybersecurity become mandatory for OEM?

A: This is really a question for national agencies, that oversee the legal requirements for vehicles that are allowed on the roads. However, regulations such as UNECE WP.29, that covers more than 60 countries demonstrates that it is possible to bring cybersecurity requirements into law and at the same time that it can be harmonized on a global level to minimize the impact and cost to OEMs.

Q: Cybersecurity Hotline can be possible for consumers?

A: This will be an OEM-by-OEM decision, but there is no reason why a Cybersecurity Hotline could not be supported along with other approaches for consumer to report concerns to OEMs.

Q: How do you combine OTA with cybersecurity?

A: Over the Air software updating capabilities, form part of the wider cybersecurity architectures for modern vehicles. The ability to support secure OTA updates, in a vehicle enables OEMs to keep the wider cybersecurity systems up to date and to rapidly deploy patches when new vulnerabilities are identified.

For any further information, please contact: info@trustonic.com

www.trustonic.com