ITEA Cyber Security Advisory Board (CySAB) report

Meeting 6 July 2021, online

On 6 July 2021, the first ITEA CySAB meeting took place with the following Advisory Board members:

Company/Organisation	Country	Represented by
Academic Medical Center of the University of Amsterdam	The Netherlands	Sylvia Olabarriaga
AVL	Austria	Eric Armengaud
Ericsson	Turkey/Sweden	Emrah Tomur
Ford Otosan	Turkey	Safa Çalışkan
Koçfinans	Turkey	Özden Gebizlioğlu Özvural
NXP	Belgium	Joppe Bos
PAL Robotics	Spain	Francesco Ferro
Saab	Sweden	Stefan Hagdahl
Siemens Mobility	Germany	Andres G. Guilarte
Signify	The Netherlands	Sandeep Kumar
Turkcell	Turkey	Emin İslam Tatli

ITEA is a Eureka Cluster stimulating the creation and execution of R&D&I projects that are funded by national public authorities and aiming to build up innovative research projects that are based on urgent needs and requirements of customers and end-users.

The ITEA Cyber Security Advisory Board is established to understand the urgent cyber security needs and cyber security challenges as input for the ITEA Community as well as to enable a board of organisations to learn and to get inspired from each other, and to create collaboration among its members and between members and the ITEA Research Community.

The CySAB meeting was set up to introduce the members to each other and to build trustful connections between them. Therefore, the main subject was to share the urgent requirements of each organisation and to highlight potential collaboration and research opportunities related to cyber security. This report covers the challenges that are shared by each member and the potential topics to build new ITEA research projects.

Cyber security for interconnected systems

One of the challenges is that systems are more and more interconnected, and this trend creates new surfaces of attacks for systems that were in the past isolated and difficult to attack.

This challenge can for example be seen in the automotive industry where more and more vehicles are connected to the infrastructure and which might also be connected to other cars in the future. It is key to keep the connection secured and to ensure that no attack - to the endpoints (i.e. the cars) or the shared network, storage and compute infrastructure - can lead to a malicious control of the car.

We observe a similar problem in the factory where more and more production systems are connected. More connectivity improves the efficiency and the productivity of the factory but opens new doors to attack the systems. Again, new solutions need to be developed to guarantee a good level of security.

At home also the connected objects that can be modified and booted through the network are creating new security challenges. The specificities are that the devices could have limited resources and that proprietary solutions are not interoperable.

As systems gets more and more interconnected, the system complexity increases correspondingly building up a technical debt potentially mitigated through re-engineering and security-by-design.

Operational technology (OT) cyber security

Digitalisation transforms the industry and more and more IT security and OT security are interrelated. The field of IT security needs to address new challenges that were in the past only OT concerns.

A very important aspect is that the lifetime of the solutions is not anymore counted in years but in decades. The challenge is to provide cyber security solutions for infrastructures that are developed to last 30-50 years. It is mandatory to deal with more adaptive solutions that can evolve over time to cope with attacks that are not exactly known at design time.

The operational data exchanges are increasing as the number of vulnerabilities to cover. The OT systems have to embed security monitoring features to control these new risks.

Trust within the supply chain

At each level of the supply chain, you need to establish the trust between the supplier and the users. It can be B2B transactions or between the supplier and the final customer.

One aspect of this challenge is to put in place security assurance methods. Some new real-time an automated verification solutions are expected that could help to warranty a good level of security. The development of compliance and audit methods is also an important challenge to reinforce the trust within the supply chain.

Another aspect could be to develop more with open-source software and to share an open stack that is the result of a common effort towards a better security level. This will also have an impact on the affordability of the trustworthy solutions and sustain the mutual trust between actors.

Worldwide standards for cybersecurity

The development of trustworthy systems is already a big challenge but if the regulations change from one region to another , the complexity becomes intractable, and the result may be weaker systems.

There is a need to work on a more unified vision of security standards. This will lead to a more mature market without national gatekeeper regulations and, as a result, a safer solution.

The lack of standards is also a concern for some customers applications. Just to mention some of them, the automation of the home or the connected watches for healthcare are two examples where proprietary solutions are dominant and prevent the development of an open and secure framework.

Real-time detection of threats

With the high number of devices and systems and the high speed of the exchange of data, manual security monitoring is no longer a solution. The development of real-time detection systems is mandatory.

In the domain of IoT, the detection of anormal behaviours has to be put in place. In the banking sector, the new mobile applications have also to be monitored and decisions to be taken in real time to allow or not the transactions. The development of a framework to monitor in real time and compare with normal behaviours would help to provide the needed security level of these applications.

For the development of these real-time threat detection solutions, it may be interesting to assign risk scores to focus the prevention actions on the more urgent issues. Another important feature is the interface with the human operators, and especially the ability to present huge amounts of data in an understandable way to the operators.

Secure identities

The multiplication of objects and the growth of automated transactions open the challenge to provide efficient solutions to manage the identity of the objects or the actors of transactions.

The main difficulties are to provide an open solution that can deal with new objects, that has low-cost and that can scale on demand. Solutions with such features will be of great help for the development of many applications, most of them using IoT devices that need to be identified in a secure way.

Authentication solutions could also be improved, and new methods based on Machine Learning (ML) are interesting. This direction should be investigated.

Privacy

Digitalisation leads to more and more data exchange and storage. Some of the data are related to information about human individuals, leading to a privacy concern. Privacy preservation becomes an important element in many domains.

This is the case in the future car, where the system will manipulate data related to the user such as fatigue monitoring. This information has to be used for the safety of the vehicle but should not be disclosed in other circumstances.

Another important use case for privacy is the development of connected objects at home. These objects can expose sensitive information related to the users. The lack of standards in this domain of connected objects is an obstacle against the development of a higher level of security.

In the healthcare sector, most of the data are very sensitive. As in this sector it is also interesting to use cloud solutions, the development of new solutions ensuring the privacy of data clouds would be beneficial.

Usability and onboarding users

If the security solutions are difficult to use, the users will try to bypass them. In several sectors, this is a big concern.

In the healthcare domain, users of the IT systems are not IT specialists. The usability of the solutions is a key element to improve the efficiency while preserving the confidentially of the data. The more transparent the security is the more accepted it will be. The security-by-design approach will help to propose a more integrated security and so to improve usability.

Other topics mentioned by the Advisory Board members

The role of AI has been mentioned by several members. First AI is an important method to improve the security solutions. It can help in the detection of attacks, in managing some responses to attacks and in the automation of the surveillance. Second, some specific security solutions have to be developed for AI systems. They have to be resilient against attacks through erroneous data and to be designed not to reveal private data.

Another topic is the lack of awareness, even in the big industry, about the risk related to cyber security. New solutions could be developed to help analyse the risks and to translate them into

potential money losses. Such tools could convince the top management to invest more in cyber security and increase the global security level of the society.

The evolution of the public key cryptography solution that we currently use in the web will be an important change that needs to be carefully managed. In less than two years from now, NIST will have selected the new algorithms that can resist to crypto attacks from quantum computers, and we will have to deploy this new public key infrastructure. The migration must be managed in a way not to open vulnerabilities.

There is more and more information shared on vulnerabilities, but the main problem becomes to keep track of all of them and to update and patch in a timely manner the systems and applications with the security fixes. When you have thousands of applications to update, this is very difficult. New solutions to help patching the known security holes would be beneficial.

To reinforce the security level, it could be good to use more simulation tools. The simulation of security attacks could be developed to make the systems more robust to such attacks.

Some intelligent threat-analysing tools are also to be developed. It is important to keep track of the discussions on the dark web or on social media that can reveal the preparation of an attack against a company.