ITEA Cyber Security Advisory Board (CySAB) report

Meeting 29 June 2023, online

On 29 June 2023, the fifth ITEA CySAB meeting took place with the following Advisory Board members:

Company	Country	Represented by
Assa Abloy	Poland/Sweden	Tomasz Grabowski
Armengaud Innovate GmbH	Austria	Eric Armengaud
Saab	Sweden	Johan Tenggren
Signify	The Netherlands	Sandeep Kumar
Vitarex Studio Ltd	Hungary	Gabor Gulyas

In addition, both Jordi Clement Chief Technology Officer, Identity and Access Management (IAM) at Thales and Christian Dietrich, who is also from Thales and member of the ITEA Steering Group, joined the meeting.

ITEA is a Eureka Cluster instrument to build innovative RD&I projects that are funded by national funding agencies and that are based on the urgent needs and requirements of end-users.

The ITEA Cyber Security Advisory Board (CySAB) has been established to understand the urgent customer needs and requirements in the cyber security domain to build up innovative research projects by the ITEA Community solving cyber security challenges. In addition, this Board enables the member organisations to learn and to get inspired from each other and to create collaboration among members and between members and the ITEA RD&I Community.

This CySAB meeting was set up to review the State-of-the-Art in identity and access management with an analysis of the main trends. It was also the opportunity to listen to the Board members providing insights into their important cyber security issues. Finally, a discussion took place regarding the ITEA CySAB portal that was set up to gather the challenges and solutions and other relevant information in one central place.

Identity and access management landscape

According to Jordi Clement, who gave a keynote during the meeting, digital identity is the basis of trusted digital interactions because we continuously need to know with whom we are dealing with and what actions are authorised for this identity to develop secure digital applications. In addition,

you must balance the usability of the controls with its efficiency. Identity management deals with employees in order to give them the access rights to applications and ensure their productivity. Today it is also increasingly important for business partners who need to access our IT systems. As ecosystems are more complex, sometimes a single company has to delegate the organisation of identity and access management to external trusted providers. Identity management is also a key technology to interact with users and consumers. It is important to onboard them as quickly as possible without friction. But this has to be balanced with risk prevention, especially in banking applications.

After this introduction, Jordi came back on the last twenty years of technology development in the field of Identity and Access Management:

- In the 2000s, IAM was very much on employee's access control to offer a single sign-on. Meta-directories were a technology to aggregate all the information to have a single view of the employees. After focusing on user lifecycle management, the role-based access management was also introduced.
- In the 2010s, the introduction of cloud-based applications and the development of customer identity management were the drivers. Another important element was the introduction of the GDPR (General Data Protection Regulation) regulation. Technologies to provide the user with the control of the privacy of her/his information and to manage consent have been developed.
- Today, besides the employees and the consumers, the management of external workforce is high on the agenda. Ensuring a high level of assurance in onboarding temporary workers is essential. AI methods are now integrated in the IAM solutions e.g. for threat detection.

The future of IAM, after centralised and federated (with your partners), is moving towards decentralised IAM. Identity will become something transactional and will not be managed per se. It will look more like credential verification. Additionally, it is important that the same person will have several personas to interact with a same company, depending on their activities. The control will also be extended to process, workload, objects and not only people. The focus will be to build frictionless, trusted and secure digital journeys based on identity credentials provided by external authorities.

Another key concept for the future landscape is digital sovereignty. The will to control over our digital destiny will shape the solutions in terms of technologies (infrastructure, encryption, etc.).

To master these trends, it is crucial to have the ability to orchestrate the digital journeys, to manage fine-grained authorisations based on accurate risk assessment and to cope with sovereignty concerns at regional, national, organisational, and individual levels.

After the keynote, a lively discussion touched the following topics:

- Risk-based approach to correctly choose the authentication methods (multi-factor authentication, TOTP, passkeys, biometrics).
- Device and service identities are connected to a user identity in most of the use cases. This link enables to manage the authorisation.

- The remaining concerns are still user-friendly features of the solutions and inclusion of all the potential users with heterogeneous technical background / knowledge (not losing people because of digital complexity).
- AI/ML methods play a central role in to improve anomalies, fraudulent account creation detection, etc. Wearables are a new technology to enable continuous authentication.
- AI/ML methods can also be used to mimic user behaviours, thereby increasing the risk.

Main priorities seen by the CySAB members

The Cyber Security Advisory Board members shared their views on the challenges of the domain that could lead to collaborative research projects.

1. Federated machine learning

Federated machine learning is already a used technology. Nevertheless, further progress is still needed to leverage the availability of decentralised data and to improve the level of security of several applications. Developing a framework to ease federated learning application design could be a good collaborative research project.

2. Large language models

The development of large language models sets new challenges. They can be misused, used to mislead users or used to insert corrupted content into libraries. The scope of a potential project could include the assessment of the ‘quality’ of the content produced by these models (especially when it involves code).

3. Traceability and trustability of complex decision processes

In industries like the automotive sector there are very complex decision processes with a lot of participants involved. A trust layer could help to get better decision-making processes in this decentralised environment (transparency and accountability for the decisions).

4. Onboarding people without cumbersome processes

In complex design chains, you have experts that do not want to be bothered by understanding the security tools. Decision-makers also often don't want to lose time in security control checks. Lighter on-boarding methods could be researched to better adapt to user profiles.

5. Trusted collaborative spaces

Automotive industry moves towards software designed cars. The car manufacturers must integrate very agile technology providers. However, the industry is regulated and has mature manufacturing processes. Some tools or methodologies could be developed to fill the gap between mature industrial environments and new innovative providers. This challenge applies to other sectors, including defence.

6. Adaption of product and production processes to new cyber security regulations

You see a lot of regulatory cyber security frameworks around the globe In Europe, new regulations such as the Cyber Resilience Act or the Radio Equipment Directive are being prepared. There is a big

challenge to adapt legacy products and the production processes to the new regulations. Any idea to help the industry to adapt to these new constraints would be welcome.

7. Responsible cyber security

Currently, the developer may provide government agencies with the private keys of end users in order to care for public safety/security. This is in clear opposition to the right of end-users to maintain the confidentiality of correspondence. Therefore, there is a need to develop appropriate 'secure cryptography' mechanisms which, on the one hand, will protect the right to privacy and, on the other hand, they will ensure access to correspondence by authorised bodies in special cases.

8. AI/ML for cyber security

The AI/ML methods, as already mentioned, could significantly improve the detection of threats and help to react against them. The voice biometric identification solutions could also be misled by application of ML generating fake voice from recording samples. Globally, the interaction of AI/ML and cyber security offers good opportunities for research projects.

9. Post-quantum cyber security

Quantum computers, that are expected in the coming years, will be able to decrypt some of the current cryptographic algorithms. The NIST (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms) has started to select new quantum-safe cryptographic algorithms. The challenges are to adapt the legacy cyber security solutions and to avoid that some sensitive data recorded today will be revealed when quantum computers become available.

In conclusion, the challenges are quite diverse and very complementary to the ones that were presented last year(https://itea4.org/publication/download/itea-cyber-security-advisory-board-report-july-2022.pdf). They are good opportunities to prepare collaborative research projects.

CySAB portal

ITEA offers a portal (https://itea4.org/cyber-security-advisory-board.html) for the CySAB members and the ITEA Community to build connections among them and to build a bridge between the CySAB and the ITEA Community. This portal presents the following sections:

- Information related to the CySAB
- Introduction of the CySAB members
- Information on challenges / project ideas
- Cyber security related news from CySAB members / ITEA (projects)
- Innovative outcomes from ITEA projects
- Cyber security related ITEA projects
- Cyber security events

The CySAB members commented that it is important to update the news section on a regular basis. ITEA could also explore the possibility of securing special conditions for attending the events mentioned in the related section.

Conclusion - Next steps

This CySAB meeting was a great opportunity to discuss the cyber security evolutions and to identify potential opportunities for new ITEA projects that could be submitted to the upcoming ITEA Call 2023. We want to thank Jordi Clement from Thales and the CySAB members for sharing their views.

It is now up to the ITEA Community to prepare related cyber security projects based on this valuable information.

For this purpose, you can benefit from the ITEA PO Days 2023 taking place on 12-13 September in Berlin. More information about this event can be found https://itea4.org/podays2023. This two-day networking event offers a great opportunity to find skilled partners to create new cyber security solutions together, so we hope to see you in Berlin!

The next CySAB meeting is planned for Q4 2023, where we would like to interact with the cyber security focused ITEA projects.