ITEA Cyber Security Advisory Board (CySAB) report

Meeting 27 June 2024, online

On 27 June 2024, the seventh ITEA CySAB meeting took place with the following Advisory Board members:

Company	Country	Represented by
Assa Abloy	Sweden	Tomasz Grabowski
Armengaud Innovate GmbH	Austria	Eric Armengaud
Ericsson	Sweden	Ömer Faruk Tuna
Turkcell	Türkiye	Emin Islam Tatli
Vitarex Studio Ltd	Hungary	Gabor Gulyas

In addition, Ifigeneia Lella from ENISA, leader of ENISA threat landscape team joined the meeting as keynote speaker.

The ITEA Cyber Security Advisory Board (CySAB) has been established to share and 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 had two objectives:

- to look at the main messages of the ENISA Threat Landscape report
- 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.

ENISA Threat landscape

ENISA is a European Union Agency based in Athens and Brussels in the field of cybersecurity. It has activities in capacity building (exercises and training), policy implementation and development, certification and operational cooperation.

Each year ENISA publishes its cybersecurity threat landscape report based on public and open data which presents the cybersecurity threats, the trends and some suggestions for protection strategies. During the meeting Ifigeneia Lella presented the content of the 2023 report.

The report distinguishes four types of threat actors: states actors, cybercriminals, hacker-for-hire actors and activists. Regarding the trends, there is a strong focus on attacking edge devices and the cybercrime market is more and more “as-a-service” model with a lot of expert services for sale (e.g. credentials for VPN and Remote Desktop Protocol breaches, blue-prints of attacks). Most of the time, the attacks start from a valid account that is accessed and can use different weaknesses as living off the land binaries to introduce corrupted files. The attacks have been adapted to target applications running in the cloud. Deepfakes and misuses of AI are also on the rise.

Data threats have increased a lot at the end of H1 2023. Unfortunately, information sharing on data threat is decreasing due to the negative impact of reporting data theft. Again, the attackers have adapted the technics to target data stored in the cloud.

Social engineering threats (phishing attacks, identity theft…) have benefited from new AI technologies but perhaps not to the extent that was feared. These attacks have been favoured by the decreased usage of multi-factor authentication because of its complexity.

Malware has risen. Due to Microsoft evolution on macros, the attackers have adapted their methods (e.g. use of containers files). More attacks target mobile with spyware that can even come pre-installed.

Ransomware is at a record level for the last ENISA Threat report period. Most of the attacks are based on the use of malicious URLs. The emphasis is now more on data extorsion rather than on data encryption as in the past.

Foreign Information Manipulation and Interference (FIMI) has increased due to more conflicts and more hacktivist groups. The use of AI has favoured these threats. A market has emerged to sell disinformation as a service.

In summary, the threat actors are very agile and fast to use new technologies. Even if the landscape is not complete due to unreported attacks, cybersecurity attacks have increased. To react it is important to share information and the best practices and to develop coordinated actions.

The next version of ENISA threat landscape is expected in September 2024. There are some changes, mainly in the way of operating but there is also some progress from law enforcement organisations.

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. Local LLM models for applications using sensitive data

The first challenge mentioned (not specific to cybersecurity only) is the availability of LLMs that can be used locally, not sharing sensitive data and addressing languages that are not mainstream. Currently the use of commercial models like ChatGPT is not relevant because you have to export data that you want to keep private and the cost of these commercial models can also be a barrier. **Availability of LLMs that you can use locally, with good performances for not frequently used languages would enable many applications especially in the healthcare sector.**

2. AI for cyber-attack protection

AI is already used in cybersecurity. For example, AI is used for botnet detection, source analysis, attack surface management (login page detection with image recognition technologies). Nevertheless, **more can be done** and it is relevant to prepare collaborative projects in this field.

3. How to secure AI applications

There are some specific risks of attacks for AI application relying on AI models. It can happen at different stages of the DevOps process. Understanding the risk **and putting in place more security in the DevOps cycle of AI applications is an important challenge**. The trustworthy, the robustness, the explainability, the auditability, the accountability, the fairness, the leakage of private data of AI applications are hot topics that require more research.

4. Attack surface management

As applications are more complex and more connected, the attack surface has increased. It is especially the case when you have connection of new applications with legacy applications. **New methods for attack surface detection and management are a relevant topic for future research projects.**

5. Management of the cybersecurity warnings

In May 2024, more than 25 critical vulnerabilities were published. For organisations having complex IT systems, it is very difficult to follow all the alerts and to check whether the available patches have been installed everywhere. **Development of new tools to help to manage the process of vulnerability tracking and curation is a good research project topic.**

6. Security of IT architecture

Security relies most of the time on a usage of technologies in a well-structured architecture. The role of active directories and of API is more in more central in developing a sound IT architecture. So, **any project that can increase the efficient and security of active directories and can improve the management and monitoring of APIs will have a positive impact on cybersecurity.**

7. Protection against jamming

Even if this topic is not new, **protection against jamming is still a hard topic in the protection of telecommunication networks**. Especially with the development of applications with more edge devices that rely on robust wireless communication.

8. Inheritance of weakness in the supply chain and supply chain management

The management of the supply chain is complex, especially for large companies. Sometimes you have to rely on solutions that can import weaknesses in your own systems especially when there are a limited number of potential suppliers. **New solutions to detect the weaknesses in the supply chain and to monitor them are a demand from the market.**

9. Misuse of Generative AI

The emergence of generative AI has created new threats like creation of deepfakes. **The detection of these deepfakes is a difficult technical challenge with a large impact for the society. The protection against phishing attacks created by generative AI is another concern.** There are opportunities for collaborative research projects on these topics.

10. Software defined vehicle

In the automotive sector, the trend is to develop the concept of software defined vehicles. This trend opens new security challenges with the switch toward the collaboration of several data services providers. The transition from a physical product sold by one company to software services provided by a group of companies creates a big security issue. This transition from a physical product towards a software driven asset is also happening in other sectors and changes the value creation process and the business models. **Solutions or tools to support this digital transition with a high level of protection against potential threats and easing the certification are relevant objectives for future research projects.**

11. Continuity in healthcare delivery

In healthcare a patient is in contact with many caregivers who may have only a limited vision of the patient data. Solutions helping to provide a more holistic and complete vision of a patient's health will generate benefits both for the patient and the healthcare system. It is a way to increase the quality of the cares given and to optimise the healthcare system. **The challenge is to create new data spaces and to manage sensitive data with a high privacy level.** With such a platform providing privacy, confidentiality, availability, it will be easier to develop innovative healthcare solutions using this foundation.

It is noticed by several Board members that a lot of research projects develop interesting proof-of-concepts but not aways follow up by adoption. Some public funded projects also generate results that could be exploited by organisations external to the consortium. If the reuse of public funded project results is increased, it will generate important gains. It is not per se a topic of an ITEA project, but it is important when creating new projects to think about an approach that will facilitate the transition from proof-of-concept to effective use and a wide reuse of the project results.

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-meeting-report-july-2023.pdf). They present 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

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 2024. We want to thank the CySAB members for sharing their vision on the most important challenges of this moment.

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

For this purpose, you can benefit from the ITEA PO Days 2024 taking place on 10-12 September in Antwerp. More information about this event can be found at https://itea4.org/podays2024. 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 Antwerp!

The next CySAB meeting is planned for Q4 2024. During this meeting, we would like to interact with the cyber security-focused ITEA projects and Project Outlines.