Report on the ITEA international customer workshop on Cybersecurity

By ITEA Vice-chairman Philippe Letellier

From 20 May to 30 June, ITEA has organised its sixth international customer workshop and this year it focused on Cyber Security which is at the heart of the digital transition to ensure it is safe and secure. The workshop was co-organised with Airbus, Atos, Bosch and KoçSistem and hosted by Atos and we are very grateful for the strong support of these ITEA Board companies.

Due to the COVID-19 pandemic it was the first ITEA customer workshop that was taken place online instead of as a physical event.

The following companies took part:

Customers	Industry	SMEs
Amadeus	Airbus	CMD
Academic Medical Center of the University of Amsterdam	Atos	Cosmian
AVL List	Bitdefender	Decknet
Axens	Bittium	Difenso
Empower	Bosch	ERSTE Software Limited
Ericsson	ENEA	Genode Labs
Ford Otosan	KoçSistem	ICTerra
IOC		IOTIQ
Koçfinans		iSecurity
Orange		Labris Networks
PAL Robotics		MedVision360
Siemens Mobility		Mondata
Signify		PICUS
Yapi Kredi Bank		SecureKey
		Starflow
French Ambassador of Digital Affairs of the Ministry of Europa and Foreign Affairs		ThinkON

ITEA's philosophy in a nutshell

ITEA is industry-driven, deals with the digital transition of all main industries and follows a unique bottom-up approach. In our hectic digital business domain, innovation is at the heart and coming from adventurous brains at a moment when others have not yet thought about it. The process is very different from the more strategically oriented innovations we observe, with the more top-down decision-making in the IC industry or the birth of Airbus, for example, with its necessary huge start-up investment. Both innovation processes, bottom-up and top-down, are necessary and target different results.

In ITEA we cultivate the bottom-up approach. It is not an easy path because you already need to invest in projects when little consensus yet exists on the direction to follow. Thus, we developed a unique methodology to evaluate and coach these kind of projects, starting with going back to the user; what are the pain points you want to solve for which users and customers? Then we challenge the project with the State-of-the-Art (SotA); why can't we solve the pain points with the existing SotA? Then, if you want to

push great ideas in our digital industry, you need access to the market, because the time-to-market windows are very short in our business domains. In ITEA we carefully check the market value chains of today and tomorrow, and how our consortia have access to them and how they can impact them. It is only when these pain points, targeted user and customer, and access to the value chains are clear, that we check the credibility of the proposed technologies to decide which project deserves the ITEA label. There is no success in ITEA without an impact on the market.

We created the international customer workshops to ensure that our R&D programme is closer to the customers. Every year we choose an important thematic for ITEA, and this year the focus was Cyber Security.

Target of the workshop

The target of the workshop is to identify the actual customer needs, in order to create new ITEA projects based on clearly stated customer or end-user requirements. For this we have defined the following steps:

- We invited a dozen of major international customers, several key Cyber Security companies and a dozen of innovative SMEs.
- We set up six interactive customer panel sessions where they express, in their wording, the challenges and pain points they experience clearly stated customer or end-user requirements basis and why they are key for them.
- The technology providers have taken time to get an in-depth understanding of these challenges and the gap in the SotA and they have started to brainstorm to define ideas to solve the different challenges.
- These ideas will be transformed in project proposals for ITEA 3 Call 7 that opens in September in conjunction with the online ITEA PO Days.

Customer sessions and associated challenges

We set up six customer sessions around challenges which concern different customers we have invited:

1 Methodology

It covers three different challenges:

- Maturity model to measure the security level of a company and an assurance approach to certify and audit a product or a service on its security
- Automation of the cybersecurity to overcome the intensity and the complexity of the attacks
- Security by design & commons

2 Procurement value chain

It covers two different challenges:

- Procurement value chain security management per itself
- Security usability to make it easier to use but also to reinforce security protecting from user bad behaviour to overcome the security barriers to access to the data they need

3 Architecture

It covers two different challenges:

- Business is organised in such a way that companies are buying, selling, merging splitting business units continuously, leading to many heterogeneous tools to ensure the security. To reduce this complexity, it requires a kind of heterogeneous legacy security tools management
- Centralised vs distributed data management, in particular in the context of cloud deployment

4 Secure IOT Architecture

It covers two different challenges:

- Secure IOT architecture per se
- How to ensure trust for all stakeholders of a business

5 AI for security and security for AI

It covers three different challenges:

- AI to support complexity of the system and of the attacks in security management
- Secure Autonomous cars special case
- AI specific attacks

6 Sovereignty

It covers four different challenges:

- Strategical autonomy to remain global but to protect his own sovereignty as a country or as a global company
- 5G infrastructure case
- Global companies are confronted to the diversity of the legal basis for each country; it requires a worldwide legal environment management
- Post-quantum cryptology

7 Transversal to sessions

During the different customer sessions three additional, transversal challenges have been discussed very often:

- Security Assurance for a product or a service protecting the IP of the technology providers and building the trust for the customer (AI, Architecture, Sovereignty)
- Collaborative security when a system or a platform is multitenant (AI, Architecture, Procurement value chain)
- Real-time security when the flow of data is real time (Architecture, IoT, Procurement value chain)

Shared challenges by the customers and project responses

1 Building trust

Any business requires trust between the stakeholders to be fluid and efficient. The digital transition strengthens the agility, fluidity and efficiency of the business, but all these advantages can be destroyed if we suffer too much from attacks. The number of attacks and the complexity of these attacks is scaling up at an incredible speed. It requires to react collectively because the attackers have a very fruitful business which allows them to invest massively to attack. We need to develop solutions to protect against the attack and to develop a level of transparency for the users to rebuild the trust in the digital transition. To move toward this target, we have discussed three main topics:

- **Maturity model** to trust a company
  - A security rating market has started in the US; a European option is needed
  - Identification of the risks and selection of the risks you can control are central to security by design
  - A maturity model will be useful for discussion between the CSO and the CEO to base the investment on security on facts rather than just on threats

- **Cyber Security Quality assurance** to trust a product service requires:
  - An agreed **maturity model**
  - Compliance rules per sector to define the meaning of secure
  - Transparency which means some trustworthy elements + audit capabilities + protection of IP and confidential data for the technology providers
  - It must also cover the operation aspect of the system, product

- **Risk awareness**
  - Methods for risk analysis to transform “risk” in a value of money to be able to make adequate investments on cybersecurity.
  - Without this transformation methodology the result is that secured system are less competitive than others
  - Automated tools to identify the risks are needed; the impact on security of small changes of the IT system should be analysed by some automated tools

Related project ideas that have been set up:

- *Trusted Community*
  - **G4 - Zero-Trust Cyber Intelligence** (Cosmian, Academic Medical Center of the University of Amsterdam, Axens, Bittium Wireless, Decknet, ERSTE Software Limited, KoçSistem, PAL Robotics, Starflow, Yapı ve Kredi Bankası)
    Creating a secure & decentralised data sharing network of cyber intelligence data
- *Maturity model*
  - **G9 – SAMARA** (KoçSistem, Axens)
    Cyber Security Maturity Model and Framework
- *Assurance*
  - **G2 - NGAST** (Bosch, Bittium Wireless)
    Software automated security testing
  - **G3 - IOT security** (Orange, Atos, Decknet, ICterra. iSecurity, Labris Networks, MedVision360, PAL Robotics)
    Making industrial tools to enable a cybersecurity assurance for substantial and high levels
  - **G15 - 5G Assurance** (Ericsson, Decknet, Nokia, Orange, PAL Robotics)
    Challenges in 5G assurance
  - **G16 - TWP** (Decknet, Academic Medical Center of the University of Amsterdam)
    Trusted Workflow Process

---

2 Collaborative security

Business is very often reorganised around multitenant platforms (e.g. energy with the sustainable energy deployment which involves an explosion of stakeholders accessing to the platform management, connected cars, procurement value chain). This requires a concept of “Bubble of security & trust”.
We must share information about security attacks in a secure way but even there is a challenge in sharing the data managed by the common platform (e.g. knowing the geographical balance in production / consumption in an energy network is key information for attackers) It will require a methodology to define classification of information to protect.
We need to create communities of trusted defenders to share securely information on attacks and on new versions of the different tools. We need to be able to understand the security maturity level of different partners and to have a framework to cooperate even with different security maturity levels.

Related project ideas that have been set up:

- **G14 – LIDIA** (AVL List, Academic Medical Center of the University of Amsterdam, Empower, PAL Robotics)
  Living Intelligent Dependability Identities for Autonomy
- **G4 - Zero-Trust Cyber Intelligence** (Cosmian, Academic Medical Center of the University of Amsterdam, Axens, Bittium Wireless, Decknet, ERSTE Software Limited, KoçSistem, PAL Robotics, Starflow, Yapı ve Kredi Bankası)
  Creating a secure & decentralised data sharing network of cyber intelligence data
- **G16 - TWP** (Decknet, Academic Medical Center of the University of Amsterdam)
  Trusted Workflow Process

---

3 Digital territories

Any security requires to define a territory to protect. This notion is not yet clear in the cyber space. The boundaries in this space are not aligned with the geographical boundaries and thus with the legal environment. When you are working with a complex procurement value chain, your partners belong to other territories than you but you have to protect the full procurement value chain and very often the attacks are coming from or through one partner in your procurement value chain.

It requires a definition and protection when sometimes borders of the IT system to secure are rather fuzzy. In particular, there is the special case of the procurement value chain.

Related project ideas that have been set up:

- **G17 – ECP** (Atos)
  European eCitizen Platform

---

4 Real-time security

How to ensure security when the process to secure is real time and that its data can be impaired at any moment and generate some great damage to the process? It requires to consider:

- How to check the reactiveness of security management?
- Multi-edge cloud architecture pushes the cloud closer to the end users to ensure better latency, but it generates new challenges for security.

- How to handle latency constraints as security usually introduces overhead?

Related project ideas that have been set up:

- **G1 - DTIDS** (Bosch, PAL Robotics)
  IOT Security
  - Massive attack in particular DDOS
  - Digital Twin-based Intrusion Detection Systems

---

5 Heterogeneous legacy security tools management

CSOs are confronted to numerous security tools to secure their information system. Each one requires sophisticated configurations they do not master. Each one generates multiple alerts in different formats which make the life difficult for the CSO to build a coherent global view of the security of its information system. It must be connected with the flow of versions of the different software they are using which are pushed to correct some bugs used by the attackers The result is a continuous migration phase which puts their system in a weak position. Furthermore, they must cope with scarce expert resources.

Related project ideas that have been set up:

- **G7 - Global View of security indicators/alerts** (Axens)
  Consolidated view of security indicators coming from many sources

---

6 Security automation

- AI is required for automation and autonomous decision
- Challenge to control AI autonomous decisions not to impair the business model and the customer relationship. There is a problem of scale up.

Related project ideas that have been set up:

- **G8 - XAI4CS** (KoçSistem, Atos, iSecurity)
  Explainable Artificial Intelligence (XAI) in Cyber Security
- **G13 - SOCHE** (Erste Software Limited)
  Security Operation Center with High-Performance Homomorphic Encryption
- **G10 - Cyber Security Logging and Monitoring** (KoçFinans, Academic Medical Center of the University of Amsterdam, iSecurity, Mondata)
  Cyber Security Logging and Monitoring Creating a dynamic open architecture to log and monitor systems

---

7 Secure components library

Security is always a question of system but to build a secure system there is a demand of the customer for in-depth security. It means the lower building blocks must be secured by themselves before building a secure system over it.

- With open secure commons even mid-size companies can invest and control some components that are central for their business to build critical systems
- Smallest modular secure OS
- Identify all the assets in a distributed and real-time plant
- And many other components

Related project ideas that have been set up:

- **G5 – CsiD** (Genode Labs, PAL Robotics)
  Cyber Security in Depth

---

8 Security usability

Very often security consist to block access to protect the system. But the business requires more and more agility and cooperation. Furthermore, when the security makes the system less easy to use, the users will find ways to bypass it (e.g. exchange of password, physical access, …) When we know that 60% of the attacks are from insiders, security usability is not just to make the user life easier, which is per se a noble target, but also to ensure the security itself.

- Integrate privacy inside
- Share data sets with good privacy level is needed (e.g. to fight against pandemic)
- Ensure simple but trusted right management

Related project ideas that have been set up:

- **G6 – Security Usability** (Academic Medical Center of the University of Amsterdam, AVL List, Decknet, Medvision360, Orange, PAL Robotics)
  Usability
- **G11 – PROATIA** (ERSTE Software Limited)
  Privacy Preserving Mobility and Thing Management

---

9 Internal security rules violation

Many industries must respect some compliance rules, but their own employees are often lazy to apply them. Thus, it requires a tracking of these rules in all the communication means to fight against the leakage which can have huge impact on the business, the company and the society. There is a bank use case presented by Yapi Kredi Bank.

Related project ideas that have been set up:

- **G10 - Cyber Security Logging and Monitoring** (KoçFinans, Academic Medical Center of the University of Amsterdam, iSecurity, Mondata)
  Cyber Security Logging and Monitoring Creating a dynamic open architecture to log and monitor systems

---

10 Strategic autonomy

We need to learn how to use a foreign technology in a way that we can control the game; for example if we want to use foreign cloud providers we can work to protect access to the hypervisor to provide a good security level (technology of segmentation can help to protect the critical information, in this example of the hypervisor).

Related project ideas that have been set up:

- **G16 - TWP** (Decknet, Academic Medical Center of the University of Amsterdam)
  Trusted Workflow Process

---

11 Worldwide legal environment management

How to set up a framework and a database of worldwide regulations to support the global company to master the worldwide legal environment? It requires a sophisticated browsing to identify the complexity to localise an existing product, in particular for the security side.
Another usage is when your product is attacked in a foreign country; what is the legal context you can use to react and protect your assets?

---

12 Post-quantum computing cryptography

Quantum computing will break the traditional asymmetric cryptographic model. It is shared by different customers that it can arise sooner than forecasted and it is clear that many actors are working on it behind the curtains (states as well as criminals) thus we will not know when the present cryptographic solutions will be broken.
It requires to test and choose some new cryptographic models at the European level not to be dependent on American or Chinese choices. Furthermore, we must propose some transition plan to organise the transition to these new cryptographic algorithms which are quantum safe.

Related project ideas that have been set up:

- **G12 – DEC / Data & Encryption Compliance** (Atos, Cosmian, iSecurity, PAL Robotics)
  Cryptographic governance and administration

Description Cyber Security project ideas resulting from the workshop

This customer workshop has been very successful and generated 17 project ideas based on the set of challenges described above. Some of them will merge to strengthen their potential. We can say that it is the best result we had from all customer workshops organised until now. Here below you can find a description of each project idea:

G1: DTIDS - Digital Twin-based Intrusion Detection Systems

IoT systems are often composed of small-scale or even ultra-small-scale devices with limited computing power. Because of their cost sensitivity, these devices have an extremely tight secure budget. As a result, deploying dedicated security measures on such devices can be prohibitively expensive.
In addition, most real-world IoT (eco)systems are composed of devices from different vendors such that installing security measures on these devices is simply not possible. Finally, specialised countermeasures typically protect against a particular type of attacks. A natural reaction of real-world attackers is to circumvent – rather than actually break – such countermeasures.
Intrusion Detection, on the other hand, can be performed e.g., by monitoring the behaviour of IoT devices based on their network traffic:

- no need to deploy specialised countermeasures
- 3rd party devices can be easily integrated into the security monitoring

Because any reasonable attack will cause an anomalous behavior of one or more IoT devices, the security breach will be detected regardless of what specific vulnerability was exploited

Partners interested: Bosch (Germany), PAL Robotics (Spain), iSecurity (Canada), ENEA (Sweden/France), Mellanox Technologies (Israel)

G2: NGAST - Next Generation Automated Security Testing

- Automated identification of security vulnerabilities in (network-facing) software for IoT devices (i.e. any connected embedded devices).
- Continuous integration & Continuous deployment-style automated security testing solution for identifying security vulnerabilities in software and APIs continuously during product development.
- Security testing could be performed early in the software development process, thereby allowing the developers to fix the vulnerabilities before the software is deployed.
- Use of automated methods with very few to none false positives allow to leverage the computing power nowadays available in cloud-style systems, thereby significantly reducing the cost of vulnerability detection (as opposed to e.g., manual code reviews).
- Ability to find security vulnerabilities both in software (both source code and binaries) as well as distributed systems (e.g., in APIs) using a single, unified approach eliminates the burden of using different expert tools to find different vulnerabilities.

Partners interested: Bosch (Germany), Bittium Wireless (Finland), Metodos y Tecnologia (Spain)

G3: IOT Security - Making industrial tools to enable a cybersecurity assurance for substantial and high levels

- Evaluate IoT security at a level of robustness adequate with the importance of what the IoT does
- Develop a security tool suite to be integrated in the IoT software factory chain
- Anticipate the substantial and high assurance levels of the cybersecurity act
- Design a robust IoT data exchange / data platform security ensuring end-to-end integrity and confidentiality, with adequate resilience capability

Partners interested: Orange (France), Atos (France), Decknet (France), ICterra (Turkey). iSecurity (Canada), Labris Networks (Turkey), MedVision360 (Netherlands), PAL Robotics (Spain)

G4: Zero-Trust Cyber Intelligence - Creating a secure & decentralised data sharing network of cyber intelligence data

We observe a lack of available cyber (threat) intelligence. Europe is dependent on the cyber intelligence of large foreign providers (US, Israel). The objective would be to build a European sovereign source of cyber threat intelligence.

Target is to develop and deploy a trusted secure confidential sharing network for cyber intelligence data sharing between companies and their partners or suppliers (across an industry or across a supply chain for instance), between cybersecurity agencies and the large national companies they are tasked to support, and between national cybersecurity agencies.

Privacy-preserving and confidentiality-preserving data sharing and data processing technologies including:

- encryption (symmetric & asymmetric),
- homomorphic encryption,
- functional encryption,
- secure multi-party computation,
- trusted execution environment,
- cryptographic signatures.

Trust mechanisms for entity and user authentication.

Partners interested: (Cosmian (France), Academic Medical Center of the University of Amsterdam (Netherlands), Axens (France), Bittium Wireless (Finland), Decknet (France), ERSTE Software Limited (Turkey), KoçSistem (Turkey), PAL Robotics (Spain), Starflow (Spain), Yapı ve Kredi Bankası (Turkey)

G5: CSID - Cyber Security in Depth

Actual IT systems suffer from huge attack surfaces. Root cause is their complexity.
Taming complexity via “bulk heads” for the entire software stack:

- Distrusting software by default, rigid sandboxing
- Separation of duty, segregation of sensitive data

It requires a set of low layer building blocks secured and audited to build over it secure critical system ensuring the system dimension of the security.

It targets resilient industrial and medical devices, smart city infrastructure, transportation, automotive, privacy-protecting personal computers and devices.

Partners interested: Genode Labs (Germany), PAL Robotics (Spain)

G6: Security Usability - Creating usable, transparent & auditable security solutions

Security imposes barriers that limit rightful access to the data. There is a balance between usability (the user can access the data to do what is needed) and security (access control). In practice, users work around security boundaries to get the job done, potentially compromising the security of a complex chain of interconnected systems.

The objective is to develop usable security solutions that are flexible to accommodate data access demands without overwhelming the business process. The security solutions should be applied across the trust boundaries of organisations and devices and offer means for auditability, non-repudiation, and traceability.

This will be obtained through 'transparency' of what happens concerning access to the data. By increasing transparency, we aim to increase usability because it is possible to track and verify what happened, when, why, etc. In this manner it is possible to use the data, but at the same time the system is secure because it becomes easier to monitor and trust what is actually happening.

Partners interested: Academic Medical Center of the University of Amsterdam (Netherlands), AVL List (Austria), Decknet (France), Medvision360 (Netherlands), Orange (France), PAL Robotics (Spain)

G7: Consolidated view of security indicators coming from many sources

As it already exists for the operations of IT with some standard (SNMP, MIB...), supervision of an IT system has become progressively standardised and easy to implement even when we were managing old legacy systems and new ones.

For security reporting, it is still a nightmare to interface different security systems in order to build a global dashboard, which could help us to have trends, deviation or alerts. A Siem project is too huge for small or intermediate size company.

The target would be to have standardisation like SNMP + some dashboard platform that could be able to bring a global view, even with many technology layers/providers.
There could be a connected idea which consists of establishing a standard methodology to calculate standard KPIs regarding Cyber Security Postures or Practices. Such framework could be helpful:

- not to be prisoner of solution providers when you must decide to invest. Each provider uses the threat in front of you to make business. KPIs should be a good way to be more pragmatic and more independent when you must decide.
- to benchmark yourself which could be helpful for operations, for investments ...

Partners interested: Axens (France)

G8: XAI4CS - Explainable Artificial Intelligence (XAI) in Cyber Security

Dependency level of the Cyber Security community on the good understanding of domain experts and users about leveraging functionalities of Machine Learning (ML) to combat is increasing as parallel to the employment of black-box models. Thus, the demand from the stakeholders for transparency and explainability is growing, where experts require far more information from the model than a simple binary output for their analysis. Recent approaches in the literature of Explainable Artificial Intelligence (XAI) have focused on three different areas [1]:

- creating and improving explainability methods which help users to better understand the internal workings of ML models and their outputs,
- attacks on interpreters in white box setting,
- defining the exact properties and metrics of the explanations generated by models.

Designing secure, robust and model agnostic XAI methods to cover various security properties and threat models relevant to cyber security domain has been proposed in this project idea.

[1] Kuppa, Aditya & Le-Khac, Nhien-An. (2020). Black Box Attacks on Explainable Artificial Intelligence (XAI) methods in Cyber Security.

Partners interested: KoçSistem (Turkey), Atos (France), iSecurity (Canada)

G9: SAMARA - Cyber Security Maturity Model And Framework

The challenges of this project are:

- What can be predicted in a cyber security domain?
- How usable are the predictions in cyber security?
- How to evaluate predictions in cyber security and what metrics should be used?
- How mature is my cyber security defence model?
- How can we evolve the current model and align with business goals?

The objective is to present cybersecurity maturity model and a general framework aligned with business goals, contemplating the state of the art and futuristic approaches:

- Asset & Control-based approach: Ad Hoc vulnerability assessment, scheduled vulnerability scanning, basic process, basic metrics, regulatory framework
- Analysis & Prioritisation approach: Risk focused, prioritised through analytics, measurable process, emerging metrics and trends
- Proactive approach: Attacker and threat focus, "multiple threats scanned and prioritised at the same time w/ correlation detection", threat driven metrics and process
- Business risk management: Threat and risk aligned with business goals, measurement integrated into enterprise risk management

Partners interested: KoçSistem (Turkey), Amadeus (France), Axens (France)

G10: Cyber Security Logging and Monitoring Creating a dynamic open architecture to log and monitor systems

With exponential growth of data, there are more authorised data accesses than ever which makes it more difficult to determine whether a data access is within the scope of authorised access rights. To solve this problem, log collection and correlation is required through all related systems.
The objective is to develop a mechanism to gather and standardise logs from diverse range of systems and platforms with using a dynamic open architecture while minimising integration costs and efforts.
The targeted technologies are

- Real-time logging agents: Appropriate observability mechanisms (plug-in, API, kernel hooks etc.) to probe the systems at desired points of instrumentation.
- Aggregation system: Real-time mechanism to asynchronously collecting and storing events from agents. Compression, filtering, archiving of data is utilized to save storage size.
- Analysis Engine: Preferably explainable AI, AutoML, and other appropriate rule-based, optimisation etc. models utilised in a hybrid model to evaluate aggregated logs and generate reports for impact analysis, model verification and action actuation.
- Report and Action system: System generates incident lists with estimated risk scores. Alerts and actions are triggered according to type, impact factor and other parameters.

Partners interested: KoçFinans (Turkey), Academic Medical Center of the University of Amsterdam (Netherlands), iSecurity (Canada), Mondata (Canada)

G11: PROATIA - Privacy Preserving Mobility and Thing Management

Asset management is a key need of an organisation for centuries. Physical first evolved to electronic, then it evolved to mobile, and currently scattered IoT devices are new members after mobile devices. Not only being aware, but also being able to remotely control them has a decent market since the beginning of the last decade.

This project would like to combine digital asset management, mobility management, and restricted IoT devices (including their gateways) management into one common platform. While providing such an environment, due to GDPR, it is important to take care of anonymity and privacy. Also, sensitive data, which belongs to both owner and the user of the system, born through the existing system are fragile.

It targets the mobile assets, the digital assets (licences, …) and the IOT assets

Partners interested: ERSTE Software Limited (Turkey), IOTIQ (Germany)

G12: DEC - Data & Encryption Compliance

Development of a central Crypto Governance & Administration (CGA) console able to discover, assess, suggest and maintain, centrally all the cryptographic policies of the enterprise and their lifecycle, facilitating audits, migrations, evolutions, depreciation of obsolete protocols, etc.

1. **Discover**: Based on (network and endpoint) sensors, the central CGA console will discover the cryptography (symmetric & asymmetric) technology used in the organisation.
   Integration with Data Discovery and Classification solutions is required to bring a view on the Data landscape (protected or not) as well.
2. **Assess**: Assess the strength of discovered cryptography protocols versus best practices and future threats. Correlate this info to the characteristics of the protected data through integration with data classification solutions. This provides another angle to assess the risk posed by obsolete cryptography.
3. **Suggest**: Implement a Privileged Data Management approach (PDM is to Data Management the equivalent to what Privileged Access Management is to Identity & Access Management), so customer can better balance "performance impact" (like Homomorphic Encryption) with 'information sensitivity'.
4. **Maintain**: On the longer term, the CGA console will provide a continuous view on the state of crypto on the Information System, and allow, with connectors (international standards like KMIP are already going that way) to interface with encryption tools, systems and SDKs, providing an easy and central way for customer to
   a. report to auditors on used encryption and its strength
   b. migrate any newly obsolete cryptography
   c. decommission insecure certificates,
   d. identify the impact of an Application migration (from an On Prem cryptography to a Public Cloud cryptography for example).

Use case (Post Quantum Cryptography Vs Data time expectancy value)
Related to Post Quantum Cryptography (PQC), we would be able to have a "time expectancy value" aspect of the data to protect.
In this scenario, it would be of critical importance as a data which will still have a value in 15 years and is encrypted today by asymmetric algorithms (or weak symmetric algo) is probably already at risk of being decrypted when a Large Scale Quantum computer will be able to run the Shor algorithm (given the assumption such LSQ will exist by 2035). So, for this type of data a customer might want to take the risk of using one of the "NIST PQC competition" before knowing the selected Post Quantum Cryptographic algorithms (or use a hybrid approach). This costly approach might be worth the cost/effort/latency according to the data "time expectancy value".

Partners interested: Atos (France), Cosmian (France), iSecurity (Canada), PAL Robotics (Spain)

G13: SOCHE - Security Operation Center with High-Performance Homomorphic Encryption

A security operation centre (SOC) is responsible for monitoring and analysing an organisation's data continuously. When the information is sent in plaintext form, the privacy of the data entities cannot be preserved. Besides, SOC's expertise cannot be replicated especially when Machine Learning models trained with large-scale private data in a supervised manner are employed by the SOC. One way to keep the organisation data secure while using SOC is leveraging Homomorphic Encryption and using cutting edge devices such as GPUs and FPGAs. Implementing a SOC that can efficiently and effectively work on encrypted data is the ultimate goal of this project.

Partners interested: ERSTE Software Limited, Turkey, Dakik Software Technologies, Turkey, Sabancı University, Turkey

---

G14: LIDIA - Living Intelligent Dependability Identities for Autonomy

Painpoints to solve: ensuring trust in operation for connected, **collaborative** automated systems:

- Unpredictable quality and behaviour due to high complexity of automated systems, context and perception uncertainties, as well as the black box character and potential evolution capabilities of AI components
- Openness and ad-hoc creation of systems of systems without a clear a-priori defined leader. Emerging configurations can be unknown and potentially infinite.
- Guarantee the dependability of the resulting overall service of the system of system (not obligatory of the single units)

Targeted businesses are all kind of non-closed systems and in particular, connected cars as well as the energy network.
Potential societal impact: e.g., smart mobility, more efficient use of distributed renewable energy, increase balance for open solutions and avoid monopoly solutions, sovereignty through more open solutions. Both collaborative systems (technology level) and collaborative businesses.

Partners interested: AVL List (Austria), Academic Medical Center of the University of Amsterdam (Netherlands), Empower (Finland), PAL Robotics (Spain)

G15: 5G Assurance - Challenges in 5G assurance / Confidentiality-preserving software assurance

Painpoints to solve:
To ensure trustworthiness of critical-infrastructure systems, there are market & legal trends requiring assurance of the software used in said systems. But, software often contains IPR that belongs to vendors & supply chain partners. Sharing source code is questionable due to the risk of losing control over access to the source code. There is a need to develop methodologies & tools that can aid in the evaluation of IPR-protected software while preserving commercial confidentiality.

Targeted customers / users:
Critical infrastructure stakeholder requiring software assurance for the end to end supply-chain. In particular: 5G players: equipment vendors, partner suppliers, mobile operators, standardization bodies developing assurance frameworks: 3GPP, GSMA and independent authorized certification/auditor bodies, Governmental agencies regulating procurement processes demanding Software Bill of Materials (SBOM), Energy sector, autonomous systems, IIoT ….

Partners interested: Ericsson (Sweden), Decknet (France) Orange (France), Nokia (Germany), PAL Robotics (Spain)

G16: TWP - Trusted Workflow Process

Targets:

- No loss of data in case of compromised infrastructure (e.g. ransomware),

- Ease of transaction audit,
- Secure procurement workflow,
- Trusted exchange of data between stakeholders.

Painpoints to solve:

- End-to-end data flow likely to be compromised,
- Loss of control of data-sharing platform,
- Strict monitoring of auditable transactions,
- Ensuring the stability and reliability of the production facility configuration,
- Guaranteeing the right holders the proper use of a licence.

Associated innovation:

- Data-loss prevention software,
- Flexible workgroups administration,
- File transformation audited by blockchain,
- Zero-knowledge platform aggregating different processes in order to make any intercepted data unusable

Partners interested: Decknet (France), Academic Medical Center of the University of Amsterdam (Netherlands)

G17: ECP - European eCitizen Platform

Governments, agencies and private organisations are digitalising their procedures and relying on servers or machines: Mobile apps, web portals, Kioscks, Self-X, Robots....
In order to have a single view on citizens of all ages, governments invest in a Unique citizens register with a super identifier and links it to former registers (ID-Card, Driving license, Social security, passport number…).
Private organisations could rely on those government issued identifiers for managing their digital territories.

The idea is to offer, in particular to European actors (public & private), a global service to manage centrally all their Digital IDs across all applicable digital territories.

Partners interested: Atos (France)

Conclusions

Once again, this international customer workshop reconciliated the customers concerns and the interest of technology providers (large industry as well as innovative SMEs). It occurred in a very open manner, thanks again to all participants. It has been very fruitful with many challenges shared and 17 ideas of project to build.

You are invited to use this valuable input and to create or join a customer-oriented idea for a project proposal in ITEA 3 Call 7 (https://itea3.org/onlinepodays2020/getting-started-6.html). Remember that the ITEA game is very open but based on added value of each partners, thus clarify in advance what you offer to the project and to the other partners to join a project.

We look forward to discovering your unique solutions!