View this email in your browser

Integrated cyber-physical security for health services

SAFECARE NEWSLETTER October 2020

Message from SAFECARE Coordinator, Philippe Tourron

This period has been defined by SAFECARE partners adapting to new working conditions, as work ad meetings and continue at a distance. We have agreed an amendment allowing us to postpone the entire project by three months with the European Commission; and this has supported the necessary adaptations.

All the project partners have continued their progress in design and development, which has made it possible to carry out a concrete demonstration meeting in July that was much appreciated by all participants.

Following this meeting, the very positive feedback from our Board Members allowed us to confirm and improve our work as needed. In particular, we carried out an important reflection on the ethical aspects of the project, with the development of a methodology to identify the fundamental questions of ethics in relation the development and future use of SAFECARE, allowing us to propose solutions and guidelines.

This period has also been defined by the formalization of the knowledge of end users of the health perimeter in order to build the impact cascade model. This phase is essential to provide decision support to risk managers and to all hospital operational players. A methodology has now been validated which will allow the quick completion of the modeling necessary for the following phases of simulation and demonstration in 2021.

Finally, as the second year of the project is ending, we will present our progress

to the European Commission on November 27th. This technical review is very important to enhance our efforts and make everyone's investment a reality. I am counting on you to bring your dynamism and to share our motivation for success.

SAFECARE Research Online

The results of SAFECARE partners research has been made available online for sharing and study by pracitioners in the field. It is available on the website, and includes the first set of deliverables accepted by the European Commission, related to the requirements of healthcare infrastructure security and preliminary designs of the SAFECARE system, as well as scientific papers and articles submitted on the basis of the SAFECARE research.
The research can be found here:

Deliverables and Publications
Healthcare infrastructure threat assessment and solution requirements
Physical security solutions for Healthcare infrastructure
Cybersecurity solutions for Healthcare infrastructure
Integrated Cyber-Physical security solutions for Healthcare infrastructure

Updates

"Cyber-Physical Threat Intelligence for Critical Infrastructures Security" Book Published - SAFECARE partners wrote four chapters for the open access book, produced by the European Cluster for Securing Critical Infrastructure, which SAFECARE is a founding member of.
Security Incidents in Healthcare Infrastructure during COVID-19 Crisis - SAFECARE Partners are tracking the rise in security incidents affecting healthcare infrastructure during the crisis.
SAFECARE Partners Contribution to CPS4CIP20 Workshop - The 1st International Workshop on Cyber-Physical Security for Critical Infrastructures Protection was held at ESORICS 2020, with many SAFECARE partners involved.
SAFECARE presented at ECSCI Workshop on 24/25 June - The SAFECARE project was presented at the ECSCI Workshop in June, with presentations from Isabel Praca, Elisabetta Biasin and Fabrizio Bertone.

SAFECARE Presented at ESORICS 2020

Project Progress Report

During the second year of the project, SAFECARE partners met twice through two management meetings (November 2019 and 26th May 2020) to inform all members of the consortium of the progress of the project and to decide on strategic orientations.

With the crisis situation due to Covid-19, we requested and obtained an amendment to postpone for 3 months all the tasks, deliverables and events thus bringing the end of the project to November 2021. Indeed the end-users of the domain of health were strongly impacted by crisis management and the other players had to deal with a reorganization of their activity.

A board member meeting was on held on 3rd July 2020 in order to present as a mid-term period meeting, a checkpoint meeting. The meeting was focused on the demonstration of each module already developed of the final Safecare solution. On this occasion, the Project Officer as well as representatives of DG CONNECT were present. Very constructive feedback was collected to allow the improvement of the solutions proposed by SAFECARE project.

This second year will be ending by the occurrence of the technical review programmed on the 27th November 2020, preceded by the submission of the progress report for Y2 (D2.2) at the end of October to the PO. This report have been implemented by all the WP Leaders and id currently being consolidated and reviewed by the coordinating team.

SAFECARE Ethics Review

After the Ethics Report for Year 1, a presentation of the project was made to the Ethics Board to start identifying questions on the future ethical use of SAFECARE. We were thus able to initiate a first reflection with a member of the board, Simon Rogerson, to identify the questions to ask and set up a pragmatic way to collect the ethical dilemmas that may arise during the future use of SAFECARE. We were thus able to build a first inventory of the scenarios for identifying and describing these ethical dilemmas with KUL. We then chose a scenario that mixed several teaching methods by building a role play to put into practice the identified stakeholders (suppliers of software mods, maintainers, hospital practitioners, patients, risk manager, guards, ...).

We have started to identify all the stakeholders and their links that we will put into situation with two use cases of SAFECARE: good use, error of use and malicious use. We will study the reactions of stakeholders with regard to the four ethical principles: autonomy, beneficience, non-maleficience and justice. A workshop was organized during M25 upon the principle of a role play involving all the work packages leaders as well as the APHM team participants and user representatives.

An Ethics Survey was also submitted to each WP leader in order to identify the indicators of data processing operations that may entail higher ethics risks and to evaluate the incidence of those criteria in every WP. The methodology used to elaborate this survey is: « Horizon 2020 Projects: Ethics Compliance under GDPR » de Albena Kuyumdzhieva, PhD, Programme Manager Ethics/Research Review, European Commission.

Finally, all those actions (board member interviews, research of an adapted methodology, organization of role play workshop and elaboration of an ethics survey) will come to enrich the Ethics report of Y2, which will be submitted by the end of October.

Risk Assessment of Threat Scenarios

The risk assessment of the scenarios of threat is being detailed through a methodology that combines both EBIOS - Expression of Needs and Identification of Security Objectives and BowTie methodology. The work started by the analysis of scenarios “Cyber-physical attack to steal patient data in the hospital” and “Cyber-physical attack targeting the air-cooling system of the hospital”. The detailed risk analysis is carried on in straight collaboration with WP6, in particular with the impact propagation and decision support model.

Physical Security Systems

Development of the different Physical Security Systems has been progressing well, with a machine learning and a data analytics solution of detecting tailgating, crowding, loitering, weapons, fires, faces and masked faces in video being finalised, HVAC, fire, flood, grass break, light and sound sensors being integrated and the mobile application taking its form.

Integrations between the different systems has been well defined and is work is well under way to be finished. From the floor plan of one of the hospital sites, a knowledge graph of the internal relations has been built, which sensor information, assets and alerts can be connected to, to create a visualisation for both the BTMS and the mobile application.

Cyber Security Systems

The cyber security solutions aim to cover cyber-security aspects related to e-Health, IT and BMS systems in health services by providing increased prevention and detection capabilities and improved monitoring tools while communicating with a central database in order to propose a comprehensive view of the system covering both physical and cybersecurity threats.

Over the last months, the development and integration of cyber security solutions has been progressing. The IT threat detection system is being integrated on the simulation platform and the various components, such as the intrusion prevention system (IPS), security information and event management module (SIEM) or machine learning (ML) environment, are being connected to one another. A dataset consisting of log messages featuring phishing, malware execution and file deletion has been labelled and is being used by supervised machine algorithms for training along with public datasets.

The latest version of the building management system (BMS) threat detection system has been deployed on the simulation platform and is currently being connected to the cyber threat detection system (CTMS), for alerts transmission, and the advanced file analysis system (AFAS), for analysis of extracted files. The report associated to the BMS threat detection system prototype is in the process of being written.

The advanced file analysis system (AFAS) has also been deployed on the simulation platform and successfully tested with malicious PEDICOM files, which are DICOM files (i.e. medical images) with an executable payload that can be used as malware by an attacker to infect the hospital’s system. The AFAS also is in progress of being connected to the other components of the cyber security solutions. The report associated to the AFAS prototype is in the process of being written.

Regarding the e-health devices security analytics (EDSA), the first tests of alerts transmission between the alert generation module and the CTMS have been successful. The ongoing focus is on on-device security analytics extensions and security model creation to support SAFECARE specific use cases, workflows, and integration with other SAFECARE components, e.g. the CTMS, and medical devices, i.e. interventional x-ray radiology equipment. The report associated to the EDSA prototype is in the process of being written.

The cyber threat monitoring system's (CTMS) latest version has been deployed on the simulation platform and will be connected to the other cyber security solutions components as well as to a vulnerability intelligence platform (which has also been deployed), a malware information sharing platform (MISP) and a powerful tool for visualizing impacts of incidents on the hospital's system and their potential cascading effects (identified and acquired, to be deployed). Further communication tests with the central database (T6.3) – asset information requests through its REST API – and the data exchange layer (T6.2) – cyber incidents publication through MQTT – have been successfully conducted. Sample cyber security incidents formatted according to the agreed-upon structure have been shared with WP6 partners to enable separate testing.

Integrated Cyber-Physical Solution

The SAFECARE research activities for the integration of the cyber and physical systems are making progress towards milestone 11 of SAFECARE project, that corresponds to the deployment of the data exchange layer and central database. The data exchange layer is deployed and we are working on the containerization of this module to have it ready for the deployment on the test platform and we are close to deliver the prototype of the central database. This step will allow prototypes deployed in the test platform to exchange messages with each other.

The other tasks are all making important progress. Propagation rules, at the basis of the evaluation of potential impact and cascading effects when incidents occur, have been refined and tested with 2 threat scenarios. We had a demo of the alerting engine during the WP6 conf call that involved end users of SAFECARE and demonstrated the progress made to integrate it inside the SAFECARE architecture.

After several refinements, we presented the HAMS demo at the mid-term remote progress meeting and now the prototype is ready to be integrated with the rest of the platform.

Finally, the SAFECARE Project Coordinator is leading a set of calls with

partners to integrate the EBIOS methodology, used to analyse scenarios of threat with the BowTie method, leveraged to specify the E-health risk management model.

Despite the Covid emergency, our dissemination activities are ongoing and researchers from LINKS presented the SAFECARE approach to the development of an integrated cyber-physical security solution for critical infrastructures to the 1st ECSCI Workshop on Critical Infrastructure Protection and to the 1st International Workshop on Cyber-Physical Security for Critical Infrastructures Protection.

A video of the last presentation is available at: https://www.youtube.com/watch?v=OOWTWP9JHH4

Testing the SAFECARE Solution

SAFECARE will carry out operational demonstrations to test the global solution under live conditions, through three demonstrations in hospitals (Turin, Marseille and Amsterdam) and one large scale pilot (Marseille). In recent months, SAFECARE partners have started working on these demonstrations. The first steps have been to prepare to test the full prototype on a test platform, to train security practitioners and health practitioners to use the prototypes, to deploy the test bed in an operational environment, to demonstrate the full prototype in an operational environment and, finally, to evaluate the security impact of the prototype on risk assessment.

Several partners have been working hard in the last three months, in order to have the test platform ready; SAFECARE will now be able to validate an operational prototype, to test inter-connections, to improve and adapt all prototypes to achieve a marketable solution. We shall adopt a virtual environment for target information system simulation, and through this, test scenarios and prototypes, to obtain maximum results from our work.

Communications and Dissemination

SAFECARE partners have participated in several events recently, including as part of ECSCI at an online workshop with the European Commission and through the ESORICS 2020 event.

The "*Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*" book, a collaborative effort between ECSCI partners to which SAFECARE contributed four chapters was published in September. This was

an important piece of work, and thanks to the efforts of the SAFECARE partners, SAFECARE was able to contribute in a positive way.

A draft business plan for the SAFECARE solution has also been produced by Enovacom, detailing some of the marketable innovations of the project and plotting a route to market for the final product.

Upcoming Events

With respect to the COVID-19 Crisis, SAFECARE has postponed the Awareness Event in Athens, originally scheduled for the end of May, until January, when it is expected to take place as a virtual meeting.