Cyber Security PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Cyber Security Threats and Threat Actors Training - Assurance Driven Multi- Layer, end-to-end Simulation and Training

D8.5: The THREAT-ARREST dissemination and exploitation report v1[†]

Abstract: This deliverable provides the 1st version of the dissemination and exploitation report for the THREAT-ARREST project.

Contractual Date of Delivery	29/02/2020
Actual Date of Delivery	29/02/2020
Deliverable Security Class	Public
Editor	*Spanoudaki Sofia, Koloutsou Konstantina (STS), Marinos Tsantekidis (TUBS)*
Contributors	All partners
Quality Assurance	*George Hatzivasilis (FORTH), Fulvio Frati (UMIL)*

[†] *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786890.*

The *THREAT-ARREST* Consortium

Foundation for Research and Technology – Hellas (FORTH)	Greece
SIMPLAN AG (SIMPLAN)	Germany
Sphynx Technology Solutions (STS)	Switzerland
Universita Degli Studi di Milano (UMIL)	Italy
ATOS Spain S.A. (ATOS)	Spain
IBM Israel – Science and Technology LTD (IBM)	Israel
Social Engineering Academy GMBH (SEA)	Germany
Information Technology for Market Leadership (ITML)	Greece
Bird & Bird LLP (B&B)	United Kingdom
Technische Universitaet Braunschweig (TUBS)	Germany
CZ.NIC, ZSPO (CZNIC)	Czech Republic
DANAOS Shipping Company LTD (DANAOS)	Cyprus
TUV HELLAS TUV NORD (TUV)	Greece
LIGHTSOURCE LAB LTD (LSE)	Ireland
Agenzia Regionale Strategica per la Salute ed il Sociale (ARESS)	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. *George Hatzivasilis (FORTH)*
2. *Fulvio Frati (UMIL)*

Revisions

Version	Date	By	Overview
1.2	27/02/2020	STS , Marinos Tsantekidis (TUBS)	Addressed UMIL's comments
1.1	26/02/2020	STS, Marinos Tsantekidis (TUBS)	Deliverable ready for internal review
1.0	18/02/2020	STS	Updated Exploitation sections
0.9	14/02/2020	STS	Updated Exploitation sections
0.8	12/02/2020	ITML (George Bravos), DANAOS (Fotis Oikonomou)	ITML & DANAOS input
0.7	31/01/2020	AReSS (Antonio Chieti)	AReSS input to Section 3
0.6	30/01/2020	TUV (George Leftheriotis)	TUV input to Section 3
0.5	29/01/2020	STS	STS input to Section 3
0.4	28/01/2020	SEA (Sebastian Pape)	SEA Input to Section 2 and 3
0.3	20/01/2020	TUBS (Marinos Tsantekidis)	TUBS input to Sections 1 and 2
0.2	24/09/2019	TUBS (Marinos Tsantekidis)	TUBS contribution to ToC
0.1	24/09/2019	STS	First Draft

Executive Summary

Deliverable “D8.5 – The THREAT-ARREST dissemination and exploitation report v.1”, is a joint output of the tasks “T8.2 – Sustainability management and Business continuity” and “T8.3 – Dissemination plan and activities”. As such, the main objective of the current document is to deliver the initial dissemination and exploitation plan of the THREAT-ARREST project.

This first version of the deliverable will provide an initial analysis of the exploitation and dissemination activities of the project in terms of competitiveness and exploitation of the project results for individual project participants and the consortium as a whole. Along with the deliverable “D8.4 – The stakeholders’ engagement & online channels report v.1”, which is also due at M18, they determine the means to accomplish the milestone “MS3 – Business models, dissemination and exploitation reports”, which forms the 1st version of Business Model and market analysis report, due at M18.

The final version of this report will be in the deliverable “D8.8 – The THREAT-ARREST dissemination and exploitation report v.2”, due at M36.

Table of Contents

List of Abbreviations

AHPS Atos High Performance Security

BDS Big Data & Cybersecurity

ARI Atos Research & Innovation

CTTP Cyber Threat and Training Preparation

DFP Data Fabrication Platform

GKO Global Key Offering

GRC Governance, Risk and Compliance

IH Innovation Hub

IoT Internet of Things

JVT Jasima Visualization Tool

SIEM Security Information and Event Management

List of Figures

1 Introduction

The objective of this report is to summarize the dissemination and exploitation activities carried out by the THREAT-ARREST consortium during the first half of the project.

The THREAT-ARREST project aims to disseminate its results and findings intensively to various communities. *Research publications and event presentations* that target various groups of academic and industrial researchers, add scientific weight and credibility to our findings. *Press releases and news articles* are used to publish project results to both technical and general audience, as well as public seminars and general articles in both the technical and non-technical press. The project's *website and social media* is used to provide open access to project results, public deliverables, software tools, technical reports, white papers, etc., and serves as a key resource for those wishing to use the project results, whether they are academic researchers, scientific personnel, commercial or independent software developers or private individuals.

Another important goal of the project is to maximize the exploitation of its outcomes and the successful implementation of its findings. Each of the consortium partners has devised an exploitation plan and in this deliverable, they report the progress made based on this plan.

The deliverable is organised as follows: Section 2 deals with the dissemination activities of all partners: Section 2.1 lists the objectives of the project for completeness. Section 2.2 details the papers already published in peer-reviewed conferences and journals. Section 2.3 lists several talks, seminars, and presentations (with accompanying photos) carried out by the project partners. In Section 2.4, the academic partners detail in which way they incorporated the project into their programs. In Section 2.5, there is a list of additional dissemination activities. Section 2.6 deals with the project's website and its progress so far. In Section 2.7, the partners list their plans for future dissemination. Finally, in Section 2.8, there is a comparison of the archived efforts against the initially set goals.

Following, Section 3 is about the exploitation activities. Section 3.1 mentions the overall aim of the exploitation strategy, for completeness. Section 3.2 offers some background on the exploitation activities and in Section 3.3, the consortium partners list their individual strategies, ending with Section 3.4, where a joint exploitation plan is devised.

Closing the deliverable, we offer our conclusions in Section 4.

2 Dissemination

In the following pages, we list the publications presented by the consortium in conferences as well as the presentations made at various events and forums, related to the project. Additional coverage of the project through other dissemination channels is also presented in this document, including releases in the popular press and references to the project. During the first half of THREAT-ARREST, the consortium published a total of ***17 peer-reviewed papers***, plus ***13 presentations, talks, and seminars***.

2.1 Dissemination Objectives

Four categories of dissemination channels, have been established, each accompanied by its own content strategy paper. This combined approach ensures efficient dissemination of the technical activities of THREAT-ARREST based on the target audience's needs and involvement.

2.1.1 Online dissemination

The online channel is aimed at primary and secondary targets with diverse information needs and involvement.

Project's website: The site (www.threat-arrest.eu) is a key instrument for supporting the dissemination of the research results. We regard the website as a "second stop" useful to primary targets who have already been reached via the other channels. Its aim is to provide sound support for those wishing to become champions of the THREAT-ARREST approach within their organizations, providing access to deliverables and presentation materials that support championing THREAT-ARREST adoption. Key results are published on the website, but also added-value services will be offered such as support in using THREAT-ARREST methodology. The project website was set up at a very early stage (M01) and is updated conscientiously and regularly.

Push announcements: The project is present on the major professional social networks, in particular Facebook (www.facebook.com/Threat-Arrest-266454357324031/), LinkedIn (www.linkedin.com/in/threat-arrest-706485175/), and Twitter (twitter.com/ArrestThreat). Contacts already available to project partners were used to kick-start this group, which is a major instrument for recruiting interested parties. THREAT-ARREST social community group is the target for continuous informal communication with members, who can find brief first-hand reports from THREAT-ARREST research and development activities, increasing the timeliness of dissemination.

Regular Newsletter: Starting from M4, a regular quarterly newsletter is being sent out to interested parties outside the project partners including major stakeholders recruited via the other channels. The newsletter relies on a well-balanced mix of dissemination and infotainment content. All partner organisations contribute to the newsletter, which is made available free of charge through electronic means.

Brochure: A THREAT-ARREST folder and brochure was created in M3, distributed in all venues where project partners were involved in, and updated regularly. Distribution also includes a high–quality electronic version in portable document formats (e.g. PDF), which is downloadable from the website.

Technical video: A professional THREAT-ARREST technical video (www.youtube.com/watch?v=Nr6wejCKKsIS) of estimated 5 minutes of duration was developed in M04. It has been uploaded in YouTube and is also accessible via the project's website. The video focuses on the technical advancements of the THREAT-ARREST methodology and approach, targeting the technical and business community of the Internet of Things (IoT).

2.1.2 Scientific publications

THREAT-ARREST partners have been carefully selecting publication venues based on their scientific excellence and impact, privileging where possible open access publishing. Conferences and journals that are targeted for scientific dissemination include:

Journals: International Journal of Internet of Things; Advances in Internet of things (Scientific Research open access); ACM Transactions on Software Engineering and Methodology; ACM Transactions on Information and Systems Security; IEEE Transactions on Secure and Dependable Computing, IEEE Transactions on Information Forensics and Security; Computers and Security; IEEE/ACM Transactions on Networking; Springer International Journal of Information Security; Springer Wireless Personal Communications; Elsevier Network Security;

Magazines: IEEE Security and Privacy; IEEE Cloud Computing; and IEEE Internet Computing.

Conferences: ACM Conference on Computer and Communications Security; ESORICS – European Symposium on Research in Computer Security; ACM/IEEE International Conference on Cyber-Physical Systems; IEEE International Conference on Pervasive Computing and Communications; IFIP International Information Security and Privacy Conference; IEEE Symposium on Security and Privacy; ACM Conference on Computer and Communications Security; ACM Conference on Data and Application Security and Privacy; IEEE International Conference on Internet of Things; and European Conference on Smart Objects, Systems and Technologies.

Special Issues in Scientific Journals: The partners will take the initiative of jointly creating special issues in the area of IoT in scientific journals, and invite top international colleagues to be part of the initiatives.

2.1.3 Organization of International Scientific Events

In order to attract interest to our work and enhance the visibility of our contributions at an international level we have already started organizing several international scientific events and will continue to do so.

Organization of conferences: THREAT-ARREST will organize one significant international conference in the core research areas of the project.

Organization of workshops: THREAT-ARREST will organize two international scientific workshops throughout its duration, co-located with one of the top-tier conferences identified above.

Organization of Summer Schools on Cyber Security Training and Simulation: THREAT-ARREST will organise two summer schools. These will be aimed at delivering knowledge to researchers, and professionals on cyber security training and simulation platforms. Our plan is to organize these summer schools in M18 and M36 and to attract at least 30 attendees in each. To be cost effective, these will be organized in the premises of academic partners.

2.1.4 System-level demonstrations

THREAT-ARREST partners will demonstrate the project's platform capabilities to several related venues.

Demonstrations in fairs and exhibitions: THREAT-ARREST will seek to organize at least one demonstration of the project technical results in major international fairs and exhibitions, such as IFSEC International.

Demonstrations in EU related events: THREAT-ARREST will seek to organize and at least two demonstrations of the project technical results in EU related events, such as Net-Futures.

Demonstrations in major international conferences: THREAT-ARREST will seek to organize and at least two demonstrations of the project technical results in major international conferences, such as IEEE ICC and IEEE GLOBECOM.

2.2 Published conference and journal papers

The THREAT-ARREST Consortium aims to disseminate the work carried out to many venues through a number of academic papers. In the first half of the project, we had ***17 publications*** on a variety of subjects. They are listed below, along with their abstracts.

1) J. Najar and V. Prevelakis, **"A Secure and Efficient File System Access Control Mechanism (FlexFS)"** in the International workshop on Information & Operational Technology (IT & OT) security systems IOSec, September 2018

   Abstract: The FlexFS approach provides an effective credential-based access control mechanism while ensuring file access performance equivalent to that of the normal file system. This is achieved by decoupling the file system naming and access control layer from the block I/O layer. By intercepting and redefining file system API calls in libc (e.g. open(2)), we allow any existing executable to use FlexFS while keeping FlexFS as a user-level system without any changes to the kernel. This allows for rapid experimentation without impacting system stability.

2) M. Hamad, M. R. Agha, and V. Prevelakis, **"ProSEV: Proxy-Based Secure and Efficient Vehicular Communication"** in 2018 IEEE Vehicular Networking Conference (VNC), December 2018

   Abstract: Vehicular Ad hoc Network (VANET) is a very promising approach that aims to improve vehicle and road safety, traffic efficiency, as well as comfortability to both drivers and passengers. Different types of applications were implemented to achieve these goals. Some of these applications require the exchanging of multiple and ordered messages as well as the existence of a stable Internet connection. However, the high node mobility of VANET seems to be one of the main stumbling blocks for adopting such applications. In this paper, we have investigated through a real experiment, how the VANET mobility imposes challenges in establishing and maintaining a long-lasting connection. In addition, we have proposed a mechanism to improve the communication efficiency over VANETs. Our solution is based on the concept of intelligent proxies that can be sent from, say, one Roadside Unit to a vehicle so that the negotiation between them can be delegated to the proxy and take place locally. Using the proxy will reduce the number of exchanged network messages among vehicles and infrastructure, overcome the intermittent and short-lived connectivity challenge of the high mobility vehicular network and, consequently, increase the communication efficacy. Also, we have presented a framework that allows such proxies to operate safely and securely.

3) F. Marcantoni, M. Diamantaris, S. Ioannidis, J. Polakis, **"A Large-scale Study on the Risks of the HTML5 WebAPI for Mobile Sensor-based Attacks"** in The World Wide Web (WWW'18) Conference, May 2019

   Abstract: Smartphone sensors can be leveraged by malicious apps for a plethora of different attacks, which can also be deployed by malicious websites through the HTML5 WebAPI. In this paper we provide a comprehensive evaluation of the multifaceted threat that mobile web browsing poses to users, by conducting a large-scale study of mobile-specific HTML5 WebAPI calls used in the wild. We build a novel testing infrastructure consisting of actual smartphones on top of a dynamic Android app analysis framework, allowing us to conduct an end-to-end exploration. Our study reveals the extent to which websites are actively leveraging the WebAPI for collecting sensor data, with 2.89% of websites accessing at least one mobile sensor. To provide a comprehensive assessment of the potential risks of this emerging practice, we create a taxonomy of sensor-based attacks from prior studies, and present an in-depth analysis by framing our collected data within that taxonomy. We find that 1.63% of websites could carry out at least one of those attacks. Our findings emphasize the need for a standardized policy across browsers and the ability for users to control what sensor data each website can access.

4) G. Hatzivasilis, O. Soultatos, P. Chatziadam, K. Fysarakis, I. Askoxylakis, S. Ioannidis, G. Alexandris, V. Katos, G. Spanoudakis, **"WARDOG: Awareness detection**

watchdog for Botnet infection on the host device" in IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, May 2019

Abstract: Botnets constitute nowadays one of the most dangerous security threats worldwide. High volumes of infected machines are controlled by a malicious entity and perform coordinated cyber-attacks. The problem will become even worse in the era of the Internet of Things (IoT) as the number of insecure devices is going to be exponentially increased. This paper presents WARDOG – an awareness and digital forensic system that informs the end-user of the botnet's infection, exposes the botnet infrastructure, and captures verifiable data that can be utilized in a court of law. The responsible authority gathers all information and automatically generates a unitary documentation for the case. The document contains undisputed forensic information, tracking all involved parties and their role in the attack. The deployed security mechanisms and the overall administration setting ensures non-repudiation of performed actions and enforces accountability. The provided properties are verified through theoretic analysis. In simulated environment, the effectiveness of the proposed solution, in mitigating the botnet operations, is also tested against real attack strategies that have been captured by the FORTHcert honeypots, overcoming state-of-the-art solutions. Moreover, a preliminary version is implemented in real computers and IoT devices, highlighting the low computational/communicational overheads of WARDOG in the field.

5) G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. I. Tsatsoulis, **"Review of Security and Privacy for the Internet of Medical Things (IoMT)"** in 1st International Workshop on Smart Circular Economy (SmaCE), May 2019

Abstract: Day-by-day modern circular economy (CE) models gain ground and penetrate the traditional business sectors. The Internet of Medical Things (IoMT) is the main enabler for this interplay of CE with healthcare. Novel services, like remote sensing, assisting of elder people, and e-visit, enhance the people's health and convenience, while reducing the per-patient cost for the medical institutions. However, the rise of mobile, wearable, and telemedicine solutions means that security can no longer be examined within the neat, physical walls as it was considered before. The problem for a healthcare system further increases as the Bring Your Own Device (BYOD) reality, affects the way that the health services are accommodated nowadays. Both patients and healthcare staff utilize their personal devices (e.g. smart phones or tablets) in order to access, deliver, and process medical data. As the IoMT is materialized and the underlying devices maintain so valuable data, they become a popular target for ransomware and other attacks. In the CE case, the problem is further emerging as several of these assets can be used over-and-over by many actuators. However, medical users and vendors are less aware of the underlying vulnerabilities and spend less on the IoMT security. Nevertheless, the risk from exploiting vulnerabilities can be drastically reduced when the known and relevant controls are placed. This paper presents an overview of the core security and privacy controls that must be deployed in modern IoMT settings in order to safeguard the involved users and stakeholders. The overall approach can be considered as a best-practices guide towards the safe implementation of IoMT systems, featuring CE.

6) G. Hatzivasilis, N. Christodoulakis, C. Tzagkarakis, S. Ioannidis, K. Fysarakis, G. Demetriou, M. Panayiotou, **"The CE-IoT Framework for Green ICT Organizations"** in 1st International Workshop on Smart Circular Economy (SmaCE), May 2019

Abstract: The growth of the global middle class provokes significant increment in product consumption. As the available resources are limited, Circular Economy (CE) raises as a promising initiative towards the sustainable development. Except from the traditional approaches of reusing or recycling products, the current trend utilizes modern computer technologies and involves a data-driven aspect. The Internet of Things (IoT) is the main enabler for the integration of CE with technology. This paper proposes a framework for implementing the cooperative vision of CE and IoT. Via this solution, a pilot system is developed in a medium size telecommunication company for administrating the lifecycle of the deployed electronic equipment and the management of the related supply chains. Mechanisms and devices are maintained/repaired/fabricated in a regular basis, green computing techniques are efficiently applied, and the productive period is prolonged. When the business upgrades the system, the retired counterparts can be sold in start-ups or gifted in third-world countries. The overall approach extends the working period of the well-maintained electronic assets not only for the examined business but for the collaborating organizations as well. Recycling companies can then trace this supply chain and the assets' status in order

to define their investment strategy at the end-consumer, contributing in the reduction of the electronic waste problem in the third-world.

7) G. Hatzivasilis, O. Soultatos, S. Ioannidis, G. Spanoudakis, V. Katos, G. Demetriou, **"MobileTrust: Secure Knowledge Integration in VANETs"**, in ACM Transactions on Cyber-Physical Systems – Special Issue on User-Centric Security and Safety for Cyber-Physical Systems, September 2019

Abstract: Vehicular Ad hoc NETworks (VANET) are becoming popular due to the emergence of the Internet of Things and ambient intelligence applications. In such networks, secure resource sharing functionality is accomplished by incorporating trust schemes. Current solutions adopt peer-to-peer technologies that can cover the large operational area. However, these systems fail to capture some inherent properties of VANETs, such as fast and ephemeral interaction, making robust trust evaluation of crowdsourcing challenging. In this article, we propose MobileTrust – a hybrid trust-based system for secure resource sharing in VANETs. The proposal is a breakthrough in centralized trust computing that utilizes cloud and upcoming 5G technologies in order to provide robust trust establishment with global scalability. The ad hoc communication is energy-efficient and protects the system against threats that are not countered by the current settings. To evaluate its performance and effectiveness, MobileTrust is modelled in the SUMO simulator and tested on the traffic features of the small-size German city of Eichstatt. Similar schemes are implemented in the same platform in order to provide a fair comparison. Moreover, MobileTrust is deployed on a typical embedded system platform and applied on a real smart car installation for monitoring traffic and road-state parameters of an urban application. The proposed system is developed under the EU-founded THREAT-ARREST project, to provide security, privacy, and trust in an intelligent and energy-aware transportation scenario, bringing closer the vision of sustainable circular economy.

8) G. Hatzivasilis, P. Chatziadam, N. E. Petroulakis, M. Mangini, C. Kloukinas, A. Yautsiukhin, M. Antoniou, D. G. Katehakis, M. Panayiotou, **"Cyber Insurance of Information Systems"** at the 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), September 2019

Abstract: Nowadays, more-and-more aspects of our daily activities are digitalized. Data and assets in the cyber-space, both for individuals and organizations, must be safeguarded. Thus, the insurance sector must face the challenge of digital transformation in the 5G era with the right set of tools. In this paper, we present CyberSure - an insurance framework for information systems. CyberSure investigates the interplay between certification, risk management, and insurance of cyber processes. It promotes continuous monitoring as the new building block for cyber insurance in order to overcome the current obstacles of identifying in real-time contractual violations by the insured party and receiving early warning notifications prior the violation. Lightweight monitoring modules capture the status of the operating components and send data to the CyberSure backend system which performs the core decision making. Therefore, an insured system is certified dynamically, with the risk and insurance perspectives being evaluated at runtime as the system operation evolves. As new data become available, the risk management and the insurance policies are adjusted and fine-tuned. When an incident occurs, the insurance company possesses adequate information to assess the situation fast, estimate accurately the level of a potential loss, and decrease the required period for compensating the insured customer. The framework is applied in the ICT and healthcare domains, assessing the system of medium-size organizations. GDPR implications are also considered with the overall setting being effective and scalable.

9) G. Hatzivasilis, P. Chatziadam, A. Miaoudakis, E. Lakka, A. Alessio, M. Smyrlis, G. Spanoudakis, A. Yautsiukhin, M. Antoniou, N. Stathiakis, **"Towards the Insurance of Healthcare Systems"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Abstract: Insurance of digital assets is becoming an important aspect nowadays, in order to reduce the investment risks in modern businesses. GDPR and other legal initiatives makes this necessity even more demanding as an organization is now accountable for the usage of its client data. In this paper, we present a cyber insurance framework, called CyberSure. The main contribution is the runtime integration of certification, risk management, and cyber insurance of cyber systems. Thus, the framework determines the current level of compliance with the acquired policies and provide early notifications for potential

violations of them. CyberSure develops CUMULUS certification models for this purpose and, based on automated (or semi-automated) certification carried out using them, it develops ways of dynamically adjusting risk estimates, insurance policies and premiums. In particular, it considers the case of dynamic certification, based on continuous monitoring, dynamic testing and hybrid combinations of them, to adapt cyber insurance policies as the conditions of cyber system operation evolve and new data become available for adjusting to the associated risk. The applicability of the whole approach is demonstrated in the healthcare sector, for insuring an e-health software suite that is provided by an IT company to public and private hospitals in Greece. The overall approach can reduce the potential security incidents and the related economic loss, as the beneficiary deploys adequate protection mechanisms, whose proper operation is continually assessed, benefiting both the insured and the insurer.

10) O. Soultatos, K. Fysarakis, G. Spanoudakis, H. Koshutanski, E. Damiani, K. Beckers, D. Wortmann, G. Bravos, M. Ioannidis, **"The TREAT-ARREST Cyber-Security Training Platform**" at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Abstract: Cyber security is always a main concern for critical infrastructures and nation-wide safety and sustainability. Thus, advanced cyber ranges and security training is becoming imperative for the involved organizations. This paper presets a cyber security training platform, called THREAT-ARREST. The various platform modules can analyze an organization's system, identify the most critical threats, and tailor a training program to its personnel needs. Then, different training programmes are created based on the trainee types (i.e. administrator, simple operator, etc.), providing several teaching procedures and accomplishing diverse learning goals. One of the main novelties of THREAT- ARREST is the modelling of these programmes along with the runtime monitoring, management, and evaluation operations. The platform is generic. Nevertheless, its applicability in a smart energy case study is detailed.

11) L. Goeke, A. Quintanar, K. Beckers, S. Pape, **"PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Abstract: Social engineering is the clever manipulation of human trust. While most security protection focuses on technical aspects, organisations remain vulnerable to social engineers. Approaches employed in social engineering do not differ significantly from the ones used in common fraud. This implies defence mechanisms against the fraud are useful to prevent social engineering, as well. We tackle this problem using and enhancing an existing online serious game to train employees to use defence mechanisms of social psychology. The game has shown promising tendencies towards raising awareness for social engineering in an entertaining way. Training is highly effective when it is adapted to the players context. Our contribution focuses on enhancing the game with highly configurable game settings and content to allow the adaption to the player's context as well as the integration into training platforms. We discuss the resulting game with practitioners in the field of security awareness to gather some qualitative feedback.

12) I. Somarakis, M. Smyrlis, K. Fysarakis, G. Spanoudakis**, "Model-driven Cyber Range Training: A Cyber Security Assurance Perspective"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Abstract: Security demands are increasing for all types of organisations, due to the ever-closer integration of computing infrastructures and smart devices into all aspects of the organisational operations. Consequently, the need for security-aware employees in every role of an organisation increases in accordance. Cyber Range training emerges as a promising solution, allowing employees to train in both realistic environments and scenarios and gaining hands-on experience in security aspects of varied complexity, depending on their role and level of expertise. To that end, this work introduces a model-driven approach for Cyber Range training that facilitates the generation of tailor-made training scenarios based on a comprehensive model-based description of the organisation and its security posture. Additionally, our approach facilitates the automated deployment of such training environments, tailored to each defined scenario, through simulation and emulation means. To further highlight the usability of the proposed approach, this work also presents scenarios focusing on phishing threats, with increasing level of complexity and difficulty.

13) C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, L. Mauri, **"A model driven approach for cyber security scenarios deployment"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Abstract: Cyber-ranges for training in threat scenarios are nowadays highly demanded in order to improve people ability to detect vulnerabilities and to react to cyber-threats. Among the other components, scenarios deployment requires a modeling language to express the (software and hardware) architecture of the underlying system, and an emulation platform. In this paper, we exploit a model-driven engineering approach to develop a framework for cyber security scenarios deployment. We develop a domain specific language for scenarios construction, which allows the description of the architectural setting of the system under analysis, and a mechanism to deploy scenarios on the OpenStack cloud infrastructure by means of HEAT templates. On the scenario model, we also show how it is possible to detect network configuration problems and structural vulnerabilities.

The presented results are part of our ongoing research work towards the definition of a training cyber-range within the EU H2020 project THREAT-ARREST.

14) V. Prevelakis, M. Hamad, J. Najar and I. Spais, **"Secure Data Exchange for Computationally Constrained Devices"** at the International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), September 2019

Abstract: The need for secure communications between IoT devices is paramount. However, due to computational constraints and the need for lightweight publish/subscribe type of communications, traditional mechanisms for secure communications such as TLS and IPsec cannot be used directly. In this paper we present a new model for secure exchange of information that is based on off-line symmetric key encryption of the data and the use of policy-based credentials for the release of the encryption keys. Using the mechanism presented in this paper, the sender does not need to establish a direct network connection with the receiver, but can employ a store-and-forward transmission method. End-to-end data security is achieved by encrypting the data before the transfer, and sending the encryption key via an Aegis Secure Key Repository (ASKR) server. By encrypting the data off-line, the transmission can be carried out as fast as possible.

15) M. Tsantekidis and V. Prevelakis, **"Efficient Monitoring of Library Call Invocation"**, at the Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), October 2019

Abstract: The ability to monitor when user code invokes a library function offers numerous advantages. For example, during black-box testing of code, high-level control-flow integrity (CFI) checking, run-time access-control policy enforcement and so on. However, for this technique to be useful it must be efficient and able to function even when the target application is provided only as a statically linked executable. In an earlier paper, we demonstrated how library calls may be intercepted using wrappers. But, this approach works only with dynamically linked code and requires labour-intensive processing of the function arguments. Under the current scheme, each library - either dynamically or statically linked - constitutes a separate code region. At any point in time, only pages belonging to that one region are marked as executable, so when code branches to a page outside the 'home' region, it will land in a non-executable page, a fault will occur and the kernel will take over. By adding suitable code to the kernel, we can determine (a) whether the call should go ahead, (b) whether the arguments are acceptable and (c) ensure that the kernel will be informed when the code returns from the called function. In this paper, we present our technique by analysing the interception of a known exploit of the NGINX server. We show that our mechanism can detect and contain the attack and discuss the performance overheads of our mechanism.

16) S. Maghool, N. Maleki-Jirsaraei, M. Cremonini, **"The coevolution of contagion and behavior with increasing and decreasing awareness"**, PLOS ONE open access publication), December 2019

Abstract: Understanding the effects of individual awareness on epidemic phenomena is important to comprehend the coevolving system dynamic, to improve forecasting, and to better evaluate the outcome of possible interventions. In previous models of epidemics on social networks, individual awareness has often been approximated as a generic personal trait that depends on social reinforcement, and used to introduce variability in state transition probabilities. A novelty of this work is to assume that individual awareness is a function of several contributing factors pooled together, different by nature and dynamics,

and to study it for different epidemic categories. This way, our model still has awareness as the core attribute that may change state transition probabilities. Another contribution is to study positive and negative variations of awareness, in a contagion-behavior model. Imitation is the key mechanism that we model for manipulating awareness, under different network settings and assumptions, in particular regarding the degree of intentionality that individuals may exhibit in spreading an epidemic. Three epidemic categories are considered—disease, addiction, and rumor—to discuss different imitation mechanisms and degree of intentionality. We assume a population with a heterogeneous distribution of awareness and different response mechanisms to information gathered from the network. With simulations, we show the interplay between population and awareness factors producing a distribution of state transition probabilities and analyze how different network and epidemic configurations modify transmission patterns.

17) G. Hatzivasilis, O. Soultatos, E. Lakka, S. Ioannidis, D. Anicic, A. Broring, L. Ciechomski, M. Falchetto, K. Fysarakis, G. Spanoudakis, **"Secure Semantic Interoperability for IoT Applications with Linked Data"**, at the IEEE Global Communications Conference (GLOBECOM), December 2019

Abstract: Interoperability stands for the capacity of a system to interact with the units of another entity. Although it is quite easy to accomplish this within the products of the same brand, it is not facile to provide compatibility for the whole spectrum of the Internet-of-Things (IoT) and the Linked Data (LD) world. Currently, the different applications and devices operate in their own cloud/platform, without supporting sufficient interaction with different vendor-products. As it concerns the meaning of data, which is the main focus of this paper, semantics can settle commonly agreed information models and ontologies for the used terms. However, as there are several ontologies for describing each distinct 'Thing', we need Semantic Mediators (SMs) in order to perform common data mapping across the various utilized formats (i.e. XML or JSON) and ontology alignment (e.g. resolve conflicts). Our goal is to enable end-to-end vertical compatibility and horizontal cooperation at all levels (field/network/backend). Moreover, the implication of security must be taken into consideration as the unsafe adoption of semantic technologies exposes the linking data and the user's privacy, issues that are neglected by the majority of the semantic-web studies. A motivating example of smart sensing is described along with a preliminary implementation on real heterogeneous devices. Two different IoT platforms are integrating in the case study, detailing the main SM features. The proposed setting is secure, scalable, and the overall overhead is sufficient for runtime operation, while providing significant advances over state-of-the-art solutions.

2.3 Talks, seminars and presentations

As part of the broader dissemination effort for THREAT-ARREST, we presented various aspects of the project at several venues attracting the interest not only of the security training community, but the wider research community as well.

1) Bird&Bird presented a study on Big Data analysis[1] with a focus on privacy and cybersecurity during the ERA Summer Course on EU Data Protection Law
2) Prof. Vassilis Prevelakis from TUBS hosted a talk on "Security of mixed criticality components in the vehicle" at the 7th International Workshop on Mixed Criticality Systems (MCS)
3) Prof. Takis Varelas from DANAOS, during the presentation of "Seahealth" project, mentioned THREAT-ARREST as related to maritime training and awareness regarding healthcare issues onboard their vessels
4) Benoit Van Asbroek, Julien Debussche, Jasmien César from Bird&Bird hosted a talk on "Data Breaches at the Crossroads of Privacy, Fintech and Corporate Law" at Data Law Camp: Construire un droit des données, Designing Data Law
5) TUBS also presented the project's poster (see Appendix) at the 2019 HiPEAC conference

[1] https://www.era.int/cgi-bin/cms?_SID=NEW&_sprache=en&_bereich=artikel&_aktion=detail&idartikel=127745

6) Julien Debussche, Jasmien César, Simon Mortier, Alexandra Voinescu from Bird & Bird hosted a talk, at a company seminar, on "Dealing with data breaches: best practices", in June 2019
7) UMIL presented the project's poster at the 2nd Summer School on Industry Digital Evolution "Beyond Transformation: Evolving the Digital Enterprise" (Carovigno, Italy), in July 2019
8) Lara Mauri (UMIL) held a talk at the 2nd Summer School on Industry Digital Evolution, presenting the THREAT-ARREST project, in July 2019
9) George Hatzivasilis (FORTH) hosted a talk at the training session on business and technical personnel of the Cypriot Internet provider CABLENET, on cyber-security training for critical infrastructure owners, in August 2019 (Figure 1)

Figure 1: G. Hatzivasilis at CABLENET

10) Georgios Leftheriotis (TÜV Hellas) presented the THREAT-ARREST project in the $(ISC)^2$ Greek Chamber event in September 2019 (Figure 2)

Figure 2: G. Leftheriotis at (ISC)² Greek Chamber

11) Prof. Vassilis Prevelakis (TUBS) gave the keynote speech at the at the IOSEC-MSTEC-FINSEC workshop, on Cybersecurity for the Protection of Critical Infrastructures, at ESORICS in September 2019 (Figure 3)

Figure 3: V. Prevelakis at IOSEC-MSTEC-FINSEC workshop

12) The project was, also, presented at several other venues (Figures 4-8)

Figure 4: M. Smyrlis (SPHYNX) and M. Tsantekidis (TUBS) at NIS Summer School 2019

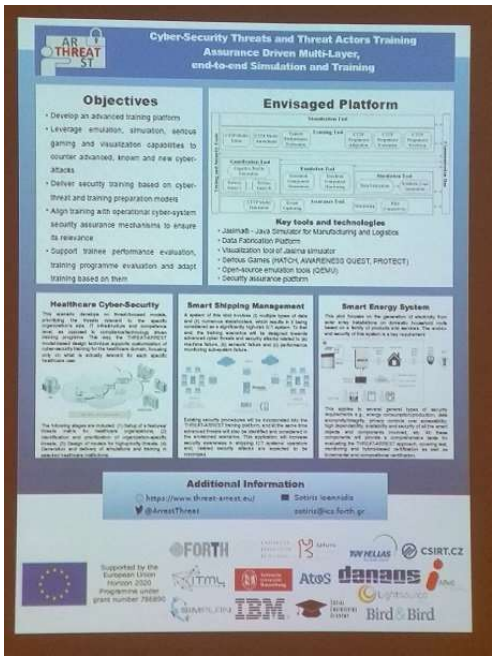


Figure 5: Poster presentation at IEEE CAMAD 2019

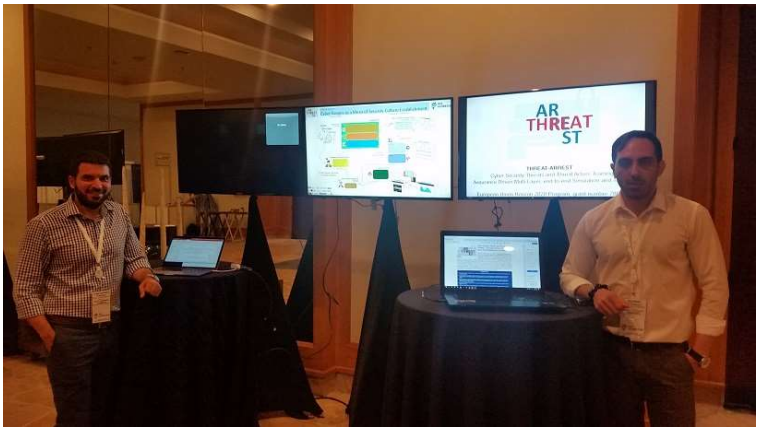


Figure 6: G. Fysarakis (SPHYNX) and G. Hatzivasilis (FORTH) presenting the project during the interactive sessions at IEEE GLOBECOM 2019

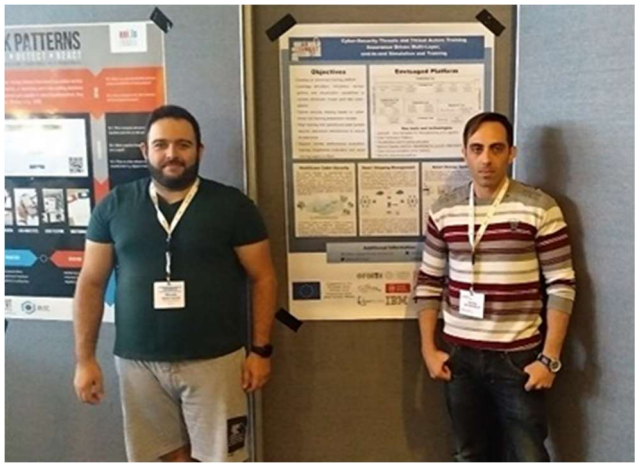


Figure 7: O. Soultatos (FORTH) and G. Hatzivasilis (FORTH) presenting the project poster at ESORICS 2019

Figure 8: G. Bravos (ITML) presenting THREAT-ARREST at the 2nd workshop of EU research and innovation maritime projects

13) DANAOS hosted at their premises the "2nd Workshop of EU Research & Innovation Maritime Projects" (November 2019, more than 100 attendees), where THREAT-ARREST was presented among other projects

2.4 Academic Dissemination

There have been three recent graduates that were granted Bachelor degrees at the University of Milan, in the Cybersecurity programme:

- Francesco Gallese, **"Feasibility study of a cyber range on OCCP platform"**, *Bachelor thesis.* Advisor: Elvinia Maria Riccobene, co-advisor: Fulvio Frati
- Andrea Sorrentino, **"Model-driven design of a language for the specification of attack scenarios in a cyber range"**, *Bachelor thesis.* Advisor: Elvinia Maria Riccobene, co-advisor: Chiara Braghin
- Alberto Porchera, **"Definition of attack scenarios for training systems"**, *Bachelor thesis.* Advisor: Chiara Braghin

2.5 Other Dissemination Activities

During the first half of the project, the following additional dissemination activities were carried out:

1) TÜV Hellas contributed in TÜV NORD's "Internord" Magazine regarding the THREAT-ARREST project, as well as participated in an international exhibition related to its scope. Moreover, they updated their corporate web sites with project information.
2) Bird&Bird published a press release[2] about the THREAT-ARREST project on the company's website. Furthermore, they published on their blog and other news magazines a series of articles on the legal and ethical issues and opportunities of Big Data, in particular cybersecurity and data breaches ((Debussche, César and Mortier, 2019), (Debussche, César, De Moortel and Mortier, 2019)).
3) TUBS updated its workgroup's website[3] with news of its participation in the project.
4) We successfully organize the "1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC[4]) workshop", in conjunction with the ESORICS 2019 conference (Figure 9), as well as, we co-organize the "Special Session on Security & Privacy for Intelligent, 5G-enabled IoT Ecosystems", in conjunction with the IEEE CAMAD 2019 conference (Figure 10).

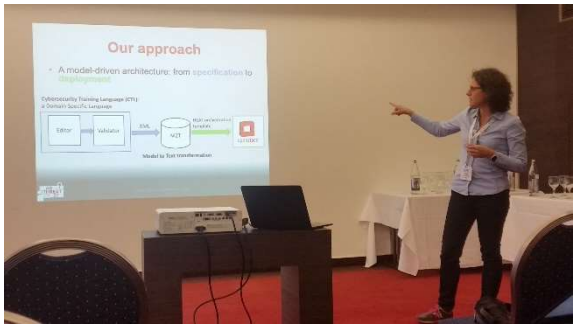


Figure 9: MSTEC workshop at ESORICS 2019

Figure 10: Special Session at IEEE CAMAD 2019

[2] https://www.twobirds.com/en/news/press-releases/2018/uk/bird-and-bird-participates-in-eu-cybersecurity-project-threat-arrest

[3] https://www.ida.ing.tu-bs.de/en/research/embedded-security/#projects

[4] https://www.threat-arrest.eu/html/mstec/

5) Consortium partners disseminated the workshop at several platforms (Facebook, LinkedIn, Twitter, HiPEAC community).

6) Bird&Bird mentioned THREAT-ARREST when delivering a presentation on the EU Data Economy: "Data Law – Why It Matters to Business"[5] at Vesalius College.

7) ARESS published an online article ((Chieti, Maglio, Petrarolo and Tanzarella, 2019)) on "Cyber risks in healthcare organizations and the insight of using the THREAT-ARREST platform for training".

8) ARESS published a brochure[6] about its activities and projects, where THREAT-ARREST is mentioned. (Figure 11 and Figure 12).

Figure 11: Cover of the brochure edited by ARESS

Figure 12: Page of the brochure edited by ARESS, dedicated to THREAT-ARREST

9) FORTH co-organized ENISA's 2019 summer school, where a Serious Games training session was held by SEA and several consortium partners participated and supported (Figure 13).

Figure 13: L. Goeke (SEA) overseeing a tabletop, security, gaming session

10) A technical video[7] was released and presented at several venues (Figure 14).

5 https://www.vesalius.edu/data-law/

6 https://www.slideshare.net/gorgonister/aress-salute-e-sociale-si-evolvono

7 https://www.youtube.com/watch?v=Nr6wejCKKsI

Figure 14: Starting image of the project's video

11) The project's brochure has been distributed in several venues (see Appendix). It is also available in electronic form, on the website, as a downloadable file in PDF format.

12) Regular newsletters are being posted on several online platforms (see Appendix). They are also available in electronic form, on the website, as a downloadable file in PDF format.

13) THREAT-ARREST established a liaison with the Cyberwatching.eu project and particularly its Cybersecurity and Privacy Project Radar[8], which provides a birdseye view of the complete collection of EU funded projects in the cybersecurity space. This way we are able to communicate and interact with other projects in similar domains. THREAT-ARREST's project page[9] was created and is being actively maintained and updated regularly.

14) SEA updated its website[10] with news of its participation in the project.

15) SEA presented and discussed the project within the European Project Cybersecurity4Europe[11] in WP3, WP8 and WP9 working groups.

16) SEA visited the it-sa[12] IT-security trade fare 2019 in Nuremberg to present the THREAT-ARREST project in conversations with relevant exhibitors.

17) SEA participated in the information and networking event IT-Risikofaktor Mensch[13] (IT risk factor human) in Augsburg (Germany). SEA had the chance to introduce the THREAT-ARREST project briefly after the regular talks. Additionally, SEA presented the project during the networking part of the event in conversations with other participants and the distributed the project brochure.

2.6 Planned Dissemination

1. DANAOS will present THREAT-ARREST and disseminate printed material in their booth at the POSIDONIA maritime exhibition in Athens – June 2020 (more than 20000 visitors). They will also present the project's system/technology to DANAOS user

8 https://www.cyberwatching.eu/technology-radar
9 https://www.cyberwatching.eu/projects/996/threat-arrest
10 https://www.social-engineering.academy/en/#portfolio
11 https://cybersec4europe.eu/
12 https://www.it-sa.de/en
13 https://zentrum-digitalisierung.bayern/veranstaltungen/it-risikofaktor-mensch-2/

meetings in May 2020. This will be a 5-day workshop organised for users of DANAOS Information System with a worldwide attendance (more than 200 visitors). In this event, DANAOS's engagement with new technologies and innovative projects will be demonstrated (including the THREAT-ARREST project).

2. The 4th regular newsletter is being prepared and will be released shortly. Others will follow on a regular basis.
3. Dr. Sotiris Ioannidis (FORTH) is one of the guest editors of "Future and Emerging topics in Security for Cyber-Physical Systems", a special issue of Future Internet (ISSN 1999-5903) – a scholarly peer-reviewed open access journal on Internet technologies and the information society, published online by MDPI. The special issue is in the process of receiving manuscript submissions (https://www.mdpi.com/journal/futureinternet/special_issues/Security_for_Cyber_Physical_Systems).
4. We will plan organize the 2nd MSTEC workshop in conjunction with the ESORICS 2020 conference, in Guildford, Surrey, UK (http://esorics2020.sccs.surrey.ac.uk/).
5. Initial plans have been made to organize a CyberRange/CyberSecurity related conference. This will be held in Athens, Greece and will target more than 100 attendees. It will be a 2-day event (Day 1: main Conference for CyberRange/CyberSecurity academics/industry executives and students. Day 2: workshops - mainly for students)
6. TUV HELLAS as part of the deliverable "D8.9 – Contribution to Standards", is organising contacts with key executives of $(ISC)^2$, ISACA, CSA and other standardization bodies.

2.7 Evaluation of the first half of the project

In this chapter, we compare the THREAT-ARREST dissemination activities for the first half of the project against the key performance indicators (KPIs) defined in the project proposal (below in parentheses). In this way, we can verify whether the project dissemination objectives have been met.

Push announcements (Success Indicator: ≥50 announcements): Regular announcements and posts have been pushed through social media (Facebook, LinkedIn, Twitter) (see the deliverable "D8.4 – The stakeholders' engagement & online channels report v.1" for more detailed information). On each of the platforms, more than 35 posts have already been made, totalling to more than 100 posts so far.

Regular Newsletter (Success Indicator: ≥9 newsletters): Three newsletters have circulated at this stage of the project. The fourth regular newsletter is being prepared.

Brochure (Success Indicators: ≥2.000 hard copies distribution in ≥10 events): 2000 hard copies have been printed and are actively distributed at all the events where one or more of the consortium partners attend.

Technical video (Success Indicators: ≥1000 views, ≥10 event presentations): 265 views have been registered so far for the project video, which has been presented to more than 5 events where one or more of the consortium partners have attended.

Journal publications (Success Indicator: ≥10 publications): Three journal papers have been published so far (4, 7, 16 in Section 2.2)

Magazine publications (Success Indicator: ≥10 publications): Three magazine papers have been published so far ((Debussche, César and Mortier, 2019), (Debussche, César, De Moortel and Mortier, 2019), (Chieti, Maglio, Petrarolo and Tanzarella, 2019))

Conference publications (Success Indicator: ≥12 publications): 14 conference papers have been published so far (rest of papers in Section 2.2)

Special issues (Success Indicators: ≥2 issues, ≥10 selected papers/issue): One special issue is about to be released online.

Conference organization (Success Indicators: ≥1 event, ≥100 attendees/event): None so far

Workshops organization (Success Indicators: ≥2 events, ≥30 attendees/event): The MSTEC workshop was organized in conjunction with ESORICS 2019, where 30 persons attended. Moreover, DANAOS hosted the "2nd Workshop of EU Research & Innovation Maritime Projects" in November 2019. Also, we co-organize a Special Session in the IEEE CAMAD 2019, where more than 30 persons attended.

Summer schools (Success Indicators: ≥2 events, ≥30 attendees/event): The ENISA summer school 2019 was co-organised by FORTH, where more than 100 persons attended.

Exhibition demonstrations (Success Indicator: ≥1 demo): None so far.

EU demonstrations (Success Indicator: ≥2 demos): The Serious Games training session at the ENISA summer school was held in September 2019.

Conference demonstrations (Success Indicator: ≥2 demos): The Emulation Tool and the overall THREAT-ARREST approach was demonstrated during the interactive sessions at the IEEE GLOBECOM 2019 conference.

3 Exploitation

3.1 Overall Aim

The main goal of the exploitation plan is the continuation of the THREAT-ARREST project beyond the end of the project funding. For that, different elements will be described: exploitable item, individual exploitation strategies, and joint exploitation plans.

3.2 Exploitation Background

The THREAT-ARREST platform will be consisted of a number of individual tools from the industrial partners. This section includes the exploitation plans of these tools.

3.2.1 Analysis of exploitable items

3.2.1.1 Sphynx Assurance Platform

STS aims to exploit the Cyber Threat and Training Preparation (CTTP) Models and Programmes Specification Language and the CTTP Models and Programmes Specification Tool as a basis for allowing its Assurance platform to also be used as tool to generate training scenarios for security experts (e.g., auditors) and training and awareness programmes for users of all levels of expertise (e.g., end users, system administrators), focusing on cyber systems of private and public organisations in the healthcare and telecoms sectors, which are the focus markets of the company. This extension will not only allow the generation of said scenarios and programmes, but also the incorporation of these within the assurance platform in a twofold manner: i) as input for assessing the probability that human-caused security & privacy incidents (stemming from the lack of user training and awareness) will occur; ii) as a means of mitigating the risks associated with said incidents. These scenario extensions will also be used for processing and assessing what-if scenarios, to enable a more realistic and evidence-based approach to the cost-benefit analyses features of the assurance platform.

3.2.1.2 Social Engineering Academy Gamification

SEA aims to exploit the advancements of the serious games HATCH and PROTECT within THREAT-ARREST. Before the start of THREAT-ARREST, HATCH ((Beckers and Pape, 2016), (Beckers, Pape and Fries, 2016)) was already developed and scenarios for a common office environment, energy provides, and consulting companies existed. Furthermore, a legal analysis regarding German laws was performed (Kipker *et al.*, 2018), differentiating between the application of the game for security requirement elicitation and training and awareness raising. For the application of HATCH for training and awareness raising, there have already been first evaluations ((Beckers *et al.*, 2017), (Sailer *et al.*, 2017)). PROTECT is based on PERSUADED (Aladawy, Beckers and Pape, 2018) which already existed as prototype before the start of THREAT-ARREST with a card-deck covering a standard scenario.

Within the THREAT-ARREST project, new scenarios for HATCH and PROTECT were developed. PROTECT was also refactored and a large part of the source code has been rewritten with the aim to allow an easier configuration of the card-deck and many aspects of the gameplay (Goeke *et al.*, 2019).

3.2.1.3 Information Technology for Market Leadership Training Tool

ITML aims to exploit specifically the advancements implemented in the Training Tool within THREAT-ARREST, in order to reach several potential new markets offering interactive, real-time assessment environments for model-driven training in numerous fields. In particular, ITML aims to further extend the capabilities of the training tool in order to provide advanced training services for big data analytics, real-time ML-based analytics, real-time anomaly

detection etc. Towards this direction, interactive and real-time assessment functionalities will be exploited.

3.2.1.4 IBM's data fabrication tool

IBM aims to exploit the extended and enhanced version of its Data Fabrication Platform (DFP) technology. The new technology version will be capable to fabricate synthetic realistic cyber security events for the TREAT-ARREST training and simulation framework. The extended tool will be used to both fabricating off-line synthetic data to support all the project use cases and fabrication of the security events logs of the simulated scenarios. The technology is based on a "rule guided" data fabrication methodology. In rule guided data fabrication, the data and meta-data logic is extracted automatically and is augmented by application logic and testing logic modelled by the user. The extended version of the DFP tool automatically extract the simulated scenario properties from the project CTTP model.

3.2.1.5 SIMPLAN Simulation tool

SIMPLAN aims to exploit the further development of the Jasima simulator including the process visualization into a support tool for cyber security trainings. The focus of development is on the realistic simulation of cyber threats, e.g. on the basis of real event logs, in a web-based environment. This means, among other things, that the simulator must be able to take data from external sources and communicate with other software, such as training platforms, in order to be able to exchange the results of the simulation. The processes and states of the simulation are to be visualized appropriately in order to give the user a comprehensible understanding of the simulated processes and the results. With this development we want to approach providers of cyber security trainings and training software in order to extend their offer with a simulation and thus achieve an even better training effect.

3.3 Individual Exploitation Strategies

This section describes the individual exploitation strategies of the THREAT-ARREST industrial partners.

3.3.1 Sphynx Technology Solutions AG

STS will use the outcomes of THREAT-ARREST for strengthening its service and product portfolio. STS plan is to augment the capabilities of its security assurance and certification platform in ways that will enable it to support the delivery of cyber security training programmes (e.g., providing monitoring and dynamic testing for CTTP models and programmes, establishing interoperability with emulation and simulation environments etc) and, therefore, be used as a tool for this purpose.

From a technical perspective, the strategy of STS for achieving this exploitation route will be to develop mechanisms supporting the implementation of continuous assurance by executing the assurance sub model of CTTP models, and developing appropriate APIs for its platform to provide access to the monitoring/testing evidence and checks required as part of CTTP programmes. As of today, STS was able to create the CTTP grammar and develop the initial CTTP models and programmes. It also provided the appropriate APIs to the THREAT-ARREST's training tool in order to read the CTTP core model and sub-models which will be used to initiate the training process.

3.3.2 ATOS Spain S.A.

ATOS's exploitation activities in THREAT-ARREST will be performed by the Innovation Hub unit in ATOS Research & Innovation (ARI), the R&D hub for emerging technologies and a key reference for the whole Atos group.

The Innovation Hub (IH), created in 2018 within ARI, is fostering the incubation of assets coming from R&D projects to build commercial solution based on innovation results. Through the creation of "shuttles" we mature these assets and create for them all marketing and business material needed to put them into the market.

The general strategy of exploitation is to evaluate the THREAT-ARREST results for added value to ATOS portfolio of security solutions, particularly offering advanced training capabilities for professionals of relevant sectors, such as critical infrastructures, to gather specialized skills on cybersecurity. The expected result of exploitation is to enrich ATOS's training offerings through cyber range platforms such as THREAT-ARREST.

ATOS foresees different lines of exploitation for THREAT-ARREST:

- Horizontal exploitation: Positioning THREAT-ARREST outcomes within ATOS technology services offering. This has a two-fold approach: i) the improvement of existing products in the Global Key Offering (GKO) portfolio by incorporating partial results from THREAT-ARREST to existing solutions, or ii) by offering THREAT-ARREST as a standalone product based on the final platform version.

  It is worth mentioning the following two:
  - Big Data & Cybersecurity (BDS) is in charge of solutions addressed to the protection of Critical Infrastructures and Homeland Security.
  - ATOS High Performance Security (AHPS) service that is managed by the Security Information and Event Management (SIEM) service provided of ATOS, is targeting customers with more than 3000 monitored devices (event sources), and billions of collected events per month.

  Atos results may be presented to relevant managers to analyze how to provide added value to the divisions' portfolio.

- Vertical exploitation: Positioning specific THREAT-ARREST advances in the field of cyber security training and preparedness to the following lines: i) the GKO on cyber-security, ii) the Cyber Threat Management Services within the Managed Services portfolio, and iii) the Governance, Risk and Compliance (GRC) offering.

3.3.3 IBM Israel – Science and Technology LTD

IBM's role in this project is to fabricate synthetic realistic security attacks. IBM established the IBM security unit which offers solutions in security intelligence, endpoint detection, security vulnerability detection, penetration testing, Malware analysis and more. IBM research lab in Haifa is working closely with the IBM security unit brands and incorporate innovations into their products, for example the security products of Guardium, Trusteer and Xforce. IBM has been named by Gartner as a leader in a number of security fields. Participation in THREAT-ARREST project, including close collaboration with the use case partners will help guide the next generation of security products. In addition, Israel has a rapidly emerging security community including hundreds of companies and start-ups developing and building innovative security solutions. IBM is the main sponsor of the major security conference in Israel, CyberTech, and actively helps incubating new start-ups in the IBM accelerator. We may use IBM's connections in Israel security community to present THREAT-ARREST innovative ideas. IBM research may exploit the outcomes of the project internally to enhance the security and quality of IBM products by collaborating with IBM security services and externally as part of the IBM security offerings or as a cloud service on any IBM platform. We will ensure that relevant IBM business units which are involved with developing the company's relevant products and services are aware of the technologies developed in the THREAT-ARREST

project and will consider them for inclusion in products, as well as in factoring the project innovation into the overall IBM product strategy.

3.3.4 Social Engineering Academy GMBH

SEA was able to develop new scenarios for the security requirement elicitation game HATCH, i.e. for the Smart Shipping domain (Pilot 3), as well as to improve existing ones. Furthermore, partly based on the results of the HATCH-sessions within the ENISA summer school, attack and defence cards for the Online-Game PROTECT were derived for all three domains (smart energy, healthcare and smart shipping). Thus, the context of the THREAT-ARREST project allows the development of new domain-specific scenarios, which enable SEA to target new domains and therefore increase the set of potential customers.

3.3.5 Information Technology for Market Leadership

ITML will exploit the outcomes of THREAT-ARREST, to enhance its market position with respect to intelligent management of advanced security threats, as well as on providing training services in multiple domains. Moreover, ITML's vision through THREAT-ARREST is to exploit the advanced visualisation, gamification and training tools on the basis of the project's findings, which can be used to enhance its current products.

Last, ITML will exploit the project's findings in enhancing and strengthening its positioning within the EU market and research domain, establishing partnerships and agreements for further collaborations with the large corporations participating in THREAT-ARREST.

In more detail, ITML aims to form strategic cooperation with stakeholders from the maritime field, the healthcare domain and the smart buildings domain, so that it can provide tailor-made services related to cyber security – based training.

3.3.6 Bird & Bird LLP

B&B has a high number of clients involved with disruptive technologies, both on the provider side and on the customer side. Several international leading companies have been assisted by the firm on issues relating to cyber-security and privacy, on judicial and extrajudicial matters, and more general with their aim of providing novel, yet legally compliant, products and services on the EU market. In the context of its work within the THREAT-ARREST project, B&B is able to keep abreast of the many legal and regulatory changes. It is also able to position itself on the legal market as a market leader by researching the most innovative legal issues and providing legal advice in relation thereto, with a practical and business mind. Not only does this provide to B&B a competitive advantage and enables it to position itself towards its international clients, but it also gives B&B the ability to showcase its first-hand knowledge and expertise and to get involved in EU policy making. Business development opportunities are expected by leveraging on the research results and the practical know-how gained during the project. This should hopefully allow enlarging B&B's current work in relation to its targets and reduce investments in relation to the research of novel legal issues. For instance, in relation to privacy, the research performed on the application of new obligations under the GDPR can be reused in other contexts and for an array of targets in various sectors.

3.3.7 DANAOS Shipping Company LTD

DANAOS as leading operator in container sea transportation, chartering out ships to major shipping liners will exploit on innovative solution of THREAT-ARREST in order to: (i) train and familiarize company's crew and offshore personnel to potential cyber-threats in shipping operation thus boosting up situational awareness on cyber risks; (ii) strengthen DANAOS security plan against these threats and assist company for the adoption of the ideal and most

effective framework for efficient protection, while at the same time (iii) enhance DANAOS leading position and reputation in maritime trade by ensuring that charterers interests, vessel integrity against cyber vulnerabilities and data protection remains a priority. In this context, DANAOS will exploit over threat-arrest technology so to incorporate cyber security training framework to the overall company's training modelling capitalizing mostly on company's existing technology infrastructure and training curriculums. Scope of DANAOS is to explore the possibility to integrate threat-arrest platform with bridge and incident command simulators, part of company's training equipment, thus structuring and offering multi-scale combined training scenarios performed in a similar to the ship environment.

3.3.8 TUV HELLAS TUV NORD

TÜV NORD's exploitation strategy focuses on utilizing the Project's outcomes in order to participate and be able to offer innovative, "certifiable", Cyber Range-based Cybersecurity Training Services. Such specialized Training & Certification Services are anticipated to be of high demand in the immediate & near future, as they will satisfy the needs both of specialized Technical Training as well as of covering / satisfying the changing European Legislation landscape requirements (NIS Directive, GDPR Regulation etc.).

The Group's exploitation potential is significant, as it is a Global Services Group, with core activities in Industrial Services, Mobility, Training, Natural Resources, Aerospace and IT, covering more than 70 Countries, with more than 14,000 Employees and thousands of Clients.

To this extent, TÜV is already actively involved in the:

- "Standardization" part of the Project, designing / planning a Strategy so that the Consortium can (a) continuously investigate opportunities for THREAT-ARREST to contribute to existing security training standards and (b) take necessary actions to "influence" the training content / be recognized as an affiliated programme of International / European Organizations like ISACA, (ISC)2, SANS – GIAC et.al. To this extent, TÜV will also utilize and gain upon collaborating with these International Organizations.
- "Certification of CTTP Programmes" part of the Project, preparing a framework of methodological guidelines, checklists and tools support, which will enable the analysis and improvement of CTTP training programmes.

3.3.9 LIGHTSOURCE LAB LTD

Lightsource Labs (LSE) mission is to improve the utilisation of solar PV and battery storage assets and generate financial benefits for homeowners. LSE's solutions combine the power of advanced Internet of Energy technologies with cutting-edge artificial intelligence and big data analytics, in order to help customers, optimise asset utilisation, balance energy demand and unlock financial opportunities.

LSE will look to exploit the THREAT-ARREST project as a training platform on which its employees, partners and stakeholders can be educated on cyber security concerns with regard to LSE infrastructure and the energy sector as a whole. LSE hope to utilise the THREAT-ARREST platform as the main training platform for all employees who require cyber security risk awareness and incident handling training. The training scenarios will help improve cyber security risk awareness for device installers and homeowners as well as prepare them on how to deal with potential cyber-threats. Use of the platform to run advance simulated threats will guide the company towards defining an effective security response plan in order to efficiently and effectively deal with potential security treats. LSE is looking to exploit the ability to run advanced simulated training scenarios in order to train our system administrators, solidify our procedures and protect our cyber physical systems.

LSE while not a WP or task leader in within WP8 will provide input and asset where required to raise awareness of the THREAT-ARREST concept, developments and findings to relevant stakeholders from large industry and SMEs within the energy sector. Where possible, LSE will collaborate with the other domains represented THREAT-ARREST (shipping and healthcare) as well as other relevant industrial sectors. LSE will assist WP 8 partners in developing a feasible and effective stakeholder plan, which will be customised for target groups as well as including an appropriate engagement plan. LSE will assist partners in identifying a key set of activities which will assist with executing the dissemination strategy. LSE will also assist WP8 partners in the implementation of an interactive portal to inform the general public as well as relevant stakeholders about key achievements of THREAT-ARREST, this will also include a social media presence providing maximum visibility and public awareness. Where possible, LSE will participate in EC events relevant to THREAT-ARREST.

When and where appropriate, LSE will focus on our existing network of SME associations via participation at industry events, which aims to expand communication of THREAT-ARREST results to a wider number of value chain participants.

To facilitate the market sustainability and Business continuity of THREAT-ARREST, LSE will assist WP8 partners in conducting market analysis in the short and long-term run (up to 5 years after the project) by performing a detailed analysis of costs assisting with the determination of 'real costs' in terms of operating the training platform. This will also include the development of a detailed THREAT-ARREST Business Plan and marketing strategy

LSE staff have a successful track-record of providing business plans, marketing strategies as well as exploitation plans in other H2020 funded projects including EMSODEV and EMSO-Link. THREAT-ARREST dissemination plan and activities will be generated to direct the end-user, academic and software partners by providing a detailed dissemination roadmap. LSE also has expertise in the development of specific project roadmaps for H2020 projects such as COOP+ and will provide expertise when and where required. The THREAT-ARREST dissemination plan will include specific milestones for publications in journals, presentations in scientific conferences, participation in exhibitions and will also organize a number of research-oriented workshops and events and LSE will provide input where required by WP8 partners.

3.3.10 SIMPLAN AG

The exploitation strategy for SimPlan is based on services offered around Jasima as well as licensing the software itself. Jasima is the discrete-event simulation library used as the core of THREAT-ARREST's Simulation Tool and the new Jasima Visualization Tool (JVT) is used within THREAT-ARREST to visualize the state of simulated and emulated cyber-system components.

SimPlan has the full copyright on the simulation library Jasima and JVT, meaning we can license it under any commercial license we like. The core of the discrete-event simulation library is offered under the AGPL license. SimPlan plans to release the components developed within THREAT-ARREST to support cyber-security trainings also under this license after the project has finished. Using the AGPL license, anyone can use the simulation component as he wants to but would have to open-source it if a derived work is created and distributed. In addition to that, the software is also available using a commercial license not requiring to release the source code of derived work (dual licensing). We are currently also discussing implementing a freemium model, offering an extended set of components with a commercial license, while the basic functionality is offered free of charge using AGPL licensing.

Services around cyber-security training will likely be the main exploitation strategy for SimPlan, fitting SimPlan's business model very well. Such services would include creating/extending simulation components as required to implement specific training scenarios as well as the creation of customized visualization scenarios. Given SimPlan's large customer base in manufacturing and logistics we also envision that they are interested in cyber-security trainings for, e.g., industrial IoT scenarios.

3.3.11 Agenzia Regionale Strategica per la Salute ed il Sociale

ARESS is a technical-operational and instrumental body of the Apulia Region in support of the definition and management of social and health policies, at the service of the Apulia Region in particular and of the public administration in general and operates as an agency for study, research, analysis, verification, consultancy and technical-scientific support. ARESS aims to organize and improve, through the continuous monitoring and verification of results, the readiness of the regional health system to respond to the needs and expectations of the health demand of the citizens of Puglia (about 4 million people). As a strategic Agency, it acquires and develops new strategic and organizational knowledge. Therefore, it experiments with paths of innovation and improvement, analyses and disseminates the best existing social-healthcare protocols both nationally and internationally, promotes and verifies innovative management models of clinical governance in compliance with the need to rationalise and optimise expenditure from the regional budget, particularly in the issues related to the use of ICT tools. Since cyberattacks are exponentially growing in heath sector, raising awareness in human operators (medical, administrative and technical staff) about these risks is vital. In fact, some cybersecurity threats are caused by human errors or ignorance. The ARESS target is to organize and improve, the readiness of the regional health information system to respond to the threats of malicious persons attacking healthcare sector. For this reason, it identifies, plans and promotes lines of development in the field of cybersecurity so that health and social welfare are not compromised by the essential use of new technologies. Moreover, it can foster and increase virtuous relations in the health and social-health field between the world of research, the business sector and the community, through the exploitation of the project results, so as to standardize best practices in the field of cybersecurity for the health sector, to be used over the whole Apulian region or at a wider level.

3.4 Joint Exploitation Plan

The THREAT-ARREST consortium is seeking actively to find routes of joint potential exploitation of the project's framework and platform or its individual components, based on opportunities arising in specific markets. Potential instruments that will be used for this purpose include contribution to the standards and a dedicated workshop -planned by the Consortium- on Joint Exploitation & Business Planning matters, within the next Project Plenary meeting.

Specific plans will be deployed during the course of the project, and as per the Consortium Partner's discussions / agreements on the final Business Model – also related to the future deliverable "D8.6 – Market Analysis, Business & Marketing Plan v.2", due at M30.

A final product/solution acting as a joint commercialization path will be designed and followed. This will include a collective strategy / path for the integrated product, as depicted in Figure 15 below:

Figure 15: THREAT-ARREST commercialization path

Moreover, as shown in Figure 16 (see Appendix 2), specific synergies exists among the various WP8 Tasks & Deliverables, including Joint Exploitation matters.

More specifically, one of the important Joint Exploitation Tasks / Activities is the one related to the "Contribution to Standards" (T8.4 – D8.9) and the Certification of CTTP Programmes (T8.5 – D8.5). The task "T8.4 – Contribution to Standards" is already on-going (from M13 until M36). The Objective of this action is within the overall Project's Objective #8 ("Ensure the uptake, commercialization, and the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework) and the related KPI-8.5 ("Achieve affiliated programme status for at least one of the following security training programmes: ISACA – CISA/CISM, $(ISC)^2$ – CISSP, CSA – Cloud Security, SANS – GIAC").

Related to this: (i) a "Training & Technical Standards-related Stakeholders inventory" is being built, (ii) a shortlist of targeted Stakeholders has already been drawn, and (iii) a specific "key contacts plan" has been drawn and is being implemented.

More details and overall evaluation regarding the Contribution to Standards and the success of this Joint Exploitation will be included in the deliverable "D8.9 – THREAT-ARREST contribution to standards report", due at M36.

4 Conclusions

This report presented a first update about the dissemination and exploitation plans by the partners of the THREAT-ARREST consortium. These plans are still preliminary since the technological development is still ongoing. Every partner involved in the project has its own exploitation and dissemination plans to carry on for the whole duration of the project.

In these 1.5 past years, many dissemination activities have been conducted, through different channels, such as events participation and sponsorships, scientific publications, website and social network activities, formal and informal meetings with several potential stakeholders of the project. Moreover, each partner of the consortium leaded several exploitation activities, which range from commercial uses to consulting services and insurance products.

Finally, this analysis will be refined by each partner during the next months as the THREAT-ARREST technologies mature. The next and final version of this report will be made in the deliverable “D8.8 – THREAT-ARREST dissemination and exploitation report v.2”, due at M36.

References

[1] Debussche, J., César, J. and Mortier, S. (2019) 'Big Data & Issues & Opportunities: Cybersecurity', Available at https://www.twobirds.com/en/news/articles/2019/global/Big-Data-and-Issues-and-Opportunities-Cybersecurity, https://www.lexology.com/library/detail.aspx?g=a776a13b-1f03-441d-be8b-f77a47c4263b, https://digitalbusiness.law/2019/01/big-data-issues-opportunities-cybersecurity/.

[2] Debussche, J., César, J., De Moortel, I., and Mortier, S. (2019) 'Big Data & Issues & Opportunities: Breach-related obligations', Available at https://www.twobirds.com/en/news/articles/2019/global/Big-Data-and-Issues-and-Opportunities-Breach-related-obligations, https://www.lexology.com/library/detail.aspx?g=10bbca2b-964e-43de-878f-de9982aed48e, https://digitalbusiness.law/2019/02/big-data-issues-opportunities-breach-related-obligations/.

[3] Chieti, A., Maglio, G., Petrarolo, V., and Tanzarella, C. (2019) 'Cyber risks in healthcare organizations and the insight of using the THREAT-ARREST platform for training', Available at https://www.agendadigitale.eu/sicurezza/cybersecurity-per-la-sanita-digitale-larma-strategica-e-la-formazione/.

[4] Aladawy, D., Beckers, K. and Pape, S. (2018) 'PERSUADED: Fighting social engineering attacks with a serious game', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11033 LNCS, pp. 103–118. doi: 10.1007/978-3-319-98385-1_8.

[5] Beckers, K. *et al.* (2017) 'Creativity techniques for social engineering threat elicitation: A controlled experiment', *CEUR Workshop Proceedings*, 1796, pp. 4–5.

[6] Beckers, K. and Pape, S. (2016) 'A Serious Game for Eliciting Social Engineering Security Requirements', *Proceedings - 2016 IEEE 24th International Requirements Engineering Conference, RE 2016*, pp. 16–25. doi: 10.1109/RE.2016.39.

[7] Beckers, K., Pape, S. and Fries, V. (2016) 'HATCH: hack and trick capricious humans--a serious game on social engineering', in *Proceedings of the 30th International BCS Human Computer Interaction Conference 30*, pp. 1–3.

[8] Goeke, L. *et al.* (2019) '{PROTECT} - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks', *Computer Security - {ESORICS} 2019 International Workshops, {MSTEC} 2019, Luxemburg, September 26-27, 2019, Revised Selected Papers*, 2, pp. 1–17.

[9] Hatzivasilis, G., et al., 2019a. MobileTrust: Secure Knowledge Integration in VANETs. ACM Transactions on Cyber-Physical Systems – Special Issue on User-Centric Security and Safety for Cyber-Physical Systems, ACM, vol. 4, issue 3, Article no. 33, pp. 1-15.

[10] Hatzivasilis, G., et al., 2019b. WARDOG: Awareness detection watchdog for Botnet infection on the host device. IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, IEEE, vol. 4, pp. 1-15.

[11] Hatzivasilis, G., et al., 2019c. Secure Semantic Interoperability for IoT Applications with Linked Data. IEEE Global Communications Conference (GLOBECOM 2019), IEEE, Waikoloa, HI, USA, 9-13 December 2019, pp. 1-7.

[12] Hatzivasilis, G., et al., 2019d. Towards the Insurance of Healthcare Systems. 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol. 11981, Luxembourg, 27 September 2019, pp. 1-14.

[13] Hatzivasilis, G., et al., 2019e. Cyber Insurance of Information Systems. 24th IEEE International Workshop on Computer Aided Modeling and Design of

Communication Links and Networks (CAMAD 2019), IEEE, Limassol, Cyprus, 11-13 September 2019, pp. 1-7.

[14] Hatzivasilis, G., et al., 2019f. Review of Security and Privacy for the Internet of Medical Things (IoMT). 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-8.

[15] Hatzivasilis, G., et al., 2019g. The CE-IoT Framework for Green ICT Organizations. 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-7.

[16] Kipker, D.-K. *et al.* (2018) 'Juristische Bewertung eines Social-Engineering-Abwehr Trainings', *State of the Art: IT-Sicherheit für Kritische Infrastrukturen*, (October), pp. 112–115. Available at: https://www.itskritis.de/_uploads/user/IT-Sicherheit Kritische Infrastrukturen–screen.pdf#page=112.

[17] Sailer, M. *et al.* (2017) 'Förderung von IT-Sicherheitsbewusstheit durch spielbasiertes Lernen - eine experimentelle Studie', *Tagung der Sektion ``Empirische Bildungsforschung'' -- Educational Research and Governance (AEPF 2017)*, 49(ID: 276/EPS10:3), p. 2882. Available at: https://aepf2017.de/data/abstracts.pdf.

Appendix 1

THREAT-ARREST Brochure

AR THREAT ST

Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training

OBJECTIVES

- Develop the means for specifying cyber security threat training and preparation models and programs to drive the realization of the training process
- Develop emulation capabilities enabling the creation of virtual cyber system components, subjecting them to cyber-attacks for training purposes, and enabling trainees to take appropriate response actions and hands-on experience against these cyber-attacks
- Develop multi-layer simulation capabilities enabling the realistic simulation of cyber systems, their usage and security attacks launched on them, through synthetic events at all layers in the implementation stack of these systems and their components reflecting realistic system conditions
- Develop cyber-security training based on serious games and enable trainees to get engaged in cyber-defence, elicit threats and learn about attacks
- Develop key capabilities for the effective delivery of CTTP programs, i.e. the visualization of the operation and state of cyber systems and the emergence and effects of attacks against them; assessing trainee performance in CTTP programs and adapting them depending on it; and assessing the overall effectiveness of a CTTP program and evolving it accordingly
- Align training and simulation with the continuous security assurance of real operational cyber systems, by integrating the developed capabilities into a common platform together with security assurance assessment capabilities
- Demonstrate the use of the THREAT-ARREST framework for effective training against cyber-attacks in the domains of smart energy, healthcare and transport (shipping), using real operational cyber systems within the domains as pilots and, through them, evaluate and validate the framework
- Ensure the uptake, commercialization, and the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework

Supported by the European Union Horizon 2020 Programme under grant number 786890

Training

Data Fabrication Platform: The DFP supports the definition of CTTP models and programmes, the presentation of learning materials/exercises of CTTP programmes, enables trainee actions in response to cyber threats, interactions with simulated and/or emulated cyber system components, trainee performance evaluation, CTTP programme evaluation and adaptation. The platform is extendible allowing new rule types to be added by users and automatically integrated in the platform. It is, also, capable of generating data from scratch, inflating existing databases or files, moving existing data and transforming data from previously existing resources.
Advancements by THREAT-ARREST: Translation of simulation specifications in CTTP models and statistical profiles into DFP rules to enable synthetic event generation for the purposes of THREAT-ASSERT.

Emulation

Emulation tools: The emulation platform provides the automated generation of emulated cyber-system components, in the form of interconnected virtual machines equipped with the appropriate software stack, as well as their interconnections in Physical and/or Software Architecture Layers (PAL/SAL) of a cyber system. It also enables interaction with the trainees.
Advancements by THREAT-ARREST: Combination and expansion of the capabilities of the emulation and penetration testing software/frameworks in order to achieve the automated generation and interconnection of emulated cyber system components. Enabling of trainees to perform security mitigation tasks. Selection of cyber-system components and attacks based on CTTP models.

Assurance

Security assurance platform: This platform supports the continuous assessment of the security of the cyber system through the combination of runtime monitoring and dynamic testing in order to provide information about the status of the actual cyber system. It also collects runtime system events and generates alerts that provide the basis for setting up realistic simulations. Furthermore, it enables the configuration of security assessment, reporting and certification to the needs of different stakeholders ranging from senior management to external auditors and regulators.
Advancements by THREAT-ARREST: (a): Offering customizable security data analytics applied to data-at-rest and live, streaming data. Off-the-shelf hardware components coupled with a custom software engine to provide a clear upgrade path, without vendor-specific lock-in. (b): Development of mechanisms to support the connectivity and use of the platform as part of a cyber threat training framework. Mechanisms supporting the implementation of continuous assurance by executing the assurance sub model of CTTP models, APIs for monitoring/testing evidence and checks reporting etc.

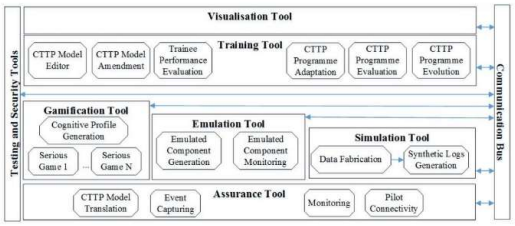
THREAT-ARREST APPLICATIONS

Smart Shipping Management

This pilot envisions to validate the THREAT-ARREST platform and provide feedback in regards to its effectiveness in the shipping industry. A system of this kind involves (i) multiple types of data and (ii) numerous stakeholders, which results in it being considered as a significantly high-risk ICT system. To that end, within this pilot, scenarios will be built and training will be designed towards advanced cyber threats and security attacks related to (a) machine failure, (b) sensors' failure and (c) performance monitoring sub-system failure. Existing security procedures will be incorporated into the THREAT-ARREST training platform, and at the same time advanced threats will also be identified and considered in the envisioned scenarios. This THREAT-ARREST application will increase security awareness in shipping ICT systems' operators and, security attacks related to the aforementioned failures are expected to be minimized. Moreover, this pilot will help towards (i) identifying specific threats jeopardizing the operations of ICT systems in the Shipping Management industry and (ii) engaging multiple stakeholders from the shipping industry in the exploitation of the THREAT-ARREST training platform.

THREAT-ARREST aims to develop an **advanced training platform** incorporating **emulation**, **simulation**, **serio gaming** and **visualization** capabilities to adequately prepare stakeholders with different types of responsibility a levels of expertise in defending high-risk cyber systems and organizations to **counter advanced, known** and **u cyber-attacks**. The THREAT-ARREST platform will deliver security training, based on a **model driven** approa where **cyber threat and training preparation (CTTP) models**, specifying the potential attacks, the security contr of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will **dr** the **training process**, and **align it** (where possible) with **operational cyber system security assurance** mechanis to ensure the relevance of training. The platform will also support **trainee performance evaluation** and **traini programme evaluation** and **adapt training programmes** based on them. The effectiveness of the framework will **validated** using a **prototype implementation** interconnected with **real cyber systems pilots** in the areas of sm energy, healthcare and shipping, and from **technical**, **legal** and **business perspectives**.

ENVISAGED PLATFORM AND PROJECT ENHANCEMENTS



Visualisation

Visualisation tool of Jasima simulator: The visualisation platform enables the visualisation of simulations a the effect of training actions on simulated systems. It, also, facilitates the creation, parameterization a interaction with the simulation and training platforms. Moreover, it enables users to parameterize scenari trigger simulations and view their outcomes.
Advancements by THREAT-ARREST: (a): Extension by visualization layers (Web, Mobile Device, Windo Client) based on existing technology, as required for presenting the outcomes of simulation/emulation of cybe system components in the project. (b): Leveraging serious gaming elements in order to increase learni motivation for small and medium groups.

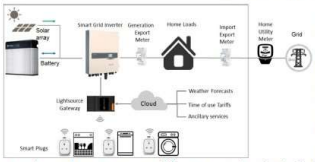
Serious Gaming

Serious Games tools: These tools host various serious games, scenarios and training evaluation mechanism which enable trainees to develop skills in being resilient to and preventing social engineering attacks (e. phishing, impersonation attacks etc.). The provided games are driven by the threats and assumptions specified CTTP models (security assurance).
Advancements by THREAT-ARREST: Enhancement of the various serious games with (i) advanced scenari of cyber threats' mitigation and (ii) new visualisation components.

Simulation

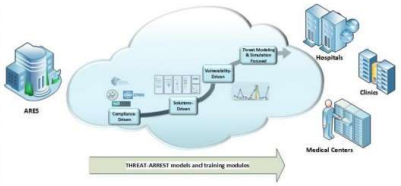
Jasima®-Java Simulator for Manufacturing and Logistics: Jasima generates synthetic system logs a simulates individual cyber system components and networks of such components to enable the simulation entire training scenarios defined in CTTP programmes.
Advancements by THREAT-ARREST: Configuration and adoption of the simulator in order to meet the nee of the THREAT-ARREST training platform (i.e., simulation of different layers in the cyber syste implementation stack.

Smart Energy System



This pilot focuses on the generation of electricity from solar array installations on domestic household roofs based on a family of products and services. The end-to-end security of the Smart Energy System (SES) is a key requirement. This applies to several general types of security requirements e.g., energy consumption/production data anonymity/ integrity; privacy controls over accessibility; high dependability, availability and security of all the smart objects and components involved, etc. All these components will feature in the CTTP scenarios and programmes providing a comprehensive basis for evaluating the THREAT-ARREST approach. In particular, our expectation is that the SES pilot security requirements will cover test, monitoring and hybrid-based certification as well as provide scenarios and requirements for incremental and compositional certification.

Healthcare Cyber-Security Training



This is a scenario showcasing model-based generation and delivery of training tailored to healthcare organizations of different sizes. This scenario will radically move away from current compliance-driven and technology-driven training programs, which are designed with the suppliers' interests and capabilities in mind. Instead, it will develop on threat-focused models, prioritizing the threats relevant to the specific organization's size, IT infrastructure and competence level. This way, the THREAT-ARREST model-based design technique will support customization of cyber-security training for the healthcare domain, focusing only on what is actually relevant for each specific healthcare user. The Healthcare Cyber-Security Training scenario includes the following stages: (1) Set up of a features/threats matrix for healthcare organizations, (2) Identification and prioritization of organization-specific threats, (3) Design of THREAT-ARREST models for high priority threats, (4) Generation and delivery of model-based simulations and training in selected healthcare institutions. In the end, this pilot will: (a) provide actionable information on cyber-security threats/proper responses and on medical device vulnerabilities, (b) establish an operational framework for alleviating healthcare data breaches, (c) spread best practices in public health, safety science and cyber-physical systems security to address the challenges associated with healthcare cyber-security risks and (d) develop a training framework to assess patient safety and public health risks associated with cybersecurity vulnerabilities and mitigate the risks.

PROJECT DETAILS	MORE INFORMATION
Start Date: 2018-09-01	Web: https://www.threat-arrest.eu/
Duration: 36 months	Twitter: @ArrestThreat
Project Cost: €6,431,125	Facebook: @Threat-Arrest-2664543573240 31
Project Coordinator: FORTH	LinkedIn: @/in/threat-arrest-706485175/

Newsletter Issue 1 (January 2019)

Cyber-Security Threats and Threat Actors Training
Assurance Driven Multi-Layer,
end-to-end Simulation and Training

JANUARY 2019 – ISSUE 1

Newsletter

Overview

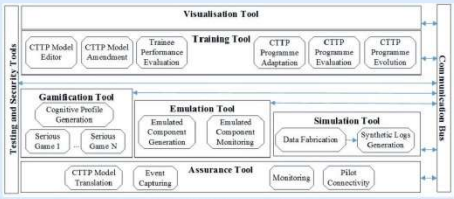
THREAT-ARREST is funded by the European Commission Horizon 2020 programme under Grant Agreement No. 786890, launched on September 2018.

It has a four-year duration and its main scope is to develop **an advanced training platform** incorporating **emulation, simulation, serious gaming** and **visualization** capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to counter **advanced, known** and **new cyber-attacks**.

The THREAT-ARREST platform will deliver security training, based on a **model driven** approach where **cyber threat and training preparation (CTTP)** models, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will **drive** the **training process**, and **align it** (where possible) with **operational cyber system security assurance** mechanisms to ensure the relevance of training.

The platform will also support **trainee performance evaluation** and **training programme evaluation** and **adapt training programmes** based on them. The effectiveness of the framework will be **validated** using a **prototype implementation** interconnected with real **cyber-systems pilots** in the areas of smart energy, healthcare and shipping, and from **technical, legal** and **business perspectives**.

In this issue:



The THREAT-ARREST platform

Kick-off meeting

The THREAT-ARREST **physical kick-off meeting** was successfully held on September 19th, 2018 at the premises of FORTH in Heraklion – Crete, Greece!!

Publicity

- TÜV Hellas contributed in TÜV NORD's "Internord" Magazine regarding the THREAT-ARREST project, as well as participated in an international exhibition related to its scope. Moreover, they updated their corporate web sites with project information
- Bird&Bird published a press release about the THREAT-ARREST project on the company's website. They also presented a study on Big Data analysis with a focus on privacy and cybersecurity during the ERA Summer Course on EU Data Protection Law. Furthermore, they published on their blog and other news magazines a series of articles on the legal and ethical issues and opportunities of Big Data, in particular cybersecurity and data breaches (link 1, link 2, link 3)
- The Technical University of Braunschweig updated its workgroup's website with news of its participation in the project. They also presented the project's poster at the HiPEAC conference. Moreover, the head of the group, Prof. Vassilis Prevelakis, hosted a talk on "Security of mixed criticality components in the vehicle" at the 7th International Workshop on Mixed Criticality Systems (MCS)
- Prof. Takis Varelas from DANAOS mentioned THREAT-ARREST as related to maritime training and awareness regarding healthcare issues onboard their vessels
- Project flyers have been distributed in several venues

Publications

Jihane Najar and Vassilis Prevelakis , **"A Secure and Efficient File System Access Control Mechanism (FlexFS)"** in the International workshop on Information & Operational Technology (IT & OT) security systems IOSec, September 2018

Mohammad Hamad, Mustafa R. Agha , and Vassilis Prevelakis , **"ProSEV: Proxy-Based Secure and Efficient Vehicular Communication"** in 2018 IEEE Vehicular Networking Conference (VNC), December 2018.

Follow us

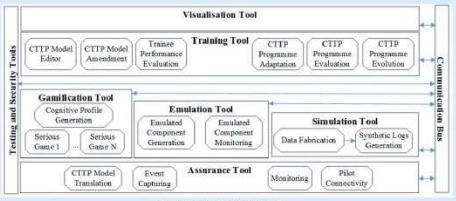
Newsletter Issue 2 (May 2019)

Cyber-Security Threats and Threat Actors Training
Assurance Driven Multi-Layer,
end-to-end Simulation and Training

MAY 2019 – ISSUE 2

Newsletter

Progress



The THREAT-ARREST platform

CTTP models/programmes creation: Definition/refinement of Cyber Threat and Training Preparation (CTTP) language requirements, for each of the different sub-models (Core Assurance, PAL, SAL, Deployment, Simulation/Emulation, CTTP Training programme). Definition/refinement of areas of focus and scope of the training programs. Expansion of cyber system model (CSM) to cover physical, hardware and software parts of the cyber system, as well as information regarding their deployment. Addition of elements of the Assurance Model as part of the main CSM, depicting the relationship between threats, assets, vulnerabilities and the associated risk, as well as the controls that may be used to mitigate said risk. Development of parts of the Training, Simulation and Emulation sub-models, considering the training scenarios that will have to be covered, as well as the involved simulated and emulated assets. Initial sketching of an elementary training scenario featuring an email phishing attack, and how this scenario would be implemented and carried out within the THREAT-ARREST platform. Production of a first draft of the CSM (including SAL, PAL, and Deployment sub-models).

Emulation tool: Definition of the emulation tool, its architecture and its interfaces with the rest of the platform. Definition of its requirements. Decomposition into sub-components and modules: (a) Emulation Compiler - translation of the CTTP Emulation sub-model in actual configurations, (b) Emulation Engine - application of configurations on target architecture, (c) Emulation Repository – storage for images of generic operating systems, pilots nodes and specific simulation machines to instantiate in order to deploy the emulation environment. Deployment of a simple infrastructure on the platform based on XML–type configuration derived from the CTTP Emulation sub-model. Simple network setup by (a) based on the network connection specified in the provided configuration.

In this issue:

Training and Visualization tools: Specification of the overall architecture and identification of an initial set of components/elements to be supported. Partners coordination regarding the integration of serious games into the THREAT ARREST platform. Initial analysis on the tools' communications and data flow, the data formats and the need for secure communications. Development of the first architectural concepts for visualization. Definition of possible threat scenarios of the pilot users. Development of the technical design and implementation of visualization and simulation including the integration of the training platform. Refinement of communications and data flow between the Assurance tool and the Simulation and Emulation tools. Introduction of a new component, Dashboard, to integrate in a unified and user-friendly way the various functional and management interfaces envisaged in the platform. Agreement on several requirements and features of the Communication Bus component. Refinement and integration of the Identity & Access Management component. Agreement on stronger integration of the Gamification tool in the platform: (a) how to enable finer-grained configuration of the serious games and use them for non-social-engineering attacks training, (b) how to use the CTTP models as input to such games' configuration and the need to provide additional configuration details with respect to trainees' performance/profile, (c) how to enable the Gamification tool provide results on the trainee's progress during a serious game round and not only at the end of the game with the overall results. Clarification of the training and visualization components' structure. Initial discussions on the integration of synthetic and real event logs to be used by the simulation.

Simulation Environment: Identification of several communication aspects, (e.g., publish/subscribe mechanisms for selective and asynchronous data communication). Research on existing solutions of network security simulations. Definition and creation of the concept and high-level architecture of the technology for synthetic security events fabrication. Further detailed discussions on the usage of a message broker for asynchronous communication and the integration between the emulation and simulation components. Development of an initial version of the CTTP sub-model for instantiating a simulated scenario. Initial design and implementation of the real event logs statistical profiling module. Interconnection of the Data Fabrication Platform with the with Assurance, Training, Gamification and Emulation modules. Provision of details about the architecture of the simulation components, especially on how to integrate them with the visualization components. Definition of the simulated components and their desired behaviour needed for pilot scenarios.

Legal framework: Continued definition of the basic legal and security requirements of the platform and analysis of the entire project's requirements focusing on the privacy and security aspects.

Publicity

- Submission and acceptance of a proposal for the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC) workshop in conjunction with the ESORICS 2019 conference.
- Dissemination of the workshop at several platforms (Facebook, LinkedIn, Twitter, HIPEAC community)
- A series of articles on the legal and ethical issues and opportunities of Big Data, in particular cybersecurity and data breaches, posted on several platforms (link 1, link 2, link 3) (Bird & Bird)
- Presentation on the EU Data Economy: "Data Law – Why It Matters to Business" at Vesalius College (Bird & Bird)
- Talk on "Data Breaches at the Crossroads of Privacy, Fintech and Corporate Law" at Data Law Camp: Construire un droit des données, Designing Data Law (Benoit Van Asbroek, Julien Debussche, Jasmien César – Bird & Bird)

Publications

F. Marcantoni, M. Diamantaris, S. Ioannidis, J. Polakis, **"A Large-scale Study on the Risks of the HTML5 WebAPI for Mobile Sensor-based Attacks"** in The World Wide Web (WWW'18) Conference, May 2019

G. Hatzivasilis, O. Soultatos, P. Chatziadam, K. Fysarakis, I. Askoxylakis, S. Ioannidis, G. Alexandris, V. Katos, G. Spanoudakis, **"WARDOG: Awareness detection watchdog for Botnet infection on the host device"** in IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, May 2019

G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. I. Tsatsoulis, **"Review of Security and Privacy for the Internet of Medical Things (IoMT)"** in 1st International Workshop on Smart Circular Economy (SmaCE), May 2019

G. Hatzivasilis, N. Christodoulakis, C. Tzagkarakis, S. Ioannidis, K. Fysarakis, G. Demetriou, M. Panayiotou, **"The CE-IoT Framework for Green ICT Organizations"** in 1st International Workshop on Smart Circular Economy (SmaCE), May 2019

Follow us

Newsletter Issue 3 (September 2019)

AR THREAT ST

Cyber-Security Threats and Threat Actors Training
Assurance Driven Multi-Layer,
end-to-end Simulation and Training

SEPTEMBER 2019 – ISSUE 3

Newsletter

Progress

CTTP models/programmes creation: Adaptation and further development of the security assurance model, following internal feedback – UML Class Diagram, description of its objects. Focus mainly on the Cyber Range (CR) sub-model of the assurance model, including the Training, Simulation and Emulation sub-models. Description and illustration of one simple and one more complex phishing scenario based on the CR sub-model. Description of several smart home related scenarios covering various threats in such environments (device compromise, misconfiguration, internet exposure, etc.). Modelling of scenarios via the CR sub-model. Further development of the training scenarios defined for the maritime and healthcare use-cases.

Emulation tool: Development of the Emulation Tool components. Presentation of a prototype and a first demo of the tool. XML configuration file based on the CTTP emulation concepts, containing the description of the emulated architecture, as input for the Emulation Controller REST interface and deployment of the emulated architecture as well as setup of the SSH connections with the user and each virtual machine. Discussions concerning the tools' interconnection. Work on the correlation of the CTTP sub-models for deploying emulated components. Work on the inter-platform communication of the various modules through the RabbitMQ broker.

Training and Visualization tools: Further work on the design of the training tool, focusing on the structure of the Dashboard. Aggregation of technologies used in other modules, ensuring proper communication with the Dashboard and all the pilot-specific requirements for the Dashboard's functionalities. Update and finalizing of the sequence diagram for the training tool, depicting all activities (actors, classes and message exchanges) and describing all communications with the rest of the tools. Further development of the first version of the visualization module. Improvement of the gameplay for the gaming tool PROTECT. Evolving of the communications and data flow between the Training and Visualization Tools and the rest of the platform's tools.

Simulation Environment: Further discussions detailing the integration of simulation, the Data Fabrication Platform and the statistical analysis tool into the overall THREAT-ARREST platform architecture. Usage of a message broker for the asynchronous communication and integration between the emulation and simulation components. Implementation of an initial set of simulation components required for the pilots. Development of the first version of the simulated components and their connection to the first prototype of the visualization component. Further development of the module for statistical profiling of real event logs. Specification of the REST API for integrating the Data Fabrication Platform in the overall THREAT-ARREST system architecture.

Plenary meeting

The 2nd THREAT-ARREST plenary meeting was successfully held on April 10th, 2019 at the premises of ATOS in Barcelona, Spain

In this issue:

Publicity

- Organization of ENISA's summer school - Serious Games training session - Participation and support by consortium partners - Presentation of the project's video - Presentation of the project's poster - Flyer handout
- Talk hosted by Julien Debusscshe, Jasmien César, Simon Mortier, Alexandra Voinescu (Bird & Bird), at a company seminar, on "Dealing with data breaches: best practices", in June 2019
- Poster presentation at the 2nd Summer School on Industry Digital Evolution "Beyond Transformation: Evolving the Digital Enterprise" (Carovigno, Italy), in July 2019, by UMIL
- Talk hosted by Lara Mauri (UMIL), at the 2nd Summer School on Industry Digital Evolution, presenting the THREAT-ARREST project, in July 2019
- Talk hosted by George Hatzivasilis (FORTH), at the training session on business and technical personnel of the Cypriot Internet provider CABLENET, on cyber-security training for critical infrastructure owners, in August 2019
- Keynote talk by Prof. Vassilis Prevelakis (TUBS), at the 1st Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC), on Cybersecurity for the Protection of Critical Infrastructures, in September 2019

Publications

G. Hatzivasilis, P. Chatziadam, N. E. Petroulakis, M. Mangini, C. Kloukinas, A. Yautsiukhin, M. Antoniou, D. G. Katehakis, M. Panayiotou, **"Cyber Insurance of Information Systems"** at the 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), September 2019

G. Hatzivasilis, P. Chatziadam, A. Miaoudakis, E. Lakka, A. Alessio, M. Smyrlis, G. Spanoudakis, A. Yautsiukhin, M. Antoniou, N. Stathiakis, **"Towards the Insurance of Healthcare Systems"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

O. Soultatos, K. Fysarakis, G. Spanoudakis, H. Koshutanski, E. Damiani, K. Beckers, D. Wortmann, G. Bravos, M. Ioannidis, **"The THREAT-ARREST Cyber-Security Training Platform"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

L. Goeke, A. Quintanar, K. Beckers, S. Pape, **"PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

I. Somarakis, M. Smyrlis, K. Fysarakis, G. Spanoudakis, **"Model-driven Cyber Range Training – The Cyber Security Assurance Perspective"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

C. Braghin, S. Cimato, E. Damiani, F. Frati, E. Riccobene, L. Mauri, **"A model driven approach for cyber security scenarios deployment"** at the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), September 2019

Vassilis Prevelakis, Mohammad Hamad, Jihane Najar and Ilias Spais, **"Secure Data Exchange for Computationally Constrained Devices"** at the International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), September 2019

Manolis Chatzimpyrros, Konstantinos Solomos and Sotiris Ioannidis, **"You Shall Not Register! Detecting Privacy Leaks across Registration Forms"** at the International workshop on Information & Operational Technology (IT & OT) security systems (IOSec), September 2019

Follow us

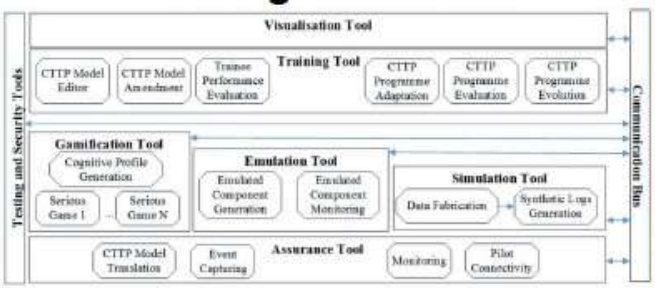
THREAT-ARREST poster

Cyber-Security Threats and Threat Actors Training Assurance Driven Multi-Layer, end-to-end Simulation and Training

Objectives

- Develop an advanced training platform
- Leverage emulation, simulation, serious gaming and visualization capabilities to counter advanced, known and new cyber-attacks
- Deliver security training based on cyber-threat and training preparation models
- Align training with operational cyber-system security assurance mechanisms to ensure its relevance
- Support trainee performance evaluation, training programme evaluation and adapt training based on them

Envisaged Platform



Key tools and technologies

- Jasima® - Java Simulator for Manufacturing and Logistics
- Data Fabrication Platform
- Visualization tool of Jasima simulator
- Serious Games (HATCH, AWARENESS QUEST, PROTECT)
- Open-source emulation tools (QEMU)
- Security assurance platform

Healthcare Cyber-Security

This scenario develops on threat-focused models, prioritizing the threats relevant to the specific organization's size, IT infrastructure and competence level, as opposed to compliance/technology driven training programs. This way, the THREAT-ARREST model-based design technique supports customization of cyber-security training for the healthcare domain, focusing only on what is actually relevant for each specific healthcare user.

The following stages are included: (1) Setup of a features/ threats matrix for healthcare organizations, (2) Identification and prioritization of organization-specific threats, (3) Design of models for high-priority threats, (4) Generation and delivery of simulations and training in selected healthcare institutions.

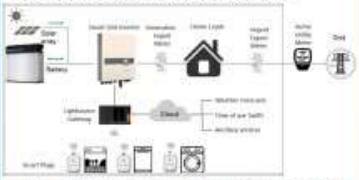
Smart Shipping Management

A system of this kind involves (i) multiple types of data and (ii) numerous stakeholders, which results in it being considered as a significantly high-risk ICT system. To that end, the training scenarios will be designed towards advanced cyber threats and security attacks related to (a) machine failure, (b) sensors' failure and (c) performance monitoring sub-system failure.

Existing security procedures will be incorporated into the THREAT-ARREST training platform, and at the same time advanced threats will also be identified and considered in the envisioned scenarios. This application will increase security awareness in shipping ICT systems' operators and, related security attacks are expected to be minimized.

Smart Energy System

This pilot focuses on the generation of electricity from solar array installations on domestic household roofs based on a family of products and services. The end-to-end security of this system is a key requirement.



This applies to several general types of security requirements e.g., energy consumption/production; data anonymity/integrity; privacy controls over accessibility; high dependability, availability and security of all the smart objects and components involved, etc. All these components will provide a comprehensive basis for evaluating the THREAT-ARREST approach, covering test, monitoring and hybrid-based certification as well as incremental and compositional certification.

Additional Information

https://www.threat-arrest.eu/
@ArrestThreat
Sotiris Ioannidis
sotiris@ics.forth.gr

Supported by the European Union Horizon 2020 Programme under grant number 786890

Appendix 2

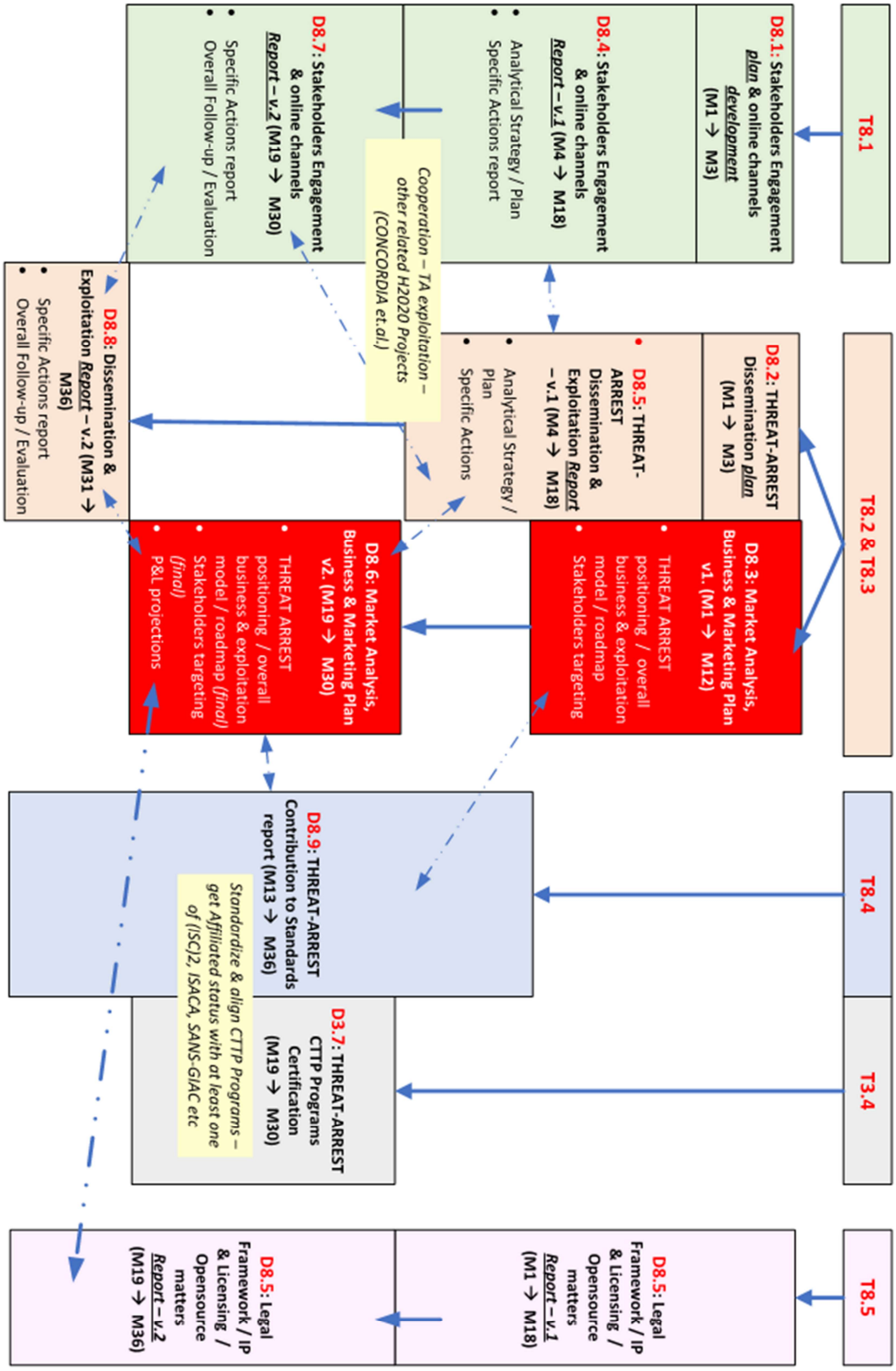


Figure 16: WP8 Tasks & Deliverables