Horizon 2020
European Union funding
for Research & Innovation

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

D8.2: The THREAT-ARREST dissemination plan †

Abstract: This deliverable provides a dissemination plan to direct the end-user, academic and software partners by providing a detailed dissemination roadmap for specific milestones for publications in journals, presentations in scientific conferences, participation in exhibitions and organization of a number of research oriented workshops and events.

Contractual Date of Delivery	30/11/2018
Actual Date of Delivery	30/11/2018
Deliverable Security Class	Public
Editor	*Marinos Tsantekidis (TUBS)*
Contributors	All partners
Quality Assurance	*George Hatzivasilis (FORTH), Stelvio Cimato, Elvinia Riccobene, Fulvio Frati (UMIL)*

† *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation program 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
Università degli Studi di Milano (UMIL)	Italy
ATOS Spain S.A. (ATOS)	Spain
IBM Israel – Science and Technology LTD (IBM)	Israel
Socal Engineering Academy GMBH (SEA)	Germany
Information Technology for Market Leadership (ITML)	Greece
Bird & Bird LLP (B&B)	United Kingdom
Technische Universität 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 Sanitaria Pugliese (ARES)	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. *George Hatzivasilis (FORTH)*
2. *Stelvio Cimato, Elvinia Riccobene, Fulvio Frati (UMIL)*

Revisions

Version	Date	By	Overview
1.0	30/11/2018	Editor	Final version
0.9	28/11/2018	Editor	Addressed reviewers' comments
0.8	27/11/2018	Editor	Pre-final version
0.7	22/11/2018	Editor	Added contribution from LSE
0.6	19/11/2018	Editor	Added contribution from ARESS
0.5	2/11/2018	Editor	Added contribution from ATOS, B&B
0.4	22/10/2018	Editor	Added contribution from SEA, TUBS
0.3	19/10/2018	Editor	Added contribution from UMIL
0.2	18/10/2018	Editor	Added contribution from SIMPLAN, ITML, FORTH
0.1	17/10/2018	Editor	First Draft, added contribution from Danaos

Executive Summary

This deliverable presents the dissemination plans of the partners of the THREAT-ARREST consortium, including publications at the popular press, online postings, circulation of printed material and participation in international scientific events. It is developed under task “T8.3: Dissemination plan and activities”.

Table of Contents

List of Tables

List of Figures

1 Introduction

The THREAT-ARREST consortium realizes that in order to achieve maximum impact on the society as well as the environment, it is of utmost importance to ensure the involvement of relevant stakeholder groups. To this end, THREAT-ARREST aims to raise awareness and engagement through a number of initiatives, including among others, pursuing synergies, organizing showcases, workshops and campaigns, as well as other communication and dissemination activities.

Thus, the content below includes a mapping of the project's partners to specific dissemination activities and responsibilities throughout the duration of the project. This guide towards dissemination strategy facilitates the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework, which constitutes one of the project's main objectives.

This deliverable (D8.2 – The THREAT-ARREST dissemination plan) is part of Work Package (WP) 8 which tackles the issues of the project's dissemination. The main contribution is the presentation of the partners' dissemination strategy and is the first outcome of task T8.3 (Dissemination plan and activities). The plan will be monitored throughout the project's lifetime and reported on in the related deliverables (D8.5 and D8.8).

The rest of the document is structured as follows: **Chapter 2** highlights the main dissemination plan devised for the duration of the project. **Chapter 3** details each partner's future plans regarding the dissemination activities. **Chapter 4** concludes and links the deliverable content with other related tasks/deliverables.

2 Dissemination plan

The purpose of THREAT-ARREST's dissemination efforts is to influence stakeholders' view, so that they will become aware of the project's new ideas, services and results, and ultimately adopt it. The following action items have been identified for the different partners:

- Academic partners will disseminate in the scientific community the research achievements obtained within the project (e.g. (Ferrera et al., 2018)). They will target very high-profile publication venues for the security, critical infrastructures and system engineering domains (e.g. (Hatzivasilis et al., 2018; Hatzivasilis et al., 2017a; Hatzivasilis et al., 2017b)). Academic partners will also incorporate the project results within their advanced educational activities. Integration of results in advanced studies is known to have the capability of filling the gap between classical technical disciplines and interdisciplinary socio-technical domains like energy, health and smart transport applications.
- Industrial partners will present the project results in industrial fairs, exhibitions and gatherings of decision makers, creating the opportunity for one-on-one, bilateral communication with key decision makers. Events will include major international forums for cyber security solution providers and consumers such as CYBERSEC (CYBERSEC 2018), ISF (ISF 2018), FIC (FIC 2017) and others.
- The consortium as a whole will support THREAT-ARREST's circle of continuous technical communication with the community through presence in social media groups (see Table 1) and on forums. These communications will be aimed at secondary targets and at increasing the general awareness.

Table 1 – Social media groups

Platform	URL
LinkedIn	https://www.linkedin.com/in/threat-arrest-706485175/
Facebook	https://www.facebook.com/Threat-Arrest-266454357324031/
Twitter	https://twitter.com/ArrestThreat
Google+	https://plus.google.com/u/0/115167926033743047032

Three categories of dissemination channels, listed in the following, will be 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 Online dissemination

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

Project website: The site is a key instrument for supporting the dissemination of the research results. We regard the Web site as a "second stop" useful to primary targets who have already been reached via the other channels. Its aim will be 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 will support championing THREAT-ARREST adoption. Key results will be published on the website, but also added–value services will be offered such as support in using THREAT-ARREST methodology. The project website [https://www.threat-arrest.eu/] was set up at a very early stage (M1) and is updated conscientiously and regularly. Figure 1 shows the website's homepage.

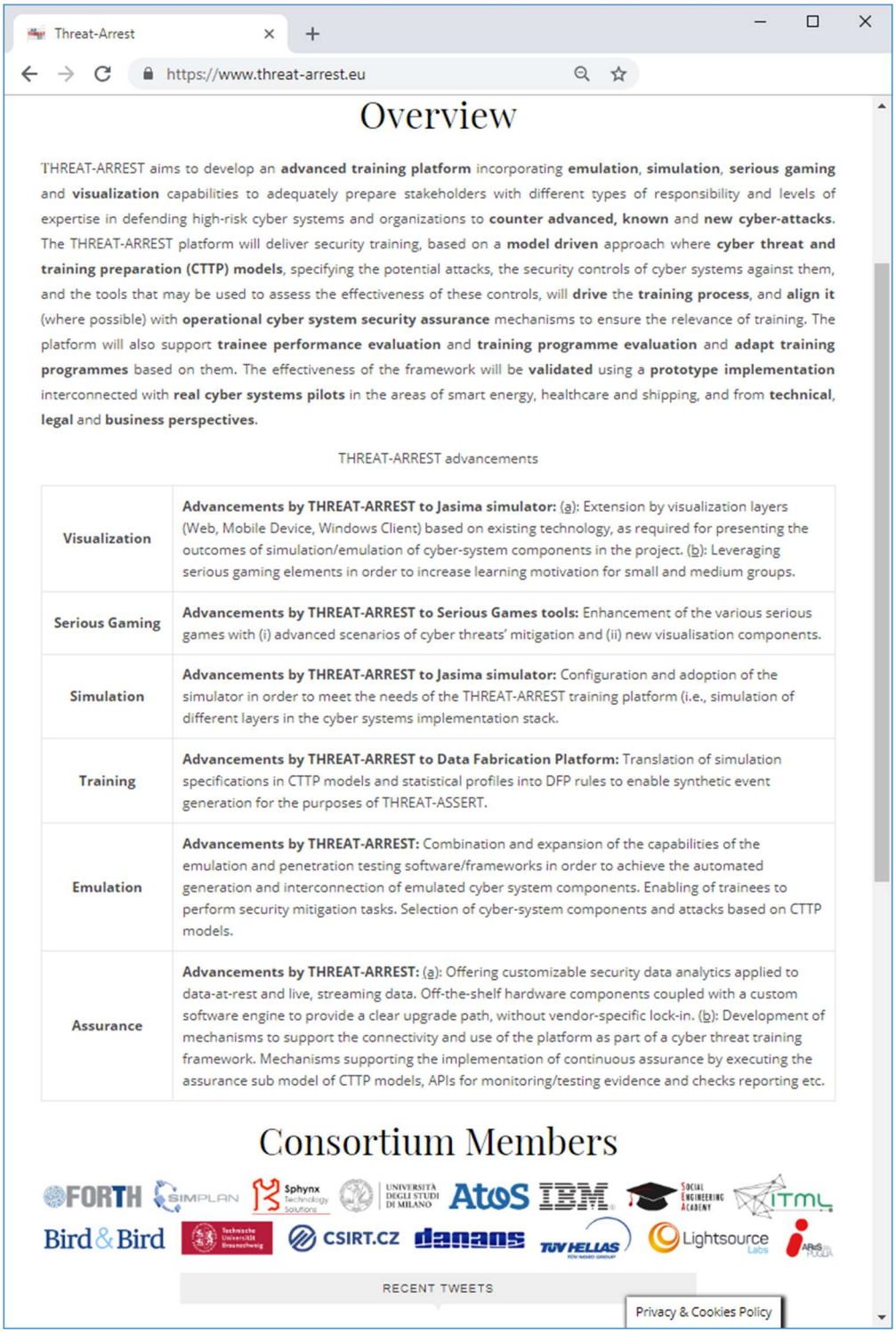


Figure 1 – Homepage of project's website

Push announcements: The project will be present on the major professional social networks, in particular LinkedIn and via a special interest group that will correspond to a THREAT-ARREST hashtag on Twitter. Contacts already available to project partners will be used to kick-start this group, which will be a major instrument for recruiting interested parties. THREAT-ARREST social community group and Twitter hashtag are the target for continuous informal communication with members, who will 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 will be sent out to interested parties outside the project partners including major stakeholders recruited via the other channels. The newsletter will rely on well balanced mix of dissemination and infotainment content. All partner organisations will contribute to the newsletter, which will be made available free of charge through electronic means.

Brochure: A THREAT-ARREST folder and brochure (see Appendix: The THREAT-ARREST brochure) was created and distributed in M3 and will be updated regularly. Distribution also includes a high–quality electronic version in portable document formats (e.g. PDF), which is downloadable from the website.

Technical videos: By M4, a preliminary THREAT-ARREST video will be developed, introducing the project's main aspects and objectives to the public. In 2019 when we will have more concrete technical results to showcase, a second video of estimated 5 minutes of duration will be produced, that will focus on the technical advancements of the THREAT-ARREST methodology and approach, targeting the technical and business community of IoT.

2.2 Scientific publications

THREAT-ARREST partners will carefully select their publication venues based on their scientific excellence and impact, privileging where possible open access. Potential conferences and journals that will be 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.

2.3 Organization of International Scientific Events

Organization of one conference: THREAT-ARREST will organize one significant international conference in the core research areas of the project. Our goal will be to enhance the visibility of our contributions at international level.

Organization of two workshops: THREAT-ARREST will organize a series of two international scientific workshops throughout its duration. Our plan is to hold the workshops in conjunction with one of the major international conferences identified above (e.g. ESORICS) in the next two years of the project (i.e. 2019, 2020). A possible title for the workshop series is

Holistic Cyber Systems Security (HCSS), although we are currently exploring other suggestions.

Organization of two 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. One Summer School is already scheduled to take place in 2019 (NIS'19, see Section 1.2.1) and our plan is to organize the remaining one closer to the end of the project, in order to be able to present more tangible technical results. We expect to attract at least 30 attendees in each one. To be cost effective these will be organized in the premises of academic partners.

2.4 System-level demonstrations

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 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 at least two demonstrations of the project technical results in major international conferences, such as IEEE ICC and IEEE GLOBECOM.

The following table provides a quantification of the project's dissemination activities, and sets a basis for verifying whether the project dissemination objectives have been met via Key Performance Indicators (KPIs). Furthermore, it provides an estimation of the achieved quantified activities per project phase.

Table 2 – Dissemination KPIs

Tool	Description	Success Indicators	Estimation
(i) Online dissemination			
Project website	Web access to deliverables, technical results and presentation materials of THREAT-ARREST	≥1.000 accesses annually ≥100 downloads	(Downloads) M1-18: ≤40 M19-36: ≥60
Push announcements	Regular push announcements through social media (Twitter, LinkedIn, ResearchGate)	≥50 announcements	M1-18: ≤20 M19-36: ≥30
Regular Newsletter	Regular quarterly newsletter with the technical activities of THREAT-ARREST	≥9 newsletters	M1-18: ≤3 M19-36: ≥6
Brochure	High–quality electronic brochure with the technical approach and activities of THREAT-ARREST	≥2.000 hard copies distribution in ≥ 10 events ≥2.000 downloads	(Downloads) M1-18: ≤800 M19-36: ≥1200
Technical videos	High-quality video presentations of the objectives and technical aspects of THREAT-ARREST	≥1000 views ≥ 10 event presentations	(Views) M1-18: ≤400 M19-36: ≥600
(ii) Scientific publications			
Journal publications	Publications in International referred technical journals in cyber security related subjects	≥10 publications	M1-18: ≤4 M19-36: ≥6
Magazine publications	Publications in International magazines in cyber security related subjects	≥10 publications	M1-18: ≤4 M19-36: ≥6
Conference publications	Publications in International referred technical conferences in cyber security related subjects	≥12	M1-18: ≤4 M19-36: ≥8

Special issues	Preparation of special issues in international referred technical journals and magazines	≥2 ≥10 selected papers/issue	(Papers) M1-18: ≤4 M19-36: ≥6
(iii) Organization of International Scientific Events			
Conference organizations	Organization of international conferences in cyber security related domains	≥1 events ≥100 attendees (each)	M1-36: ≥1
Workshops	Organization of workshops	2 workshops ≥30 attendees (each)	M1-18: ≥1 M19-36: ≤1
Summer schools	Organization of international summer schools in cyber security training and simulation	≥2 events ≥30 attendees (each)	M1-18: ≥1 M19-36: ≤1
(iv) System-level demonstrations			
Exhibition demonstrations	Major fairs and exhibitions such as Cyber Security Europe at IP EXPO Europe, INFOSEC	≥1 demos	M1-36: ≥1
EU demonstrations	Major EU events such as meetings and workshops organized by ENISA (ENISA 2018) and SANS information security courses' events (SANS Institute 2018)	≥2 demos	M1-18: ≥1 M19-36: ≤1
Conference demonstrations	Major conferences such as GLOBECOM, ICC	≥2 demos	M1-18: ≥1 M19-36: ≤1

3 Partners' involvement in the dissemination activities

In this chapter, we detail each partner's future plans regarding the dissemination activities including – but not limited to – publications in conferences / popular press, appearances in fairs / exhibitions and printed / online newsletter circulation.

3.1 Foundation for Research and Technology – Hellas (FORTH)

- TV-poster presentation during the 21st International Symposium on Research in Attacks, Intrusions and Defences (RAID2018 (RAID 2018))
    - More than 120 attendees participated
- Project dissemination by FORTH at the Researcher's Night 2019, Heraklion, Greece
    - Project banner
    - Individual stand for answering questions regarding the project.
- Organization of the 6th Network and Information Security (NIS'19) Summer School 2019 (collaboration between FORTH and ENISA)

3.2 SIMPLAN AG (SIMPLAN)

- Paper presentation at upcoming ASIM simulation conference(s) (2020 and / or 2021)
- Participation in upcoming LogiMAT Stuttgart fairs (2019, 2020, 2021)
- Participation in upcoming HMI Hannover fairs (2019, 2020, 2021)
- Participation in Transport Logistic Munich fair, 2019
- Update of customer newsletter with information on the project
- Update of company's website [https://www.simplan.de/en/] with information on the project

3.3 Sphynx Technology Solutions AG (STS)

- Plans to attend all project-driven dissemination and communication events (e.g. joint publications, conference special sessions, technology demonstrators)
    - Participated in the 5th Network and Information Security (NIS'18) Summer School 2018 Heraklion, Crete, organised by FORTH and ENISA.
- Paper presentations at upcoming conference(s)
- Article publications in academic journals
- Project demonstrations in academic & industry events
- Update of company's website [http://www.sphynx.ch/] with information on the project
- Publications as joint work with other THREAT-ARREST partners
    - Surveys on available training platforms
    - Surveys on assurance-driven service deployment

3.4 Università degli Studi di Milano (UMIL)

- Article in IEEE Transactions on Services Computing Journal
- Paper presentation at IEEE Computer Society Signature Conference on Computers, Software and Applications (COMPSAC) and federated workshops
- Paper presentation at upcoming IEEE Services federated conferences
- Organization of IEEE Services in Milan, July 2019
    - Expected audience for the whole conference: 400 attendees
- Organization of SAPSE workshop, 2019 (in conjunction with COMPSAC)
    - Expected audience for the whole conference: 500 attendees
- Presentation of project results to undergraduate students and researchers
- Master's program on Security for Computer Systems and Networks
    - System and Network Security course
    - Tools and developed platform tested and exploited for educational purposes
- Involvement in the International Research and Innovation Centre in Intelligent Digital Systems (IRIXYS) in collaboration with INSA Lyon and the University of Passau, at doctoral level
    - Focus on multimedia, data security as well as distributed and pervasive systems
    - IRIXYS can be target for high-level dissemination activities for project results

3.5 ATOS Spain S.A. (ATOS)

- Update of company's website [https://atos.net] – Atos Research & Innovation (ARI) section to reflect the activities of the project
- Issue of press releases at national and global level
- Promotion of latest news and achievements through social media channels
- Articles publication on the project outcomes in relevant press media, e.g.:
    - ERCIM News (ERCIM News 2016)
    - Research.eu (Research*EU 2018)
- Participation in events of different levels, including industry events and conferences, to disseminate and promote the THREAT-ARREST project, e.g.:
    - The annual ICT conference (ICT 2018)
    - The XII International Industrial Cybersecurity Congress in Europe
    - The 7th ENISA/EC3 Workshop (EC3 Workshop 2018)
    - ASLAN2019 (ASLAN 2018)
- Collaboration with other EC-funded projects related to the field of cyber range, such as CYBERWISER.EU (CYBERWISER 2018)

3.6 IBM Israel – Science and Technology LTD (IBM)

- Active participation in all the project-dedicated workshops and presentation of technical contributions to the audience
- Active participation in the demo sessions of relevant industry events and scientific conferences during and after the project
- Publication of the project's progress and results in the IBM newsletters (at least in two releases)
- Publication of IBM's public deliverables, data, results and white papers on the project website
- Update of the project's social media channels (blogs, Twitter account, etc.) with IBM's progress and results during the project.
- Posts on the social media channels of all relevant IBM's communication, exploitation and dissemination activities
- Publication of the project's info and results in Israelian security-related forums (e.g. CyberTech) and IBM internal security seminars.

3.7 Social Engineering Academy GMBH (SEA)

- Paper presentation at upcoming conference(s)
- Product exhibition at upcoming fairs/forums
- Newsletter circulation
- Update of company's website with information on the project

3.8 Information Technology for Market Leadership (ITML)

- Paper presentation at upcoming ICT conference(s)
- Participation in ICT events
- Participation in the European Big Data Value Association (BDVA) Forum, 2018

3.9 Bird & Bird LLP (B&B)

- Participation in relevant events dealing with disruptive technologies, with a focus on cyber-security
- Articles publication in journals and magazines, about the relevant legal issues that may arise in the context of the THREAT-ARREST project
- Participation in international legal conferences
- Leverage and re-use (to the extent possible) of the legal analyses performed in the context of THREAT-ARREST
- Publication and dissemination – as much as possible – of the deliverables with the aim of boosting visibility and assisting international clients with their specific compliance issues and programmes

- Dissemination of the project results through social media
- Update of company's website [https://www.twobirds.com/] with press releases and news about the project
    - One press release already published (Bird & Bird 2018)

3.10 Technische Universität Braunschweig (TUBS)

- Already presented paper: 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
- Paper presentation: Mohammad Hamad, Mustafa R. Agha and Vassilis Prevelakis, **"ProSEV: Proxy-Based Secure and Efficient Vehicular Communication"** in *IEEE Vehicular Networking Conference (VNC)*, December 2018
- Paper presentation at upcoming conference(s)
- Relevant articles in computer systems security journals
- Collaboration with other THREAT-ARREST partners for publications
- Newsletter preparation, editing and circulation
- Creation and distribution of a brochure/leaflet presenting the technical approach and activities of the project
- Production and release of a promotional video presenting the technical aspects of the project
- Participation in HiPEAC conference, 2019
    - **"Security of mixed criticality components in the vehicle"**, Invited talk by prof. Vassilis Prevelakis, in the *7th International Workshop on Mixed Criticality Systems (MCS) – Safe and secure embedded performance computing for industrial, intelligent and autonomous applications*
    - Submitted paper (awaiting response): Mohammad Hamad, Marinos Tsantekidis, Vassilis Prevelakis, **"Intrusion Response System for Vehicles – Challenges and Solutions"**, *CS2: Workshop on Cryptography and Security in Computing Systems*
    - Poster presentation
    - Brochure/leaflet distribution
- Submitted paper: Mohammad Hamad, Marinos Tsantekidis, Vassilis Prevelakis, **"Red–Zone: Towards an Intrusion Response Framework for Vehicles"**, *5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS)*
- Update of the workgroup's website with news of participating in the project [https://www.ida.ing.tu-bs.de/en/research/projects/embedded-security/#projects]
- Publication of a chapter called **"Security for Heterogeneous Systems"** in a book titled **"Heterogeneous Computing Architectures: Challenges and Vision"**
- Presentation of project results in the graduate seminar program

- Discussions on the project in the course on Hot Topics in Security

3.11 CZ.NIC, ZSPO (CZNIC)

- Presentations at upcoming events(s)
- Participation in the 6th Network and Information Security (NIS'19) Summer School 2019, which will be organized by FORTH and ENISA.

3.12 Danaos Shipping Company Limited (DANAOS)

- Article in Scientific Journal of Hellenic Operation Research Society (HELORS)
- Relevant articles in maritime / technology journals
- Paper presentation at Hellenic Operational Research Society Conference, 2019
- Paper presentation at Digital Ship Conference, 2019
- Participation in POSIDONIA Maritime Exhibition, 2020
    - Statistics from 2018 (Posidonia 2018)
        - More than 2.000 exhibiting companies
        - More than 20.000 visitors
- Hosting of Danaos user meetings
    - 500 visitors from the maritime industry users of Danaos ERP
- Showcase of Danaos EU research projects in maritime industry event
    - Planned for early 2019
    - Expected attendees: 150-200
- Planned educational activities based on the THREAT-ARREST maritime pilot framework, since Danaos is one of the three use-case providers
- Newsfeed/feedback for THREAT-ARREST in printed and online newsletters for both Danaos shipping and Danaos Research Centre
- Dissemination of project results to more than 1000 subscribed platform members of DanaosOne [https://www.danaos1.com] collaborative platform
- Regular updates to the newsfeed of Danaos Shipping [https://www.danaosshipping.gr/] and Danaos Research Center [https://web2.danaos.gr/research/] websites

3.13 TUV HELLAS TUV NORD S.A. (TUV)

- Posting of a full presentation/scope of THREAT ARREST in TUV NORD's "Internord" Magazine
    - Four editions per year
    - 15,000 copies, circulated all over the World, to both TUV NORD employees as well as many Industrial/Market Partners
    - Flexible time/period of posting (2019 and/or 2020)

- Posting related to THREAT-ARREST in TUV NORD's International Newsletter (monthly)
    - Flexible time/period of posting (2019 and/or 2020)
- Posting of THREAT-ARREST on TUV NORD & TUV HELLAS websites and corporate social media
- Participation (as part of a TUV NORD – TUViT participation) in at least two major industrial exhibitions/fairs related to the THREAT-ARREST's scope (Cybersecurity/ Industrial Security etc.)

3.14 LIGHTSOURCE LAB LTD (LSE)

- Plans to attend all project-driven dissemination and communication events (e.g. joint publications, conference special sessions, technology demonstrators)
- Paper presentations at upcoming conference(s)
- Project demonstrations in industry events
- Update of company's website with information on the project (due to the rebranding of the company, no decision on the domain name has been made yet)
- Publications as joint work with other THREAT-ARREST partners
- Product exhibition in upcoming fairs/forums

3.15 Agenzia Regionale Strategica per la Salute ed il Sociale (ARESS)

- Update of AReSS's website [https://www.sanita.puglia.it/web/aress/] – Programs & Projects section to reflect the activities of the project
- Event presentation of THREAT-ARREST project to public and private stakeholders
- Publication of specific Guidelines for ASL (Local Health Authority) in Puglia Region
- Presentation of project results in the Master post Lauream of the health professionals and in the internal seminars
- Poster presentation in annual Health Forum Risk Management in Florence
- Dissemination of the final report between the ASL (Local Health Authority) in Puglia Region
- Articles publication in journals and magazines, about the relevant cyber-security issues in the health sector that may arise in the context of the THREAT-ARREST project
- Dissemination of the project results through social media

4 Conclusion

To ensure broad recognition and dissemination of THREAT-ARREST's activities and results, we have compiled and presented here a concrete strategy to make the project known to various interested parties from several domains. Digital content – including push notifications, a technical video and a newsletter – will be pushed through the project's website as well as its social media accounts. A printed brochure detailing several aspects of the project will be distributed in a number of venues and will also be offered in electronic format for downloading from the website. Articles and research papers will be published on major scientific conferences, journals and magazines. Furthermore, the consortium will be responsible for organizing international scientific events, as well as system-level demonstrations at relevant events. Each of the partners will undergo and participate in specific planned activities, aiming to promote their part in the project as well as the whole project's agenda at a diverse set of venues and stakeholders. The progress of these activities will be monitored throughout the project's lifetime and reported on in the related deliverables (D8.5 and D8.8).

5 References

[1] CYBERSEC 2018, "CYBERSEC Forum". Available from: <https://cybersecforum.eu/en/> [28 November 2018]

[2] Ferrera, E., et al., 2018. IoT European Security and Privacy Projects: Integration, Architectures and Interoperability. CRIStin – SINTEF, Next Generation Internet of Things. Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation. Book Chapter 7, pp. 207-292.

[3] Hatzivasilis, G., et al., 2018. The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel IIoT Protocol, evaluated on a Wind Park's SDN/NFV-enabled 5G Industrial Network. Computer Communications – Special Issue on Energy-aware Design for Sustainable 5G Networks, Elsevier, vol. 119, pp. 127-137.

[4] Hatzivasilis, G., et al., 2017a. SCOTRES: Secure Routing for IoT and CPS. IEEE Internet of Things Journal (IoT), IEEE, vol. 4, issue 6, pp. 2129-2141.

[5] Hatzivasilis, G., et al., 2017b. AmbISPDM: Managing Embedded Systems in Ambient Environment and Disaster Mitigation Planning. Applied Intelligence, Springer, vol. 48, issue 6, pp. 1623-1643.

[6] ISF 2018, "Information Security Forum". Available from: <https://www.securityforum.org> [28 November 2018]

[7] FIC 2017, "International Cybersecurity Forum". Available from: <http://www.cybersecurity-review.com/international-cybersecurity-forum-fic-2017/> [28 November 2018]

[8] ENISA 2018, "European Union Agency for Network and Information Security". Available from: <https://www.enisa.europa.eu/events> [28 November 2018]

[9] SANS Institute 2018, "Information Security Training". Available from: <https://www.sans.org/security-training/by-location/all> [28 November 2018]

[10] RAID 2018, "The 21st International Symposium on Research in Attacks, Intrusions and Defenses". Available from: <www.raid2018.org> [28 November 2018]

[11] ERCIM News 2016. Available from: <https://ercim-news.ercim.eu/call> [28 November 2018]

[12] Research*EU 2018, "Research*eu magazines | CORDIS | European Commission". Available from: <https://cordis.europa.eu/research-eu/home_en.html> [28 November 2018]

[13] ICT 2018. "ICT 2018: Imagine Digital - Connect Europe". Available from: <https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe> [28 November 2018]

[14] EC3 Workshop 2018, "7th ENISA/EC3 Workshop". Available from: <https://www.enisa.europa.eu/events/7th-enisa-ec3-workshop/7th-enisa-ec3-workshop> [28 November 2018]

[15] ASLAN 2018, "Asociación @asLAN - Tecnologías para acelerar la Transformación". Available from: <https://aslan.es> [28 November 2018]

[16] CYBERWISER 2018, "CYBERWISER.eu | Cyber Range & Capacity Building in Cybersecurity". Available from: <https://cyberwiser.eu/> [28 November 2018]

[17] Bird & Bird 2018, "Bird & Bird participates in EU Cybersecurity project THREAT-ARREST". Available from: <https://www.twobirds.com/en/news/press-releases/2018/uk/bird-and-bird-participates-in-eu-cybersecurity-project-threat-arrest> [28 November 2018]

[18] Posidonia 2018, "The International Shipping Exhibition - Facts and Figures 2018". Available from: <http://posidonia-events.com/pages/facts-and-figures-2018/> [28 November 2018]

Appendix: The THREAT-ARREST brochure

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

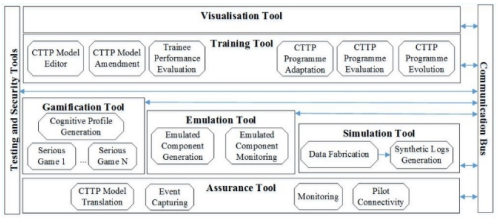
OBJECTIVES

- 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 these 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

THREAT-ARREST aims 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**.

ENVISAGED PLATFORM AND PROJECT ENHANCEMENTS



Visualisation

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

Serious Gaming

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

Simulation

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

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

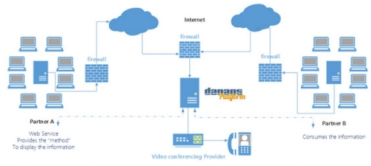
Emulation tools: The emulation platform provides the automated generation of emulated cyber-system components, in the form of interconnected virtual machines equipped with the appropriate software stack, as well as their interconnections in Physical and/or Software Architecture Layers (PAL/SAL) of a 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.

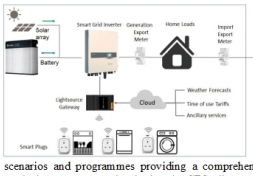
THREAT-ARREST APPLICATIONS

Smart Shipping Management



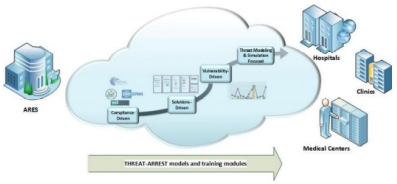
This pilot envisions to validate the THREAT-ARREST platform and provide feedback in regards to its effectiveness in the shipping industry. A system of this kind involves (i) multiple types of data and (ii) numerous stakeholders, which results in it being considered as a significantly high-risk ICT system. 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.

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
Start Date: 2018-09-01
Duration: 36 months
Project Cost: €6,431,125
Project Coordinator: FORTH

MORE INFORMATION
Web: https://www.threat-arrest.eu/
Twitter: https://twitter.com/ArrestThreat
Facebook:
Email: Sotiris Ioannidis, sotiris@ics.forth.gr