Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things

Newsletter Vol. 1— November 2019

Welcome to our 1rst issue of CYBER-TRUST Newsletter. The project newsletters will keep you regularly updated with the progress of our project and the news that relate to it.

Table of Contents

We will regularly keep you updated with the most recent news about the status of the project.. Moreover, we kindly invite you to also regularly consult our website: http://cyber-trust.eu

We are happy to invite you to follow our activities with this newsletter and we are looking forward to your feedback.

Yours sincerely,

The CYBER-TRUST consortium

Project quick info

Start date: 2018-05-01
End date: 2021-04-30
Duration: 36 Months
Reference:
GA n° 786698
Budget: 2.998.182,50 €
Funding:2.998.182,50 €
H2020-DS-SC7-2017

Contacts

Project coordinator:
Dimitris Kavallieros
email: d.kavallieros@kemea-research.gr

Technical coordinator:
Nicholas Kolokotronis
email: nkolok@uop.gr

Learn more about our project, follow us and get involved:

- https://cyber-trust.eu/
- ✉ d.kavallieros@kemea-research.gr
- https://www.linkedin.com/groups/13627755/
- https://www.facebook.com/cybertrust/
- https://twitter.com/CyberTrustEU

This project has received funding from the European Union’s Horizon 2020 research and innovation program.

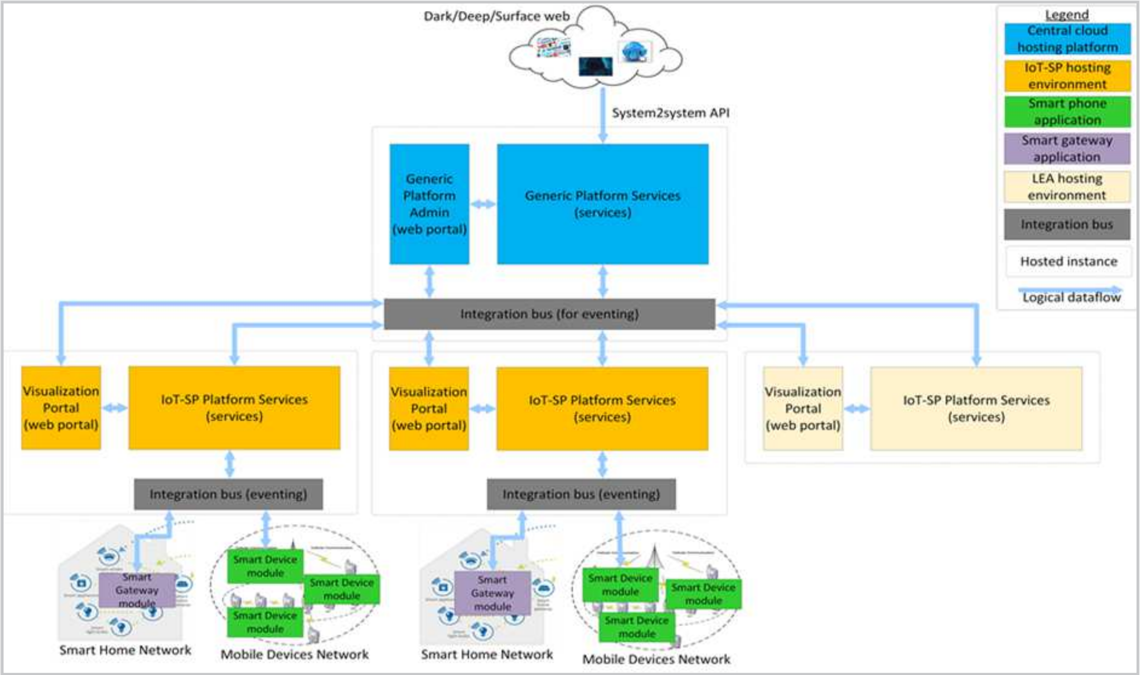
About the Cyber-Trust project

Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things is a 36-month long research project in the Digital Security Focus Area, co-funded by the Horizon 2020 Framework Programme of the European Union, under the Grant Agreement no. 786698. Its principal goal is to revolutionise the way cyber-security systems are built and operate. By establishing an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, by performing high-quality interdisciplinary research in key areas, the Cyber-Trust project aims to develop novel technologies and concepts to tackle the grand challenges towards securing the ecosystem of IoT devices. The high-level project objectives, which summarize the specific challenges of the work programme are:

Create a new paradigm for the NG cyber-security defense systems.
Quickly detect and effectively respond to sophisticated cyber-attacks.
Deliver advanced solutions for collecting forensic information.
Minimize impact on sensitive data protection and user's privacy.

During the first phase of the project life, emerging trends in cyber-attacks have been identified to guide the definition of use case scenarios, collection of the end-user requirements, the regulatory framework is being analysed and the impact of the proposed methods to fundamental rights, data protection and privacy is being assessed. Currently, the project is in the second phase, which is the Platform design. In this phase, the Cyber-Trust platform reference architecture is created, incorporating inputs from the first phase, translated into technological tools to be built in Phase 3 of the project life.

The main outputs of this phase are the platform's prototype, verifying the milestone Mi2 (Cyber-Trust rapid prototype), and its final specifications at the end of the phase, which are associated with milestone Mi3 (Cyber-Trust architecture and design specifications).


Dark/Deep/Surface web
System2system API
Generic Platform Admin (web portal)
Generic Platform Services (services)
Integration bus (for eventing)
Visualization Portal (web portal)
IoT-SP Platform Services (services)
Visualization Portal (web portal)
IoT-SP Platform Services (services)
Visualization Portal (web portal)
IoT-SP Platform Services (services)
Integration bus (eventing)
Integration bus (eventing)
Smart Gateway module
Smart Device module
Smart Device module
Smart Device module
Smart Home Network
Mobile Devices Network
Smart Gateway module
Smart Device module
Smart Device module
Smart Device module
Smart Home Network
Mobile Devices Network
Legend
Central cloud hosting platform
IoT-SP hosting environment
Smart phone application
Smart gateway application
LEA hosting environment
Integration bus
Hosted instance
Logical dataflow

Cyber-trust Run-time Solution Overview

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Academic Publications

We have now published 19 research work papers!

The research undertaken in the Cyber-Trust project has already led to 19 research publications, of which 16 were accepted and presented in peer-reviewed international conferences and three in peer-reviewed journals. The research work papers are developed to help advance the knowledge base that underpins the formulation and implementation of relevant policies in Europe, and to engage with relevant communities, stakeholders and practitioners in the research, again with the aim of supporting relevant policies and providing a clear view of the project results. All research papers are available on publishers' websites and most of them have an e-print copy that is available as open access in the "arXiv" repository.

Our research papers include:

1. Grammatikakis, K. P., Ioannou, A., Shiaeles, S., & Kolokotronis, N. (2018, August). WiP: Are Cracked Applications Really Free? An Empirical Analysis on Android Devices. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 730-735). IEEE. DOI: https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00127,arXiv: https://arxiv.org/abs/1903.04793.
2. Bendiab, K., Kolokotronis, N., Shiaeles, S., & Boucherkha, S. (2018, August). WiP: A Novel Blockchain -Based Trust Model for Cloud Identity Management. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*(pp. 724-729). IEEE. DOI: https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126, arXiv: https://arxiv.org/abs/1903.04767
3. Ali., M., Shiaeles, S., Ghita, B., Papadaki, M., Agent-based Vs Agent-less Sandbox for Dynamic Behavioral Analysis, 2018 Global Information Infrastructure and Networking Symposium (GIIS), GIIS2018, IEEE DOI: https://doi.org/10.1109/GIIS.2018.8635598, arXiv: https://arxiv.org/abs/1904.02100.
4. Siracusano, M., Shiaeles, S., Ghita, B., Detection of LDDoS Attacks Based on TCP Connection Parameters, 2018 Global Information Infrastructure and Networking Symposium (GIIS), GIIS2018, IEEE DOI: https://doi.org/10.1109/GIIS.2018.8635701, arXiv: https://arxiv.org/abs/1904.01508.
5. Gkotsopoulou, O., Charalambous, E., Limniotis, K., Quinn, P., Kavallieros, D., Sargsyan, G., Shiaeles, S., Kolokotronis, N.,Data Protection by Design for Cybersecurity Systems in a Smart Home Environment, In *2019 IEEE 1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft)*, Paris,France, June 24-28,2019 IEEE. DOI: TBA. , arXiv: https://arxiv.org/abs/1903.10778
6. Baptista, I., Shiaeles, S., Kolokotronis, N., A Novel Malware Detection System Based On Machine Learning and Binary Visualization, In * 2019 1st International Workshop on Data Driven Intelligence for Networks and Systems (DDINS)*, Shanghai,China, May 20-24,2019, IEEE, DOI: TBA, arXiv: https://arxiv.org/abs/1904.00859.
7. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., Pavue, C., Blockchain Solutions for Forensic Evidence Preservation in IoT Environments, In * 2019 1st International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft), Paris, France, June 24-28,2019, IEEE, arXiv: https://arxiv.org/abs/1903.10770 .
8. Vassilakis, C., Blockchain technologies for leveraging security and privacy, In * 2019 Homo Virtualis 2, no. 1, pp.7-Special issue "Blockchain and disruptive technologies: Interdisciplinary perspectives", ISSN: 2585-3899, March 2019, Homo Virtualis, DOI: 10.12681/homvir.20188.

This project has received funding from the European Union's Horizon 2020 research and innovation program.

9. Kolokotronis, N., Limniotis, K., Shiaeles, S., Griffiths, R., Secured by Blockchain: Safeguarding Internet of Things Devices, In *2019 IEEE Consumer Electronics Magazine, vol.8, N.3, pp.28-34, May, 2019,IEEE,
DOI: https://doi.org/10.1109/MCE.2019.2892221 , arXiv: https://arxiv.org/abs/1903.04794 .

10. Constantinides, C., Shiaeles, S., Ghita, B., & Kolokotronis, N., (2019), A Novel Online Incremental Learning Intrusion Prevention System, In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE. DOI: TBA., arXiv: TBA.

11. Robert Shire, Stavros Shiaeles, Keltoum Bendiab, Bogdan Ghita, Nicholas Kolokotronis. "Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation". In : *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer, Cham, 2019. p. 65-76. DOI https://doi.org/10.1007/978-3-030-30859-9_6.

12. Aimilia Panagiotou, Bogdan Ghita, Stavros Shiaeles, Keltoum Bendiab. FaceWallGraph: Using Machine Learning for Profiling User Behaviour from Facebook Wall. In : *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer, Cham, 2019. p. 125-134. DOI https://doi.org/10.1007/978-3-030-30859-9_11.

13. Stavros Shiaeles ; Nicholas Kolokotronis ; Emanuele Bellini. "IoT vulnerability data crawling and analysis. In : *2019 IEEE World Congress on Services (SERVICES)"*. IEEE, 2019. p. 78-83. *DOI:* 10.1109/SERVICES.2019.00028.

14. Nicholas Kolokotronis ; Sotirios Brotsis ; Georgios Germanos ; Costas Vassilakis ; Stavros Shiaeles. On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection. In : *2019 IEEE World Congress on Services (SERVICES)*. IEEE, 2019. p. 21-28. DOI: 10.1109/SERVICES.2019.00019.

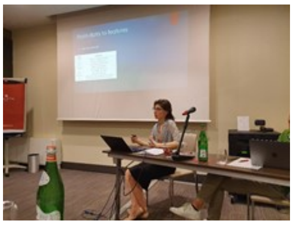
15. aris Koloveas ; Thanasis Chantzios ; Christos Tryfonopoulos ; Spiros Skiadopoulos. "A crawler architecture for harvesting the clear, social, and dark web for IoT-related cyber-threat intelligence". In : *2019 IEEE World Congress on Services (SERVICES)*. IEEE, 2019. p. 3-8. DOI: 10.1109/SERVICES.2019.00016.

16. Thanasis Chantzios, Paris Koloveas, Spiros Skiadopoulos, Nicholas Kolokotronis, Christos Tryfonopoulos, Vassiliki-Georgia Bilali, Dimitris Kavallieros. The quest for the appropriate cyber-threat intelligence sharing platform.

17. Muhammad Ali , Stavros Shiaeles, Nathan Clarke, Dimitrios Kontogeorgis. A proactive malicious software identification approach for digital forensic examiners. *Journal of Information Security and Applications*, 2019, vol. 47, p. 139-155. DOI: https://doi.org/10.1016/j.jisa.2019.04.013.

18. SARGSYAN, Gohar, CASTELLON, Nicolas, BINNENDIJK, Raymond, et al. Blockchain Security by Design Framework for Trust and Adoption in IoT Environment. In: 2019 IEEE World Congress on Services (SERVICES). IEEE, 2019. p. 15-20. DOI: 10.1109/SERVICES.2019.00018.

19. Bellini, E., Bagnoli, F., Ganin, A. A., & Linkov, I. (2019, July). Cyber Resilience in IoT network: Methodology and example of assessment through epidemic spreading approach. In 2019 IEEE World Congress on Services (SERVICES) (Vol. 2642, pp. 72-77). IEEE. DOI: 10.1109/



This project has received funding from the European Union’s Horizon 2020 research and innovation program.

Other Publications

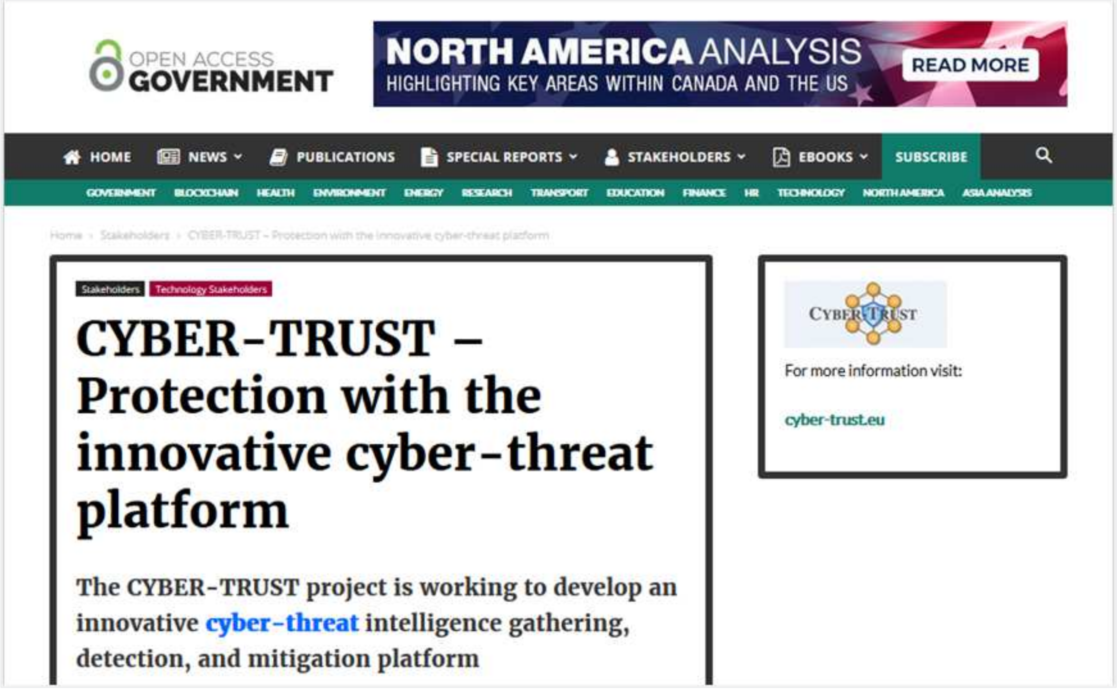
Partners from CSCAN and UOP have been published several articles that promote the Cyber-Trust project in the renowned magazine "Open Access Government". This magazine is a Google News Approved website that has a wide audience across the public and private sectors, including the Research / Innovation. The Open Access Government magazine has a wide audience across the public and private sectors, including the Research / Innovation and the local and central government sector. The magazine has more than 400, 000 participants from different public and private sectors, with more than 70,000 participants from the Research/ Innovation sector. Open Access Government main publication gets distributed quarterly to over 100 000 key individuals, such as MEPs, EU commissioners, Government, Academic and Business leaders. Also, the website receives an average of 25 000 visits weekly.

The Open Access Government publications include:

1. **CYBER-TRUST – Protection with the innovative cyber-threat platform:**

   This article promotes the Cyber-Trust project through the "Technology Stakeholders" rubric of the Open Access Government website. It provides an overview of the Cyber-Trust project, the involved partners and the scientific publication in Conferences and Journals done in the first year of the project life.

   Link to the article: https://www.openaccessgovernment.org/cyber-trust/67800/



CYBER-TRUST – Protection with the innovative cyber-threat platform

The CYBER-TRUST project is working to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform

2. **Cyber-Trust: Safeguarding IoT and building trust through blockchain**

   Cyber-Trust partners from CSCAN and UOP have been published an article entitled "Cyber-Trust: Safeguarding IoT and building trust through blockchain" in the Open Access Government Magazine issue of July 2019 (Pages 432-433). The article presents an overview of the current security issues and vulnerabilities raised form IoT devices with flawed design or poor configuration. In order to overcome these drawbacks, the blockchain is presented as a pertinent technology to help stakeholders to better protect their assets against large-scale advanced cyber-attacks.

   Link to the article in Open Access Government Magazine issue of July 2019 (Pages 432-433):

   https://www.openaccessgovernment.org/open-access-government-july-2019/67940/

OPEN ACCESS GOVERNMENT
ISSN 2516-3817 • July 2019
302
BUILDING A SUSTAINABLE FUTURE FROM OUR OCEANS
IN THIS ISSUE

PROFILE

Cyber-Trust: Safeguarding IoT and building trust through blockchain

Dr Stavros Shiaeles, University of Plymouth and Dr Nicholas Kolokotronis, University of Peloponnese discuss how Cyber-Trust is being used to Safeguard Internet of Things (IoT)

PROFILE

3. **Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework:**

   Cyber-Trust partners from CSCAN and UOP have been published an article entitled "Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework" in the Open Access Government. The article presents an overview of the current security issues and vulnerabilities raised form IoT. The article presents an overview of the current security issues and vulnerabilities raised form IoT devices and the importance of intelligent intrusion response systems (iIRS) in enhancing the capability of intrusion detection systems to respond to advanced cyber-attacks. The article highlights the benefit of combining ML-based intrusion detection systems (IDS) and GCSMs (Graphical cyber security models) for iIRS.

   Link to the article: https://www.openaccessgovernment.org/advanced-cyber-attacks/73967/

Effective response and mitigation of advanced cyber-attacks via an intelligent cyber-defence framework

September 24, 2019

© Anergule |

Dr Nicholas Kolokotronis from the University of Peloponnese and Dr Stavros Shiaeles, School of Computing, Faculty of Technology at the University of Portsmouth, impart their expert thoughts on effective response and mitigation of advanced cyber-attacks via an intelligent cyber–defence framework

Both authors have received funding from the EU's Horizon 2020, under grant agreement 786698.

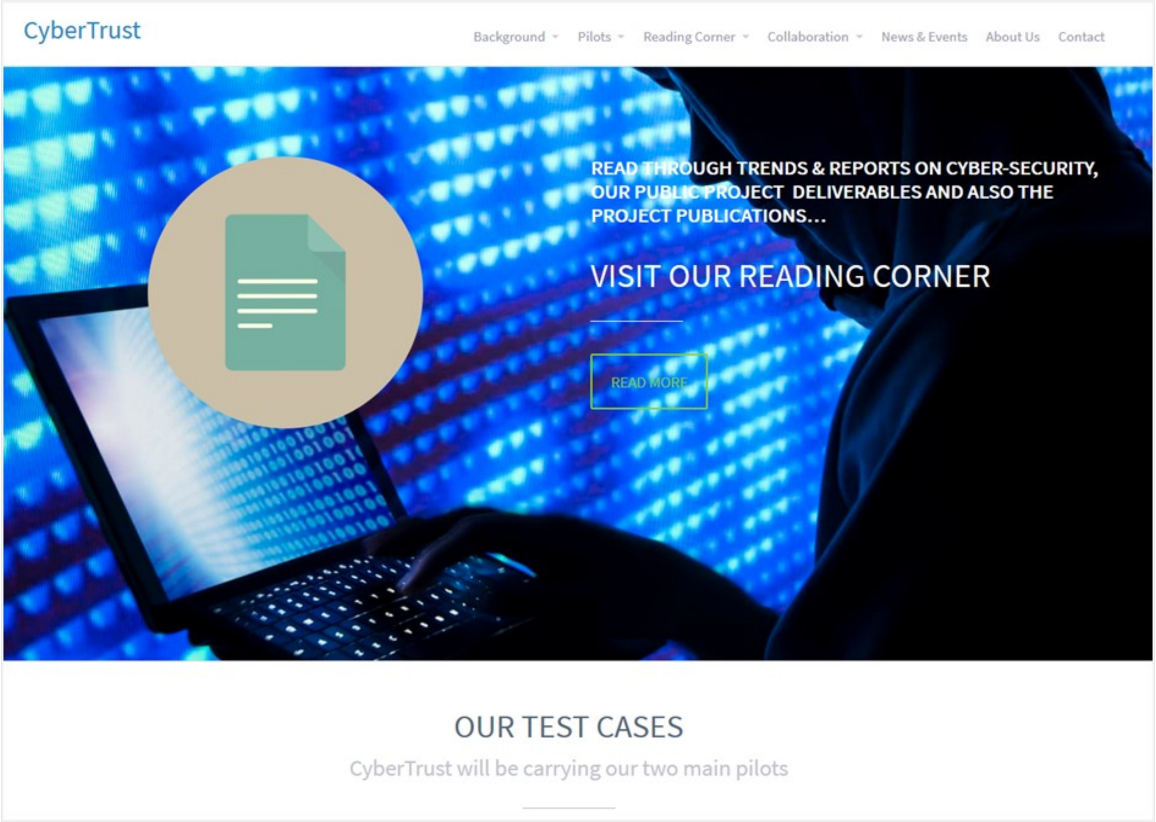
Website and blogs

Website

The project's website was created to inform the stakeholders on the latest developments in Cyber-Trust project, its progress and generate interest of all the related communities with the exciting news in the research progress of the project. The website has been officially released since the end of August 2018, meaning that it has been online for 14 months. IT hosts blog and news pages where the consortium can share ideas and report technological achievements as they arise in the project; it is open to individual entities to allow active participation. The monitoring of website usage and traffic is accomplished with the free Google Analytics service. The web traffic statistics show that the website is currently attracting a significant number of visitors and in total 1500 users have visited the Cyber-Trust website with a total of 4157page views.

Additionally, on an average visit, the user visits approximately 2 pages with a visit of 1 minutes and 36 seconds. So far, the project website has gathered most visitation from Europe with most traffic occurring midday onwards between Wednesdays and Fridays. The top three countries are Greece (45%), Cyprus (39%) and UK (14%) and occupy 98% of visitation.

Link to the website: https://cyber-trust.eu/.



READ THROUGH TRENDS & REPORTS ON CYBER-SECURITY, OUR PUBLIC PROJECT DELIVERABLES AND ALSO THE PROJECT PUBLICATIONS...

VISIT OUR READING CORNER

OUR TEST CASES

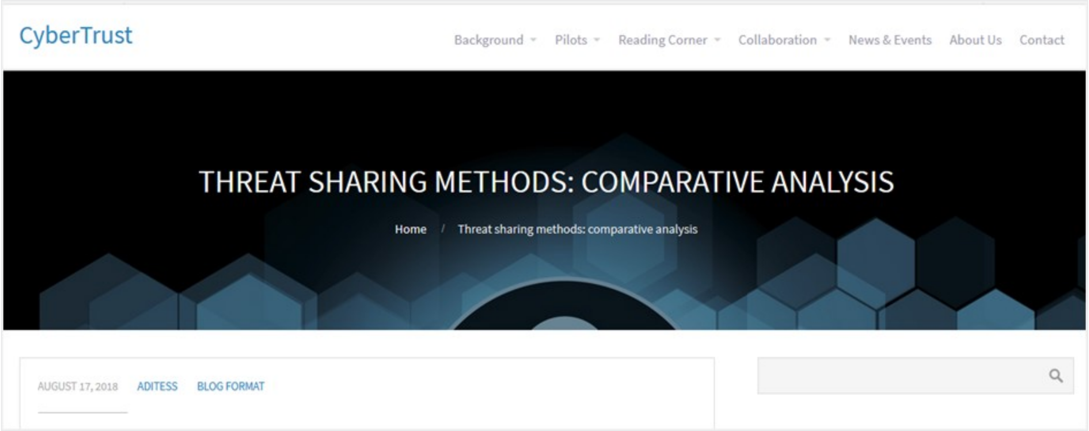
CyberTrust will be carrying our two main pilots

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Blog Post: “Threat sharing methods: comparative analysis”

A blog post has been added on our website on August 17, 2018. The blog provides an overview on the importance of Threat Intelligence in helping organization identify, assess, monitor, and respond to cyber threats. This is also the preamble of the work that will follow in work package 5 (Key proactive technologies and cyber-threat intelligence) of the Cyber-trust project.

Link to the full article: https://cyber-trust.eu/2018/08/17/threat-sharing-methods-comparative-analysis/



THREAT SHARING METHODS: COMPARATIVE ANALYSIS

Home / Threat sharing methods: comparative analysis

AUGUST 17, 2018 ADITESS BLOG FORMAT

Social media

Communication of Cyber-Trust activities and outcomes to the social media are performed through its Facebook Page and Twitter account and LinkedIn. Social media accounts have been set up with the aim to communicate a simplified presentation of the core activities of Cyber-Trust to general public. Overall, project social media accounts have a following of 28 members on LinkedIn, 53 followers on Twitter and 50 followers on Facebook.

Twitter

The twitter profile has gathered approximately 5K impression over the so far spanned period with the months of May and September 2019 gaining most interest.

Link to the twitter account: https://twitter.com/CyberTrustEU

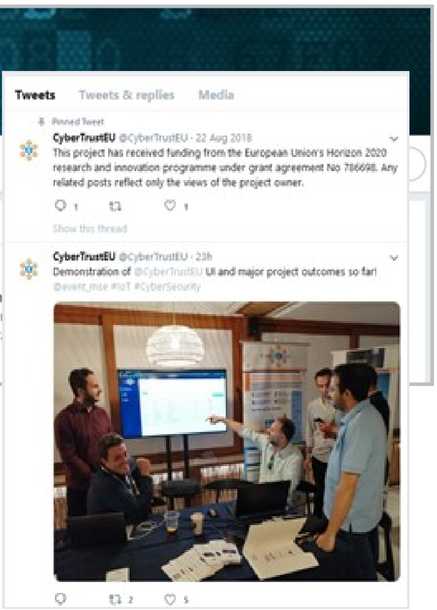
CyberTrustEU
@CyberTrustEU

This project receives funding from the @EU_H2020 Research & Innovation Programme. Any related tweets reflect only the views of the project owner. #CyberTrust

Pinned Tweet

CyberTrustEU @CyberTrustEU · 22 Aug 2018

This project has received funding from the European Un research and innovation programme under grant agree related posts reflect only the views of the project owner.



Pinned Tweet

CyberTrustEU @CyberTrustEU · 22 Aug 2018

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. Any related posts reflect only the views of the project owner.

Show this thread

CyberTrustEU @CyberTrustEU · 23h

Demonstration of @CyberTrustEU UI and major project outcomes so far! @event_mse #IoT #CyberSecurity

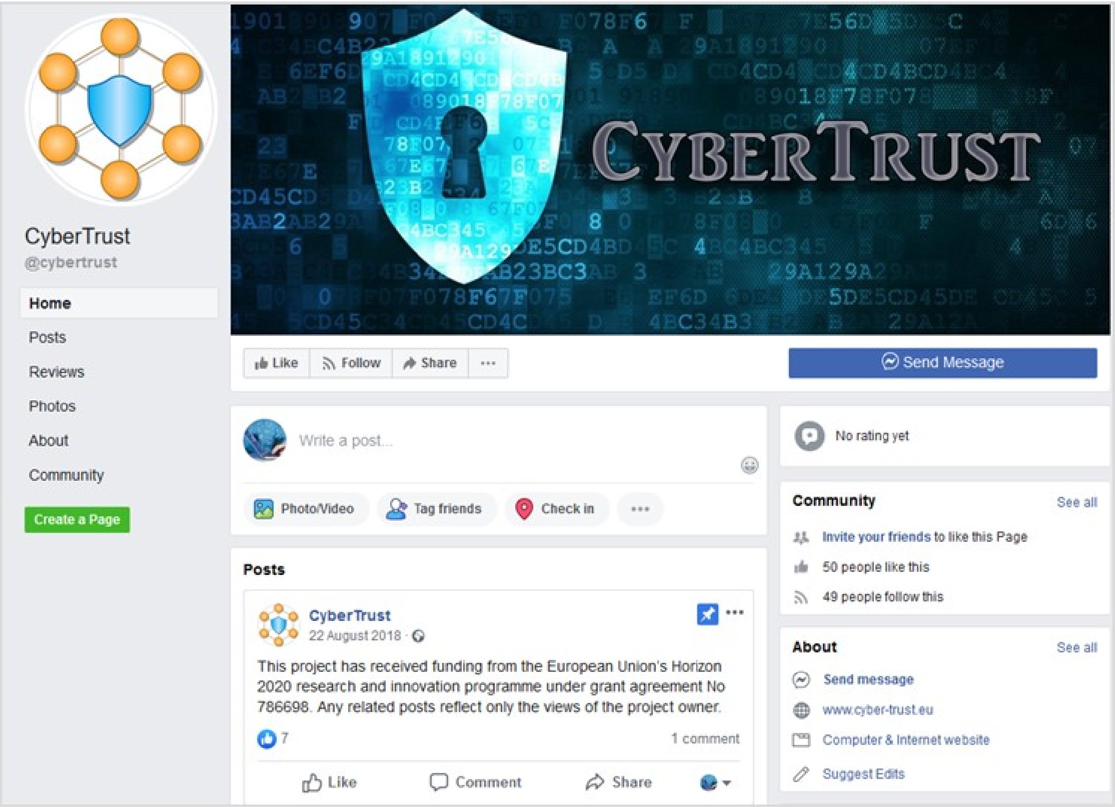
Month	Tweet Impressions	Engagements
Apr 2019	2.0K	13
Mar 2019	2.1K	15
Feb 2019	1.2K	10
Jan 2019	2.0K	11
Dec 2018	3.0K	25
Nov 2018	3.7K	99

This project has received funding from the European Union’s Horizon 2020 research and innovation program.

Facebook

The overall activity of the Cyber-Trust Facebook page has reached more than 1050+ users and gained engagement from 225+ users, the Facebook page gathered more than 90% of its interest organically. Cyber-Trust Posts appeared in the feed of almost 4000 Facebook users. The project Facebook page has so far concentrated 50 followers with 14 activity items. Facebook will be used as the channel of preference for the promotion of events in which consortium members will be participating.

Link to the Cyber-Trust Facebook page: https://www.facebook.com/cybertrust/



Posts

CyberTrust
22 August 2018

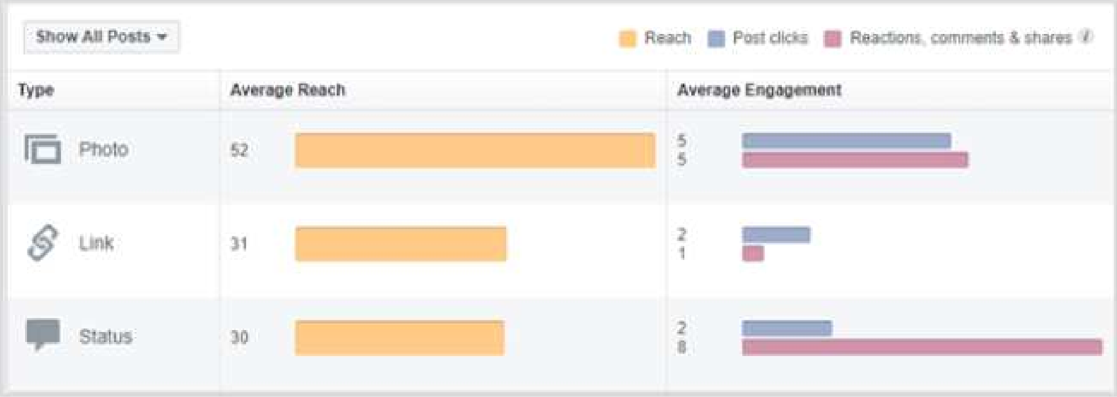
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. Any related posts reflect only the views of the project owner.

7 · 1 comment

Community · See all
Invite your friends to like this Page
50 people like this
49 people follow this

About · See all
Send message
www.cyber-trust.eu
Computer & Internet website
Suggest Edits

Engagement over post types



Cyber-Trust dissemination events

Cyber-trust partners organised and participated in several scientific and industry events, conferences and meetings, where they had the chance to present the results of the project. Also, several meetings were conducted where the Cyber-trust project and ideas were presented and discussed with potentially interested parties.

Organised events

The organised events in the first year of the project life include:

- **Co-organisation of the Mediterranean Security Event (MSE 2019) with the community of Security R&D stakeholders in the European Union, Fodele (Heraclion), Crete (Greece), 29-31 October 2019.**

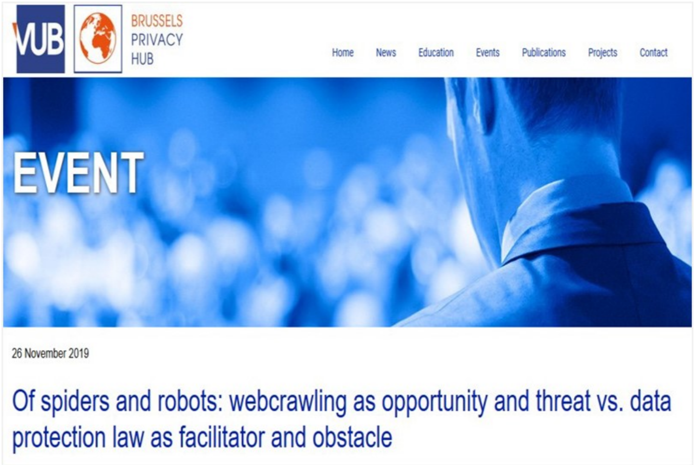
  The Mediterranean Security event focuses on multiple security-oriented research areas that have been identified as of high priority by EU. MSE2019 embraces the need for a trust-based, multilateral and cross-sectoral cooperation among the community of Security R&D stakeholders in the European Union. MSE2019 is not only an event but also an active international community integrating the experience and transferring the knowledge of experts and professionals.

  Link to the event: https://mse2019.kemea-research.gr/

- **Organisation of the Panel "Of spiders and robots: web crawling as opportunity and threat vs. data protection law as facilitator and obstacle" in cooperation with the Brussels Privacy Hub, 26 November 2019 .**

  This event was co-organised by the Horizon 2020-funded research project Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things and the Brussels Privacy Hub. The event was coordinated by VUB, with the participation of the partners from KEMEA and CGI. The panellists gave an overview of what web crawling entails from a technical point of view and outline the purposes of the use of web crawling in business, research and law enforcement. Building on that technical description, the discussion moved to the implementation of the EU data protection law and the compatibility with the data protection principles. Preventive, protective and informative measures deployed by website operators were also presented and debated.

  Link to the event: https://www.brusselsprivacyhub.eu/events/26112019.html



26 November 2019

Of spiders and robots: webcrawling as opportunity and threat vs. data protection law as facilitator and obstacle

This project has received funding from the European Union's Horizon 2020 research and innovation program.

- **Organization of IEEE SERVICES CSR-IoT workshop that was held from 8-13 July in Milan, Italy.**

  The workshop focuses on both the theoretical & practical aspects of the security, privacy, trust and resilience of IoT networks, devices, applications, and services as well as novel ways of dealing with their vulnerabilities and mitigating sophisticated cyber-attacks.

  Link to the CSR-IoT workshop website: https://conferences.computer.org/services/2019/workshops/cybersecurity_workshop.html

IEEE CONFERENCES

THE 1ST IEEE SERVICES WORKSHOP ON CYBER SECURITY AND RESILIENCE IN THE INTERNET OF THINGS

- **Co-organization of the first International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft), June 24-28, 2019**.

  The event was co-organization with the EU Cyber-Security and 5G projects: ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD and 5GENESIS. the workshop was co-hosted at 5th IEEE International Conference on Network Softwarization (NetSoft 2019) that was held in Paris, France on June 24-28, 2019.

  Link to the CSR-IoT workshop website: https://www.astrid-project.eu/secsoft/.

SecSoft 2019

The 1st International Workshop on

Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures

co-located with IEEE NetSoft 2019

June 24th, 2019 – Paris, France

https://www.astrid-project.eu/secsoft/

- **Organization of a special session at the 2018 IEEE Global Information Infrastructure and Networking Symposium (GIIS 2018), 23–25 Oct. 2018**

  The event was held in Thessaloniki, Greece, 23–25 Oct. 2018. The special session focused on areas under consideration by Cyber-Trust such as Blockchain applications in IoT, Cyber-threat intelligence, IoT and cloud forensics, etc.

  Link to the conference website: http://giis-2018.org/

Global Information Infrastructure and Networking Symposium (GIIS 2018)

October 23-25, Thessaloniki, Greece

Updates/News:

Extended versions of selected papers will be invited to Special Issues for Wiley Internet Technology Letters and MDPI Telecommunications

The program of the conference has been released!

Keynote Speakers announced!

Important Dates:

- Recent Results paper submission: **August 26**
- Paper submission: ~~July 30~~ **August 19 (extended)**
- Notification of paper acceptance: **September 5 7**
- Registration and upload of Camera-Ready papers: **September 23**

GIIS 2018 is collocated with **IEEE 5G/IoT Summit**. More information will be announced very soon!

This project has received funding from the European Union’s Horizon 2020 research and innovation program.

Upcoming event

Computers, Privacy and Data Protection (CPDP), 22-24 January, 22-24 January 2020

Cyber-trust partners from VUB prepare towards the organisation of a panel at CPDP 2020 (January 2020), which will be held from 22 to 24 January 2020. Data Protection and Artificial Intelligence is the theme of this year's conference. CPDP is a non-profit platform originally founded in 2007 by research groups from the Vrije Universiteit Brussel, the University de Namur and Tilburg University. The platform holds every year a conference in Brussels (Belgium) which attracts more than 1000 attendees from academia, industry, government, EU institutions, tech and law enforcement. Cyber-Trust will be represented, as research project, with a panel on **"AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection?"**

More information on the conference can be found here: https://www.cpdpconferences.org/

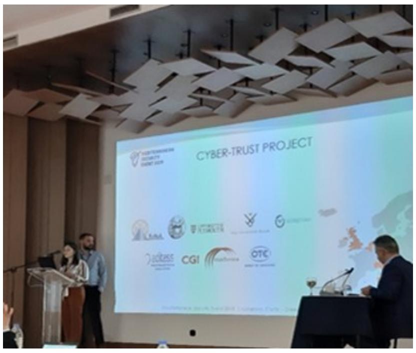
13th INTERNATIONAL CONFERENCE 22 - 24 JAN 2020 BRUSSELS, BELGIUM
CPDP 2020 DATA PROTECTION AND ARTIFICIAL INTELLIGENCE
ABOUT
CONTRIBUTE
SPONSORS & PARTNERS
ATTEND
CONTACT
CPDP2020
REGISTER NOW!
Early bird fees available till November 30, 2019

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Events participation

The main purpose of participating in events including workshops, conferences and meeting, is to raise awareness of the project and to gauge the level of interest and impact of the project on the wider community.

To this end, the members of the consortium have attended several events that include:



Presentation of CyberTrust at Mediterranean Security Event (MSE), Crete, Greece, 29th-31st October 2019

Centre of Security Studies (KE.ME.A.) which is the Project Coordinator of Cyber-Trust project organized Mediterranean Security Event (MSE). The event had more than 270 participants, more than 50 presentations and a variety of workshops. Cyber-Trust Coordinator Dimitrios Kavallieros and Vasiliki-Georgia Bilali presented "Meeting the needs of Information Sharing Among LEAs and ISPs" and promoted the Cyber-Trust's aspects and achievements. The presentation took place in the 3rd day of the MSE which was dedicated to Cyber-Security projects.

Link to the event: https://www.brusselsprivacyhub.eu/events/26112019.html

Show case Cyber-Trust at the DIGILINCE 2019 event, October 2, 2019

During the event DIGILENCE 2019 (Digital Transformation, Cyber Security and Resilience) Cyber-Trust project was introduced among Cybersecurity solutions for IoT environments. The project's advisory board member Mary Jo de Leeuw was a speaker in the event and Gohar Sargsyan from CGI was a support partner.

Link to the event: https://digilience.org/

Presentation of CyberTrust at Urban Security International Mayors' Forum and EUNWA Annual conference, Venice, Italy, September 2-3, 2019

A Thousands Cities, Millions of Citizens: A Vision for our Future Urban Security International Mayors 'forum took place in Venice, Italy between Sept 2-3, 2019 in coloration with EUNWA annual conference. The event was opened by the Mayor of Venice.

Some 50 city mayors were present and 14 of which were speakers which included, Antwerp, NYC, Prague, Moscow, Lisbon among others. The event was about sharing the safety and security of each country/city citizens and learning from each other how best to contribute to each other business. EUNWA was one of the partners of the event and also organised its annual conference linked to this mayor event. Among other safety cybersecurity was one of the key topics on today's life for vulnerable citizens. After a welcome note during the urban security event, CGI's Gohar Sargsyan presented Cyber-Trust to the mayors, LEA representatives and EUNWA members. The project was received with high interest and will be followed up with interested parties. Elisavet Charalambous from ADITESS as a support technology partner of EUNWA was also involved and supported further clarifications and questions on Cyber-Trust.

Link to the event:
https://www.miict.eu/2019/09/26/miict-project-in-eunwa-conference-in-venice-2-3-september-2019/

This project has received funding from the European Union's Horizon 2020 research and innovation program.

National Computer Security Incident Response Team

The National CSIRT-CY envisions the increase of the security posture of The Republic of Cyprus by enhancing cyber protection of its National Critical Information Infrastructures (CII), banks and ISPs.

Presentation of the Cyber-Trust project to National CSIRT-CY, May & September 2019

ADITESS had the chance to present the Cyber-Trust project and the two sides agreed in keeping a continuous communication link as regards the updates on project's results. Furthermore, in the near future and future meetings ways of exploitation of the Cyber-Trust project's outputs will be discussed more thoroughly. National CSIRT-CY (https://csirt.cy/) envisions the increase of the security posture of The Republic of Cyprus by enhancing cyber protection of its National Critical Information Infrastructures (CII), banks and ISPs.

National CSIRT-CY shall coordinate and assist CII owners/administrators, banks and ISPs to ensure the existence of (at least) a minimum level of security, by implementing proactive and reactive security services to reduce the risks of network information and cyber security incidents, as well as respond to such incidents as and when they occur. National CSIRT-CY shall also undertake awareness actions in order to educate the local population and National stakeholders about the adverse effects of cyber threats and cybercrime. In an earnest effort to enhance the security posture of the nation, the National CSIRT-CY shall provide timely advisories to all its constituents and make necessary efforts to introduce advanced security services such as security testing, vulnerability scanning, and active network monitoring.

Thank you for your interest in the European Cybersecurity Month

Staying secure online

October is CyberSecMonth

Show case CyberTrust in European Cybersecurity months at HSD, The Hague, The Netherlands, October, 2019

Each year The Hague Security Delta (HSD), in cooperation with partners, organise and host Cybersecurity events in October. This year, in conjunction with the European Cyber-security month, HSD supported entire month of the events instead of one week like previous years. October was announced as cybersecurity month with series of events also in The Netherlands by HSD.

Among other cybersecurity solutions, CGI show-cased Cyber-Trust project within this event in different occasions (workshops, innovation room, and show case sessions).

BILETA Belfast: Back to the futures?

BILETA Annual Conference 2019, Queen's University Belfast

Participation to the BILETA Annual Conference 2019 "Back to the futures?" 16-17 April 2019

Cyber-trust partner from VUB Prof. Paul Quinn gave a talk about "The Concept of Sensitive Data –Still fit for purpose?" at this event, which takes place at Queen's University Belfast, UK. The conference is organised by the British, Irish Legal Education, and Technology Association (BILETA) and attracts every year a significant number of academics and legal practitioners in the field of law and technology from all over the world. It also offers publication opportunities in high-ranking peer reviewed journals and various research funding schemes.

Link to the event: https://biletabelfast.net/plenary-and-parallel-sessions-tuesday-and-wednesday/

Participation to the H2020 Project-Clustering workshop, 28 March 2019.

The Workshop is organized by the GHOST project aiming at establishing tight connections with relative H2020 projects in the field of cybersecurity in IoT and relative domains and took place on 28th of March 2019, in Athens.

The website of GHOST Project is: https://www.ghost-iot.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Participation to the "13th Meeting of the Community of Users on Secure, Safe, Resilient Societies" workshop, 25-29 March 2019

This workshop is an annual event co-organised by DG HOME and DG CONNECT of the European Commission. In this event, Cyber-Trust partner from UoP gave the talk entitled "Mining for cyber-threat intelligence to improve cyber-security risk mitigation", in the area of cybersecurity intelligence and the thematic group on cyber-crime and security.

Participation to the MEDIA4SEC - Innovative Market Solutions Workshop, Brussels, Belgium, 27 September 2018.

In this workshop, the Cyber-Trust project was presented among many other innovative solutions related to the investigation of cybercrime and cybersecurity. The Event focused on the impact of social media platforms and information revealed by such platforms.

Website of the workshop: http://media4sec.eu/workshops/solutions/

Participation to the European Conference on Networks and Communications (EuCNC 2018), 18-21 June 2018.

"Cyber-Trust: An innovative cybersecurity platform for IoT" was presented at EuCNC 2018, which is the 27th edition of a successful series of a conference in the field of tele-communications, sponsored by the European Commission.

Website of the event: https://www.eucnc.eu

Participation to the 6th "Exposec-DefenseWorld" conference Athens, 15 May, 2018.

"Defending against cyber-attacks" was presented at the event which took place at the Hellenic Armed Forces Officers' Club (LAED) in partnership with The American-Hellenic Chamber of Commerce."

Website of the event: www.exposecdefenseworld.gr/

Forecasting changes in the migration flows using Open Sources

Participation to the Industry workshop by invitation - border security at FRONTEX, 16 October 2018.

Cyber-trust project was presented in the Industry workshop with the focus on migration topic - relevant security and safety services introduced in the event.

Participation to the Cybersecurity Week - The Hague Security Delta, Netherlands, 02-05 October 2018.

Cyber-trust partner CGI together HSD (The Hague Security Delta) participated in the event in the innovation room introducing Cyber-Trust among other CGI security and safety solutions and services.

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Presentation of the project during the ASGARD project Hackathons in Lisbon, May, 2019

The ASGARD hackathon is a bi-annually arranged event within the 42-month ASGARD (EU Restricted H2020) project with a rather large consortium and great attention from security stakeholders. During this event, project partners may present interesting technologies and the project relevant to ASGARD's interest.

Participation to the Workshop "Leadership Government", 14 January, 14 February, 14 March and 15 April 2019

Cyber-Trust partner from CGI participate to leadership event with Lead experts and decision makers of Industry and Government sector. Dr Gohar Sargsyan from CGI presents and discusses Cyber-Trust project and high-level design architecture principles being applied on the project to shape the framework and solution. The meetings are by invitation only and gather government industry leaders

Meetings

Several meetings took place between Cyber-Trust partners and the full spectrum of stakeholders, including police, government, academia, and industry. the most interesting are:

Academic visit to the EU Agency for Fundamental Rights (FRA), 2 September 2019 – 31 October 2019

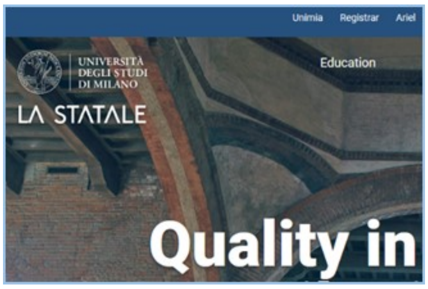
The European Union Agency for Fundamental Rights (FRA) is the EU's centre of fundamental rights expertise. Olga Gkotsopoulou, member of the Cyber-Trust project and legal researcher at LSTS/VUB, during her study visit contributed to the agency's activities with her research in privacy and data protection, in particular with relation to WP3.

Information about the Handbook:

https://fra.europa.eu/en/project/2018/handbook-european-law-relating-cybercrime-and-fundamental-rights

Academic visit to Erasmus, 25 September 2018.

During the academic visit, the presentation entitled "**Democratising social interactions: the case of distributed social networks**" was presented. The presentation involved an overview of technical issues and related solutions pertaining a wide range of distributed applications. In this context, the Cyber-Trust project was presented.



Meeting with the SEcure Service-oriented Architectures Research Lab team at University of Milan – SESAR Lab (Milan), 11 October 2018

A meeting was held at the University of Milan, SEcure Service-oriented Architectures Research Lab. The goal of the meeting was to present the project and to explore next opportunities of collaboration especially in the application of blockchain technology.

This project has received funding from the European Union's Horizon 2020 research and innovation program.

Meeting with the international research group of the Center for Cyber Security at University of Florence – Center for Cyber Security (Florence), 3 October 2018

A meeting was held at the University of Florence with the international research group of the Center for Cyber Security. The goal of the meeting was to discuss the possible common research field for synergies in research and technology transfer

Meeting with Swedish police customer, 27 June 2018

Gohar Sargsyan on behalf of project consortium presented the Cyber-Trust project among other security and safety projects where CGI participates in Stockholm, Malmo and Rotterdam, 27 June 2018.

Meeting with advisory board member Geleyn Meijer and ICT department / digital security, 21 June 2018.

Partners from CGI met advisory board member Geleyn Meijer and ICT department / digital security in Amsterdam, The Netherlands. The meeting was held in 21 June 2018, where the Cyber-Trust project is presented as well as the status of the project.

Other events

Membership in research group, 1 April 2019

The LSTS Cyber and Data Security Lab is a hub, consisting of academics and practitioners, that conducts research on topics of cybercrime, cybersecurity, data protection and privacy from an interdisciplinary perspective. In cooperation with them, Olga Gkotsopoulou, as participant of the Cyber-Trust project, will be engaged in various dissemination and communication activities, with direct relation to WP3.

This project has received funding from the European Union’s Horizon 2020 research and innovation program.