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

Welcome to our 3nd 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/
ttps://www.facebook.com/cybertrust/

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

Welcome to the third issue of the Cyber-Trust newsletter, September 2020

This issue provides the dissemination and communication activities undertaken by consortium partners of Cyber-Trust during the period of the project life from April 2020. It detailed the dissemination activities, which have been undertaken in this period, together with the potential future events. The detailed description of the dissemination activities involved during this period shows that the partners have been involved in many important activities to disseminate the project and raise its presence, noting that due to force majeure and emergency lockdown measures for the containment of COVID-19, several events where Cyber-Trust partners are involved have been postponed and rescheduled.

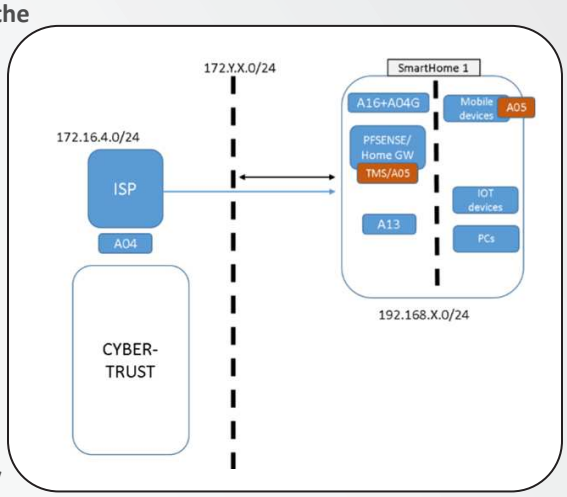
This issue of the Newsletter is available on the Cyber-Trust project website (https://cybertrust.eu/newsletters/) as well as the project social media including Facebook, Tweeter and LinkedIn.

30 September, 2020

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

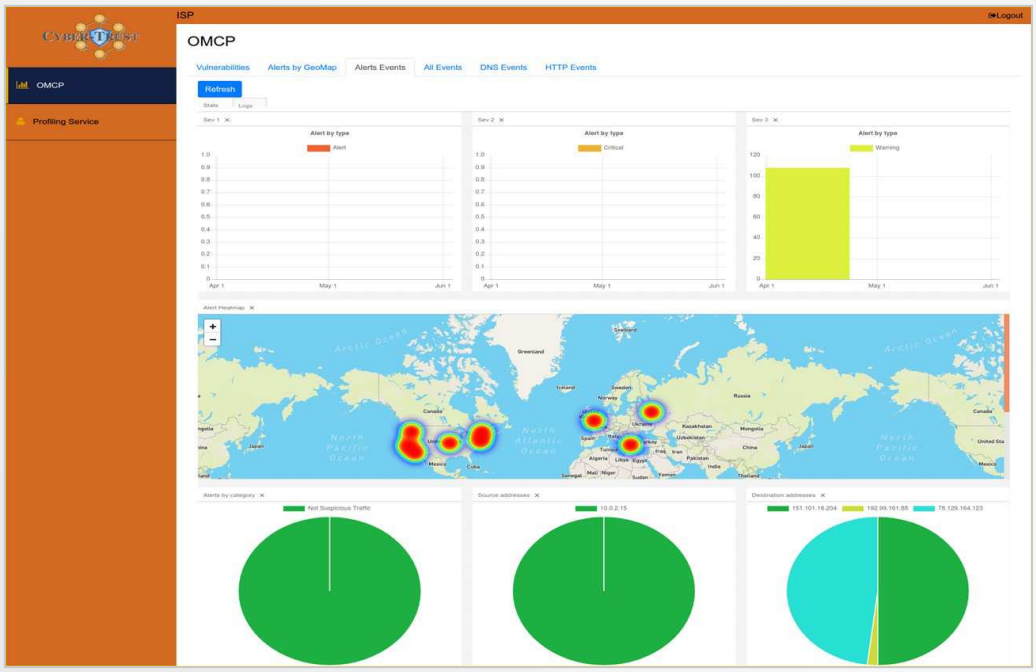
Deployment of Cyber-Trust Integrated Platform

For the needs of the evaluation and testing of the pilots, the Cyber-Trust Testbed has been prepared. The testbed is mainly located on OTE's infrastructure with a significant amount of resources located at KEMEA premises. Additionally, A light server is also provided by ADITESS for the deployment of the Profiling Service, Authentication and Authorization System as well as the Message BUS. To increase the performance and reduce network (over internet, VPN) latencies, the server is physically hosted on OTE premises.



Simulated Smart Home

The deployment of Cyber-Trust platform (not including the Smart Homes) is hosted on OTE premises with static IP configuration accessible by the smarthome networks. The smart home (SM) environments are implemented by using a number of virtualized devices, divided into small groups where a separate pfSense instantiation will be acting as a gateway for each SM, as depicted as presented in the Figure. Based on the smart home configuration, we proceeded to the setup and configuration of 750 smart homes.



ISP Visualisation: With visualisation component, users and officers have the possibility to get details about all the events generated by the cyber the Cyber-Trust's platform as well as general statistics about the alerts and other events.

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

Academic Publications

We have now published 33 research work papers!

The research undertaken in the Cyber-Trust project has already led to 33 research publications, of which 29 were accepted and presented in peer-reviewed international conferences and 4 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.

Link to all publications on the Cyber-Trust Website: https://cyber-trust.eu/publications/

The new research publications include:

A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain

Authors: Richard Brown, Gueltoum Bendiab, Stavros Shiaeles, Bogdan Gita

This research work presents a novel multimodal authentication system that relies on machine learning and blockchain, with the aim of providing a more secure, transparent, and convenient authentication mechanism. The proposed system combines two important biometrics: fingerprint, face with the age and gender features. The supervised learning algorithm Decision Tree (DT) has been used to combine the results of the biometrics verification process and produce a confidence level related to the user. This authentication mechanism is proposed in order to fulfil the objectives of a more secure, and transparent authentication mechanism, need for IoT security. The initial experimental results show the efficiency and robustness of the proposed multimodal systems. This work is related with the work carried out in the work-packages WP5 (Key proactive and cyber-threat intelligence), WP6 (advanced cyber-attack detection and mitigation) and WP7 (Distributed ledger technology for enhanced accountability).

The paper was presented in the 12th International Networking Conference (INC2020), that was held in 19-21 September 2020, Rhodes, Greece. **Due to the COVID 19 sanitary crisis, the INC 2020 was run as all-digital conference.** The paper will be available at the springer publisher's website.

Link to the conference: http://www.inc-conference.org/

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

Academic Publications

A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning.

Authors: Luke Barlow, Gueltoum Bendiab, Stavros Shiaeles and Nick Savage

The paper entitled "A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning" studied the detection and mitigation techniques proposed for preventing phishing attacks, which noticed a dramatical increase in the number of attacks against multiple industry sectors and critical infrastructures. In order to address the limitations of the studied approaches, this work investigated the efficiency of the approach proposed in the context of the Cyber-Trust project in preventing and mitigating phishing attacks. From the initial experimental results, the method seems promising and being able to fast detection of phishing attacker with high accuracy. Moreover, the method learns from the misclassifications and improves its efficiency. This scientific publication is directly related with the work carried out in the work-packages WP6 (Advanced cyber-attack detection and mitigation) of the Cyber-Trust project.

The paper was accepted and presented in the 2ed IEEE Services Workshop on Cyber security and Resilience in the Internet of Things (CSIOT) that was held in conjunction with the 2020 IEEE World Congress on Services (SERVICES 2020), on October 19-23, 2020 in Beijing, China.

Privacy Issues in Voice Assistant Ecosystems

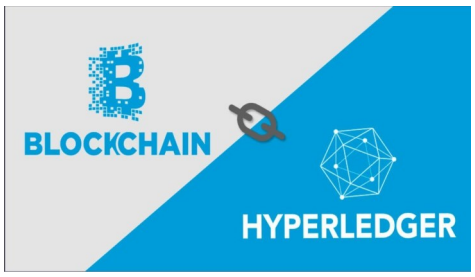
Authors: Georgios Germanos, Dimitris Kavallieros, Nicholas Kolokotronis, and Nikolaos Georgiou

This paper presented the types and the location of personal data artefacts within the ecosystems of three popular voice assistants; after having set up a testbed, and using IoT forensic procedures. The privacy evaluation includes the companion apps of the assistants, as the permissions they require before their installation on an Android device were compared.

The paper was accepted in the 2ed IEEE Services Workshop on Cyber security and Resilience in the Internet of Things (CSRIOT) that was held in conjunction with the 2020 IEEE World Congress on Services (SERVICES 2020), on October 19-23, 2020 in Beijing, China. The paper will be available at the IEEE publisher's website. This work is directly related to the work carried out in the work-package WP8 (Pilot implementation, testing and evaluation) of the Cyber-trust project.

On the Security and Privacy of Hyperledger Fabric: Challenges and Open Issues

Authors: Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Gueltoum Bendiab and Stavros Shiaeles



This research work studied the security and privacy issues related to the Hyperledger Fabric technology used in the Cyber-Trust project as a permissioned distributed platform to combats cyber-attacks and assist the evidence collection. It separated the attack surface of Hyperledger Fabric into four components, namely, consensus, chaincode, network and privacy -preserving mechanisms, in all of which an attacker (from inside or outside the network) can exploit the platform's design and gain access to or misuse the network. In addition, the paper highlighted the appropriate counter-measures that can be taken in each component to address the corresponding risks and provide a significantly secure and enhanced privacy preserving Fabric network. This work can aid developers to avoid security flaws and implementations that can be exploited by attackers but also motivate further research to harden the platform's security and the client's privacy

The paper was accepted and presented in the 2ed IEEE Services Workshop on Cyber security and Resilience in the Internet of Things (CSIOT) that was held in conjunction with the 2020 IEEE World Congress on Services (SERVICES 2020), on October 19-23, 2020 in Beijing, China.

It is worth noting Due to the COVID 19 sanitary crisis, the 2ed IEEE Services Workshop on Cybersecurity and Resilience in the Internet of Things (CSRIOT 2020) was run as all-digital conference. The research papers presented in this workshop will be published on the IEEE publisher's website.

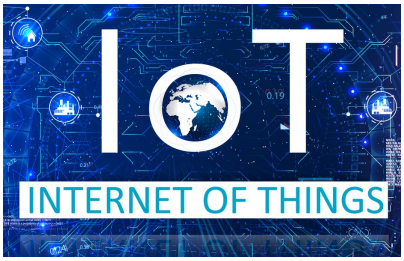
Link to the workshop: https://conferences.computer.org/ services/2020/workshops/csriot2020.html

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

Academic Publications

A Trust Management System for the IoT domain

Authors: Christos-Minas Mathas, Costas Vassilakis, Nicholas Kolokotronis



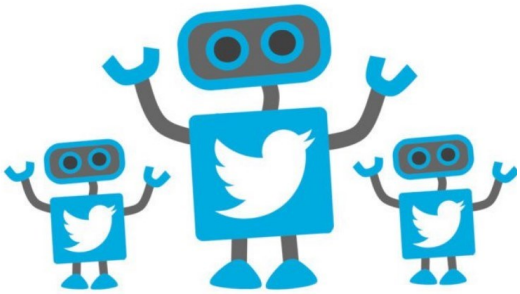
The paper entitled "A Trust Management System for the IoT domain" presented a trust-and risk-based approach to security, which considers status, behaviour and associated risk aspects in the trust computation process, while additionally, it captures user-to-user trust relationships which are propagated to the device level, through user-to-device ownership links. This work is directly related to the work carried out in the work-package WP5 (Key proactive and cyber-threat intelligence) of the Cyber-trust project.

The paper will be presented in the 2ed IEEE Services Workshop on Cyber security and Resilience in the Internet of Things (CSIOT) that was held in conjunction with the 2020 IEEE World Congress on Services (SERVICES 2020), on October 19-23, 2020 in Beijing, China. **Due to the COVID 19 sanitary crisis, CSRIOT 2020 will run as an all-digital conference.** The paper will be available at the IEEE publisher's website.

Link to the workshop: https://conferences.computer.org/ services/2020/workshops/csriot2020.html

BotSpot: Deep Learning Classification of Bot Accounts within Twitter

Authors: Christopher Braker, Gueltoum Bendiab, Stavros Shiaeles, Nick Savage, and Konstantinos Limniotis



This paper introduced a novel approach that uses Deep Learning to detect spam bot accounts. This kind of bot accounts is mainly created to conduct malicious tasks such as spreading of fake news, spams, malicious software and other cyber-crimes. Research studies found that up to 17% of Twitter active accounts are bots, which correspond to nearly 48 million accounts. The proposed approach relies on the Multi-layer Perceptron Neural Network and a set of nine features that include account, tweets and graph-related features. The Neural Network is trained on a dataset that consists of 760 normal and bot twitter accounts. Similarly, it was tested on a dataset of 100 twitter accounts either bot and normal. The initial experiments show promising results with 92% accuracy. This work is directly related to the work carried out in the work-package WP6 (advanced cyber-attack detection and mitigation).

The paper was presented in the 20th International Conference on Next Generation Wired/Wireless Advanced Networks and System (NEW2AN 2020) that was held August 26 - 28, 2020, St. Petersburg, Russia. **Due to the COVID 19 sanitary crisis, I 2020 was run as all-digital conference.** The paper will be available at the springer publisher's website.

Link to the conference: http://www.new2an.org/#/

SoMIAP: Social media images analysis and prediction framework

Authors: Yonghao Shi, Gueltoum Bendiab, Stavros Shiaeles, and Nick Savage

This research work introduced a novel approach for location prediction based on the image analysis of the photos posted on social media. This approach combines two main methods to perform image analysis; place and face recognition. The first method is used to determine the location area in the analysed image. The second is used to identify people in the analysed image, by locating a face in the image and comparing it with a dataset of images that have been collected from different social platforms. This method can be used to keep track of malicious actions and threats such as the paedophile hunter activities, grooming and planned criminal activities. It is also very effective in case of an emergency, incident or crisis, where local authorities can achieve situational awareness in a short space of time because of the speed of social media in providing visual snapshots of the incidents that took place.

The paper was presented in the 20th International Conference on Next Generation Wired/Wireless Advanced Networks and System (NEW2AN 2020) that was held August 26 - 28, 2020, St. Petersburg, Russia. **Due to the COVID 19 sanitary crisis, I 2020 was run as all-digital conference.** The paper will be available at the springer publisher's website.

Link to the conference: http://www.new2an.org/#/

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

Academic Publications

Advanced Metering Infrastructures: Security Risks and Mitigation

Authors: Gueltoum Bendiab, Konstantinos-Panagiotis, Ioannis Koufos, Nicholas Kolokotronis, Stavros Shiaeles

This research paper explored the security challenges That are today facing the Advanced Metering Infrastructures (AMIs). Especially, it provided an overview of the AMIs security requirements and the most common security risks for these critical infrastructures along with their impact. In order to address these issuers, especially zero-day attacks, which are the most dangerous attacks on AMIs, this paper proposed a novel Machine Learning (ML) intrusion Detection/Prevention System (IDS/IPS) to get optimal decisions based on a variety of factors and graphical security models. This scientific publication is directly related with the work carried out in the work-packages WP5 (Key proactive and cyber-threat intelligence), WP6 (advanced cyber-attack detection and mitigation) of the Cyber-Trust project.

The paper was presented in the First International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020) that was held in conjunction with the ARES workshops EU Projects Symposium 2020 at 15th International Conference on Availability, Reliability and Security, form August 25 – August 28, 2020. Due to the COVID 19 sanitary crisis, EPESec 2020 was run as a virtual conference.

Link to the paper: https://dl.acm.org/doi/10.1145/3407023.3409312

Threat landscape for smart grid systems

Authors: Christos-Minas Mathas, Konstantinos Panagiotis Grammatikakis, Costas Vassilakis, Nicholas Kolokotronis, Vasiliki-Georgia Bilali, Dimitris Kavallieros

This research paper explored the threat landscape of smart grids, identified threats that are specific to this infrastructure, provided an assessment of the severity of the consequences of each attack type, discerned features that can be utilized to detect attacks and listed methods that can be used to mitigate them. It is directly related with the work carried out in the work-packages WP5 (Key proactive and cyber-threat intelligence), WP6 (advanced cyber-attack detection and mitigation) of the Cyber-trust project.

The paper was presented in the First International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020) that was held in conjunction with the ARES workshops EU Projects Symposium 2020 at 15th International Conference on Availability, Reliability and Security, form August 25 – August 28, 2020. Due to the COVID 19 sanitary crisis, EPESec 2020 was run as a virtual conference. The paper is now available at the ACM publisher's website.

Link to the workshop: https://www.ares-conference.eu/ workshops-eu-symposium/epesec-2020/ .

It is worth noting Due to the COVID 19 sanitary crisis, the First International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020) was run as all-digital conference. The research papers presented in this workshop will be published on the ACM publisher's website.

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

Academic Publications

Detection of Insider Threats using Artificial Intelligence and Visualisation.

Authors: Koutsouvelis, Vasileios and Shiaeles, Stavros and Ghita, Bogdan and Bendiab, Gueltoum

This paper presented the insider threats that are considered as the most damaging risk factors for the IT systems and infrastructure of a company or an organisation; identification of insider threats has prompted the interest of the world academic research community, with several solutions having been proposed to alleviate their potential impact. This work proposed an innovative approach to prevent and mitigate insider threats based on the user's behaviours. For the implementation of the experimental stage described in this study, the Convolutional Neural Network (CNN) algorithm was used to identify malicious behaviour and implemented via the Google TensorFlow program. The CNN classifier was trained to identify potential threats from images produced by the available dataset. From the examination of the images that were produced and with the help of Machine Learning, the question whether the activity of each user is classified as "malicious" or not for the Information System was answered. This work is directly related with the work carried out in the work-packages WP6 (Advanced cyber-attack detection and mitigation) of the Cyber-Trust project

The paper was accepted and presented in the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 2020. **Due to the COVID 19 sanitary crisis, I 2020 was run as all-digital conference.** The paper is now available at the publisher's website.

Link to the paper: https://ieeexplore.ieee.org/document/9165337/

IoT Malware Network Traffic Classification using Visual Representation and Deep Learning

Authors: Gueltoum Bendiab, Stavros Shiaeles , Abdulrahman Alruban , Nicholas Kolokotronis

This research work proposed a novel IoT malware traffic analysis approach using deep learning and visual representation for faster detection and classification of new malware (zero-day malware). The detection of malicious network traffic in the proposed approach works at the package level, reducing significantly the time of detection with promising results due to the deep learning technologies used. To evaluate the proposed method performance, a dataset was constructed, which consists of 1000 pcap files of normal and malware traffic that are collected from different network traffic sources. The experimental results of Residual Neural Network (ResNet50) were very promising, providing a 94.50% accuracy rate for detection of malware traffic. This work is directly related with the work carried out in the work-package WP6 (advanced cyber-attack detection and mitigation) of the Cyber-Trust project.

The paper was presented in the 6th IEEE Conference on Network Softwarization (NetSoft) that was held as a virtual event, from June 29 to July 3, 2020! The paper is now available at the IEEE publisher's website.

Link to the paper: https://ieeexplore.ieee.org/document/9165381

On the Security of Permissioned Blockchain Solutions for IoT Applications

Authors: Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles

This work is focused on permissioned blockchain platforms and it investigated the consensus protocols used, aiming at evaluating their performance and fault tolerance as the main selection criteria for (in principle highly insecure) IoT ecosystem. The results of the research paper provided new insights on the essential differences of various consensus protocols and their capacity to meet the Internet of Thing (IoT) needs. This work is directly related to the work carried out in the work-package WP8 (Distributed ledger technology for enhanced accountability) of the Cyber-trust project

The paper was presented in the 6th IEEE Conference on Network Softwarization (NetSoft) that was held as a virtual event, from June 29 to July 3, 2020! The paper is now available at the IEEE publisher's website.

Link to the paper: https://ieeexplore.ieee.org/abstract/document/9165480

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

Web site Blog Posts

Partners from CSCAN and UOP have been published two blog posts with the purpose to promote the Cyber-Trust project, inform the stakeholders on the latest developments and generate interest of all the related communities with the exciting news in the research progress of the project.

The recently published blog posts are:

Blockchain solutions and chain-of-custody

Sotirios Brotsis, Nicholas Kolokotronis, 5 July 2020.

This blog post highlighted the blockchain solution that has been used in the context of the Cyber-Trust project to prevent malicious activities and enhance the security of IoT environments. The proposed blockchain is used to safely store the collected forensic evidence after the identification of a cyber-attack, or a compromised device in the network. The evidentiary information is stored as raw data in an off-chain database, while the hashes and metadata of the evidence are stored on the blockchain.

The Cyber-Trust blockchain is a permissioned distributed platform, which is built on top of Hyperledger Fabric in order to provide a proper digital Chain-of-Custody (**CoC**) by recording and preserving a chronological history of each digital evidence so that it can be later queried from LEAs, or when verification of proper functioning is needed and parts of the system's software have to be patched or updated reliably. This means that properties, like the firmware of a device, the configuration files, etc., are registered into the CTB, at the beginning of the system's operation, and verified if needed against a history of previously valid states, in order to ensure that they have not been tampered with. More details can be found in the blog post on the Cyber-trust Website.

Link to the blog post: https://cyber-trust.eu/2020/07/29/blockchain-solutions-and-chain-of-custody/

Data visualisation for Zero-Day malware detection

Gueltoum Bendiab, Stavros Shiaeles, 29 Jun 2020.

This blog post overview the new approaches proposed to prevent and mitigate potential malware threats using binary visualisation and machine learning. This kind of solutions has been proposed to tackle limitations in convolutional anti-malware tools, especially incapability to detect zero-day cyber-threats. This technique has proven to be effective in detecting zero-day malware because it leverages the structural similarity between known and new malware binaries. Moreover, visual analysis helps analysts to accurately capture and highlight malicious behaviour of malware samples, thus helping increase the efficiency of malware detection.

In this context, many projects have proposed to turn malware into images that can be used to spot more threats like the Microsoft and Intel project called STAMINA (Static Malware-as-Image Network Analysis), which converts input binary files into grayscale images so that, a deep learning algorithm can process and classify them. However, “Malware-Squid” approach, which is proposed in the context of the Cyber-trust project was announced two years before the announcement of the STAMINA project. Cyber-Trust project is progressing well, and the Malware-Squid approach shows promising results with the Suricata NIDS. Final results from this project will be published in research papers. In this context, Cyber-Trust team announce that this new approach will greatly help anti-malware tools, especially NIDSs, to effectively detect zero-day attacks and reduce the surface of security threats. More details can be found in the blog post.

Link to the blog post: https://cyber-trust.eu/2020/07/02/data-visualisation-for-zero-day-malware-detection/

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

Organised dissemination events

In this period, Cyber-Trust partners organised and participated in several scientific and industry events, conferences, and meetings, where they had the chance to present and discuss the results of the project with potentially interested parties.

The organised events in this period of the project life include:

Organisation of the 12th International Network Conference 2020 (INC2020)

21 September, 2020

Cyber-trust partners have participated in the organised the 12th International Network Conference (INC 2020). INC events have always attracted an international audience and papers on a wide range of topics. INC 2020 provides access to the papers from our proceedings via our Open Access Repository.

All accepted and presented papers will be published by **Springer Lecture Notes in Networks and Systems.**

Link to the conference: http://www.inc-conference.org/?page=home

Due to the COVID 19 sanitary crisis, the INC 2020 was run as all-digital conference. The research papers presented in this conference will be published on will be published by Springer Lecture Notes in Networks and Systems.

Invitation

We invite you to participate in the International Network Conference (INC 2020). The event will be held over the 19-21st September 2020 Virtually due to COVID-19 pandemic. This symposium, the twelth in our series, will bring together leading figures from academia and industry to present and discuss the latest advances in networking technologies from research and commercial perspectives.

INC events have always attracted an international audience and papers on a wide range of topics. Feedback at all previous events was extremely positive and it is intended that INC 2020 will build upon this success.

Details of our previous events are available from our past events page. We also provide access to the papers from our proceedings via our Open Access Repository.

Important dates

~~**25 June 2020**~~ **30 July 2020:**
Deadline for submission of papers

15 August 2020:
Notification of paper acceptance

25 August 2020:
Deadline for camera-ready paper submission and author registration

Paper Submission, review and publication

Authors are invited to submit full papers, not exceeding 15 pages (including all figures, tables and references) by 30 July 2020. Authors exceeding 15 pages will be charged with 50 Euro per additional page. A comprehensive set of instructions for preparing camera ready papers as well as the templates to follow can be found here. Please refer to this before submission. Authors are strongly encouraged to use the Word template for ease of paper formatting.

Papers can be submitted to the conference paper management system here . All papers will be double-blind reviewed by at least two members of the Programme Committee. All accepted and presented papers will be published by **Springer Lecture Notes in Networks and Systems.**

Extended versions of selected papers will be published by MDPI Electronics Journal, Special Issue on Networks and Cyber Security, Journal IF 2.412.

Back to top

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

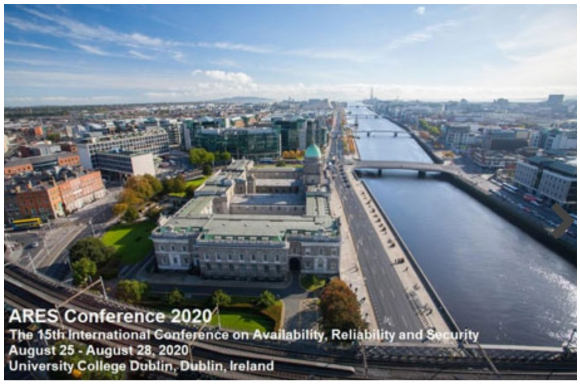
Organised dissemination events

Co-organization of the First International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020).

August 25 – August 28, 2020

Within the framework of fulfilling its scope, Cyber-Trust co-organizes EPESec 2020 in conjunction with ARES workshops EU Projects Symposium 2020 at 15th International Conference on Availability, Reliability and Security. The Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2020) aims at collecting the most relevant ongoing research efforts in the EPES security field. EPESec also serves as a forum for relevant projects in order to disseminate their security-related results, boost cooperation, and foster the development of the EPES Security Community made of security experts and practitioners. Topics of interest include:

- Security policies
- Risk analysis and management
- Vulnerability assessment and metrics
- Awareness, training and simulation
- Security standards
- Privacy and Anonymity in smart/ micro grids
- Threat modelling
- Security architectures
- Access control
- Malware and cyber weapons
- Intrusion detection and visualization
- Defense in depth
- Monitoring and real time supervision
- Perimeter security
- Safety-security interactions
- Cyber security engineering
- Secure communication protocols
- Formal models for security
- Hardware Security
- Resilient ICS/CPS
- Application Security
- Secure Firmware
- Incident Response and Digital Forensics
- Case studies



The Workshop is co-organized by SDN-microSENSE, FORESIGHT, CYBER-TRUST and SPEAR. Based on the current situation of the coronavirus COVID-19 pandemic sanitary crisis, the workshop was run as a virtual conference.

Link to ARES 2020 – http://www.ares-conference.eu

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

Organised dissemination events

Organization of the Second International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft 2020).

29 June – 3 July, 2020

The Second International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft 2020) is a joint initiative from EU Cyber-Security and 5G projects: ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD and 5GENESIS. The organisation of this workshop (https://www.astridproject.eu/secsoft/) co-hosted at 6th IEEE International Conference on Network Softwarization (NetSoft 2020) that was planned to be held in Ghent, Belgium on 29 June- 3 July, 2020. IEEE NetSoft 2020 aims at bringing together students, researchers and security experts on areas under consideration by Cyber-Trust. Indicative topics of interest included:

- Cyber-security platforms and architectures for digital Services
- Security, trust and privacy for industrial systems and the IoT (including smart grids (SGs)).
- Monitoring and advanced data collection and analytics.
- Virtual and software-based cyber-security functions.
- Orchestration of security functions.
- Novel algorithms for attack detection and threat identification.
- Intelligent attack mitigation and remediation.
- Machine learning, big data, network analytics.
- Secure runtime environments, including trustworthy systems and user devices.
- Formal methods for security and trust.
- Novel threat and attack models.
- Authentication, Authorization and Access control.
- Honeypots, forensics and legal investigation tools.
- Threat intelligence and information sharing

Based on the current situation of the coronavirus COVID-19 pandemic sanitary crisis, the 6th IEEE International Conference on Network Softwarization (IEEE NetSoft 2020) will run as a virtual conference On June 29 – 3 July, 2020.

Link to the workshop:

- https://cyber-trust.eu/secsoft-2020/
- https://www.astrid-project.eu/secsoft/

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

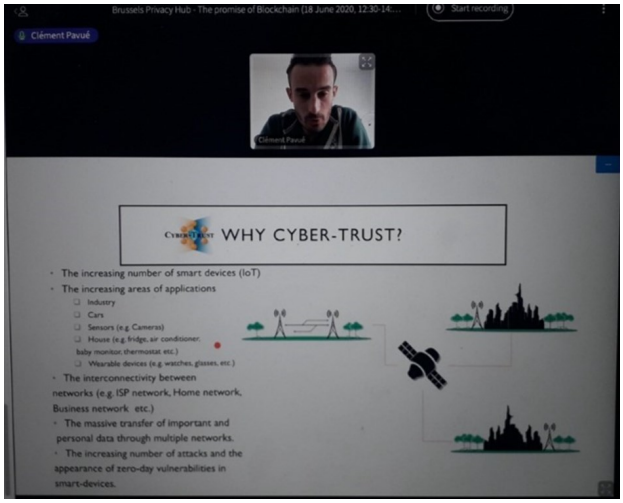
Organised dissemination events

Organization of a Standalone Panel (Webinar) entitled Promise of "Blockchain": DLT-based applications re-shape data storage and sharing, but can they be compliant with the EU data protection law?

18 June 2020

The **Brussels Privacy Hub** and the **Health and Ageing Law Lab (HALL)** in synergy with the Horizon 2020-funded research projects: **Cyber-Trust**| Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things, **FASTER**| First responder Advanced technologies for Safe and efficienT Emergency Response, and **LOCARD** | Lawful evidence collecting and continuity platform development present the panel 'The Promise of "Blockchain": DLT-based applications re-shape data storage and sharing, but can they be compliant with the EU data protection law?'

In recent times, much discussion has taken place among policymakers, academia and the private sector. Distributed Ledger Technologies (DLT) for data storage and sharing offer high potential and benefits in various contexts. Albeit, their use may give birth to implications with respect to data protection law. Design choices - giving preference to more centralised or decentralised solutions, opting for a permissioned or permissionless type of DLT, or resorting to an on-chain/off-chain scheme - create complications for researchers, DLT experts and businesses, as they can lead to different legal considerations, provided the characteristics specific to each application as well as the inherent limitations of each technology. Design choices can render compliance with the data protection and privacy framework easier or impossible and thus, can have a significant impact on the success of a project or product. The panel will address issues relating to DLT-based applications beyond Blockchain, understanding which questions have to be asked during the conceptualization and design of a solution as well as during its actual implementation.



The panellists, focusing on three innovative use cases of DLT (cyber-security, law enforcement and emergency response), will further address more general concerns and other issues, including the basic technical characteristics of DLTs and the current state-of-the-art. The backend legal research supporting those design choices will be extensively discussed. All in all, Blockchain -enthusiasts or skeptics, attendees will have the opportunity to hear about novel technical solutions which aim to render DLT-based applications compliant with data protection law and ensure the enforcement of data subjects' rights, such as the notion of Private Data, the adoption of different access levels and the Time To Live (TTL) feature.

Due to the COVID 19 crises, the event took place online. The event and the synergy are directly related to the work of WP3 (Legal issues: data protection and privacy) and WP7 (Distributed ledger technology for enhanced accountability).

Relevant dissemination links:

- https://www.brusselsprivacyhub.eu/events/18062020.html
- https://twitter.com/scorechain/status/1272919542482849792?s=20
- https://twitter.com/LSTSblog/status/1270616672676777985
- https://hall.research.vub.be/en/the-promise-of-%E2%80%9Cblockchain%E2%80%9D-dlt-based-applications-re-shape-data-storage-and-sharing-but-can-they-be

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

Coming events

Organisation of the IEEE SERVICES 20: 2nd IEEE Services Workshop on Cyber Security and Resilience in the Internet of Things (CSRIOT).

October 18-24, 2020

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. Topics of interest include :

- Blockchain applications in IoT
- Cyber-threat intelligence
- Game-theoretic security for IoT
- Identity management and access control for IoT
- IoT and cloud forensics
- Lightweight cryptography for IoT
- Malware detection and mitigation
- Network intrusion detection/mitigation
- Privacy and data protection in IoT
- Security in mobile applications
- System and data integrity
- Trust management for IoT
- Operational recovery and continuity in IoT
- Cyber-attack resiliency IoT architecture
- Cyber Threat adaptive capacity in IoT

Link to the workshop: https://conferences.computer.org/services/2020/workshops/csriot2020.html

Due to the current COVID-19 situation, IEEE SERVICES 2020 will no longer take place in Beijing, China and will instead take place virtually. The conference dates remain as October 18 – 24, 2020. Proceedings will not be cancelled, and publications will continue as planned. All presentations are required to be given through digital means in 2020.

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

Public summary of event co-organised by Cyber-Trust

18 JUNE 2020

The public summary of the event 'The Promise of "Blockchain": DLT-based applications re-shape data storage and sharing, but can they be compliant with the EU data protection law?' was published on the Brussels Privacy Hub website and was also disseminated to the event registered participants.

The Brussels Privacy Hub hosts regular workshops, conferences and seminars on various pertinent privacy and data protection issues. For every event, the Brussels Privacy Hub publishes a post-event summary, outlining the debate and the main elements of the presentations. These summaries provide the opportunity to those who did not attend to be informed of the key points of discussion as well as to reach a wide audience interested in the topic.

This publication is directly related to the work of WP3 (Legal issues: data protection and privacy) and WP7 (Distributed ledger technology for enhanced accountability).

The public summary can be found here: https://brusselsprivacyhub.eu/publications/ws36.html

18 June 2020

The Promise of "Blockchain": DLT-based applications re-shape data storage and sharing, but can they be compliant with the EU data protection law?

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

CONSORTIUM

Center for Security Studies – KEMEA
Role in the project: As the coordinator of CYBER-TRUST, KEMEA will ensure the overall project management and take responsibility for mediation, on behalf of the consortium, with the European Commission. KEMEA will also lead the pilot implementation and validation of the CYBER-TRUST platform.

University of Peloponnese
Role in the project: UOP is technically leading the project and contributes in the cyber-threat landscape review, the development of key proactive technologies and cyber-threat intelligence, the development of solutions related to data privacy, and the security of block-chain-based solutions.

University of Portsmouth
Role in the project: UOPHEC will lead WP6 and WP9. WP6 work will be focused upon the DDoS/RoQ attacks on network using deep packet inspection, network anomaly detection and protocol analysis to export the features needed to identify these attacks. In WP9, UOPHEC is responsible for defining the project's dissemination strategy.

Vrije Universiteit Brussel
Role in the project: VUB leads the Working Package 3 (WP3), concerning legal issues with emphasis on data protection and privacy. Project participant: Olga Gkotsopoulou, LL.M.

Scorechain S.A.
Role in the project: Scorechain is the expert in the Blockchain technology. We lead the work to implement a distributed technology to secure and enhance the CYBER-TRUST platform accountability (WP7). The aim is to assess and choose an efficient architecture to implement device authority management, device registration and secure storage of misbehaviour evidence.

Advanced Integrated Technology Solutions & Services ADITESS Ltd.
Role in the project: ADITESS will serve as the system's integrator in the project and will also ensure system deployment during the pilot execution. ADITESS will provide support to all technical and test case partners during the preparation, execution and evaluation of CYBER-TRUST. Additionally, ADITESS will also lead T6.2 for the implementation of solutions for device tampering detection and remediation. ADITESS as an SME will participate in dissemination and exploitation activities for the communication of CYBER-TRUST outcomes.

CGI Nederland B.V.
Role in the project: CGI is leading the design of the overall CYBER-TRUST platform architecture and development of a rapid prototype (WP4), guides the translation of legal recommendations into technical requirements, and is leading the project's exploitation strategy.

Mathema S.R.L.
Role in the project: Within Cyber-Trust, Mathema is devoted to implement an Interactive 2D dashboard for IoT monitoring and an innovative 3D-VR IoT visualization tool for augmenting the capability of complex network inspection.

OTE
Role in the project: OTE has the role of the end-user, who will integrate the resulting security platform on premise. As the end-user, OTE will be involved in the definition of user and infrastructure requirements and will provide the testbed infrastructure for piloting the CYBER-TRUST platform.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. The content of this website does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content. Therefore, any communication