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

Welcome to our 6th 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

Contacts

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

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

Dissemination manager :
Stavros Shiaeles, Gueltoum Bendiab
email: stavros.shiaeles@port.ac.uk,
gueltoum. bendiab@port.ac.uk,

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/

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

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

Editorial

Dear reader,

In this last issue of the Cyber-Trust Newsletter you will find updates on the project and highlights on our achievements over the last months, including activities and research publications, introduced by the Cyber-Trust's partners, next events and more. Our project has come to an end and for our last issue we want to present the activities and the tools that we have produced during the last period of the project life. Most of them are already available in our website.

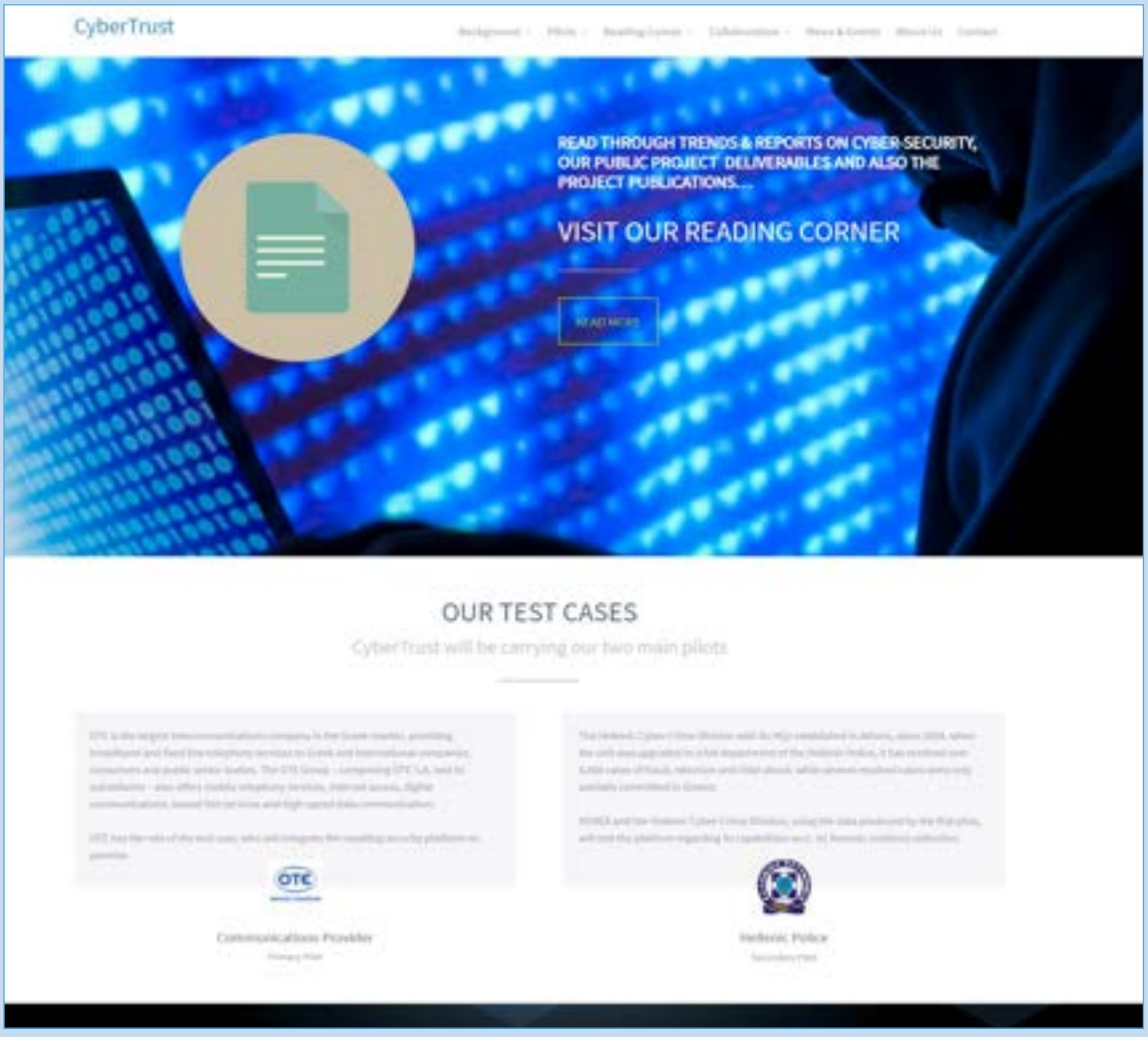
Don't forget to visit our YouTube channel and view our new video. Stay tuned with our project website and social media and browse our news and project progress.

- **https://www.linkedin.com/groups/13627755/**
- **ttps://www.facebook.com/cybertrust/**
- **https://twitter.com/CyberTrustEU**

Project Details

- **Project no. 786698**
- **Research and Innovation Action: Co-funded by the Horizon 2020 Framework Programme of the European Union.**
- **Project Start date: May 1st, 2018 (36 months duration)**

Please visit the site (https://cyber-trust.eu/) and let us know of your comments and suggestions.



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

Academic Publications

The research undertaken in the Cyber-Trust project has already led to 49 research publications, of which 39 were accepted and presented in peer-reviewed international conferences and 8 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 are:

Understanding and Mitigating Banking Trojans: From Zeus to Emotet

Authors: Konstantinos P. Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis, Costas Vassilakis, Stavros

The work presents a multi-layer approach to network security for network-based intrusion response systems that secures modern networks of heterogeneous devices. Therefore, this paper presents a system based on a combination of a graphical network security model and a game theoretic model of cyber-attacks that was tested on a testbed with Windows machines infected with Trojans; experimental results showed that the proposed system effectively blocked Trojans' network communications effectively preventing data leakage and yielding encouraging results for future work.

The paper was presented in the IEEE International Conference on Cyber-Security and Resilience that was held on 26-28 July 2021. Due to the COVID 19 sanitary crisis, the IEEE the IEEE International Conference on Cyber-Security and Resilience was run as all-digital conference. The paper will be available at the IEEE publisher's website.

The work presented in this paper is directly related to the work carried out in work-package 2, 6 and 8 (WP2, WP6 and WP8).

Link to the conference: https://www.ieee-csr.org/

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

Academic Publications

Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT

Authors: Joseph R Rose, Matthew Swann, Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis

This paper explores the potential of using network profiling and machine learning to secure IoT against cyber-attacks. The proposed anomaly-based intrusion detection solution dynamically and actively profiles and monitors all networked devices for the detection of IoT device tampering attempts as well as suspicious network transactions. Any deviation from the defined profile is considered to be an attack and is subject to further analysis. Raw traffic is also passed on to the machine learning classifier for examination and identification of potential attacks. Performance assessment of the proposed methodology is conducted on the Cyber-Trust testbed using normal and malicious network traffic. The experimental results show that the proposed anomaly detection system delivers promising results with an overall accuracy of 98.35% and 0.98% of false-positive alarms.

The paper was presented in the 3rd International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft) that was held on 2 July 2021 in Tokyo, Japan. Due to the COVID 19 sanitary crisis, the conference was run as all-digital conference. The paper is now available at the IEEE publisher's website**.** This work is directly related to the work conducted in package 6 (WP6) of the project.

Link to the conference: https://www.astrid-project.eu/secsoft/

On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids

Authors: Mathas, Christos-Minas, Costas Vassilakis, Nicholas Kolokotronis, Charilaos C. Zarakovitis, and Michail-Alexandros Kourtis

This research paper evaluates the current state of the vulnerabilities in IoT software utilized in smart grid applications from a source code point of view. To that end, we identified and analysed open-source software that is used in the power grid and the IoT domain that varies in characteristics and functionality, ranging from operating systems to communication protocols, allowing us to obtain a more complete view of the vulnerability landscape.

The results of this study can be used in the domain of software development, to enhance the security of produced software, as well as in the domain of automated software testing, targeting improvements to vulnerability detection mechanisms, especially with a focus on the reduction of false positives.

The work presented in this paper is directly related to the work carried out in work-packages 2 and 8 (WP2 and WP8), firstly elaborating on the threat landscape in the IoT and secondly providing aspects that can be considered for as scenarios in the evaluation of the CyberTrust solution.

This article is published on the Special Issue 5G Enabled Energy Innovation (ISSN 1996-1073), in the MDPI open access journal "**energies (impact factor 3.004, CITESCORE 4.7 SCOPUS)".**

Energies 2021, 14(10), 2818; https://doi.org/10.3390/en14102818

Link to the paper: https://www.mdpi.com/1996-1073/14/10/2818

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

Academic Publications

Social Media Monitoring for IoT Cyber-Threats

Authors: Sofia Alevizopoulou, Paris Koloveas, Christos Tryfonopoulos, and Paraskevi Raftopoulou

In this work, which is entitled "Social Media Monitoring for IoT Cyber-Threats ", the authors are focused on social media monitoring to investigate real-time Cyber-Threat Intelligence detection from the Twitter stream. Initially, they compare and extensively evaluate six different machine-learning based classification alternatives trained with vulnerability descriptions and tested with real-world data from the Twitter stream to identify the best-fitting solution. Subsequently, based on their findings, they propose a novel social media monitoring system tailored to the IoT domain; the system allows users to identify recent/trending vulnerabilities and exploits on IoT devices. Finally, to aid research on the field and support the reproducibility of their results they publicly release all annotated datasets created during this process.

The paper was presented in the IEEE International Conference on Cyber-Security and Resilience that was held on 26-28 July 2021. Due to the COVID 19 sanitary crisis, the IEEE the IEEE International Conference on Cyber-Security and Resilience was run as all-digital conference. The paper will be available at the IEEE publisher's website. The work presented in this paper is directly related to the work carried out in work-package 6 and 8 (WP6 and WP8).

Link to the conference: https://www.ieee-csr.org/

CHAINGE: A Blockchain Solution to Automate Payment Detail Updates to Subscription Services

Authors: David Buckley, Gueltoum Bendiab, Stavros Shiaeles, Nick Savage , Nicholas Kolokotronis

In this paper, the authors propose a novel approach to automate, manage and simplify the Financial Supply Chain involved in the process of updating and managing payments to user' subscriptions. This is done by utilising the Hyperledger Sawtooth blockchain framework, that allows a consumer to enter their payment card details in a central digital wallet and link their subscriptions to their cards. The card being updated triggers an event on the blockchain, which allow for the payment details to be updated on subscription systems automatically.

The verification tests performed on the prototype of the proposed system shows that its current implementation has been securely achieved.

The paper was presented in the IEEE International Conference on Communications (ICC) that was held on 14-23 June 2021 in Montreal. Due to the COVID 19 sanitary crisis, the IEEE International Conference on Communications (ICC) was run as all-digital conference.

The paper is now available at the IEEE publisher's the IEEE website. The work presented in this paper is directly related to the work carried out in work-package 6 and 7 (WP6 and WP7).

Link to the conference: https://icc2021.ieee-icc.org/

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

Academic Publications

Privacy issues in Android applications - The cases of GPS navigators and fitness trackers

Authors: S. Monogios, K. Magos, K. Limniotis, N. Kolokotronis and S. Shiaeles

The research paper studies privacy issues in the mobile ecosystem, focusing on two important types of smart applications which process personal data to a large extent: GPS navigators and fitness tracking applications. More precisely, for both types of applications, an indicative list of popular apps is being analysed through appropriate experimental environment, aiming to identify the underlying personal data processing that takes place. Our analysis illustrates that both GPS navigation apps and fitness trackers have access to several types of users data, while they may allow for personal data leakage towards third parties such as library providers or tracking services without providing always adequate or precise information to the users.

This research work is directly related to the work carried out in work-package 5, 6 and 7 (WP5, WP6 and WP7).

The paper has been accepted - but not published yet - to the International Journal of Electronic Governance (IJEG), Indre-Science Publishers, 2021.

Link to the journal: https://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijeg

inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence

Authors: Paris Koloveas, Thanasis Chantzios, Sofia Alevizopoulou, Spiros Skiadopoulos , Christos Tryfonopoulos

In this work, the authors put forward inTIME, a machine learning-based integrated framework that provides an holistic view in the cyber-threat intelligence process and allows security analysts to easily identify, collect, analyse, extract, integrate, and share cyber-threat intelligence from a wide variety of online sources including clear/deep/dark web sites, forums and marketplaces, popular social networks, trusted structured sources (e.g., known security databases), or other datastore types (e.g., pastebins). "inTIME" is a zero-administration, open-source, integrated framework that enables security analysts and security stakeholders to (i) easily deploy a wide variety of data acquisition services (such as focused web crawlers, site scrapers, domain downloaders, social media monitors), (ii) automatically rank the collected content according to its potential to contain useful intelligence, (iii) identify and extract cyber-threat intelligence and security artifacts via automated natural language understanding processes, (iv) leverage the identified intelligence to actionable items by semi-automatic entity disambiguation, linkage and correlation, and (v) manage, share or collaborate on the stored intelligence via open standards and intuitive tools.

The work presented in this paper is directly related to the work carried out in work-packages 2 and 8 (WP2 and WP8).

The paper has been published in the MDPI open access journal electronics.

Link to the journal paper: https://www.mdpi.com/2079-9292/10/7/818/htm

Electronics (IF 2.397) Pub Date : 2021-03-30 , DOI: 10.3390/electronics10070818

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

Academic Publication

User-Generated Pseudonyms Through Merkle Trees

Authors: Kermezis, Georgios, Konstantinos Limniotis, and Nicholas Kolokotronis

This work presents a pseudonymisation technique based on Merkle trees. More precisely, by exploiting inherent properties of the Merkle trees as cryptographic accumulators, the authors illustrate how user-generated pseudonyms can be constructed, without the need of a third party.

Each such pseudonym, which depends on several user's identifiers, suffices to hide these original identifiers, whilst the unlinkability property between any two different pseudonyms for the same user is retained; at the same time, this pseudonymisation scheme allows the pseudonym owner to easily prove that she owns a pseudonym within a specific context, without revealing information on her original identifiers. Compared to other user-generated pseudonymisation techniques which utilize public key encryption algorithms, this new approach inherits the security properties of a Merkle tree, thus achieving post-quantum security.

The research is published in the 9th Annual Privacy Forum, APF 2021, Oslo, Norway, June 17–18, 2021, Proceedings, Springer. The work presented in this paper is directly related to the work carried out in work-packages 5 (WP5).

DOI: https://doi.org/10.1007/978-3-030-76663-4_5

Link to the paper: https://link.springer.com/chapter/10.1007/978-3-030-76663-4_5

Moving–Target Defense Techniques for Mitigating Sophisticated IoT Threats

Authors: Konstadinos Panagiotis Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis

Securing the constantly evolving IoT threat landscape is a challenging problem, with severe consequences when not tackled appropriately. In response to that challenge, the field of moving-target defense has developed, to address these threats by utilizing game-theoretic approaches to respond to them while maintaining a high level of availability.

This work presents an implementation of an intrusion response system, which uses a Bayesian attack graph to model the complex state of the network and its hosts, and a partially observable Markov decision process to choose optimal mitigation actions. In order to cope with novel and unknown network attacks, like Zero-day exploits, an alert management policy was added to focus the POMD Pon the current state of the network and provide short-term mitigation actions.

Finally, the system was evaluated against five scenarios (Mirai, Zeus, Zero-day, 10 malicious traffic replays, and Black Energy) executed in a simulated SOHO environment. Evaluation results showed its high effectiveness against traditional threats, and a slight increase in effectiveness against novel threats.

The work presented in this paper is directly related to the work carried out in work-packages 6 and 8 (WP6 and WP8). This work is accepted for publication in the Cyber-Trust exploitation book.

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

Academic Publications

Insider Threat Detection using Deep Autoencoder and Variational Autoencoder Neural Networks

Authors: Efthimios Pantelidis, Gueltoum Bendiab , Stavros Shiaeles, Nicholas Kolokotronis

Internal attacks are one of the biggest cybersecurity issues to companies and businesses. Despite the implemented perimeter security systems, the risk of adversely affecting the security and privacy of the organization's information remains very high. Actually, the detection of such a threat is known to be a very complicated problem, presenting many challenges to the research community. Therefore, this paper investigates the application of the deep neural networks Autoencoder (AE) and Variational Auto-encoder (VAE) in detecting malicious insiders automatically, without human intervention. These two deep neural networks have proved their effectiveness in discovering high quality, non-linear features for anomaly detection, in various fields. They can learn different levels of representations from the input data based on the multi-layer structures. Moreover, The VAE could generate new data from the source dataset. In this study, the AE and VAE neural networks have been implemented using the Python programming language with the Keras library and the TensorFlow environment. While the validation is performed on the public CERT (version r4.2). This version of the dataset contains both normal and malicious user activities that are generated from 1000 simulated employees. The comparison results with our previous models indicate that the Variational Autoencoder neural network provides the best overall accuracy in detecting internal threats with a lower false-positive rate.

The paper was presented in the IEEE International Conference on Cyber-Security and Resilience that was held on 26-28 July 2021. Due to the COVID 19 sanitary crisis, the IEEE the IEEE International Conference on Cyber-Security and Resilience was run as all-digital conference. The paper will be available at the IEEE publisher's website.

The work presented in this paper is directly related to the work carried out in work-package 2, 6 and 8 (WP2, WP6 and WP8).

Link to the conference: https://www.ieee-csr.org/

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

Press Releases

During this last period of the Cyber-Trust project life, Partners have been published several press releases with the purpose to promote the 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 released press are:

Cyber-Trust: Καινοτόμες λύσεις κυβερνο-ασφάλειας

ADDITESS, 23 July 2021

The press release "Cyber-Trust: **Καινοτόμες λύσεις κυβερνο-ασφάλειας**" was disseminated through:

1. the e-channels of the Cypriot platform InBusiness (https://www.imhbusiness.com/en) Magazine that has a monthly readership of more than 50,000. It is the only monthly business magazine in Cyprus that provides comprehensive overview of all segments of economy, technology, and interrelated issues.

   The link can be found here :Cyber-Trust: Καινοτόμες λύσεις κυβερνο-ασφάλειας | IN Business News | Υπηρεσίες (reporter.com.cy)

2. InBusiness Magazine daily newsletter sent to 50,000 business opinion leaders.

Pilot Evaluation Strategy and Road ahead

KEMEA, 12 February 2021

The press release **'Pilot Evaluation Strategy and Road ahead'** was released on the Cyber-Trust website on 12 February 2021. The press release offers a concise overview of the methodology to be adopted during the first pilot evaluation plan for the assessment of the verification analysis and the target class of end-users.

The outcome of a positive and transparent first pilot phase would be a stable base for the second and final phase of pilot implementation and, ultimately, a landmark in the cyber security ecosystem.

Reference: Cyber-Trust: Pilot Evaluation strategy and road ahead – CyberTrust (cyber-trust.eu)

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

Blogposts

Forensic evidence storage through blockchains: Scorechain in Cyber-Trust Project

SCHORCHAIN, July 2021

The blogpost titled "**Forensic evidence storage through blockchains: Scorechain in Cyber-Trust Project**" provides information about the role of the SCHORCHAIN partner in the Cyber-Trust project

Scorechain' s role in this project was to provide a blockchain for partners both private for instance Internet Service Provider (ISP) and public Law Enforcement Agency (LEA). One of the responsibilities of this blockchain is to allow partners to safely share information about alleged malicious activity between them. In this context, "safe" means that information is guaranteed to circulate without any modification from malicious sources. More specifically, information sharing will potentially be used in a court. By doing this, the blockchain is used as a way to provide a reliable, decentralized, and traceable Chain of Custody.

Given this legal constraint, Scorechain chose to use Hyperledger Fabric as a framework to build our blockchain. One of the key factors in the adoption of Hyper Ledger was the newly added feature of private data to store forensic evidence. This allows data producers to store information on the blockchain without sharing it directly with the other peers of the chain. Indeed, a partner has to require through an on-chain protocol access to the data. Thus, an LEA having a warrant will be able to access information on the blockchain. Moreover, the private data feature comes with Time-To-Live (TTL) capabilities. This means that data producers will specify according to their legal jurisdiction constraint how long the forensic evidence will remain on the blockchain, after that period, no one even themselves will be able to access the data.

The blogpost has been published on the SCORCHAIN web site.

Link to the blogpost:

Forensic evidence storage through blockchains: Scorechain in Cyber-Trust Project - Scorechain Blog

Device-Level Attacks: Targeting the Android Smartphones

ADITESS, June 2021,

In Cyber-Trust project, the detection of malicious activity at device level is done by the Smart Device Agent which mainly monitor performance, network and other activity of the IoT device (e.g., Android smartphone). It is worth mentioning, that other techniques and third-party solutions can also be integrated and benefit from their detection capacity. However, this is not part of the current focus. While the experimental evaluation is done using malware running on Android OS, the SDA methodology is more generic and can be adapted for other OS (already developed for Linux and Windows) and other embedded (IoT) systems that are hosting an OS.

The Blogpost titled "Device-Level Attacks: Targeting the Android Smartphones" aims to provide a high-level overview of a device monitoring and particularly the Android OS devices part of the work done in WP6. The article introduces the need to protect the Android OS towards malicious software and presents the monitoring field covering the binaries, the runtime status, the network activity, and the processes running on the device.

Link to the blogpost: https://cyber-trust.eu/2021/06/15/device-level-attacks-targeting-the-android-smartphones/

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

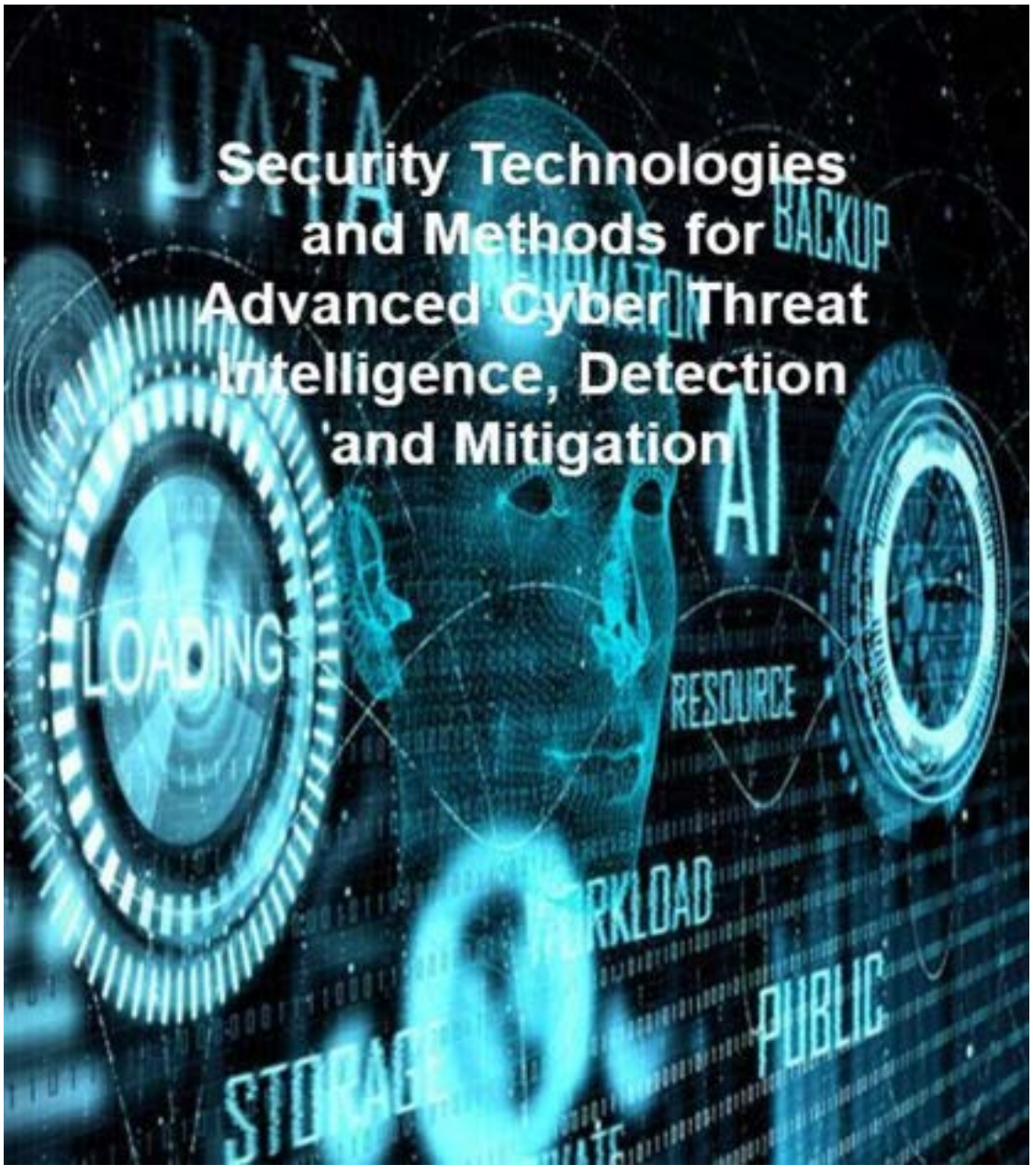
Cyber-Trust exploitation book

Business Conference Presentation and Publication

July 2021

Since the project is more research focused engaging world-class scientists, research and industry experts, the project partners decided to produce and publish a book focusing on exploitation aspects of the project and potential commercialization. The partners believe this will boost exploitation and market uptake of the project results and will be instrumental and potential client conversations. The book is Open Access and will be published by Now publisher Inc., an international high-level publisher, it will be published open access in high level scientific digital platforms.

The Book will also be intended to be sold and the authors will get royalties. Only the fact, that fact that the book will be Open Access will lead to greater global exploitation and dissemination and readership, which in turn improves the chances of higher citations and referencing, which are of course important to authors especially the authors in the research area. As for the client conversations, this book will demonstrate as a tangible outcome of the Cyber-Trust project and highlight the achievements.



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

Organised events

Demonstration and Evaluation Workshop

28 June 2021

The Demonstration and Evaluation Workshop was the second pilot and the final Evaluation Workshop of the Cyber-Trust project, targeting to assess the Cyber-Trust platform.

The objectives of the Demonstration and Evaluation workshop were:

- To provide and receive feedback on the project's legal objectives and aspects.
- To assess the platforms functionalities
- To measure evaluators platform usability (e.g., satisfaction, ease of use etc.)
- To receive feedback from professionals in the practitioners' domains in order to make future improvements.
- To validate the Cyber-Trust platform's superiority by carrying out the second PoC pilot.


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

Invitation to join Cyber-Trust Demonstration and Evaluation Workshop 28th of June 2021 organized by the Cyber Trust Consortium.

SCOPE of the Workshop

Dear Madam/Sir,

The Cyber-Trust consortium invites you to participate in the second and the final Evaluation Workshop of the Cyber-Trust project, which will take place on 28th of June 2021 virtually via GoToMeeting platform.

The research project "Cyber-Trust – Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things" was launched under the EU funding mechanism of H2020. The conceptualization behind this funding is to create an innovative cyber-threat information collecting, detection, and mitigation platform to address the grand issues of safeguarding the IoT ecosystem.

More specifically, Workshop is divided into two parts, a) an educational demonstration of the 4 different UIs and b) a hands-on training based on the test cases on which the Cyber-Trust focuses.

OBJECTIVES of the Workshop

The objectives of the Demonstration and Evaluation workshop are:

- To provide and receive feedback on the project's legal objectives and aspects.
- To assess the platforms functionalities
- To measure evaluators platform usability (e.g. satisfaction, ease of use etc.)
- To receive feedback from professionals in the practitioners' domains in order to make future improvements.
- To validate the Cyber-Trust platform's superiority by carrying out the second PoC pilot.


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

PRACTICAL INFORMATION

When	28 June 2021
Where	Online. A link will be sent to your email address upon positive response to participate in the Workshop.
Fee	None
Travel & accommodation	N/A
Registration Link	

For more information, please contact: & or visit the

CYBER-TRUST is a project that has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, under grant agreement no 786698

The Workshop started with the demonstration of the platform by the Consortium members. More specifically, the demos of the four dedicated User Interfaces (UIs) of Cyber-Trust, the demo of Kibana experts' interface as well as the demo of Cyber-Trust's Android Application. The scope was to educate the evaluators to platform's capabilities.

Then a synchronous scenario took place, where the evaluators started to execute few test cases, concluding at the end of the scenario to complete a dedicated end-user evaluation questionnaire .

More information about the workshop can be found in the Cyber-Trust web site.

https://cyber-trust.eu/

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

Organised events

Organization of the CSR conference

26-28 July, 202

The technological and industrial revolution brought by **complex Cyber-Physical Systems (CPSs)** comes with new threats and cyber-attacks that exploit their inherent complexity and heterogeneity. These attacks have a significant negative impact on the operation of various services in critical sectors, like energy, transport, and communications, which provide the vital functions that our societies depend upon. Systems under attack, should exhibit resilience in the form of graceful degradation and/or operational continuity and fast recovery of core functions in order to avoid potentially uncontrolled cascading effects. To this end, the emerging field of cyber resilience can be understood as a mixture of strategies, methods, and techniques to support complex CPS adaptive capacity during cyber-attacks.

Link to the conference: https://www.ieee-csr.org/

Topics in this workshop are directly related with work carried out in work-packages WP3, WP4, WP5, WP6, and WP7. The special session's proceedings will be made available at the publisher's website (https://ieeexplore.ieee.org/). It is also expected that the accepted and presented workshop papers will be published in the workshop proceedings before the end of 2021 and will be made available at the publisher's website, (https://ieeexplore. ieee.org/.

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

Events participation

Science Business alignment focused workshop - Cybersecurity

CGI, 13-14 July, 202

As a member at Science|Business CGI partner is engaged in a number of events, including large public events and closed focused or board sessions to drive the future combining the science with business. In this series closed workshops have been organised to closely look into each growing topics, which included Cybersecurity. Within this session, CGI presented Cyber-Trust project as an example of European multidisciplinary partnership research and innovation project which has a potential for business. Particular attention was given to the similar projects presented by other participants with regards the efforts to be taken to translate the scientific results into business. Suggestions have been made to offer methods and vehicles for such transformation or set updated criteria with stronger business results association between science and business.

Security Challenges in Modern 5G Environments

OTE, 06 November 2020

The following Workshop was organised by OTE, by focusing upon Security Challenges in Modern 5G Environments, as a side-event within the 22nd Infocom World Conference & Exhibition, one of the biggest annual events for Industry in ICT, in Greece. The Conference took place in Athens (Greece) on November 6, 2020. The Cyber-Trust project also received visibility as presenter.

Infocom World Conference & Exhibition 2020: "Transforming Greece: The 5G and Fiber Enablers – The Future is Now!".

For the particular event was held online due to COVID-19 restrictions under the title:

"Scientific Meeting: Perspectives and Challenges for the Development of Innovative 5G Applications and Services, through Modern Research Activities".

The activity took place in the scope of Part 5 (Security Challenges in Modern 5G Environments). One Cyber-Trust – dedicated presentations took place, as follows:

Title: "CyberTrust: Advanced Cyber-Threat Intelligence, Detection and Mitigation Platform for a Trusted Internet of Things".

*https://*divanicaravelhotel.com/, online

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

Events participation

Business Conference Presentation and Publication

06 November 2021

ADDITESS LTD as an exhibitor at the Defense Exhibition Athens 2021 (DEFEA 2021) representing one the companies in the Defense and Security industry in Cyprus, had the chance to present the CyberTrust project to different exhibitors and visitors.

DEFEA took place on 13-15 July 2021 and was under the auspices of the Hellenic Ministry of National Defense, with the support of Hellenic Manufacturers Association of Defense Material.

At DEFEA 2021, the largest and most prominent defense industries around the world participated as exhibitors, showcasing their latest technologies and the defense systems that will prevail in the future.

Impressive national pavilions with state-of-the-art products and equipment, and private companies with the most advanced solutions in every category of the defense and security sector covered the halls of the exhibition Centre, offering to visitors and officials an integrated view of the capabilities of modern military technology.

There were 315 renowned exhibiting defence industries from 22 countries and visited by 45 official national delegations, represented at political and military level, from 36 countries.

Pictures from the Workshop

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

Cyber-Trust dissemination video

Following the strategy outlined in deliverable D9.2 (Disseminations and use plan), a video (10 minutes) targeting to attract potential clients has been released during the last period of the project life. The video starts with a high-level overview of the Cyber-Trust platforms, its architecture, and main components.

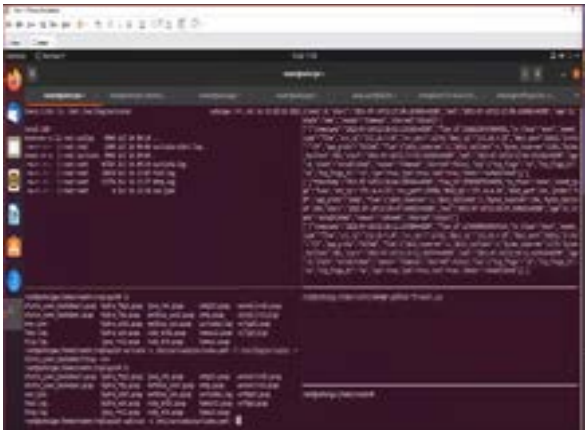
Then, it illustrates the platform capabilities in detecting known and known attacks through two different scenarios of attacks (zero-day attack and a DDoS attack with the Mairi malware).

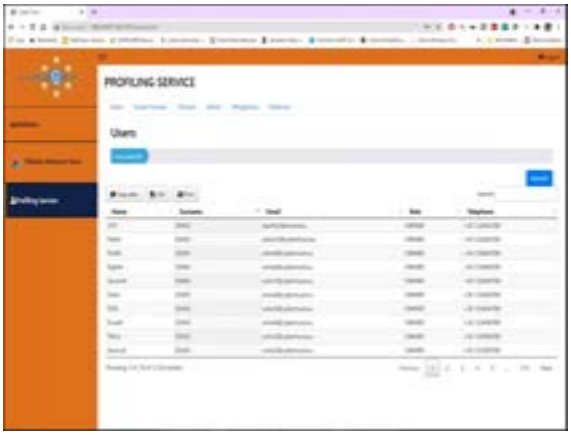
During the live testing of the attacks, the video shows the different functionalities provided by the platform visual portal to the identified Cyber-Trust end-users:

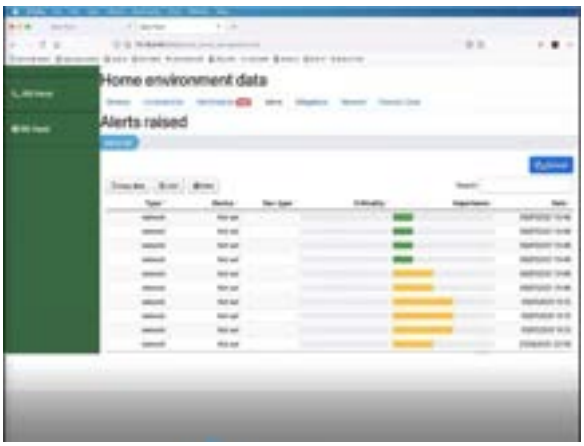
- Platform Administrator (Admin UI)
- Law Enforcement Agent (LEA UI)
- Internet Service Provider (ISP UI)
- Homeowner (SOHO UI)

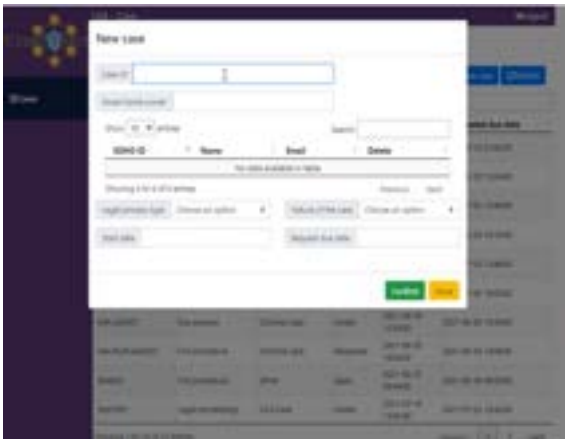
Finally, the video provides a brief conclusion about the future exploitation and research plans for the project

The video will be published on the Cyber-Trust YouTube channel and also accessible from the Cyber-Trust website and social media accounts Facebook, Tweeter and LinkedIn.









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 blockchain-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 activity related to the action reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.