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

Newsletter Vol. 4— January 2021

Welcome to our 4th 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

Dissemination manager :
Stavros Shiaeles
email: stavros.shiaeles@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/

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

Project Newsletter, 4th issue, January 2021

This issue provides the dissemination and communication activities undertaken by consortium partners of Cyber-Trust during the period of the project life from September 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

Cyber-Trust
2021
HAPPY NEW YEAR
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no. 786698. The work reflects only the authors’ view and the Agency is not responsible for any use that may be made of the information it contains.
https://cyber-trust.eu/

Prepared by Gueltoum Bendiab

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 36 research publications, of which 31 were accepted and presented in peer-reviewed international conferences and 5 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/

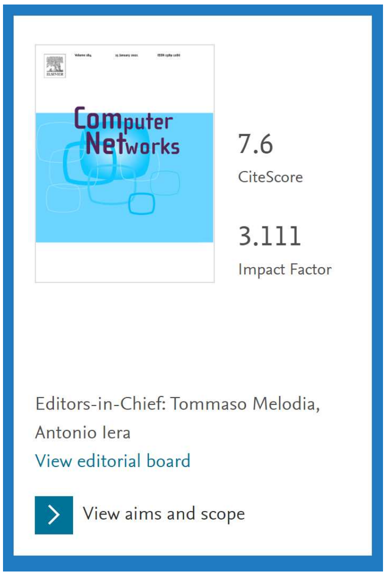
The new research publications are:

On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance

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

The research paper entitled " On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance" has been accepted for publication in the International Journal of Computer and Telecommunications Networking "Computer Networks".

This paper aims at addressing the above needs by providing a comprehensive and coherent review of the available blockchain solutions to determine their ability to meet the requirements and tackle the challenges of the IoT, using the smart home as the reference domain. Key architectural aspects of blockchain solutions, like the platforms' software and network setups, the consensus protocols used, and smart contracts, are examined in terms of their ability to withstand various types of common IoT and blockchain attacks, deliver enhanced privacy features, and assure adequate performance levels while processing large amounts of transactions being generated in an IoT environment. The analysis carried out identified that the defences currently provided by blockchain platforms are not sufficient to thwart all the prominent attacks against blockchains, with blockchain 1.0 and 2.0 platforms being susceptible to the majority of them. This seems to be in contrast with privacy preservation mechanisms, which are embraced, to varying degrees, by all platforms investigated. If the underlying consensus protocols' performance and fault tolerance is also considered, then only a small number of platforms meet the requirements of our reference IoT domain.


Computer Networks

7.6
CiteScore

3.111
Impact Factor

Editors-in-Chief: Tommaso Melodia, Antonio Iera
View editorial board

View aims and scope

The work presented in this paper is directly related to the work carried out in work-package 6 and 7 (WP6 and WP7). The paper will be available at the publisher website (https://www.journals.elsevier.com/computer-networks) in April 2021.

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

Academic Publications

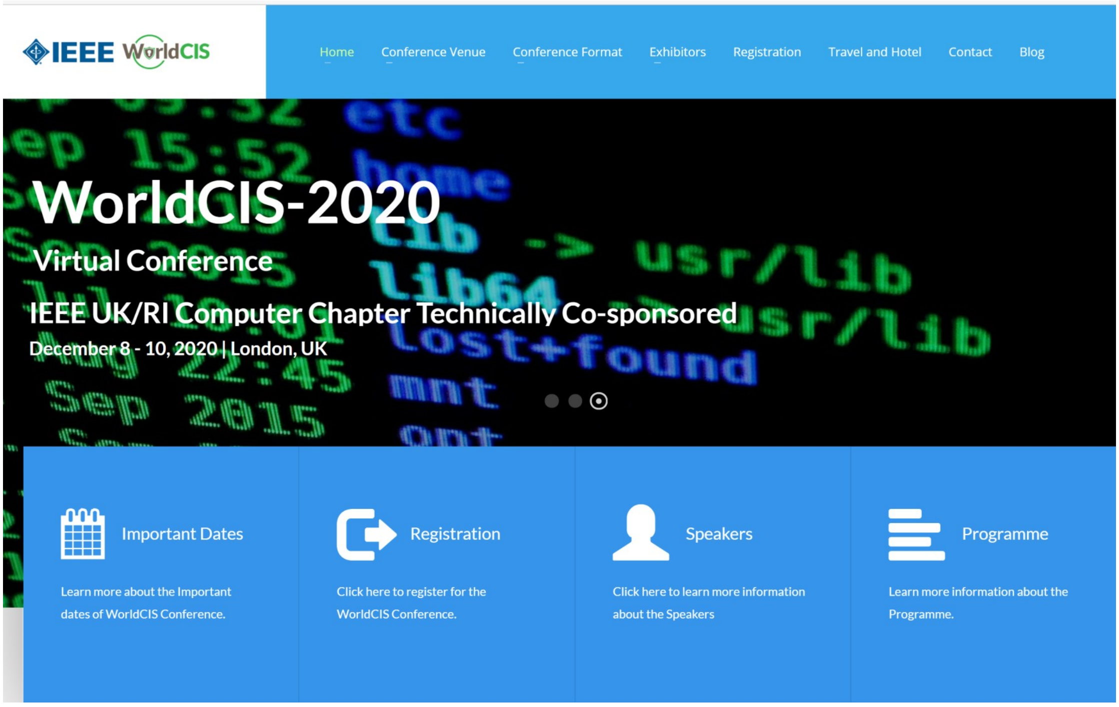
Tools for Network Traffic Generation—A Quantitative Comparison.

Authors: Matthew Swann, Joseph Rose, Gueltoum Bendiab, Stavros Shiaeles and Nick Savage

The paper titled "*Tools for Network Traffic Generation - A Quantitative Comparison*" focuses on the traffic generation task that is very important for the Cyber-Trust project testing phase. Network traffic generators are invaluable tools that allow for applied experimentation to evaluate the performance of networks, infrastructure, and security controls, by modelling and simulating the communication packets and payloads that would be produced by machines and devices on the network. Specifically for security applications, these tools can be used to consistently simulate malicious activity on the network and test the components designed to detect and mitigate malicious activities, in a highly reliable and customisable way. In order to create and demonstrate malicious replay attacks on the Cyber-Trust network, we have investigated the performance and accuracy of three of the most reviewed network traffic generators in literature, namely Cisco TRex, Ostinato and Genesids. Mainly, the comparative experiments examine the strengths and limitations of these tools in term of CPU and RAM consumption. This research paper is directly related to the work conducted in the WP6 and WP8 of the Cyber-Trust project. It will be available at the IEEE publisher's website

The paper has been refereed and accepted for the World Congress on Internet Security (WorldCIS-2020), which was held online. The congress is technically co-sponsored by IEEE UK/RI Computer Chapter.

Link to the IEEE WorldCIS-2020 virtual conference: https://www.worldcis.org/



WorldCIS-2020

Virtual Conference

IEEE UK/RI Computer Chapter Technically Co-sponsored

December 8 - 10, 2020 | London, UK

Important Dates

Learn more about the Important dates of WorldCIS Conference.

Registration

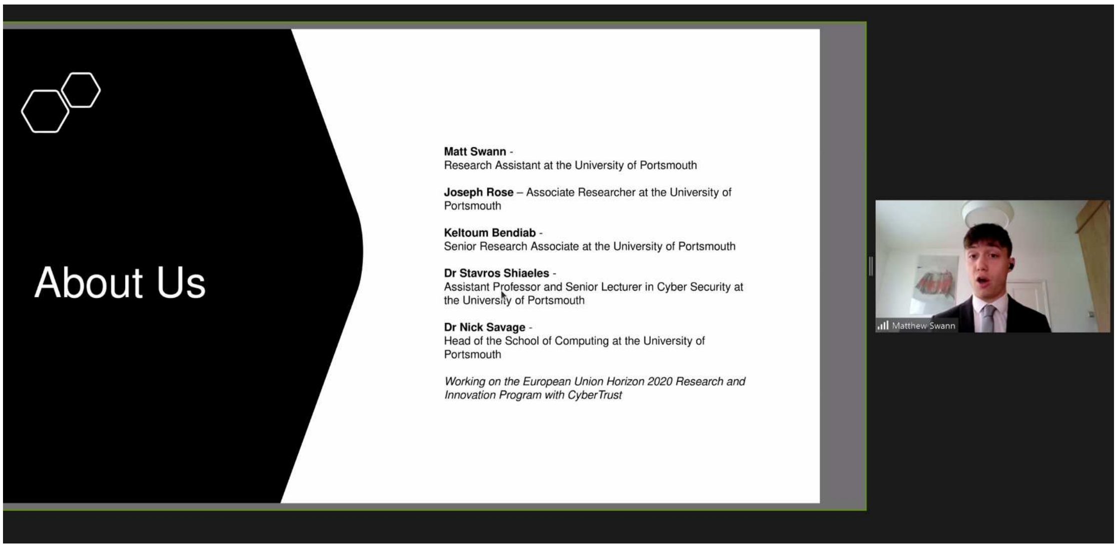
Click here to register for the WorldCIS Conference.

Speakers

Click here to learn more information about the Speakers

Programme

Learn more information about the Programme.



About Us

Matt Swann -
Research Assistant at the University of Portsmouth

Joseph Rose – Associate Researcher at the University of Portsmouth

Keltoum Bendiab -
Senior Research Associate at the University of Portsmouth

Dr Stavros Shiaeles -
Assistant Professor and Senior Lecturer in Cyber Security at the University of Portsmouth

Dr Nick Savage -
Head of the School of Computing at the University of Portsmouth

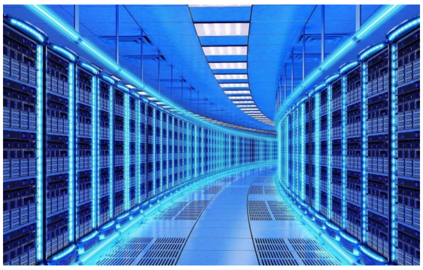
Working on the European Union Horizon 2020 Research and Innovation Program with CyberTrust

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

Academic Publications

Thermal Management in Large Data Centres: Security Threats and Mitigation

Authors: Betty Saridou, Gueltoum Bendiab, Stavros Shiaeles and Nick Savage

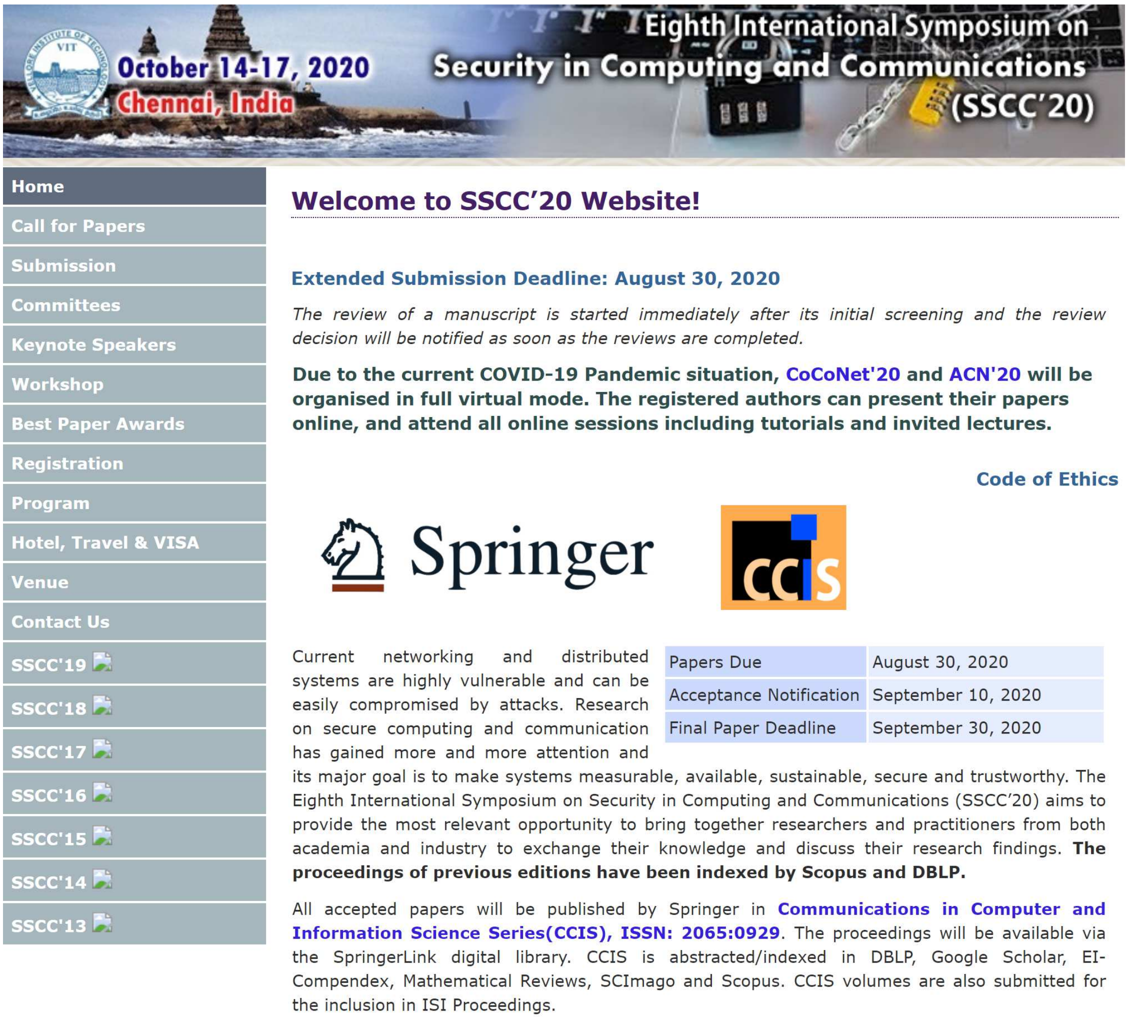


The paper entitled "*Thermal Management in Large Data Centres: Security Threats and Mitigation*" focus on the security issues and cyber-attacks aimed at specific physical components of data centres that keeps them operating. Especially, attacks against temperature monitoring and cooling systems of data centres, also known as thermal attacks, which can cause a complete meltdown. The research work analysed the potential security threats to these systems and their impact on the overall data centre safety and performance. It also studied current thermal anomaly detection methods and their limitations. Finally, it proposed a hybrid method that uses multi-variant anomaly detection to prevent thermal attacks, as well as a fuzzy-based health factor to enhance data centre thermal awareness and security.

The paper was accepted and presented in the Eighth International Symposium on Security in Computing and Communications (SSCC'20) co-affiliated with the International Conference on Applied Soft computing and Communication Networks (ACN'20). the conference was held in 14-17 October 2020, Chennai, India. **Due to the current COVID-19 Pandemic situation, CoCoNet'20 and ACN'20 were organised in full virtual mode.**

The paper will be published by Springer in Communications in Computer and Information Science Series (CCIS), ISSN: 2065:0929. The proceedings will be available via the SpringerLink digital library. This work is directly related to the work conducted in the WP6 of the Cyber-Trust project.

Link to the conference: http://www.acn-conference.org/2020/sscc2020/



Welcome to SSCC'20 Website!

Extended Submission Deadline: August 30, 2020

The review of a manuscript is started immediately after its initial screening and the review decision will be notified as soon as the reviews are completed.

Due to the current COVID-19 Pandemic situation, CoCoNet'20 and ACN'20 will be organised in full virtual mode. The registered authors can present their papers online, and attend all online sessions including tutorials and invited lectures.

Papers Due	August 30, 2020
Acceptance Notification	September 10, 2020
Final Paper Deadline	September 30, 2020

Current networking and distributed systems are highly vulnerable and can be easily compromised by attacks. Research on secure computing and communication has gained more and more attention and its major goal is to make systems measurable, available, sustainable, secure and trustworthy. The Eighth International Symposium on Security in Computing and Communications (SSCC'20) aims to provide the most relevant opportunity to bring together researchers and practitioners from both academia and industry to exchange their knowledge and discuss their research findings. **The proceedings of previous editions have been indexed by Scopus and DBLP.**

All accepted papers will be published by Springer in **Communications in Computer and Information Science Series(CCIS), ISSN: 2065:0929**. The proceedings will be available via the SpringerLink digital library. CCIS is abstracted/indexed in DBLP, Google Scholar, EI-Compendex, Mathematical Reviews, SCImago and Scopus. CCIS volumes are also submitted for the inclusion in ISI Proceedings.

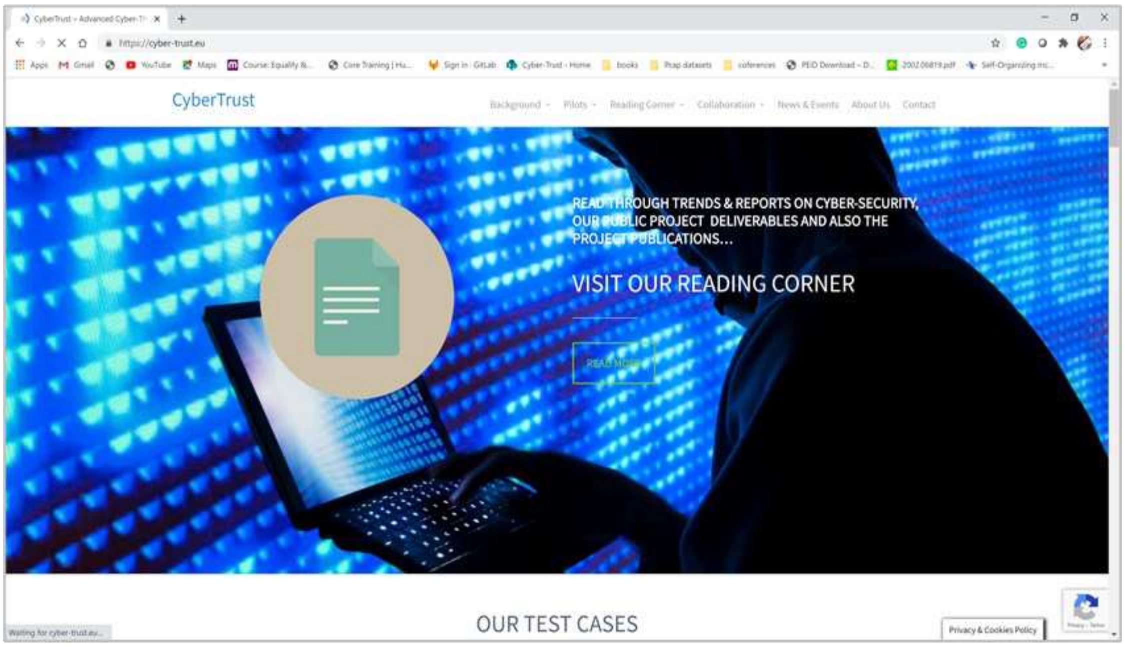
Cyber-Trust Website

Usage of the analytics platform MATOMO

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 30 months. IT hosts blogs 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.

Following the first project review outcomes, the Cyber-Trust website operators applied a number of changes on the Cyber-Trust website, with respect to third-party tools used in it. Primarily, the website operator implemented selected privacy-preserving and data protection friendly tools, based on “**EDRi’s #EthicalWebDev – guide for ethical website development and maintenance (2020)**”, including first-party cookies provided by MATOMO, replacing Google Analytics. MATOMO powers Europa Analytics, the analytics service used by the European Union institutions and agencies websites.

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



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

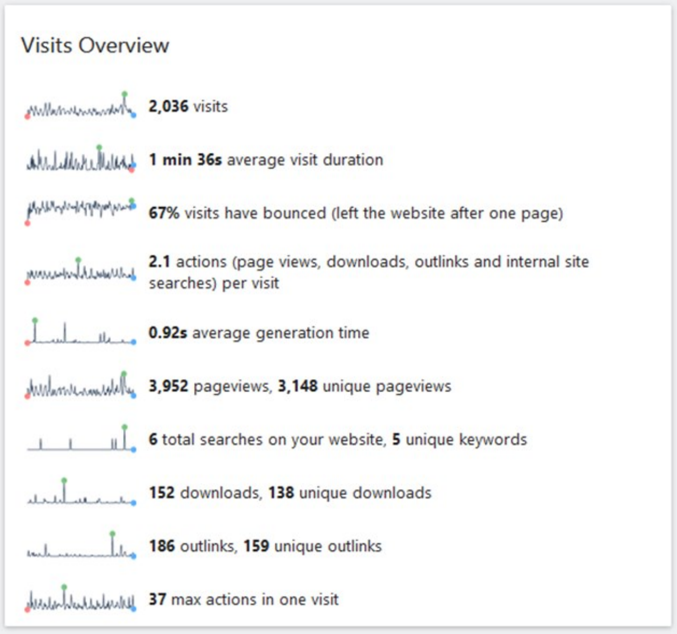
VISIT OUR READING CORNER

OUR TEST CASES

The following figures presents statistics related with the visits of the Cyber-Trust website. During the last period, about 2K users visited our website with the average visit time about 1.5 minutes. The number of maximum actions within a single visit is 37 while the number of downloads of content such as newsletters and deliverables is about 150.

Approximately the 25% of total visits are about returning visits. The average duration of returning visits is almost 3 minutes, number that indicates the interest of users reading Cyber-Trust content .

The Cyber-Trust has a world-wide visibility with the majority of visits coming from the USA.



Visits Overview

2,036 visits

1 min 36s average visit duration

67% visits have bounced (left the website after one page)

2.1 actions (page views, downloads, outlinks and internal site searches) per visit

0.92s average generation time

3,952 pageviews, **3,148** unique pageviews

6 total searches on your website, **5** unique keywords

152 downloads, **138** unique downloads

186 outlinks, **159** unique outlinks

37 max actions in one visit

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

Web site Blog Posts

Cyber-Trust Partners 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:

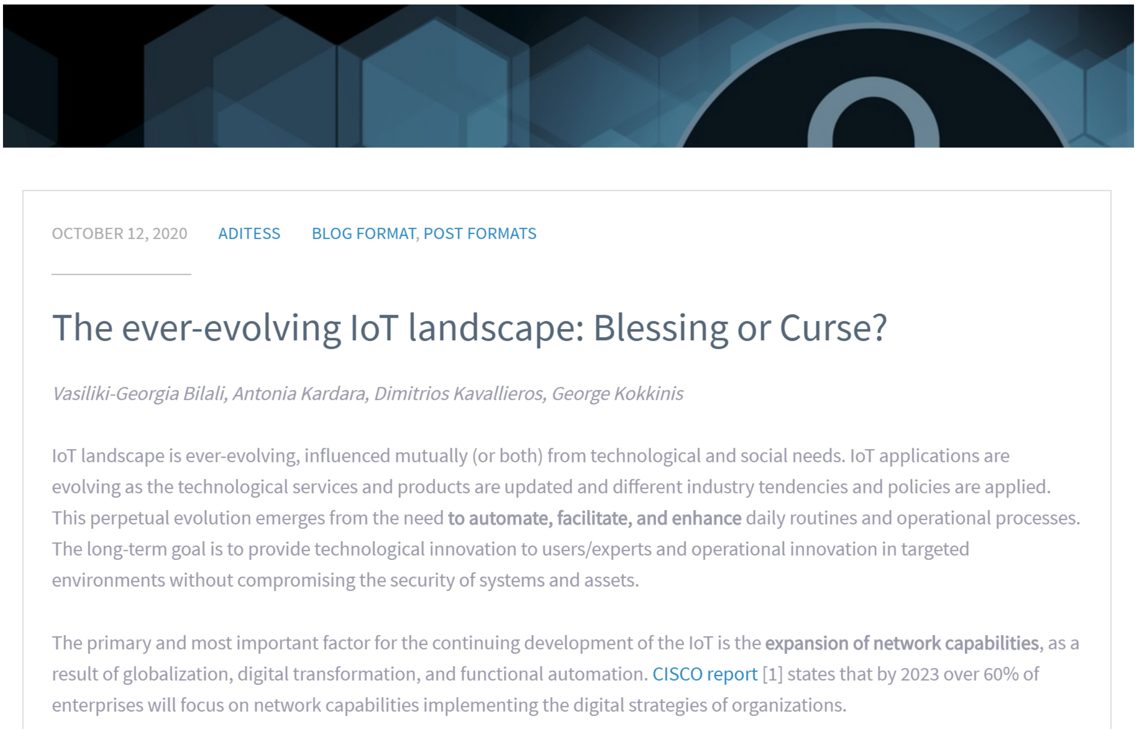
The ever-evolving IoT landscape: Blessing or Curse?

By Vasiliki-Georgia Bilali, Antonia Kardara, Dimitrios Kavallieros, George Kokkinis , 12 October 2020.

This blog post presented the continuous evolution of the IoT landscape which is bringing both technological innovations and security risks. Undoubtedly, the expansion of network capabilities gave the opportunity to many organisations all around the world to implement IoT technologies and increase their digital transformation. The dominance of Industry 4.0 gave the capability to worldwide industrial technologies to be developed. Some of these technologies are namely the predictive maintenance, the digital twins, the supply chain management etc. On the other hand, the growth of IoT botnet, the central orchestration of the ecosystem (automation) and the availability of the network are some of the aspects that have led to the expansion of threat landscape and increase the possibility of users to being attacked. In the blogpost, are introduced some security counter measures proposed by FBI.

On top of that, Cyber-Trust innovative solution came to the technology landscape to reinforce the positive side that can be derived from the IoT opportunity. The solution that promotes Cyber-Trust is aligned with the technical objectives of the project.

Link to the blog post:
https://cyber-trust.eu/2020/10/12/the-ever-evolving-iot-landscape-blessing-or-curse/



OCTOBER 12, 2020 ADITESS BLOG FORMAT, POST FORMATS

The ever-evolving IoT landscape: Blessing or Curse?

Vasiliki-Georgia Bilali, Antonia Kardara, Dimitrios Kavallieros, George Kokkinis

IoT landscape is ever-evolving, influenced mutually (or both) from technological and social needs. IoT applications are evolving as the technological services and products are updated and different industry tendencies and policies are applied. This perpetual evolution emerges from the need **to automate, facilitate, and enhance** daily routines and operational processes. The long-term goal is to provide technological innovation to users/experts and operational innovation in targeted environments without compromising the security of systems and assets.

The primary and most important factor for the continuing development of the IoT is the **expansion of network capabilities**, as a result of globalization, digital transformation, and functional automation. CISCO report [1] states that by 2023 over 60% of enterprises will focus on network capabilities implementing the digital strategies of organizations.

Web site Blog Posts

The Choice of Architecture Methodology in the Design of the Cyber-Trust System

CGI, October 2020

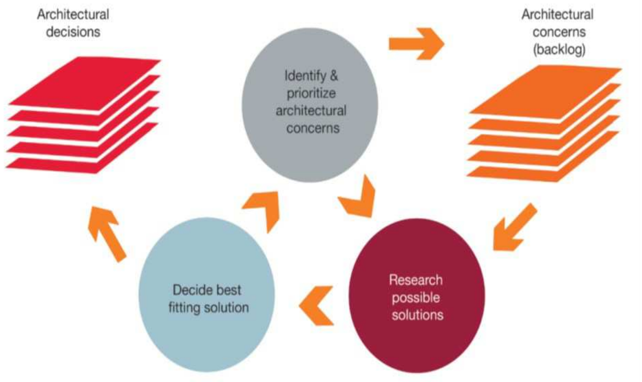
At the time when the project Cyber-Trust is progressing towards the implementation of the pilots, it's timely to talk about the architecture methodology chosen by the consortium of the project Cyber-Trust which is the backbone of the technological platform has been built. Important interim validated outcome is that the Cyber-Trust architecture is robust and resilient. The conclusive outcomes will be reported when the pilots are completed. Architecture in the digital world is not just a good idea; it is an essential discipline to safeguard the quality and future proofs of modern, complex IT-based solutions. Therefore, it is essential to choose the most efficient methodology for Cyber-Trust system architecture design which is very complex by its nature.

The architecture of Cyber-Trust is **modular** on open APIs, with flexibility to adapt and connect to existing police CAD/DBMS and provide tailor-made (cherry picking) solution. As a modular design, Cyber-Trust system is composed of separate components that can be connected together. The beauty of Cyber-Trust modular architecture is that we can replace or add any one component (module) without affecting the rest of the system. Therefore, the choice of the architectural method, which is a recognized method in the Open Group Certified Architect program, that is used in Cyber-Trust is the proven Risk- and Cost-Driven Architecture (RCDA), an agile solution architecture approach, which is a relatively new approach. It was developed to close the gaps between enter-prise and software architecture. Existing software architecture practices often are too limited in scope for the solutions that need to be archi-tected. However, enterprise architecture practices are too heavy for the agility required to manage time pressures and frequently occurring changes and uncertainty. RCDA incorporates a number of aspects from agile software development prac-tices, such as the use of a backlog of architectural concerns, to be frequently reprioritized based on economic factors like risk and cost.

During the Cyber-Trust system architecture design, RCDA method supported the architects throughout the process of interpreting stakeholders' requirements, and subsequently designing and delivering the best fitting solution in a lean, mean and agile manner. Architectural concerns and architectural decisions are weighed throughout the process, and stakeholder requirements are constantly taken into account.

When viewed as a risk and cost management discipline, architecture does not need to obstruct agility. RCDA offers a proven approach to solution architecture that is well-suited to today's agile end-users needs which is essential for Cyber-Trust.

Applying the RCDA method, setting up the Cyber-Trust architecture different practice sets are identified (requirement analysis, solution shaping, architecture validation and architecture fulfilment).


Architectural decisions
Identify & prioritize architectural concerns
Architectural concerns (backlog)
Decide best fitting solution
Research possible solutions

RCDA's architecting workflow: a backlog of architectural concerns is used to increase agility

The application of RCDA brings various advantages to Cyber-Trust:

- It **smoothens communication** between solution architects and business stakeholders – RCDA-trained architects communicate about architectural decisions and trade-offs
- A **clear and agreed set of architectural requirements** for design decisions, using objective and economically oriented trade-offs, rather than hypes or personal preferences.
- It reduces the risk of **delayed delivery and budget overruns** – RCDA sees architecture as a risk- and cost management discipline with economic awareness in the design process and avoiding "gold-plating".
- It **enhances the quality of solutions** – RCDA practices are CMMI (Capability Maturity Model Integration) compliant, and contain guidance for early and effective evaluation of quality attributes.
- It **creates transparency in costing structures** – RCDA provides traceability from architectural requirements to the costing model for the whole solution and its parts.

After the validation of the architecture, the platform development took place successfully. At this stage the pilots are ongoing. As per nature of RCDA architecture method, Cyber-Trust system is continuously being applied the principles of the method until the system is complete and operational. More information about the progress can be found in https://cyber-trust.eu/ .

Link to the blog post: https://cyber-trust.eu/2020/11/24/the-choice-of-architecture-methodology-in-the-design-of-the-cybertrust-system/.

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

Web site Blog Posts

The New EU Cybersecurity Strategy

ADITESS, January 2021

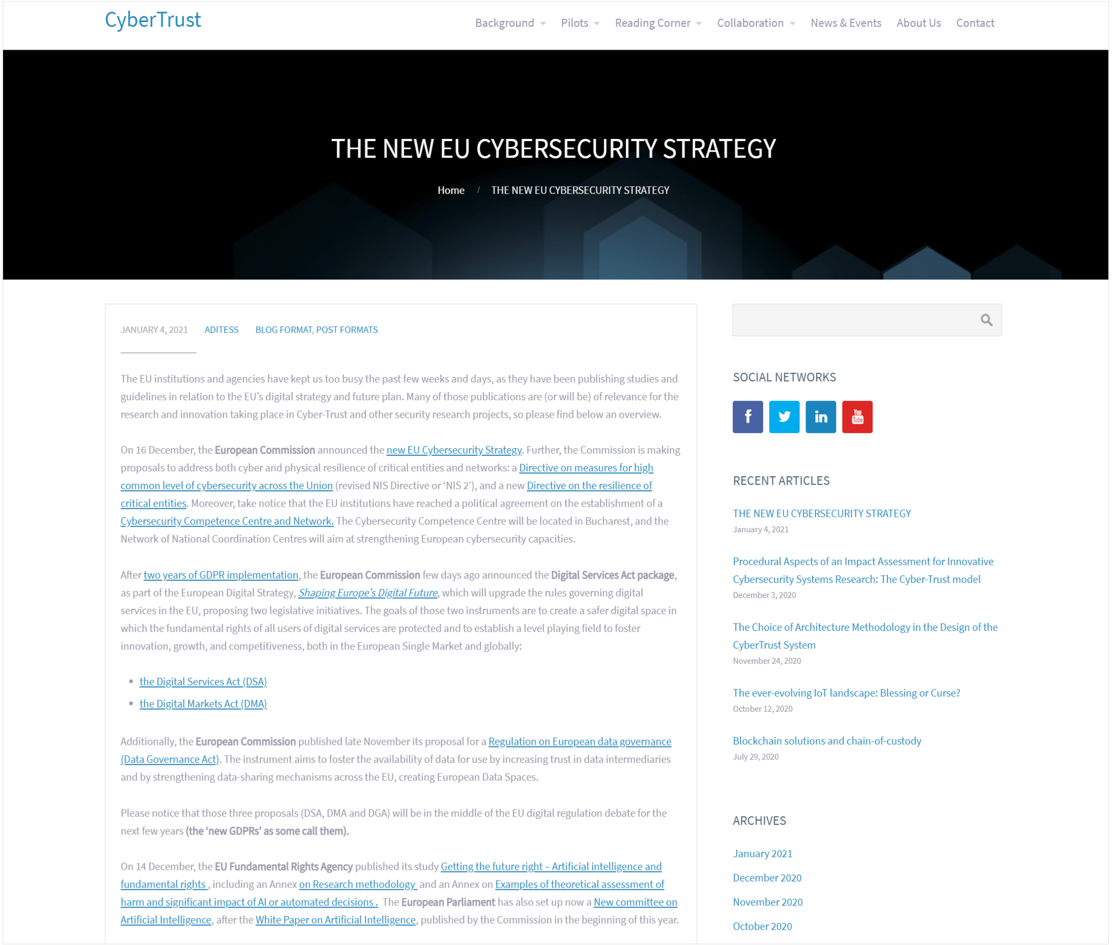
The Blog post ‘The New EU Cybersecurity Strategy was published on the Cyber-Trust website on January 2021. The blog post discusses the EU’s digital strategy and future plan and proposals to address both cyber and physical resilience of critical entities and networks. The EU institutions and agencies have kept us too busy the past few weeks and days, as they have been publishing studies and guidelines in relation to the EU’s digital strategy and future plan. Many of those publications are (or will be) of relevance for the research and innovation taking place in Cyber-Trust and other security research projects, so please find below an overview.

On 16 December, the European Commission announced the new EU Cybersecurity Strategy. Further, the Commission is making proposals to address both cyber and physical resilience of critical entities and networks: a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or ‘NIS 2’), and a new Directive on the resilience of critical entities. Moreover, take notice that the EU institutions have reached a political agreement on the establishment of a Cybersecurity Competence Centre and Network. The Cybersecurity Competence Centre will be located in Bucharest, and the Network of National Coordination Centres will aim at strengthening European cybersecurity capacities.

After two years of GDPR implementation, the **European Commission** few days ago announced the **Digital Services Act package**, as part of the European Digital Strategy, *Shaping Europe’s Digital Future*, which will upgrade the rules governing digital services in the EU, proposing two legislative initiatives. The goals of those two instruments are to create a safer digital space in which the fundamental rights of all users of digital services are protected and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally:

- the Digital Services Act (DSA)
- the Digital Markets Act (DMA)

Link to the blog post:
https://cyber-trust.eu/2021/01/04/the-new-eu-cybersecurity-strategy/



THE NEW EU CYBERSECURITY STRATEGY

JANUARY 4, 2021 ADITESS BLOG FORMAT, POST FORMATS

The EU institutions and agencies have kept us too busy the past few weeks and days, as they have been publishing studies and guidelines in relation to the EU’s digital strategy and future plan. Many of those publications are (or will be) of relevance for the research and innovation taking place in Cyber-Trust and other security research projects, so please find below an overview.

On 16 December, the **European Commission** announced the new EU Cybersecurity Strategy. Further, the Commission is making proposals to address both cyber and physical resilience of critical entities and networks: a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or ‘NIS 2’), and a new Directive on the resilience of critical entities. Moreover, take notice that the EU institutions have reached a political agreement on the establishment of a Cybersecurity Competence Centre and Network. The Cybersecurity Competence Centre will be located in Bucharest, and the Network of National Coordination Centres will aim at strengthening European cybersecurity capacities.

After two years of GDPR implementation, the **European Commission** few days ago announced the **Digital Services Act package**, as part of the European Digital Strategy, *Shaping Europe’s Digital Future*, which will upgrade the rules governing digital services in the EU, proposing two legislative initiatives. The goals of those two instruments are to create a safer digital space in which the fundamental rights of all users of digital services are protected and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally:

- the Digital Services Act (DSA)
- the Digital Markets Act (DMA)

Additionally, the **European Commission** published late November its proposal for a Regulation on European data governance (Data Governance Act). The instrument aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU, creating European Data Spaces.

Please notice that those three proposals (DSA, DMA and DGA) will be in the middle of the EU digital regulation debate for the next few years **(the ‘new GDPRs’ as some call them).**

On 14 December, the **EU Fundamental Rights Agency** published its study Getting the future right – Artificial intelligence and fundamental rights , including an Annex on Research methodology and an Annex on Examples of theoretical assessment of harm and significant impact of AI or automated decisions . The **European Parliament** has also set up now a New committee on Artificial Intelligence, after the White Paper on Artificial Intelligence, published by the Commission in the beginning of this year.

RECENT ARTICLES

THE NEW EU CYBERSECURITY STRATEGY
January 4, 2021

Procedural Aspects of an Impact Assessment for Innovative Cybersecurity Systems Research: The Cyber-Trust model
December 3, 2020

The Choice of Architecture Methodology in the Design of the CyberTrust System
November 24, 2020

The ever-evolving IoT landscape: Blessing or Curse?
October 12, 2020

Blockchain solutions and chain-of-custody
July 29, 2020

ARCHIVES

January 2021
December 2020
November 2020
October 2020

Press Releases

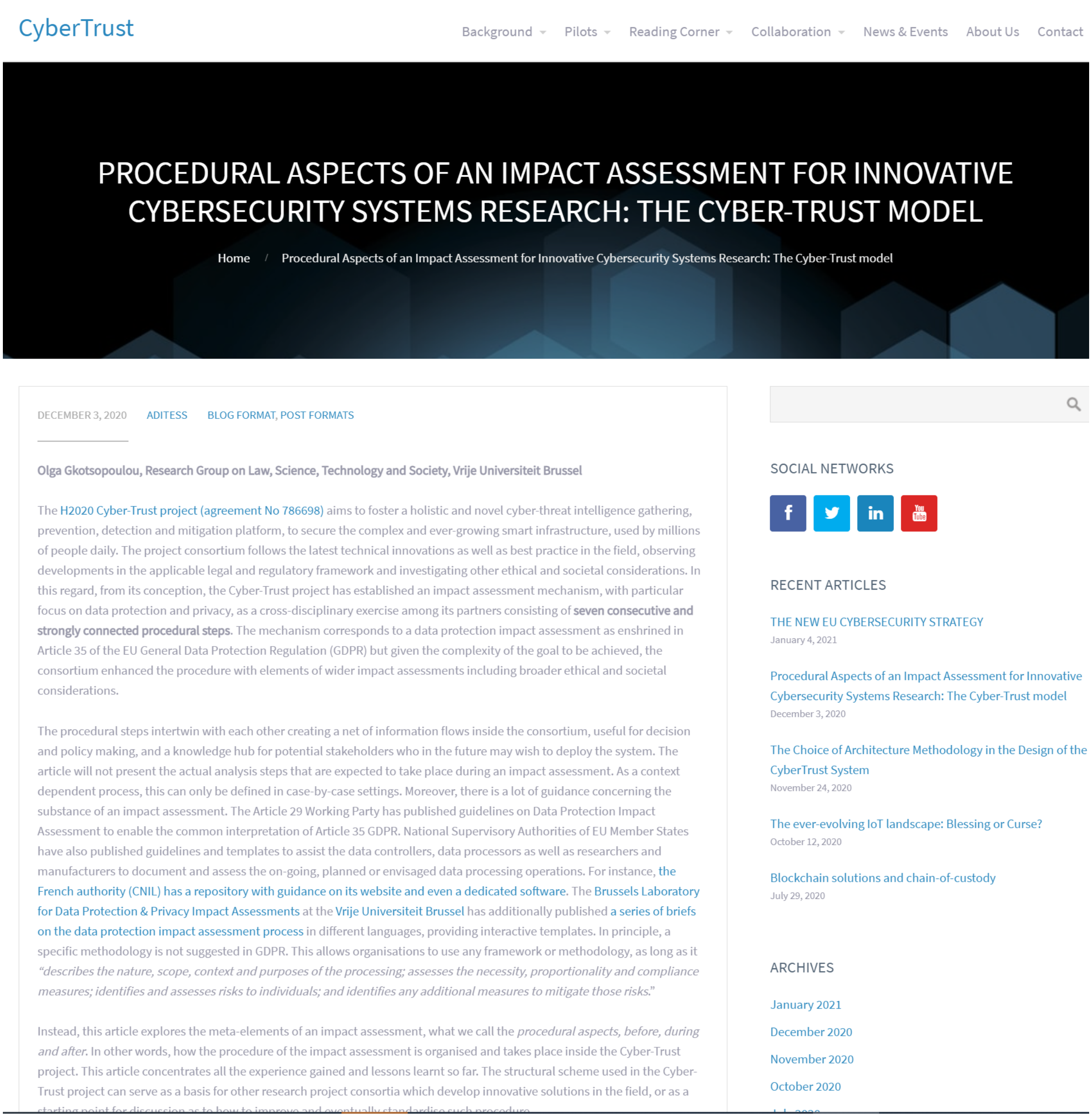
Procedural Aspects of an Impact Assessment for Innovative Cybersecurity Systems Research: The Cyber-Trust mode

VUB, December 2020

The press release ‘Procedural Aspects of an Impact Assessment for Innovative Cybersecurity Systems Research: The Cyber-Trust model’ was published on the Cyber-Trust website on 3 December 2020. The press release cumulates the lessons learnt from the impact assessment procedure followed during the project and provides a procedural model of seven clearly defined steps, which can be adopted by other cybersecurity research projects.

At the time when the project Cyber-Trust is progressing towards the implementation of the pilots, it’s timely to talk about the architecture methodology chosen by the consortium of the project Cyber-Trust which is the backbone of the technological platform has been built. Important interim validated outcome is that the Cyber-Trust architecture is robust and resilient. The conclusive outcomes will be reported when the pilots are completed. Architecture in the digital world is not just a good idea; it is an essential discipline to safeguard the quality and future proofs of modern, complex IT-based solutions. Therefore, it is essential to choose the most efficient methodology for Cyber-Trust system architecture design which is very complex by its nature.

The press release can be found here: https://cyber-trust.eu/2020/12/03/procedural-aspects-of-an-impact-assessment-for-innovative-cybersecurity-systems-research-the-cyber-trust-model/



PROCEDURAL ASPECTS OF AN IMPACT ASSESSMENT FOR INNOVATIVE CYBERSECURITY SYSTEMS RESEARCH: THE CYBER-TRUST MODEL

Home / Procedural Aspects of an Impact Assessment for Innovative Cybersecurity Systems Research: The Cyber-Trust model

DECEMBER 3, 2020   ADITESS   BLOG FORMAT, POST FORMATS

Olga Gkotsopoulou, Research Group on Law, Science, Technology and Society, Vrije Universiteit Brussel

The H2020 Cyber-Trust project (agreement No 786698) aims to foster a holistic and novel cyber-threat intelligence gathering, prevention, detection and mitigation platform, to secure the complex and ever-growing smart infrastructure, used by millions of people daily. The project consortium follows the latest technical innovations as well as best practice in the field, observing developments in the applicable legal and regulatory framework and investigating other ethical and societal considerations. In this regard, from its conception, the Cyber-Trust project has established an impact assessment mechanism, with particular focus on data protection and privacy, as a cross-disciplinary exercise among its partners consisting of **seven consecutive and strongly connected procedural steps**. The mechanism corresponds to a data protection impact assessment as enshrined in Article 35 of the EU General Data Protection Regulation (GDPR) but given the complexity of the goal to be achieved, the consortium enhanced the procedure with elements of wider impact assessments including broader ethical and societal considerations.

The procedural steps intertwin with each other creating a net of information flows inside the consortium, useful for decision and policy making, and a knowledge hub for potential stakeholders who in the future may wish to deploy the system. The article will not present the actual analysis steps that are expected to take place during an impact assessment. As a context dependent process, this can only be defined in case-by-case settings. Moreover, there is a lot of guidance concerning the substance of an impact assessment. The Article 29 Working Party has published guidelines on Data Protection Impact Assessment to enable the common interpretation of Article 35 GDPR. National Supervisory Authorities of EU Member States have also published guidelines and templates to assist the data controllers, data processors as well as researchers and manufacturers to document and assess the on-going, planned or envisaged data processing operations. For instance, the French authority (CNIL) has a repository with guidance on its website and even a dedicated software. The Brussels Laboratory for Data Protection & Privacy Impact Assessments at the Vrije Universiteit Brussel has additionally published a series of briefs on the data protection impact assessment process in different languages, providing interactive templates. In principle, a specific methodology is not suggested in GDPR. This allows organisations to use any framework or methodology, as long as it *“describes the nature, scope, context and purposes of the processing; assesses the necessity, proportionality and compliance measures; identifies and assesses risks to individuals; and identifies any additional measures to mitigate those risks.*”

Instead, this article explores the meta-elements of an impact assessment, what we call the *procedural aspects, before, during and after*. In other words, how the procedure of the impact assessment is organised and takes place inside the Cyber-Trust project. This article concentrates all the experience gained and lessons learnt so far. The structural scheme used in the Cyber-Trust project can serve as a basis for other research project consortia which develop innovative solutions in the field, or as a starting point for discussion as to how to improve and eventually standardise such procedure.

RECENT ARTICLES

THE NEW EU CYBERSECURITY STRATEGY
January 4, 2021

Procedural Aspects of an Impact Assessment for Innovative Cybersecurity Systems Research: The Cyber-Trust model
December 3, 2020

The Choice of Architecture Methodology in the Design of the CyberTrust System
November 24, 2020

The ever-evolving IoT landscape: Blessing or Curse?
October 12, 2020

Blockchain solutions and chain-of-custody
July 29, 2020

ARCHIVES

January 2021
December 2020
November 2020
October 2020
July 2020

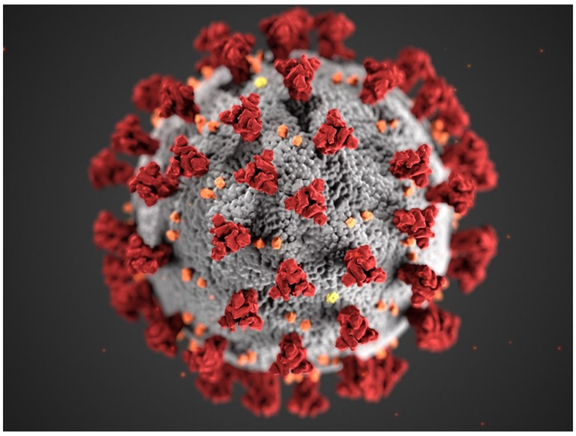
This project has received funding from the European Union’s Horizon 2020 research and innovation program.

Press Releases

Cyber Security Challenges During the COVID-19 Pandemic

Gueltoum Bendiab, Stavros Shiaeles, Gohar Sargsyan, December 2020

The press release 'Cyber Security Challenges during the COVID-19 Pandemic' was published on the Cyber-Trust website on December 2020. The press release highlights security challenges facing individuals and organisations during this unprecedented event that altered the lives of billions of people globally and greatly increased the risk of cyber-attacks .



Clearly, the 2020 year was quite challenging for organisations and individuals in terms of cybersecurity along with the adoption of new working habits, especially since the COVID-19 outbreak in March 2020. The rapid and unexpectedly broad disruption to businesses around the world has let companies struggling to maintain security and business continuity. In this new environment, cybersecurity efforts must aggressively confront the risks. Organisations should secure their newly implemented remote working practices and maximise their ability to prevent, detect and respond to threats. They should also prioritise reducing reliance on people, as well as maximising the use of process and technology to perform key cyber security activities to ensure continuity.

Cyber-Trust project provides a robust security solution for that new environment by proposing a new Intrusion Prevention System able to detect and mitigate attacks using Machine Learning (ML) and Graph Theory for an optimal decision on the threat detected. The combination of ML Intrusion Detection Systems (IDS) and Graphical Cyber Security Models (GCSMs) can lead to an innovative class of intelligent intrusion response systems (iIRS) providing dynamic security risk assessment and intelligent mitigation strategies to defend against adaptive multi-stage cyber-attacks on IoT platforms, including smart homes, optimally and autonomously. This is done by building upon advanced game-theoretic security approaches, where accurate model of attackers and defenders (players), their interactions and the IoT network parameters would be able to calculate all the possible scenarios and provide the optimal solution to be applied by IDS. This will generate a positive impact on small and medium-sized enterprises, but also to critical infrastructures and industrial IoT facilities as will be able to mitigate even (unknown) sophisticated cyber-attacks, especially in the case of large-scale crises like the COVID-19 pandemic. It will also help individual users to maintain a comfortable and safe environment in their smart homes, where any compromised device will be easily identified and prevented from gaining access to critical network resources and services.

In order to help the users to be more aware on sophisticated attacks creating serious game for security awareness. The game will aim for learning, raising awareness of risks, motivating to be up to date on potential risks and empowering users and communities on be active and safe from potential issues as a result of those risks. To do this, Game Thinking and Game Dynamics will be applied for better engage audiences and solve problems. The game will also be a very good method at teaching and training. The players will be gradually presented with information, and ensure they know the skills they need to know. The game teams will collaborate during their sprint event to tackle different risk challenges. Squad based data-driven strategy game will be designed to increase DevOps squads' risk awareness and Secure-By-Design mindset. In a nutshell, this game will offer data-driven security Gamification impacted by real-world performance, integrated in regular sprint cycle for sustained effect and will leverage squad competition and peer pressure to motivate players. This approach will facilitate faster and more effective security awareness for the users especially in the times of crisis, such as COVID-19 .

The press release can be found on the Cyber-Trust website:
https://cyber-trust.eu/2021/01/07/cyber-security-challenges-during-the-covid-19-pandemic/

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:

Live Webinar – Women Practicing Cyber-security Share About Blue Team, Career Transition and Diversity

17 December, 2020

Cyber-trust partners have participated in the organised the 12th International Network Conference (INC 2020).

Link: [http://www.inc-conference.org/.](http://www.inc-conference.org/)

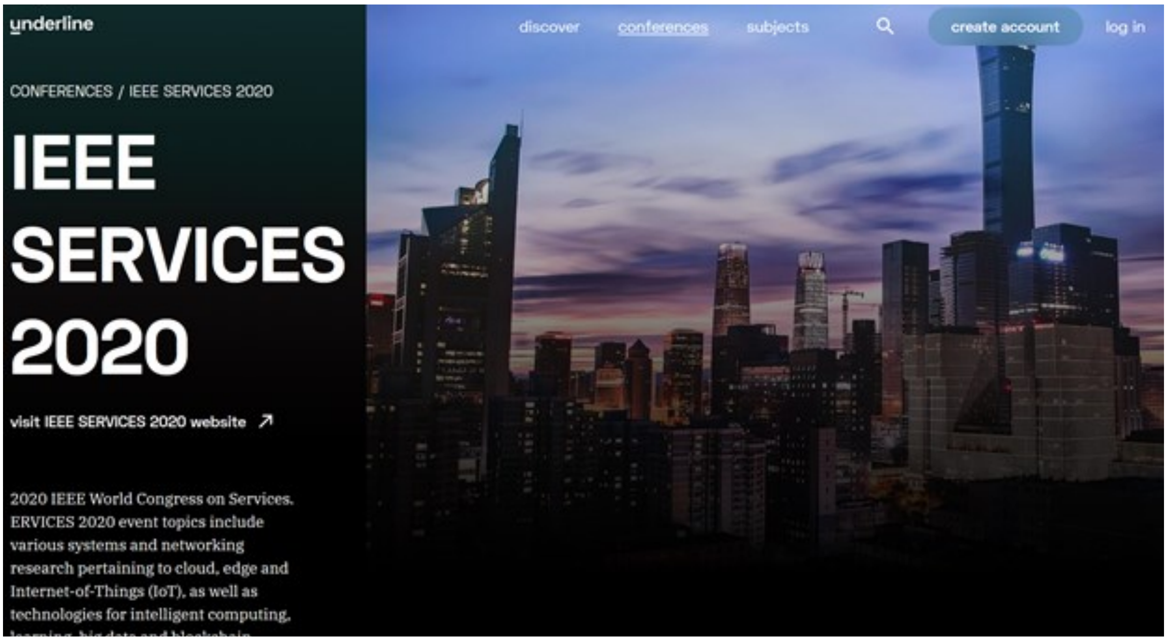
The INC events have always The webinar was organised by Dr Magda Chelly, Head of Cyber Risk Consulting, CISO, Entrepreneur March Asia. The event gathered together more than 100 experts. It was to find out more about Women in Cybersecurity and show support towards them. The event was open for men and women. Cyber-Trust project was introduced during the webinar and also women engaged in Cyber-Trust project were promoted.

Organisation of the IEEE services (CSRIOT) workshop

18-24 October, 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. **Due to the current COVID-19 situation, IEEE SERVICES 2020 did not take place in Beijing, China and instead took place virtually. Proceedings will not be cancelled, and publications will continue as planned. All presentations were given through the underline platform .**

- **Link to the workshop:** https://conferences.computer.org/services/2020/workshops/csriot2020.html
- **Link on underline:** https://www.underline.io/conferences/34-ieee-services-2020



CONFERENCES / IEEE SERVICES 2020

IEEE SERVICES 2020

visit IEEE SERVICES 2020 website ↗

2020 IEEE World Congress on Services. ERVICES 2020 event topics include various systems and networking research pertaining to cloud, edge and Internet-of-Things (IoT), as well as technologies for intelligent computing.

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

Organised dissemination events

Organisation of a scientific conference INC 2020

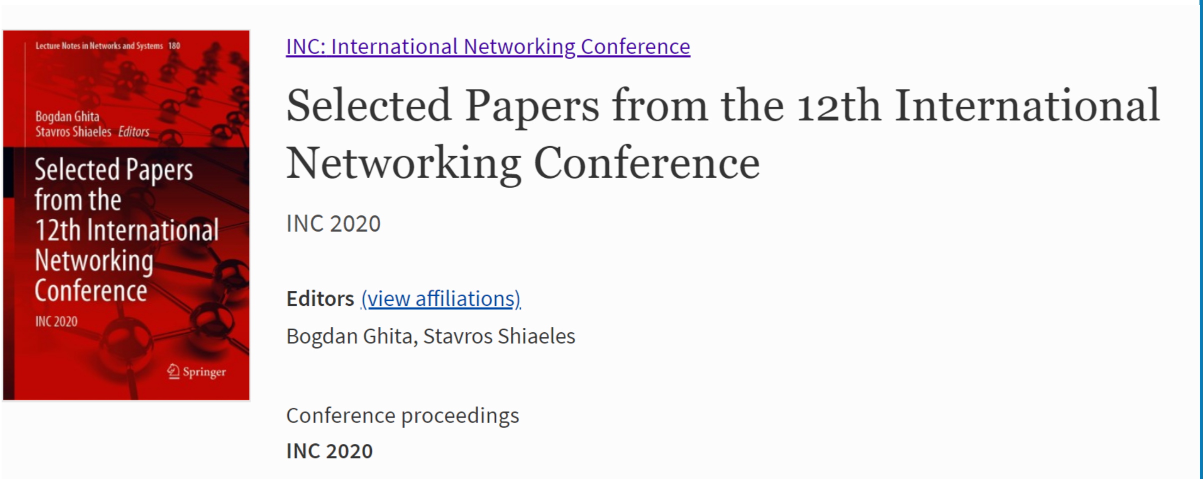
21 September, 2020

Cyber-Trust partners have participated in the organisation of 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 their proceedings via their **Open Access Repository**. Suggested topics for papers include, but are not limited to, the following:

- Network architectures: NFV, SDN, Future networks, Vehicular networking, Delay-tolerant networking, Peer to peer networks, Green networking, Network testbeds
- Traffic engineering and network management: Routing, Network coding, Network and Service management, Traffic engineering, Congestion control
- Application performance: Quality of Service, Quality of Experience, Multimedia over IP, Real time applications
- Mobile networking and services: 5G, 4G/LTE, Mobile commerce, Service discovery and management, Telecommunication services, Cloud computing
- Wireless networking: Wireless local & personal area networks, Wireless multimedia systems, Wireless protocols, Wireless sensor networks
- Internet of Things: Wireless sensor networks, NFC, RFID, Big data, measurement and visualisation
- Applications and impacts: Virtual communities, Pervasive networks, Network-enabled devices, Smart City, Smart Grid, Smart Home, Distributed Systems and middleware
- Security and privacy: Authentication and access control, Network security, Intrusion detection and response, Digital Forensics

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

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



Lecture Notes in Networks and Systems 180

Bogdan Ghita
Stavros Shiaeles *Editors*

Selected Papers from the 12th International Networking Conference

INC 2020

Springer

INC: International Networking Conference

Selected Papers from the 12th International Networking Conference

INC 2020

Editors (view affiliations)

Bogdan Ghita, Stavros Shiaeles

Conference proceedings

INC 2020

12th International Network Conference 2020 (INC2020)

Rhodes, Greece, 19-21 September 2020

Virtual Conference due to COVID-19

●○○○○○○

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

Coming events

Organisation of the SecSoft 2021 workshop

28 June-2 July 2021

The 7th IEEE International Conference on Network Softwarization (IEEE NetSoft 2021) will be held in Tokyo, Japan from June 28 to July 2, 2021 just before the Tokyo 2020 Olympic and Paralympic Games. The theme of the IEEE NetSoft 2021 "Accelerating Network Softwarization in the Cognitive Age" reflects the current trend of research in the area of network softwarization. The IEEE NetSoft 2021 showcased the latest research and development results including artificial intelligence / machine learning, self -driving and autonomic networking, policy-based network management, dynamic network slice provisioning, among other promising research areas for the sake of robust, reliable and cognitive softwarized networks.

IEEE NetSoft 2021 aimed at bringing together students, researchers and security experts on areas under consideration by Cyber-Trust. Indicative topics of interest included:

- Softwarized cloud, fog, and edge infrastructures
- Cognitive and autonomic networking
- Centralized vs distributed control, management & orchestration
- Abstractions and virtualization of resources, services and functions
- AI techniques to support network automation
- Big data analytics for managing softwarized networks
- Network slicing and slice management
- Mobility management in softwarized networks
- Programmable SDN and NFV: languages and architectures
- Policy-based and intent-based networking
- Service Function Chaining (SFC)
- Mapping and scheduling of SFC
- Container/microservice-based network functions
- Efficient network/service monitoring in SDN/NFV
- QoS and QoE in softwarized infrastructures
- Resilience, reliability, and robustness of softwarized networks
- Network softwarization for 5G.
- Network management at the edge
- Cooperative multi-domain, multi-tenant SDN/NFV environments
- Security, Safety, Trust and Privacy in virtualized environments
- SDN switch/router architecture and design
- Dynamic resource discovery and negotiation schemes
- Lifecycle management of network software
- DevOps methodologies for network softwarization
- Debugging and introspection of software-defined systems
- Softwarized platforms for Internet of Things (IoT)
- Energy-efficient and green software-defined infrastructures (SDI)
- Transition strategies from existing networks to SDN/NFV
- New value chains and service models enabled by softwarization
- Socio-economic impact and regulations for softwarization
- Experience reports from experimental testbeds and deployments

Link to the workshop: https://netsoft2021.ieee-netsoft.org/

Topics in this workshop are directly related with work carried out in work-packages 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/).

IEEE NETSOFT

IEEE International Conference on Network Softwarization
28 June-2 July 2021 // Tokyo, Japan
Accelerating Network Softwarization in the Cognitive Age

IEEE ComSoc
IEEE Communications Society

IEEE

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

Coming events

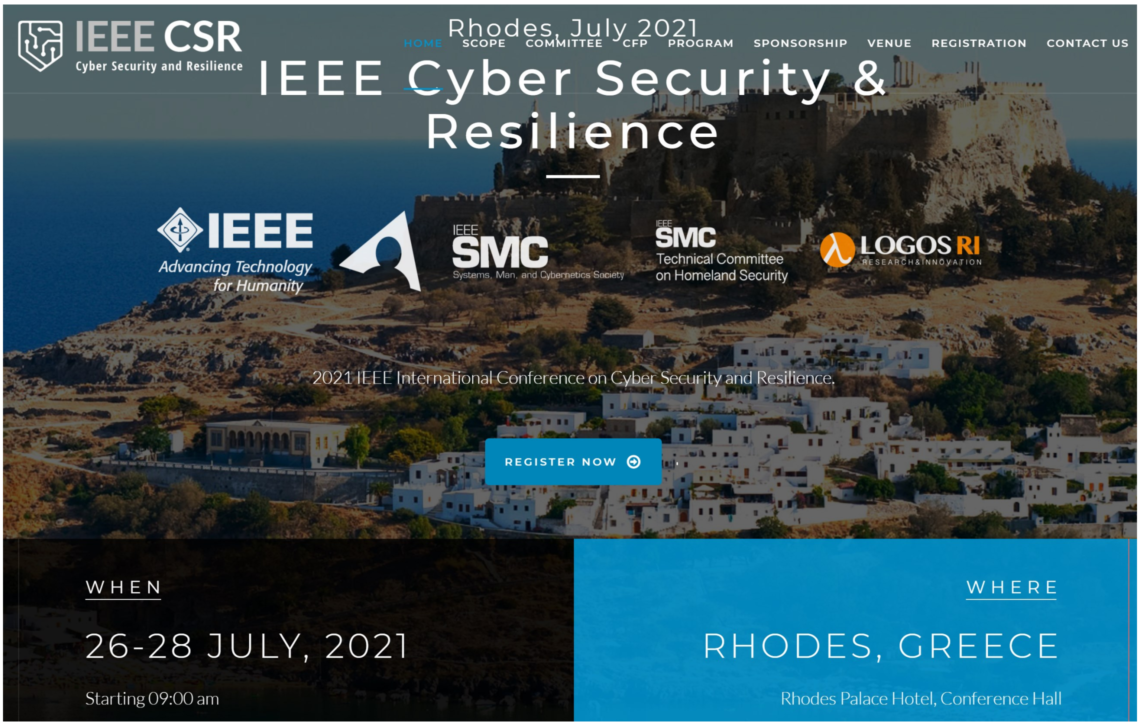
Organisation of the IEEE Cyber Security & Resilience

26-28 July, 2021

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. The conference focuses on theoretical and practical aspects of the security, privacy, trust, and resilience of networks, systems, and services as well as novel ways for dealing with their vulnerabilities and mitigating sophisticated cyber-attacks.

- Big data security and analytics,
- Blockchain and DLT security,
- Cloud-edge security and privacy,
- Cyber-security and artificial intelligence,
- Cyber-threat intelligence,
- Distributed systems security,
- Game-theoretic security,
- Forensics,
- Identity management and access control,
- Insider Threats,
- Lightweight cryptography,
- Malicious cryptography,
- Malware detection and remediation,
- Moving target defense,
- Network intrusion detection and mitigation,
- Post-quantum security,
- Privacy and data protection,
- Security Visualisation,
- Smart contracts security,
- Software security,
- System and data integrity,
- Trust management systems,
- Trusted execution environments,
- Web services security and trust

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/).



Rhodes, July 2021

IEEE Cyber Security & Resilience

2021 IEEE International Conference on Cyber Security and Resilience.

WHEN

26-28 JULY, 2021

Starting 09:00 am

WHERE

RHODES, GREECE

Rhodes Palace Hotel, Conference Hall

IEEE CSR
Cyber Security and Resilience
HOME
SCOPE
COMMITTEE
CFP
PROGRAM
SPONSORSHIP
VENUE
REGISTRATION
CONTACT US
IEEE
Advancing Technology for Humanity
IEEE SMC
Systems, Man, and Cybernetics Society
IEEE SMC
Technical Committee on Homeland Security
LOGOS RI
RESEARCH & INNOVATION
REGISTER NOW

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

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