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

Newsletter Vol. 5— April 2021

Welcome to our 5th 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.

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 include:

A Comparative Study of Traffic Generators: Applicability for Malware Detection Testbeds

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

This research paper is an extended version of the conference paper titled "*Tools for Network Traffic Generation - A Quantitative Comparison*" that has 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.

The paper 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.

ISSN 2046-3723 (Online)

Journal of Internet Technology and Secured Transactions

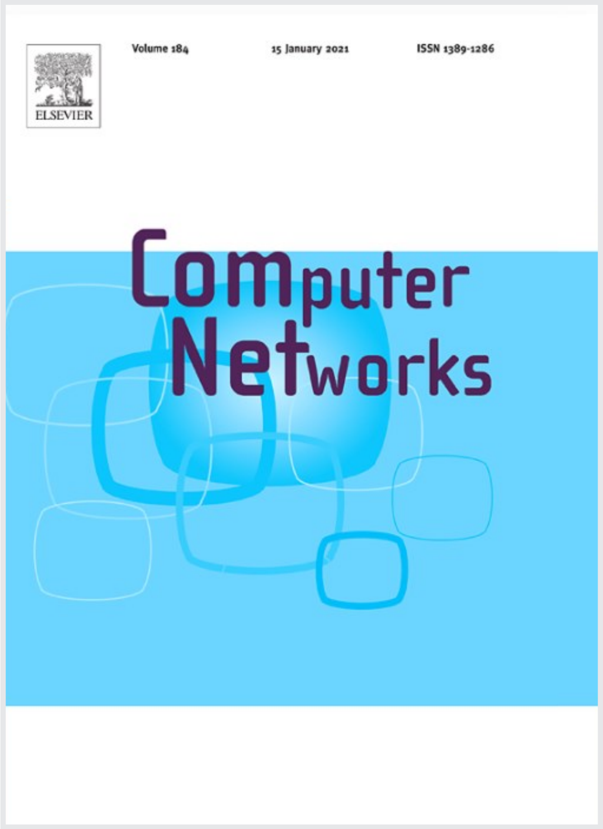
The extended paper will be published in the **Journal of Internet Technology and Secured Transactions (JITST)**, which is a peer-reviewed and open-access journal. The JITST provides an international forum for electronic publication of high-quality scholarly papers in Internet Technology and Secured Transactions. The peer review process and publications in the JITST are free (no fees apply). Authors retain the publishing rights without restrictions .

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

Academic Publications

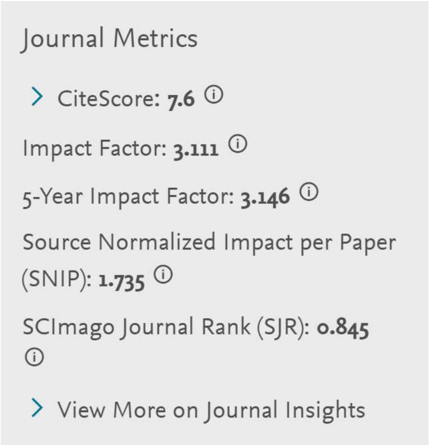
On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance

Sotirios Brotsis, Konstantinos Limniotis, Gueltoum Bendiab, Nicholas Kolokotronis, Stavros Shiaeles



Blockchain and distributed ledger technologies have received significant interest in various areas beyond the financial sector, with profound applications in the Internet of Things (IoT), providing the means for creating truly trustless and secure solutions for IoT applications. Taking into account the weak security defences that the majority of IoT devices have, it is critical that a blockchain-based solution targeting the IoT is not only capable of addressing the many challenges IoT is facing, but also does not introduce other defects, e.g., in terms of performance, making its adoption hard to achieve.

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, as well as 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. On the other side, privacy related mechanisms are being supported, to varying degrees, by all platforms investigated; however, each of the them tackles specific only privacy aspects, thus rendering the overall privacy evaluation a challenging task which needs to be considered in an Ad-Hoc basis. 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. The work presented in this paper is directly related to the work carried out in work-package 6 and 7 (WP6 and WP7).


Journal Metrics

› CiteScore: **7.6** ⓘ

Impact Factor: **3.111** ⓘ

5-Year Impact Factor: **3.146** ⓘ

Source Normalized Impact per Paper (SNIP): **1.735** ⓘ

SCImago Journal Rank (SJR): **0.845** ⓘ

› View More on Journal Insights

The paper will be published in the Computer Networks journal . *Computer Networks* is an international, archival journal providing a publication vehicle for complete coverage of all topics of interest to those involved in the **computer communications networking** area. The audience includes researchers, managers and operators of networks as well as designers and implementors. The topics covered by the journal includes **Communication Network Architectures**, **Communication Network Protocols**, **Network Services** and **Applications** , **Network Security** and **Privacy**, **Network Operation** and **Management**, **Discrete Algorithms** and **Discrete Modelling.**

- **CiteScore: 7.6**
- **Impact Factor: 3.111**

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

Academic Publications

Book, Cyber-Security Threats, Actors, and Dynamic Mitigation

Following the strategy outlined in deliverable D9.2 (Disseminations and use plan), Cyber-Trust partners have been published a book that promotes the Cyber-Trust project research activities. The book provides both a technical and state-of-the-art perspective as well as a systematic overview of the recent advances in different facets of cyber-security. It covers the methodologies for modelling attack strategies used by threat actors targeting devices, systems, and networks such as smart homes, critical infrastructures, and industrial IoT.

With a comprehensive review of the threat landscape, the book explores both common and sophisticated threats to systems and networks. Tools and methodologies are presented for precise modelling of attack strategies, which can be used both proactively in risk management and reactively in intrusion prevention and response systems. Several contemporary techniques are offered ranging from reconnaissance and penetration testing to malware detection, analysis, and mitigation. Advanced machine learning-based approaches are also included in the area of anomaly-based detection, that are capable of detecting attacks relying on zero-day vulnerabilities and exploits. Academics, researchers, and professionals in cyber-security who want an in-depth look at the contemporary aspects of the field will find this book of interest.   Those wanting a unique reference for various cyber-security threats and how they are detected, analysed, and mitigated will reach for this book often.

Link to the book:

https://www.taylorfrancis.com/books/cyber-security-threats-actors-dynamic-mitigation-nicholas-kolokotronis-stavros-shiaeles/e/10.1201/9781003006145?refId=3236a863-3165-4c50-9c1e-7c949cc025bd

DOI: https://doi.org/10.1201/9781003006145

Edition: 1st Edition

First Published: 2021

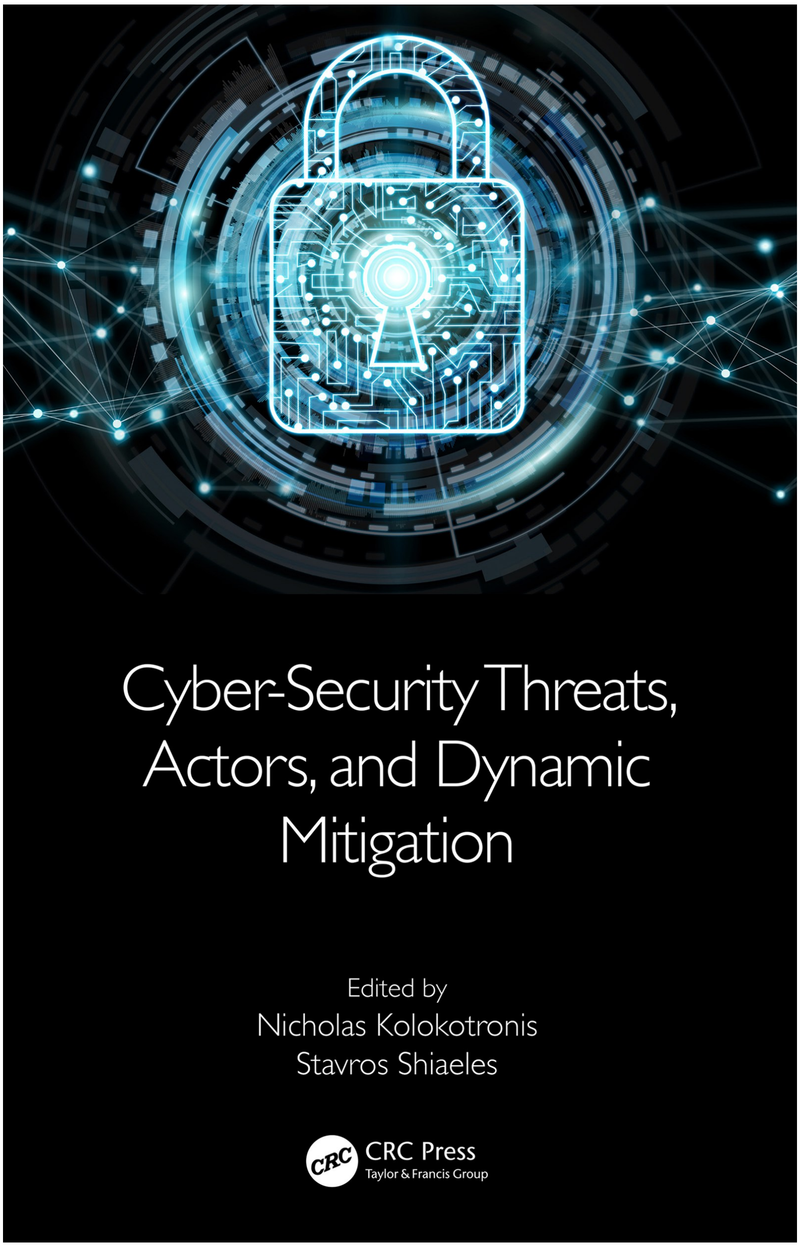
eBook Published: 5 April 2021

Pub. Location: Boca Raton

Imprint: CRC Press

Pages: 392

eBook ISBN: 9781003006145



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

Academic Publications

Book, Internet of Things, Threats, Landscape, and Countermeasures

Following the strategy outlined in deliverable D9.2 (Disseminations and use plan), Cyber-Trust partners have been published a book that promotes the Cyber-Trust project research activities. The book delves into the different cyber-security domains and their challenges due to the massive amount and the heterogeneity of devices.

This book introduces readers to the inherent concepts of IoT. It offers case studies showing how IoT counteracts the cyber-security concerns for domains. It provides suggestions on how to mitigate cyber threats by compiling a catalogue of threats that currently comprise the contemporary threat landscape. It then examines different security measures that can be applied to system installations or operational environment and discusses how these measures may alter the threat exploitability level and/or the level of the technical impact .

Professionals, graduate students, researchers, academicians, and institutions that are interested in acquiring knowledge in the areas of IoT and cyber-security, will find this book of interest.

Link to the book:

https://www.taylorfrancis.com/books/internet-things-threats-landscape-countermeasures-stavros-shiaeles-nicholas-kolokotronis/e/10.1201/9781003006152?refId=fefabbac-87d8-4101-af1e-22402676f334

Edition: 1st Edition

First Published: 2021

eBook Published: 5 April 2021

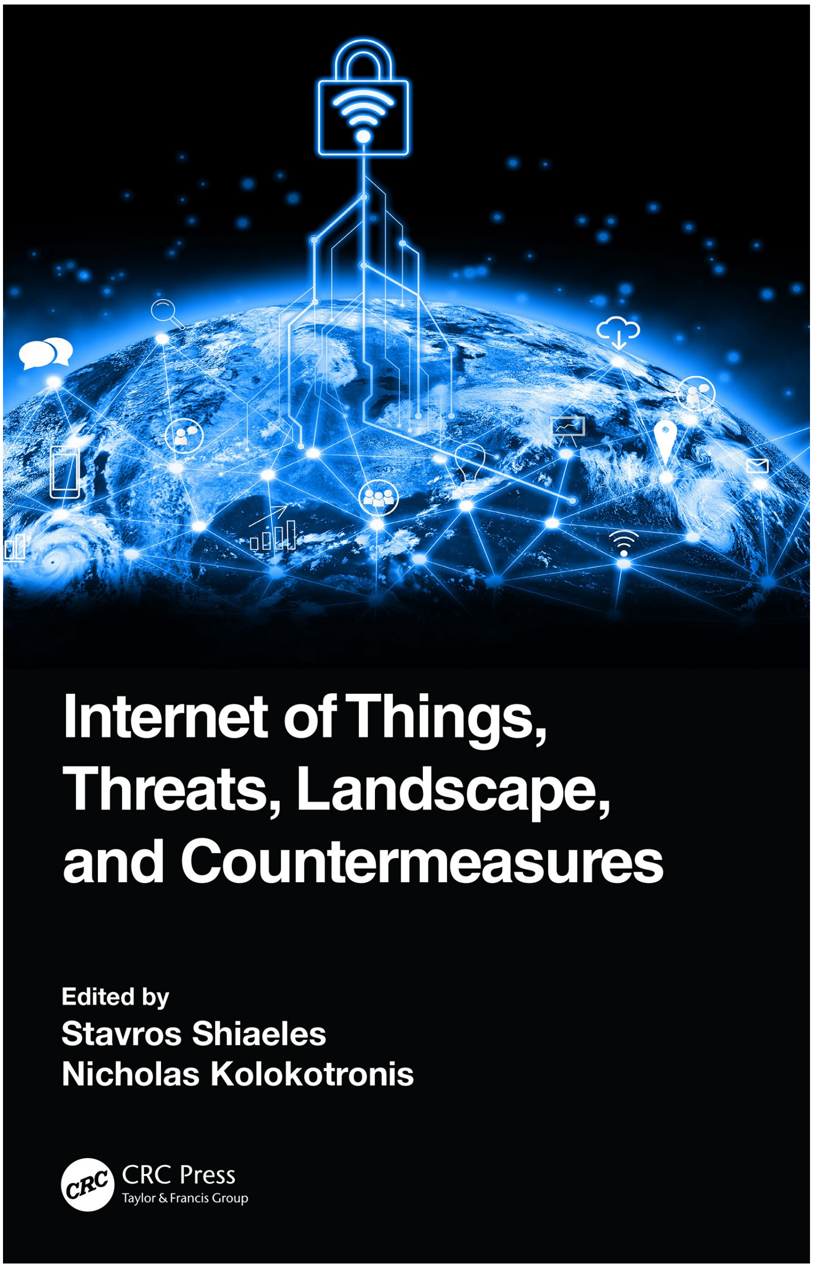
Pub. Location: Boca Raton

Imprint: CRC Press

Pages: 358

eBook ISBN: 9781003006152

DOI: https://doi.org/10.1201/9781003006152



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

Press Releases

H2020 - Cyber Trust video

KEMEA

Following the strategy outlined in deliverable D9.2 (Disseminations and use plan), Cyber-Trust partners have been published a video that promotes the Cyber-Trust project and communicates a simplified presentation of the main objectives of the project to the general public.

Link to the video on the Cyber-Trust YouTube channel:

https://www.youtube.com/watch?v=Yg3SKOmz2lo

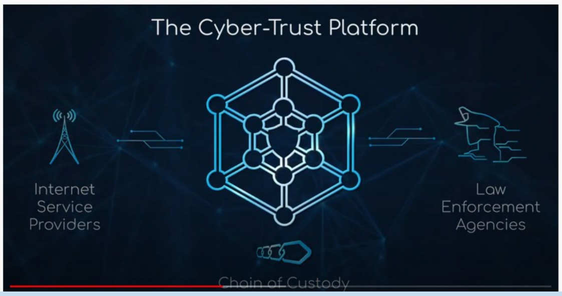
This video is available on the Cyber-Trust project website (https://cyber-trust.eu/newsletters/) as well as the project social media including the Cyber-Trust YouTube channel, Facebook, Tweeter and LinkedIn.

√ https://cyber-trust.eu/

√ https://www.linkedin.com/groups/13627755/

√ ttps://www.facebook.com/cybertrust/

√ https://twitter.com/CyberTrustEU



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

Collaboration with the SPEAR Project

To ensure cohesion with the wider research efforts undertaken by related concurrent EU projects, members of the consortium established contact and communication, in order to build up collaborations on aspects of mutual interest with the SPEAR (Secure and PrivatE smArt gRid) project.

In the context of this collaboration, the Cyber-Trust testbed will incorporate an emulated Smart home hosted by the SPEAR member, CERTH. The smart home integrates several IoT devices and multisensorial networks, as well as a PhotoVoltaic (PV) system of 10kW for energy production.

The **SPEAR (Secure and PrivatE smArt gRid)** project is a research program, funded by the Horizon 2020 framework programme of the European Union and it aims at developing an integrated platform of methods, processes, and tools for:

- timely detecting evolved security attacks using big data analytics, advanced visual-aided anomaly detection tools, and smart node trust management schemes;
- developing an advanced forensic readiness framework for collecting attack traces and preparing the necessary legal evidence in court, while preserving user private information;
- implementing an anonymous smart grid channel for mitigating the lack of trust in exchanging sensitive information about cyberattack incidents;
- performing risk analysis and awareness through cyber hygiene frameworks, while empowering EU-wide consensus, by collaborating with European and global security organizations, standardization bodies, industrial groups and smart grid operators;

exploiting the research outcomes to more critical infrastructure domains, while creating competitive business models for utilizing the implemented security tools in smart grid operators and actors across Europe.

Link to the SPEAR project website: https://www.spear2020.eu/

SPEAR
Secure and PrivatE smArt gRid
SPEAR
Advanced cybersecurity solution

This project has received funding from the European Union's Horizon 2020 programme under grant agreement No 787011

Web site Blog Posts

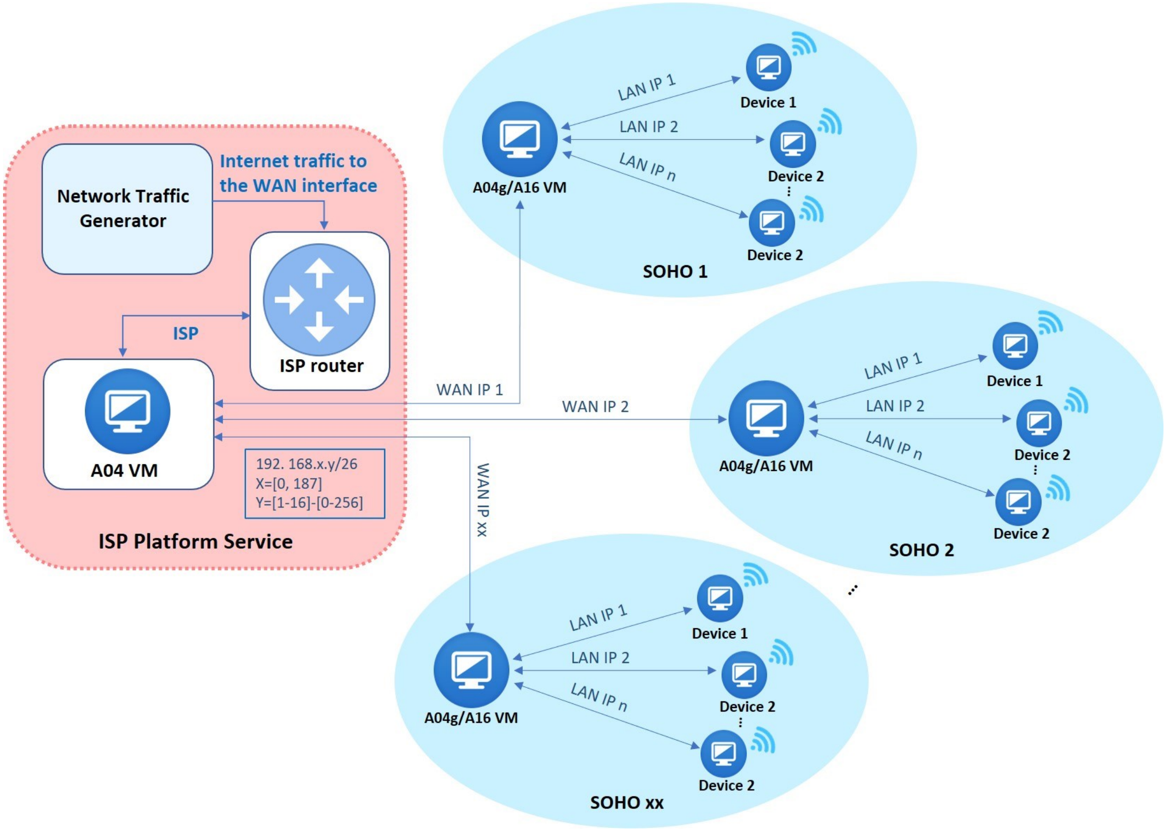
The Cyber-Trust testbed, short implementation overview

OTE, February 2021

Testbeds were always important, as all new services and products always need to be tested thoroughly, especially the ones that operate in complex environments with many prospective users, although this is not always the case. Additionally, proper testing environment and procedure can help avoid later hardships. Nevertheless, this is the case with most of the research projects at EU, where the validity of a project's outputs are checked and verified. As the pilots are progressing, This blogpost discusses the Cyber-Trust testbeds, concerning the requirements and some implementation aspects. The requirements, which came along time, for the testbeds were:

- Big enough to host the CYBERTRUST platform on the NP side and a significant number (750) of emulated and simulated Small Offices/Homes (SOHOs).
- Tight integration of the SOHO gateways with the networking cloud infrastructure, in order to be able to provide proper routing, packet sniffing, internet and DHCP to the SOHO devices,
- Produce and allow significant amounts of normal and malicious traffic to traverse the testbed, without being blocked by the inherent cloud security mechanisms, even perform DDOS attacks while the testbed retains stability
- Monitor, capture and reproduce the circulated traffic at various points within the topology for analysis and manipulation
- Provide an adequate number and variety of PC and smart home devices and OSes to make for creating realistic SOHOs.
- Perform other types of attacks and infections towards the SOHOs and monitor their reactions as well as the CYBERTRUST platform.

Link to blogpost:



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

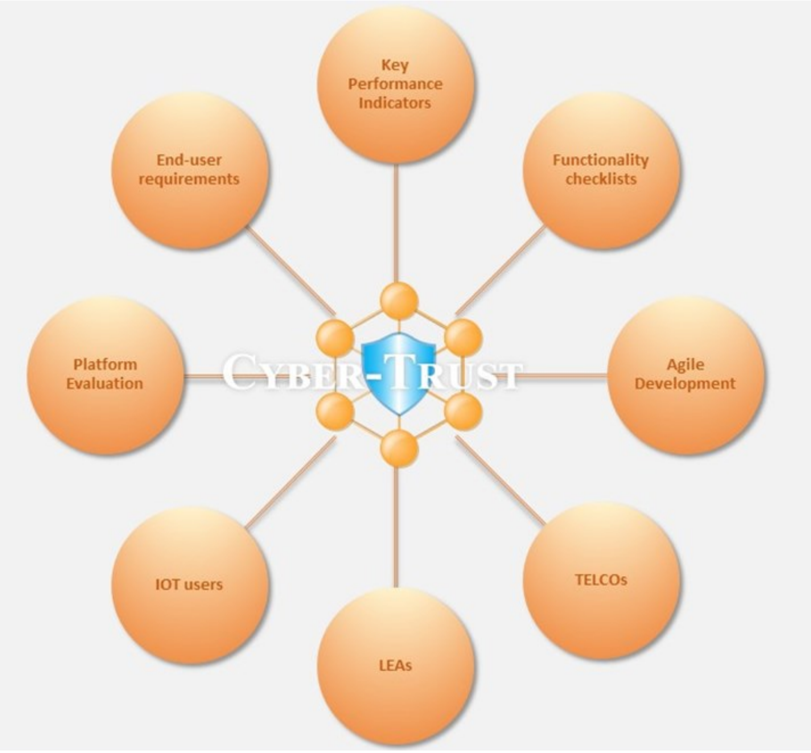
Press Releases

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

KEMEA, February 2021

To address the major challenges of securing the IoT ecosystem from cyber threats, the Cyber-Trust project has developed a revolutionary framework that will first identify, then analyse, and next mitigate these threats. To achieve this, the Cyber-Trust project conducts research in the following main cyber-security areas: a) develop state of the Art (SOTA) cyber security tools, b) identify cyber-attack and mitigate their consequence, and c) use of distributed ledger technologies. The Cyber-Trust project has developed an innovative platform based on end user specifications that formed the technical and functional requirements of the project.

The validation of the Cyber-Trust platform will be achieved in two (2) pilot phases. In both phases, Cyber-Trust functionality will be verified using several use case scenarios, developed by the potential end users: IoT device owners, Internet Service Providers (ISPs), and Law Enforcement Agencies (LEAs).



Currently, the Cyber-Trust platform is operational and ready to be tested, validated, and evaluated by its potential end-users. The testing procedures and the methodology that will be used to evaluate the platform are adequately documented in the evaluation plan of the platform. The objective of the platform evaluation is to ensure that the requested functionalities are delivered and that the end user requirements sufficiently met.

The evaluation plan includes the measurement of Key Performance Indicators (KPI), verification of the platform functionalities while an assessment questionnaire will measure the effectiveness, efficiency, satisfaction, maintainability, and reliability of the platform. As a result of this process, the three end-user groups not only will evaluate the developed platform, but also will provide feedback to improve the platform and identify issues that should be addressed by the technical team.

The data processing methodology complies with all appropriate legal measures. The evaluation process will use both qualitative and quantitative methods to process end user inputs. Results from the three end user questionnaires will be reported, along with recommendations for future platform improvements. At the end of the platform evaluation a development phase will follow to satisfy additional end *user requirements* and remedy any *issues reported*. The outcome of a successful and direct first pilot phase would not be only the solid basis for the second and final pilot implementation phase, but also for future achievements of the cybersecurity ecosystem.

Further information on Cyber-Trust is available on the project website. To stay updated on Cyber-Trust's activities and events, please get in touch with us using this form.

Link to the press release:

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

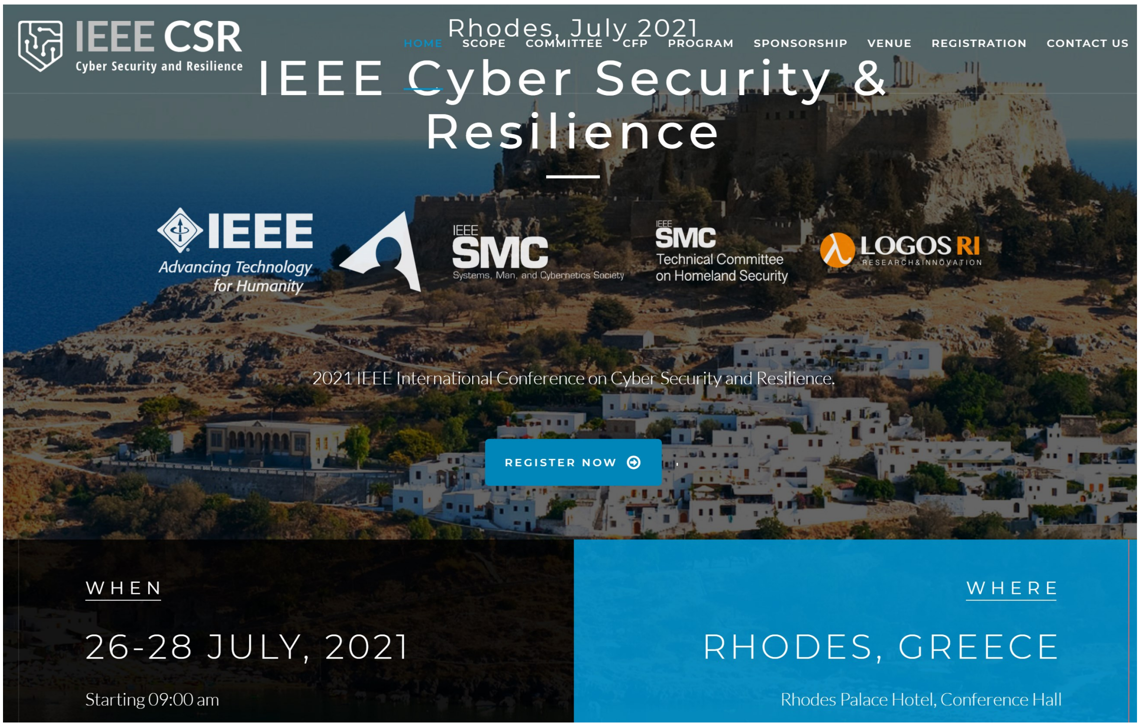
Cyber-Trust partners organising the IEEE Cyber Security & Resilience

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 conference 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/).


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

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

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.