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

CyberTrust

Newsletter Vol. 2— April 2020

Welcome to our 2nd issue of CYBER-TRUST Newsletter. The project newsletters will keep you regularly updated with the progress of our project and the news that relate to it.

Table of Contents

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

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

Yours sincerely,

The CYBER-TRUST consortium

Project quick info

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

Contacts

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

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

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

https://cyber-trust.eu/

d.kavallieros@kemea-research.gr

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

https://www.facebook.com/cybertrust/

https://twitter.com/CyberTrustEU

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

Welcome to the second issue of our newsletter, April 2020.

We are pleased to share the second issue of our newsletter, keeping you up to date with all the latest news from the Cyber-Trust Project.

This issue provides the dissemination and communication activities undertaken by consortium partners of Cyber-Trust during the period of the project life from November 2019–April 2020. It detailed the dissemination activities, which have been undertaken in this period, together with the potential future events. The detailed description of the dissemination activities involved during this period proves 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.

- √ Website: https://cyber-trust.eu/
- √ Email: d.kavallieros@kemea-research.gr
- √ LinkedIn: https://www.linkedin.com/groups/13627755/
- √ Facebook: https://www.facebook.com/cybertrust/
- √ Twitter: https://twitter.com/CyberTrustEU

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

Academic Publications

We have now published 23 research work papers!

The research undertaken in the Cyber-Trust project has already led to 23 research publications, of which 20 were accepted and presented in peer-reviewed international conferences and three in peer-reviewed journals. The research work papers are developed to help advance the knowledge base that underpins the formulation and implementation of relevant policies in Europe, and to engage with relevant communities, stakeholders and practitioners in the research, again with the aim of supporting relevant policies and providing a clear view of the project results. All research papers are available on publishers' websites and most of them have an e-print copy that is available as open access in the "arXiv" repository.

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

In the period from M19 (November 2019) until M24 (April 2020) of the project life, the research undertaken in the Cyber-Trust project has led to 04 new research publications that were accepted and will be presented in peer-reviewed international conferences.

The new research publications are:

IoT Malware Network Traffic Classification using Visual Representation and Deep Learning.

Authors: Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis

This research publication focuses on enhancing Intrusion Detection Systems (e.g. Suricata and snort) with machine learning by proposing a novel IoT malware traffic analysis approach using deep learning and visual representation for faster detection and classification of new malware (zero-day malware). Form the experiments and comparison with multiple neural networks, the Residual Neural Network with fifty layers (ResNet50) has proved that it is the most effective in the identification of malware network traffic with an overall accuracy of 94.50%. The work presented in this paper is directly related with the work carried out in the work-package 6 (WP6: "Advanced cyber-attack detection and mitigation") of the Cyber-Trust Project.

The paper was accepted and will be presented in the 2nd Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft), co-located with IEEE NetSoft 2020 that will be held in 3ed of July 2020, Ghent, Belgium. The paper will also be published in the conference proceedings and IEEE Xplore.

Note: Due to the COVID 19 sanitary crisis, IEEE NetSoft 2020 will run as a virtual conference.

IEEE Conference on Network Softwarization
29 June-3 July 2020 // Virtual Conference

IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites
IEEE NETSOFT
IEEE ComSoc IEEE Communications Society
IEEE
HOME | ABOUT NETSOFT | COMMITTEE | AUTHORS | PROGRAM | WORKSHOPS | REGISTRATION | HOTEL / TRAVEL | PATRONS

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

Detection of Insider Threats using Artificial Intelligence and Visualisation

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

This research paper investigated solutions that have been proposed to identify and alleviate the potential impact of Insider threat, which is one of the most damaging risk factors for the IT systems and infrastructure of a company or an organization. In this context, the paper studied the efficiency of Artificial Intelligence to detect malicious insider by proposing a new approach to discriminate between legitimate and malicious behaviour. For each category of users, the approach creates an image that depicted his/her activity and behaviour, as emerged from their interaction with various information systems. While the resulting images may appear visually different, they were processed through a machine learning algorithm in order to automatically recognize which subset of the users appear to exhibit malicious behaviour (and therefore posing a threat for the respective information systems) and which are legitimate/ benign ones. This approach is composed of three main steps: (a) collecting, processing, and classifying the data of the users tested; (b) visualizing the extracted data; (c) categorize the behaviour as malicious or normal.

The work presented in this paper is directly related with the work carried out in the work-package 6 (Advanced cyber-attack detection and mitigation) and work-package 7 (Distributed ledger technology for enhanced accountability).

The paper was accepted and will be presented in the 2nd Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures (SecSoft), co-located with IEEE NetSoft 2020 that will be held in 3ed of July 2020, Ghent, Belgium. The paper will also be published in the conference proceedings and IEEE Xplore.

Link to the Workshop: https://cyber-trust.eu/secsoft-2020/

A Case Study of Intra-library Privacy Issues on Android GPS Navigation Apps

Authors: Stylianos Monogios, Konstantinos Limniotis, Nicholas Kolokotronis, Stavros Shiaeles

This research paper focuses on the geolocation data and analyses five GPS applications to identify the privacy risks if no appropriate safeguards are present. Our results show that GPS navigation apps have access to several types of device data, while they may allow for personal data leakage towards third parties such as library providers or tracking services without providing adequate or precise information to the users. Moreover, as they are using third-party libraries, they suffer from the intra-library collusion issue, that could be exploited from advertising and analytics companies through apps and gather large amount of personal information without the explicit consent of the user. This work is directly related with the work carried out in the work-package 5 (Key proactive technologies and cyber-threat intelligence) of the project.

The paper was presented in the "**8th occasion of the International Conference on e-Democracy**" that was held in Athens, the cradle of democracy, on 12-13 December 2019. The paper is published in the Springer's Communications in Computer and Information Science (CCIS) series, Online ISBN 978-3-030-37545-4. The conference paper is available via the Springer digital library.

Link: https://link.springer.com/book/10.1007%2F978-3-03037545-4

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

Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study

Authors: Faisal Alsakran, Gueltoum, Bendiab, Stavros Shiaeles, Nicholas Kolokotronis

This research conference paper focuses on examining the existing Open source Intrusion Detection Systems (IDSs), in order to find the most appropriate solution for smart homes in terms of resources consumption. To this end, several open-source network-based intrusion detection systems (NIDS) are available such as ACARM-ng, AIDE, Bro IDS, Snort, Suricata, OSSEC HIDS, Prelud Hybrid IDS, Samhain, Fail2Ban, Security Onion, etc. This study helps in identifying the best IDS that can protect smart devices used in home environments with a minimum of resources consumption, which is very important for the Cyber-trust project, especially work package 6 (Advanced cyber-attack detection and mitigation).

The paper presents the results of the experimental comparison between the widely used open-source NIDSs namely Snort, Suricata and Bro IDS to find the most appropriate one for smart homes in term of resources consumption including CPU and memory utilization. The chosen IDSs are deployed inside different Linux containers known as Dockers, instead of running them IDSs directly on a VM base operating system. Each container has its resources that are separated from other containers. Experimental Results show that Suricata and Bro are the best performing NIDS for smart homes compared to snort

The paper was presented in the seventh Symposium on Security in Computing and Communications (SSCC'19), co-affiliated with the International Conference on Applied Soft computing and Communication Networks (ACN'19), co-located with the third International Conference on Computing and Network Communications (CoCoNet'19) that was held in Trivandrum, Kerala, India on December 18-21, 2019.

Link: http://www.acn-conference.org/sscc2019/

SSCC'19

7th International Symposium on Security in Computing and Communications (SSCC'19)

December 18 - 21, 2019 |Trivandrum, Kerala, India

Welcome to SSCC'19 Website!

Proceedings now available online

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.

Extended Submission Deadline	September 30, 2019(Final)
Acceptance Notification	October 20, 2019
Final Paper Deadline	November 20, 2019

▸▸Submissions are now open for three co-located workshops...

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 Seventh International Symposium on Security in Computing and Communications (SSCC'19) aims to provide the most relevant opportunity to bring together researchers and

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

Blog Post

Under the epidemic situation of COVID-19, the number of cyber-attacks has been multiplied highlighting once again the importance for data and security resilience as well as for the respective research and innovation to provide security solutions, including prevention and mitigation tools. In this context, VUB/ LSTS (Cyber-Trust partner) has created a resources and news observatory, where a collection of useful material on data protection law and the COVID-19 outbreak can be found, including issues of cyber and data security in Europe and across the world, as well as recommendations, official statements, academic publications and news. This blog is directly relating to policy work conducted in Work Package 3 (Legal issues: data protection and privacy) and in-parallel research in the areas of cyber-security and data protection

COVID-19: AMID A “PANDEMIC” OF CYBER-ATTACKS

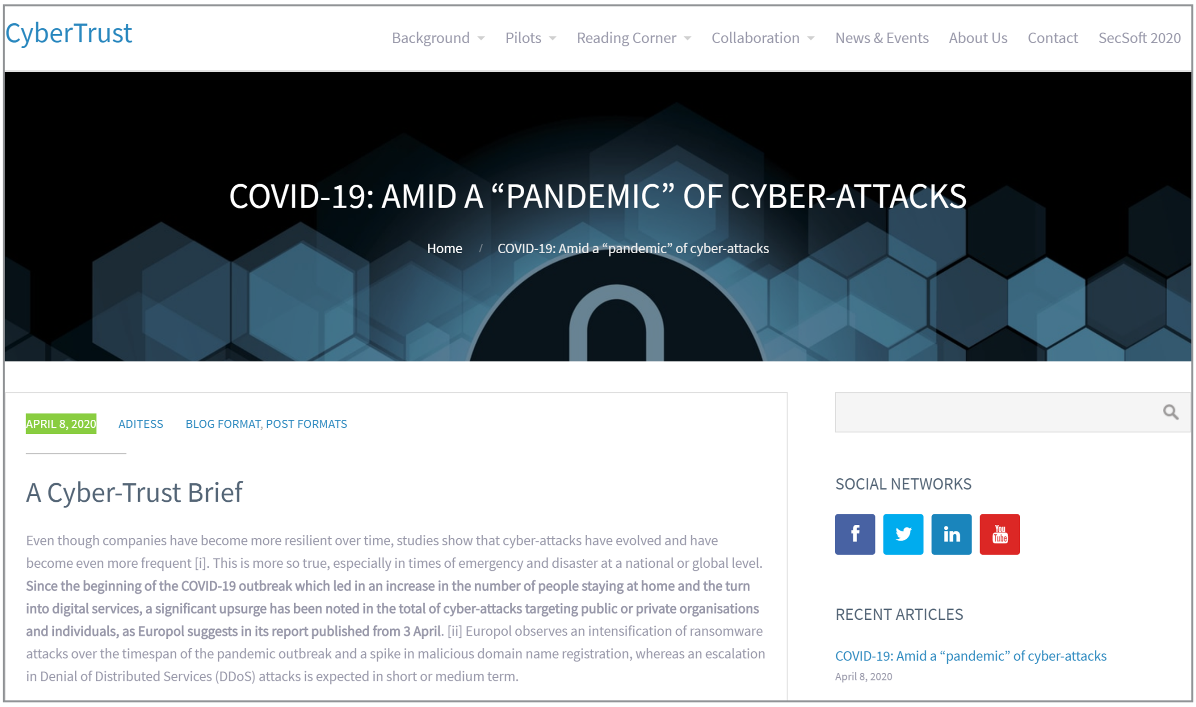
APRIL 8, 2020

During the COVID-19 pandemic, the number of cyber-attacks has been multiplied highlighting once again the importance for data and security resilience as well as for the respective research and innovation to provide security solutions, including prevention and mitigation tools. With more and more people staying at home and an urging demand for digital services in order to fulfil their daily tasks and satisfy their needs for work, healthcare, education, entertainment and social contact, more and more organizations and individuals are left exposed to vulnerability and security threats. From hospitals to national Ministries, and from teleconferencing platforms to scam and emails, threat is apparent and the risk for personal data breaches high.

This has led many EU (European Union) institutions, Agencies and bodies, (European Commission, ENISA, EUROPOL, CERTEU) as well as many state authorities, data protection authorities and law enforcement agencies to issue guidelines and recommendations on how to stay cyber-safe.

The blogpost presents an overview of those guidelines and recommendations at EU level and at national level with reference to the countries where the Cyber-Trust partners are based. It is relating to policy work conducted in WP3 and in-parallel research in the areas of cyber-security and data protection.

Link to the blog: https://cyber-trust.eu/2020/04/08/amid-apandemic-of-cyber-attacks-a-cyber-trust-brief/.



COVID-19: AMID A “PANDEMIC” OF CYBER-ATTACKS

APRIL 8, 2020

A Cyber-Trust Brief

Even though companies have become more resilient over time, studies show that cyber-attacks have evolved and have become even more frequent [i]. This is more so true, especially in times of emergency and disaster at a national or global level. **Since the beginning of the COVID-19 outbreak which led in an increase in the number of people staying at home and the turn into digital services, a significant upsurge has been noted in the total of cyber-attacks targeting public or private organisations and individuals, as Europol suggests in its report published from 3 April**. [ii] Europol observes an intensification of ransomware attacks over the timespan of the pandemic outbreak and a spike in malicious domain name registration, whereas an escalation in Denial of Distributed Services (DDoS) attacks is expected in short or medium term.

COVID-19: Amid a “pandemic” of cyber-attacks
April 8, 2020

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:

Co-oganisation of a Business workshop with thought leaders

11 February 2020,

On February 11, 2020, a business workshop within experts / thought leaders was organised to discuss the ongoing initiatives and way ahead for new partnership opportunities. Gohar Sargsyan presented Cyber-Trust for dissemination purposes. Following to discussions the thought leaders provided highly positive recommendations to start working on a follow-up opportunity. Besides the participants expressed high interest in following the development of the project especially on potential market uptake if the research results will bring.

Co-organisation of the Science and Business annual Forum

4 February, 2020, Brussels

Science|Business is a forum convening public and private sector leaders for networking, intelligence and debates on research and innovation. organises a range of events from full conferences to private briefings. Some are open to the public, some for members of our Network only. We run our own events, and we also organise bespoke events for clients. But whatever the format, every Science|Business event shares the same unique imprint: it combines expert knowledge with bringing together the people who really matter in industry, research and policy – both as speakers and as audience.

This year's annual membership event took place on the 4th of February in Brussels. CGI is a member of the network and was present in the event. The event was closed event to members only and some 100 members were present to discuss the agenda of the next year. During breakout sessions, the members had the opportunity to show case innovation, show case or any project they find suitable to the setting. Cyber-Trust was presented by Gohar Sargsyan from CGI in the breakout session and it was received very well by the participants. The session attended about 40 members.

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

Organisation of a standalone panel entitled "AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection?

23 January, 2020, Brussels (Belgium)

The following panel intitled "AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection? was organised by VUB, on behalf of Cyber-Trust, at the CPDP 2020 - Artificial Intelligence and Data Protection, one of the biggest annual conferences in the field. The conference took place in Brussels (Belgium) on 22-24 January 2020. Cyber-Trust also received visibility as event partner.

The Internet of Things (IoT) aims to establish an ecosystem of heterogeneous connected devices that communicate to deliver environments making our living, cities, transport, energy, and many other areas more intelligent. This amplifies concerns about the security of networked applications and services, based on known and unknown vulnerabilities and backdoors. More and more cybersecurity systems develop and deploy AI tools for the prevention, detection and mitigation of cyberattacks, in particular in the field of cyber-threat intelligence and device profiling, aiming to simplify the threat identification process and improve the rate of remediation response. The panel aims to reflect upon what is at stake for data protection and privacy by the use of such automated tools, provided inter alia the requirements set in the recently adopted Cybersecurity Act at EU level for enhancing cybersecurity in products and services.

Since AI appears to become increasingly integrated in cybersecurity solutions, what applications are currently deployed, what is being developed by academia, business and the LEAs, how are models trained and what is aspired for in the short- and long-term future in the security sector?

What are the advantages and challenges of using AI in the cybersecurity context with respect to data protection and privacy?

In which ways can security research reconcile privacy, data protection and cybersecurity, creating compliant designs by advancing the principles of data protection and privacy by design and by default as well as integrating the learnings of the Data Protection Impact Assessments?

Best practices and lessons learnt through hands-on experience.

13th INTERNATIONAL CONFERENCE 22 - 24 JAN 2020 BRUSSELS, BELGIUM

CPDP 2020 DATA PROTECTION AND ARTIFICIAL INTELLIGENCE

Call for Papers

CPDP2020 Call for Papers

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

The panel "**AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection**? is directly related to the work of Work Package 3 ("Legal issues: data protection and privacy") of the Cyber-Trust project.

Relevant links and promotion:

- √ https://www.youtube.com/watch?v=zXkXxmLLfI&list=PL8z0l8CAoah7nocn6fjCbeE9Ul_wNKer&index=6&t=0s
- √ https://www.cpdpconferences.org/cpdp-panels/ai-forthe-future-of-prevention-detection-and-mitigation-ofcyberattacks-what-is-at-stake-for-privacy-and-dataprotection
- √ https://twitter.com/olga_gkot/status/12202859916736 14336?s=20
- √ https://twitter.com/PaulQuinnBxl/status/12203590245 13814530

Link to the event: https://www.cpdpconferences.org/call-for-papers

AI for the future of prevention, detection and mitigation of cyberattacks: what is at stake for privacy and data protection?

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

Paul Quinn, Vrije Universiteit Brussel

Rosa Barcelo, Squire Patton Boggs

Athena Bourka, ENISA - European Union Agency for Cybersecurity

Dimitris Kavallieros, Center for Security Studies - Hellenic Ministry of Citizen Protection

Carolin Möller, Deloitte

#CPDP2020

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

Organisation of the CGI leadership conference

13-17 January, 2020, Montreal, Canada

CGI Leadership business event gathered 350 leaders from around the world including senior executives of the company between 13 and 17 of January 2020 in Montreal, Canada.

The event is a regular event for the level of Directors and higher. During this leadership conference a side event was organised dedicated to Cyber-Trust by Gohar Sargsyan. Business Innovation show was organised together with local Montreal innovation team.

A brief presentation on the screen of the event, was shown and during exhibition session. As the session was walked in in a lobby of the large event, all participants had the opportunity to walk-in and have impressions on Cyber-Trust alongside with others who stopped by for longer time to discuss.

CGI

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

Organization of the INFOCOM Business conference

26 November, 2019

INFOCOM WORLD CONFERENCE 2019

«Economy 4.0: Connected Future»

Tuesday, November 26, 2019 – Divani Caravel Hotel, Athens

The following Workshop was organised by OTE, by focusing upon 5G Security issues, as a side-event within the 21st 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 26, 2019. The Cyber-Trust project also received visibility as presenter. The event was within a Parallel Session with 3 sub-sessions in room "**MACEDONIA**" 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 Session C ("Modern Innovative Technologies and Broader 5G-related Aspects for Development and Growth with Emphasis set to Vertical Industries"). Two Cyber-Trust dedicated presentations took place, as follows:

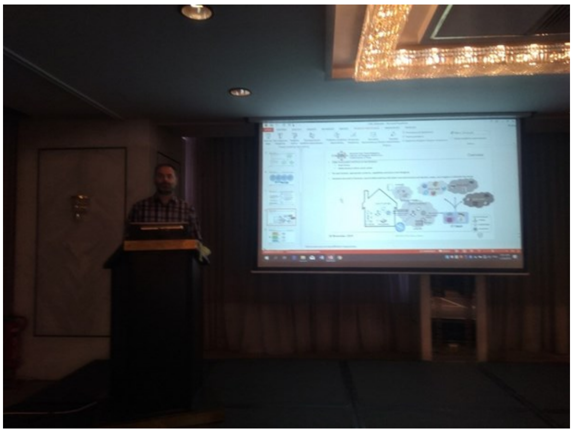
Presentation 1: Title: "Meeting the Needs of Information among LEAs and ISPs from the LEA side". **Presentation 2**: Title: "Meeting the Needs of Information among LEAs and ISPs from the ISP side".

Venue: Divani Caravel Athens Hotel, Athens, Greece : https://divanicaravelhotel.com/

Relevant links and promotions:

- √ https://www.infocomworld.gr/21o-infocom-world2019/
- √ https://www.infocomworld.gr/21o-infocom-world2019/5g-epistimoniki-synantisi-aithoysa-makedonia
- √ https://www.infocomworld.gr/presentations/2019/o te/ C20a_Kavallieros.pdf
- √ https://www.infocomworld.gr/presentations/2019/o te/ C20b_Sfakianakis.pdf

This event is directly related to the work undertaken in WP2 (Cyber-threat landscape and end-user requirements), WP4 (CYBER-TRUST framework, platform design and architecture), WP6 (Advanced cyber-attack detection and mitigation) and WP8 (Pilot implementation, testing and evaluation).



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

Organization of a standalone panel entitled "Of spiders and robots: web crawling as opportunity and threat vs. data protection law as facilitator and obstacle"

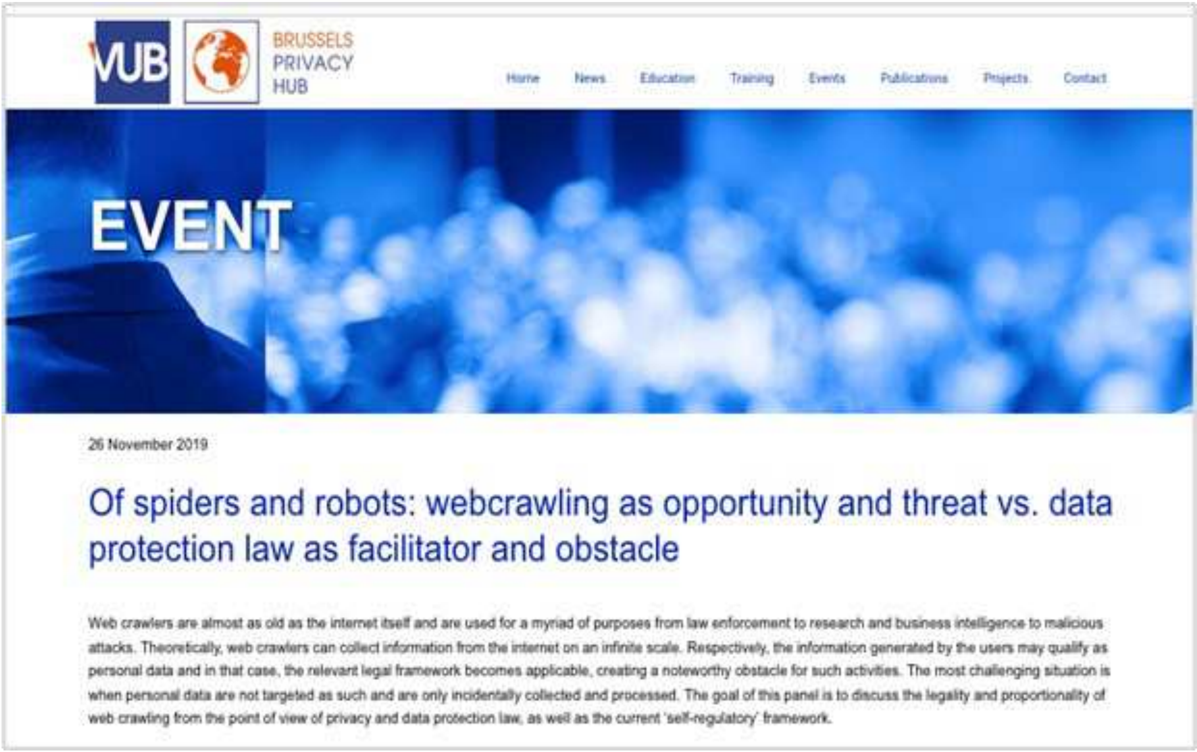
November 26, 2019

Web crawlers are almost as old as the internet itself and are used for a myriad of purposes from law enforcement to research and business intelligence to malicious attacks. Theoretically, web crawlers can collect information from the internet on an infinite scale. Respectively, the information generated by the users may qualify as personal data and, in that case, the relevant legal framework becomes applicable, creating a noteworthy obstacle for such activities. The most challenging situation is when personal data are not targeted as such and are only incidentally collected and processed. The goal of this panel was to discuss the legality and proportionality of web crawling from the point of view of privacy and data protection law, as well as the current 'self-regulatory' framework. The panellists gave an overview of what web crawling entails from a technical point of view and outlined the purposes of the use of web crawling in business, research, and law enforcement. Building on that technical description, the discussion moved to the implementation of the EU data protection law and the compatibility with the data protection principles. Preventive, protective and informative measures deployed by website operators were presented and debated.

This event is co-organised by the Brussels Privacy Hub and the Horizon 2020-funded research project Cyber-Trust | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things.

Panelists:

- √ *Constantinos Patsakis*, Assistant Professor at the Department of Informatics, University of Piraeus and Adjunct researcher at the Institute for the Management of Information Systems (IMIS) of Athena Research and Innovation Centre.
- √ *Gohar Sargsyan*, ICT Innovation Lead EU, Director Consulting Information Driven Operations and Digital Transformation, CGI Netherlands.
- √ *Georgia Melenikou*, Lawyer and Research Associate, Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection.
- √ *Dimitra Papadak*i, Lawyer and Research Associate, Center for Security Studies (KEMEA), Hellenic Ministry of Citizen Protection.



26 November 2019

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

Web crawlers are almost as old as the internet itself and are used for a myriad of purposes from law enforcement to research and business intelligence to malicious attacks. Theoretically, web crawlers can collect information from the internet on an infinite scale. Respectively, the information generated by the users may qualify as personal data and in that case, the relevant legal framework becomes applicable, creating a noteworthy obstacle for such activities. The most challenging situation is when personal data are not targeted as such and are only incidentally collected and processed. The goal of this panel is to discuss the legality and proportionality of web crawling from the point of view of privacy and data protection law, as well as the current 'self-regulatory' framework.

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

Venue: U-Residence, Vrije Universiteit Brussel, Pleinlaan 2, 1050, Brussel (Access also via Generaal Jacqueslaan 271, 1050 Brussels)

Relevant links and promotion:

- √ https://www.brusselsprivacyhub.eu/events/26112019.ht ml
- √ https://lsts.research.vub.be/en/lunchtime-panel-onweb-crawling-and-data-protection-26-november-2019vub/
- √ https://lsts.research.vub.be/en/of-spiders-and-robotswebcrawling-as-opportunity-and-threat-vs-dataprotection-law-as-facilitator/
- √ https://twitter.com/privacyhub_bru/status/1199297752 204808192

The panel "**Of spiders and robots: web crawling as opportunity and threat vs. data protection law as facilitator and obstacle**" is directly related to the work undertaken in WP3 (Legal issues: data protection and privacy) of the Cyber-trust project.

IoTCrawler deals with the challenge of crawling the internet of IoT and big data opportunity will be open to provide advanced services and application
Constantinos PATSAKIS
Gohar SARGSYAN
Georgia MELENIKOU
Dimitra PAPADAKI
BRUSSELS

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

Coming events

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

29 June – 3 July, 2020

The Second International Workshop on Cyber-Security Threats, Trust and Privacy Management in Software-defined and Virtualized Infrastructures (SecSoft 2020) is a joint initiative from EU Cyber-Security and 5G projects: ASTRID, SPEAR, CYBER-TRUST, REACT, SHIELD and 5GENESIS. The organisation of this workshop (https://www.astridproject.eu/secsoft/) co-hosted at 6th IEEE International Conference on Network Softwarization (NetSoft 2020) that was planned to be held in Ghent, Belgium on 29 June- 3 July, 2020. However, **Based on the current situation of the coronavirus COVID-19 pandemic sanitary crisis, the 6th IEEE International Conference on Network Softwarization (IEEE NetSoft 2020) will run as a virtual conference On June 29 – 3 July, 2020**. IEEE NetSoft 2020 aims at bringing together students, researchers and security experts on areas under consideration by Cyber-Trust. Indicative topics of interest included:

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

Link to the workshop: https://cyber-trust.eu/secsoft-2020/ or https://www.astrid-project.eu/secsoft/

Topics in this workshop are directly related with work carried out in work-packages WP5 (Key proactive technologies and cyber-threat intelligence), WP6 (Advanced cyber-attack detection and mitigation), and WP7 (Distributed ledger technology for enhanced accountability). 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 2020 and will made available at the publisher's website.

The 2nd International Workshop on Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures co-located with IEEE NetSoft 2020

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

Coming events

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

25-28 August, 2020

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

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

The Workshop is co-organized by:

- √ SDN-microSENSE
- √ FORESIGHT
- √ CYBER-TRUST
- √ SPEAR

TOPICS OF INTEREST INCLUDE, BUT ARE NOT LIMITED TO:

Security policies
Risk analysis and management
Vulnerability assessment and metrics
Awareness, training and simulation
Security standards
Privacy and Anonymity in smart/ micro grids
Threat modeling
Security architectures
Access control
Malware and cyber weapons
Intrusion detection and visualization
Defense in depth

Monitoring and real time supervision
Perimeter security
Safety-security interactions
Cyber security engineering
Secure communication protocols
Formal models for security
Hardware Security
Resilient ICS/CPS
Application Security
Secure Firmware
Incident Response and Digital Forensics
Case studies

ARES Conference
International Conference on Availability, Reliability and Security

August 25 – August 28, 2020

Coming up!

ARES Conference 2020

August 25 – August 28, 2020

ARES Conference 2020
The 15th International Conference on Availability, Reliability and Security
August 25 - August 28, 2020
University College Dublin, Dublin, Ireland

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

Events Participation

Nicosia Risk Forum 2019

14 November, 2019, Nicosia, Cyprus

During the last period, ADITESS partner from the Cyber-Trust project have participated in the Science and Business annual event “Nicosia Risk Forum 2019” that was held in the European University Cyprus in Nicosia, Cyprus. In this event, ADITESS partner had the chance to raise awareness of the Cyber-Trust project and to gauge the level of interest and impact of the project on the wider community of stakeholders, including academia, and industry.

The Nicosia Risk Forum 2019 event took place at European University Cyprus in Nicosia, Cyprus, November 21, 2019. “The Nicosia Risk Forum 2019 provides the platform for an array of stakeholders –hailing from government, academia and the private sector– to exchange views and experiences, making it a truly multi-disciplinary event that produces a high level of discourse at a timely juncture. An exciting line of speakers and presentations were planned.

Among others, on Nicosia Risk Forum 2019 important presentations were made by:

- √ EU Commissioner for Humanitarian Aid and Crisis Management, **Dr Christos Stylianides**
- √ HE the Minister of Foreign Affairs of the Republic of Cyprus, **Dr Nikos Christodoulides**
- √ The Deputy Government Spokeswoman, **Ms Klelia Vasileiou**
- √ Secretary General for Civil Protection of the Hellenic Republic, **Mr Nikos Hardalias**
- √ Head of NEMA, State of Israel, Mr Zeev Tsuk-Ram, VOVA Commissioner of Cyprus Civil Defense Force of the Republic of Cyprus, **Mr Andreas Frantzis.**

During the sessions of the Nicosia Risk Forum 2019 the Cyber-Trust project (https://cyber-trust.eu/) was presented by ADITESS LTD (www.aditess.com) .

Relevant links and promotions:

- √ https://cerides.euc.ac.cy/nicosia-risk-forum/
- √ https://aditess.com/main/2019/11/22/cybertrustproject-at-nicosia-risk-forum-2019/

2nd Annual Symposium
Center of Excellence in Risk & Decision Sciences (CERIDES)
Nicosia Risk Forum 2019
Thursday, 21 November 2019
Cultural Center, European University Cyprus

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

Synergies with other Projects

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 other H2020 projects.

Synergy establishment for the organisation of a standalone panel and talks

January-March 2020

On 29 April 2020, the Brussels Privacy Hub in synergy with the Horizon 2020-funded research projects LOCARD, CyberTrust and FASTER will present the panel 'The Promise of "Blockchain": DLT-based applications re-shape data storage and sharing, but can they be compliant with the EU data protection law?'

In recent times, much discussion has taken place among policy makers, academia and the private sector. Distributed Ledger Technologies (DLT) for data storage and sharing offer high potential and benefits in various contexts. Albeit, their use may give birth to implications with respect to data protection law. Design choices - giving preference to more centralised or decentralised solutions, opting for a permissioned or permissionless type of DLT, or resorting to an on-chain/off-chainscheme - create complications for researchers, DLT experts and businesses, as they can lead to different legal considerations, provided the characteristics specific to each application as well as the inherent limitations of each technology. Design choices can render compliance with the data protection and privacy framework easier or impossible and thus, can have a significant impact on the success of a project or product.

The panel will address issues relating to DLT-based applications beyond Blockchain, understanding which questions have to be asked during the conceptualization and design of a solution as well as during its actual implementation. The panelists, focusing on three innovative use cases of DLT (cyber-security, law enforcement and emergency response), will further address more general concerns and other issues, including the basic technical characteristics of DLTs and the current state-of-the-art. The backend legal research supporting those design choices will be extensively discussed.

All in all, Blockchain-enthusiasts or sceptics, attendees will have the opportunity to hear about novel technical solutions which aim to render DLT-based applications compliant with data protection law and ensure the enforcement of data subjects' rights, such as the notion of Private Data, the adoption of different access levels and the Time-To-Live (TTL) feature.

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

Due to force majeure (emergency lockdown measures for the containment of COVID-19), the above event has been postponed and will be rescheduled.

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