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

Ergebnisse

Projektinformationen

CYBER-TRUST

ID Finanzhilfevereinbarung: 786698

Projektwebsite

DOI
10.3030/786698

Projekt abgeschlossen

EK-Unterschriftsdatum
23 April 2018

Startdatum
1 Mai 2018

Enddatum
31 Juli 2021

Finanziert unter
Secure societies - Protecting freedom and security of Europe and its citizens

Gesamtkosten
€ 2 996 182,50

EU-Beitrag
€ 2 996 182,50

Koordiniert durch
KENTRO MELETON ASFALEIAS
Greece

CORDIS bietet Links zu öffentlichen Ergebnissen und Veröffentlichungen von HORIZONT-Projekten.

Links zu Ergebnissen und Veröffentlichungen von RP7-Projekten sowie Links zu einigen Typen spezifischer Ergebnisse wie Datensätzen und Software werden dynamisch von OpenAIRE abgerufen.

Leistungen

Documents, reports (29)

Dissemination activities report (1st Report)

This biannual report detail the dissemination activities carried out during the reporting period, assess their effectiveness, recommend adjustments, and plan for further actions.

Regulatory framework analysis

This report will analyse the regulatory framework that is applicate in the project regarding personal data collection and processing and will present suitable technical measures that are meeting all the legal requirements.

State-of-the-art on proactive technologies

This report will provide an overview of the state-of-the-art in the areas considered in the work package. Recommendations on the approaches and methods that are well-suited for the CYBER-TRUST platform will be made.

Threat actors' attack strategies

The report will provide a detailed modelling of the possible attack strategies used by threat actors of particular profiles in selected types of cyber-attacks targeting at devices, networks and CIIs.

CYBER-TRUST blockchain security analysis (2nd Report)

This report will present in detail the security framework adopted in the distributed ledger of the project. A first version is delivered on M24 with the results of the security analysis of the DLT framework. An updated version will be delivered on month M30 including postquantum considerations and research results on formal security models.

Threat landscape: trends and methods

In this report, an analysis of the methods and tools used by threat actors, as well as, the approaches employed for their detection and mitigation will be provided; technical reports and articles published in journals/conferences will be included

Platform's 2nd evaluation report

This deliverable presents the use case execution and the evaluation report based on the analysis of the data collected during the 2nd validation period.

Cyber-threat intelligence: architecture and methods

The report will describe the architecture of the cyber-threat intelligence gathering tool, the methods/algorithms explored and developed, as well as research results obtained from the experimental setups

Dissemination activities report (5th Report)

This biannual report detail the dissemination activities carried out during the reporting period, assess their effectiveness, recommend adjustments, and plan for further actions.

Intelligent cyber-attackers/defenders: models and results

This report will contain research results obtained in the context of cyber-security games. The performance of the proposed algorithms against advanced intelligent cyber-attackers will be supported by extensive lab simulations.

Dissemination activities report (3rd Report)

This biannual report detail the dissemination activities carried out during the reporting period, assess their effectiveness, recommend adjustments, and plan for further actions.

Privacy-preserving profiling: security and privacy

The report will describe the approach taken by the project for profiling devices and issues related to security and privacy. A cross-evaluation of current and new methods for SMC and pseudonymization will be provided

Threat sharing methods: comparative analysis

The document will conduct an evaluation of existing industry-wide vulnerability reporting and sharing frameworks and provide recommendations on the approach to be followed in the Cyber-Trust platform.

CYBER-TRUST distributed ledger architecture

This report will present in detail the foreseen architecture to provide the different services for the CYBER-TRUST platform.

Dissemination activities report (2nd Report)

This biannual report detail the dissemination activities carried out during the reporting period, assess their effectiveness, recommend adjustments, and plan for further actions.

Legal analysis of the use of evidence material

This deliverable will analyse the legal requirements that are applicate on the collection and processing of evidence for criminal investigations and related matters.

Dissemination and use plan

This report will establish in detail the project’s dissemination strategy, following the iterative procedure described in Section 2.2.2, along with the mechanism to evaluate its effectiveness. It will also indicate venues to submit scientific results

and give directions for liaising with cyber-security stakeholders, standardisation bodies, forums, and other bodies.

Trust management service: security and privacy
The report will describe the TMS service of the platform. A thorough analysis of its security against a number of attacks will also be given.

Dissemination activities report (4th Report)
This biannual report detail the dissemination activities carried out during the reporting period, assess their effectiveness, recommend adjustments, and plan for further actions.

Dissemination activities report (6th Report)
This biannual report detail the dissemination activities carried out during the reporting period, assess their effectiveness, recommend adjustments, and plan for further actions.

Distributed ledger state-of-the-art report
This report will provide an overview of the state-of-the-art in distributed ledger technology and areas like modelling, implementation, security, consensus, etc.

State-of-the-art on profiling, detection and mitigation
This report will provide an overview of the state-of-the-art in the areas considered in the work package. Recommendations on the approaches and methods that are well-suited for the CYBER-TRUST platform will be made.

Legal and ethical recommendations
This report will conclude on concrete recommendations for the design of the CYBER-TRUST platform and its tools to be developed in other technical work packages.

CYBER-TRUST end-user requirements
This report will describe the methodology used in order to extract, categorise and prioritise the end-user requirements, and their subsequent translation into technical requirements. It will be revised on month M14 following the end-user feedback during the design phase.

CYBER-TRUST blockchain security analysis (1st Report)
This report will present in detail the security framework adopted in the distributed ledger of the project. A first version is delivered on M24 with the results of the security analysis of the DLT framework. An updated version will be delivered on month M30 including postquantum considerations and research results on formal security models.

Network-level attacks: methods and results

The report will provide details about the methodology proposed for the detection and mitigation of network-level attacks. The features selection will be explained and will be supported by extensive lab simulations.

Cyber-threat intelligence sharing

The report will describe the architecture of the cyber-threat information sharing tool, including the design of the enriched VDB.

Device-level attacks: proposed solutions

The report will describe the approach taken to detect attacks targeting at devices and their remediation. Lab tests for various attacks will also be included.

CYBER-TRUST use case scenarios

The report will document the use case scenarios that will guide the development of the services and functionalities implemented by the CYBER-TRUST platform.

Other (6)

CYBER-TRUST proactive technology tools

These are the software tools that will implement the various algorithms, methods, tools, systems, etc. of the work package. A first version is delivered on month M21 that is refined during the deployment of the platform on the pilot sites.

CYBER-TRUST network tools

The deliverable will release a prototype of tools for the detection and mitigation of advanced network attacks, including network forensic aspects. A first version is delivered on month M21 that is refined during the deployment of the platform on the pilot sites.

CYBER-TRUST authority and publishing management

This includes a DLT smart-contract with reference client implementation and the documentation. It will enable CYBER-TRUST users to manage the acceptance and evocation of a new manufacturer authority on an IoT device class that enables publishing authoritative data for the device, i.e. default configuration, description of usage, firmware download URL, etc.

CYBER-TRUST visualisation tool

The deliverable will release a prototype of an advanced visualisation tool (VR/Flat based) for understanding and visually detecting cyber-threats. A first version is delivered on month M21 that is refined during the deployment of the platform on the pilot sites.

CYBER-TRUST device tools

The deliverable delivers a prototype of tools for the detection and remediation of advanced device attacks, including device forensic aspects. A first version is delivered on month M21 that is refined during the deployment of the platform on the pilot sites.

CYBER-TRUST information and evidence storage

This will deliver a deployable demo DLT platform, a smart-contract for registering IoT device information and a reference client implementation, with a forensic tool to search for evidence, documentation for the components. A first version is delivered on month M21 that is refined during the deployment of the platform on the pilot sites.

Websites, patent fillings, videos etc. (1)

CYBER-TRUST project website

This is the website dedicated to the project activities, providing services, such as mailing lists, RSS feeds, discussion forums/blogs, and webcasts/podcasts.

Veröffentlichungen

Conference proceedings (29)

A Crawler Architecture for Harvesting the Clear, Social, and Dark Web for IoT-Related Cyber-Threat Intelligence

Autoren: Paris Koloveas, Thanasis Chantzios, Christos Tryfonopoulos, Spiros Skiadopoulos
Veröffentlicht in: 2019 IEEE World Congress on Services (SERVICES), 2019, Seite(n) 3-8, ISBN 978-1-7281-3851-0
Herausgeber: IEEE
DOI: 10.1109/services.2019.00016

IoT Malware Network Traffic Classification using Visual Representation and Deep Learning

Autoren: Gueltoum Bendiab, Stavros Shiaeles, Abdulrahman Alruban, Nicholas Kolokotronis
Veröffentlicht in: 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, Seite(n) 444-449, ISBN 978-1-7281-5684-2

Herausgeber: IEEE
DOI: 10.1109/netsoft48620.2020.9165381

Insider Threat Detection using Deep Autoencoder and Variational Autoencoder Neural Networks
Autoren: Efthimios Pantelidis, Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, Seite(n) 129-134, ISBN 978-1-6654-0285-9
Herausgeber: IEEE
DOI: 10.1109/csr51186.2021.9527925

Social Media Monitoring for IoT Cyber-Threats
Autoren: Sofia Alevizopoulou, Paris Koloveas, Christos Tryfonopoulos, Paraskevi Raftopoulou
Veröffentlicht in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, Seite(n) 436-441, ISBN 978-1-6654-0285-9
Herausgeber: IEEE
DOI: 10.1109/csr51186.2021.9527964

Understanding and Mitigating Banking Trojans: From Zeus to Emotet
Autoren: Konstantinos P. Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis, Costas Vassilakis, Stavros Shiaeles
Veröffentlicht in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, Seite(n) 121-128, ISBN 978-1-6654-0285-9
Herausgeber: IEEE
DOI: 10.1109/csr51186.2021.9527960

Privacy Issues in Voice Assistant Ecosystems
Autoren: Georgios Germanos, Dimitris Kavallieros, Nicholas Kolokotronis, Nikolaos Georgiou
Veröffentlicht in: 2020 IEEE World Congress on Services (SERVICES), 2020, Seite(n) 205-212, ISBN 978-1-7281-8203-2
Herausgeber: IEEE
DOI: 10.1109/services48979.2020.00050

Cyber Resilience in IoT Network: Methodology and Example of Assessment through Epidemic Spreading Approach
Autoren: Emanuele Bellini, Franco Bagnoli, Alexander A. Ganin, Igor Linkov
Veröffentlicht in: 2019 IEEE World Congress on Services (SERVICES), 2019, Seite(n) 72-77, ISBN 978-1-7281-3851-0
Herausgeber: IEEE
DOI: 10.1109/services.2019.00027

Tools for Network Traffic Generation - A Quantitative Comparison

Autoren: Matthew Swann, Joseph Rose, Gueltoum Bendiab, Stavros Shiaeles, Nick Savage
Veröffentlicht in: World Congress on Internet Security (WorldCIS-2020) in collaboration with the International Conference for Internet Technology and Secured Transactions (ICITST-2020), World Congress on Sustainable Technologies (WCST-2020) and World Congress on Industrial Control Systems Security (WCICSS-2020), 2020, Seite(n) 24-29, ISBN 9781913572242
Herausgeber: Infonomics Society
DOI: 10.20533/worldcis.2020.0003

Threat landscape for smart grid systems
Autoren: Christos-Minas Mathas, Konstantinos-Panagiotis Grammatikakis, Costas Vassilakis, Nicholas Kolokotronis, Vasiliki-Georgia Bilali, Dimitris Kavallieros
Veröffentlicht in: Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, Seite(n) 1-7, ISBN 9781450388337
Herausgeber: ACM
DOI: 10.1145/3407023.3409229

IoT Vulnerability Data Crawling and Analysis
Autoren: Stavros Shiaeles, Nicholas Kolokotronis, Emanuele Bellini
Veröffentlicht in: 2019 IEEE World Congress on Services (SERVICES), 2019, Seite(n) 78-83, ISBN 978-1-7281-3851-0
Herausgeber: IEEE
DOI: 10.1109/services.2019.00028

A Trust Management System for the IoT domain
Autoren: Christos-Minas Mathas, Costas Vassilakis, Nicholas Kolokotronis
Veröffentlicht in: 2020 IEEE World Congress on Services (SERVICES), 2020, Seite(n) 183-188, ISBN 978-1-7281-8203-2
Herausgeber: IEEE
DOI: 10.1109/services48979.2020.00047

Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT
Autoren: Joseph R Rose, Matthew Swann, Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), 2021, Seite(n) 409-415, ISBN 978-1-6654-0522-5
Herausgeber: IEEE
DOI: 10.1109/netsoft51509.2021.9492685

A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning
Autoren: Luke Barlow, Gueltoum Bendiab, Stavros Shiaeles, Nick Savage
Veröffentlicht in: 2020 IEEE World Congress on Services (SERVICES), 2020,

Seite(n) 177-182, ISBN 978-1-7281-8203-2
Herausgeber: IEEE
DOI: 10.1109/services48979.2020.00046

On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection
Autoren: Nicholas Kolokotronis, Sotirios Brotsis, Georgios Germanos, Costas Vassilakis, Stavros Shiaeles
Veröffentlicht in: 2019 IEEE World Congress on Services (SERVICES), 2019, Seite(n) 21-28, ISBN 978-1-7281-3851-0
Herausgeber: IEEE
DOI: 10.1109/services.2019.00019

WiP: Are Cracked Applications Really Free? An Empirical Analysis on Android Devices
Autoren: Konstantinos-Panagiotis Grammatikakis, Angela Ioannou, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2018, Seite(n) 730-735, ISBN 978-1-5386-7518-2
Herausgeber: IEEE
DOI: 10.1109/dasc/picom/datacom/cyberscitec.2018.00127

WiP: A Novel Blockchain-Based Trust Model for Cloud Identity Management
Autoren: Keltoum Bendiab, Nicholas Kolokotronis, Stavros Shiaeles, Samia Boucherkha
Veröffentlicht in: 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2018, Seite(n) 724-729, ISBN 978-1-5386-7518-2
Herausgeber: IEEE
DOI: 10.1109/dasc/picom/datacom/cyberscitec.2018.00126

Agent-based Vs Agent-less Sandbox for Dynamic Behavioral Analysis
Autoren: Muhammad Ali, Stavros Shiaeles, Maria Papadaki, Bogdan V Ghita
Veröffentlicht in: 2018 Global Information Infrastructure and Networking Symposium (GIIS), 2018, Seite(n) 1-5, ISBN 978-1-5386-7272-3
Herausgeber: IEEE
DOI: 10.1109/giis.2018.8635598

Detection of LDDoS Attacks Based on TCP Connection Parameters
Autoren: Michael Siracusano, Stavros Shiaeles, Bogdan Ghita
Veröffentlicht in: 2018 Global Information Infrastructure and Networking

Symposium (GIIS), 2018, Seite(n) 1-6, ISBN 978-1-5386-7272-3
Herausgeber: IEEE
DOI: 10.1109/giis.2018.8635701

Data Protection by Design for cybersecurity systems in a Smart Home environment
Autoren: Olga Gkotsopoulou, Elisavet Charalambous, Konstantinos Limniotis, Paul Quinn, Dimitris Kavallieros, Gohar Sargsyan, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: 2019 IEEE Conference on Network Softwarization (NetSoft), 2019, Seite(n) 101-109, ISBN 978-1-5386-9376-6
Herausgeber: IEEE
DOI: 10.1109/netsoft.2019.8806694

A Novel Malware Detection System Based on Machine Learning and Binary Visualization
Autoren: Irina Baptista, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019, Seite(n) 1-6, ISBN 978-1-7281-2373-8
Herausgeber: IEEE
DOI: 10.1109/iccw.2019.8757060

Blockchain Solutions for Forensic Evidence Preservation in IoT Environments
Autoren: Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, Clement Pavue
Veröffentlicht in: 2019 IEEE Conference on Network Softwarization (NetSoft), 2019, Seite(n) 110-114, ISBN 978-1-5386-9376-6
Herausgeber: IEEE
DOI: 10.1109/netsoft.2019.8806675

Detection of Insider Threats using Artificial Intelligence and Visualisation
Autoren: Vasileios Koutsouvelis, Stavros Shiaeles, Bogdan Ghita, Gueltoum Bendiab
Veröffentlicht in: 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, Seite(n) 437-443, ISBN 978-1-7281-5684-2
Herausgeber: IEEE
DOI: 10.1109/netsoft48620.2020.9165337

The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform
Autoren: Thanasis Chantzios, Paris Koloveas, Spiros Skiadopoulos, Nikos Kolokotronis, Christos Tryfonopoulos, Vasiliki-Georgia Bilali, Dimitris Kavallieros
Veröffentlicht in: Proceedings of the 8th International Conference on Data Science, Technology and Applications, 2019, Seite(n) 369-376, ISBN 978-989-758-377-3
Herausgeber: SCITEPRESS - Science and Technology Publications
DOI: 10.5220/0007978103690376

On the Security of Permissioned Blockchain Solutions for IoT Applications

Autoren: Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles
Veröffentlicht in: 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, Seite(n) 465-472, ISBN 978-1-7281-5684-2
Herausgeber: IEEE
DOI: 10.1109/netsoft48620.2020.9165480

A Novel Online Incremental Learning Intrusion Prevention System

Autoren: Christos Constantinides, Stavros Shiaeles, Bogdan Ghita, Nicholas Kolokotronis
Veröffentlicht in: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2019, Seite(n) 1-6, ISBN 978-1-7281-1542-9
Herausgeber: IEEE
DOI: 10.1109/ntms.2019.8763842

Blockchain Security by Design Framework for Trust and Adoption in IoT Environment

Autoren: Gohar Sargsyan, Nicolas Castellon, Raymond Binnendijk, Peter Cozijnsen
Veröffentlicht in: 2019 IEEE World Congress on Services (SERVICES), 2019, Seite(n) 15-20, ISBN 978-1-7281-3851-0
Herausgeber: IEEE
DOI: 10.1109/services.2019.00018

Advanced metering infrastructures - security risks and mitigation

Autoren: Gueltoum Bendiab, Konstantinos-Panagiotis Grammatikakis, Ioannis Koufos, Nicholas Kolokotronis, Stavros Shiaeles
Veröffentlicht in: Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, Seite(n) 1-8, ISBN 9781450388337
Herausgeber: ACM
DOI: 10.1145/3407023.3409312

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

Autoren: Sotirios Brotsis, Nicholas Kolokotronis, Konstantinos Limniotis, Gueltoum Bendiab, Stavros Shiaeles
Veröffentlicht in: 2020 IEEE World Congress on Services (SERVICES), 2020, Seite(n) 197-204, ISBN 978-1-7281-8203-2
Herausgeber: IEEE
DOI: 10.1109/services48979.2020.00049

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

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

Veröffentlicht in: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), 2021, Seite(n) 1-6, ISBN 978-1-7281-9441-7
Herausgeber: IEEE
DOI: 10.1109/iccworkshops50388.2021.9473666

Book chapters (10)

A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain
Autoren: Richard Brown, Gueltoum Bendiab, Stavros Shiaeles, Bogdan Ghita
Veröffentlicht in: Selected Papers from the 12th International Networking Conference - INC 2020, Ausgabe 180, 2021, Seite(n) 31-46, ISBN 978-3-030-64757-5
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-64758-2_3

Audio Interval Retrieval Using Convolutional Neural Networks
Autoren: Ievgeniia Kuzminykh, Dan Shevchuk, Stavros Shiaeles, Bogdan Ghita
Veröffentlicht in: Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 20th International Conference, NEW2AN 2020, and 13th Conference, ruSMART 2020, St. Petersburg, Russia, August 26–28, 2020, Proceedings, Part I, Ausgabe 12525, 2020, Seite(n) 229-240, ISBN 978-3-030-65725-3
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-65726-0_21

Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study
Autoren: Faisal Alsakran, Gueltoum Bendiab, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: Security in Computing and Communications - 7th International Symposium, SSCC 2019, Trivandrum, India, December 18–21, 2019, Revised Selected Papers, Ausgabe 1208, 2020, Seite(n) 87-98, ISBN 978-981-15-4824-6
Herausgeber: Springer Singapore
DOI: 10.1007/978-981-15-4825-3_7

BotSpot: Deep Learning Classification of Bot Accounts Within Twitter
Autoren: Christopher Braker, Stavros Shiaeles, Gueltoum Bendiab, Nick Savage, Konstantinos Limniotis
Veröffentlicht in: Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 20th International Conference, NEW2AN 2020, and 13th Conference, ruSMART 2020, St. Petersburg, Russia, August 26–28, 2020, Proceedings, Part I, Ausgabe 12525, 2020, Seite(n) 165-175, ISBN 978-3-030-

65725-3
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-65726-0_16

Comparative Analysis of Cryptographic Key Management Systems
Autoren: Ievgeniia Kuzminykh, Bogdan Ghita, Stavros Shiaeles
Veröffentlicht in: Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 20th International Conference, NEW2AN 2020, and 13th Conference, ruSMART 2020, St. Petersburg, Russia, August 26–28, 2020, Proceedings, Part II, Ausgabe 12526, 2020, Seite(n) 80-94, ISBN 978-3-030-65728-4
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-65729-1_8

Thermal Management in Large Data Centres: Security Threats and Mitigation
Autoren: Betty Saridou, Gueltoum Bendiab, Stavros N. Shiaeles, Basil K. Papadopoulos
Veröffentlicht in: Security in Computing and Communications - 8th International Symposium, SSCC 2020, Chennai, India, October 14–17, 2020, Revised Selected Papers, Ausgabe 1364, 2021, Seite(n) 165-179, ISBN 978-981-16-0421-8
Herausgeber: Springer Singapore
DOI: 10.1007/978-981-16-0422-5_12

User-Generated Pseudonyms Through Merkle Trees
Autoren: Georgios Kermezis, Konstantinos Limniotis, Nicholas Kolokotronis
Veröffentlicht in: Privacy Technologies and Policy - 9th Annual Privacy Forum, APF 2021, Oslo, Norway, June 17–18, 2021, Proceedings, Ausgabe 12703, 2021, Seite(n) 89-105, ISBN 978-3-030-76662-7
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-76663-4_5

Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation
Autoren: Robert Shire, Stavros Shiaeles, Keltoum Bendiab, Bogdan Ghita, Nicholas Kolokotronis
Veröffentlicht in: Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 19th International Conference, NEW2AN 2019, and 12th Conference, ruSMART 2019, St. Petersburg, Russia, August 26–28, 2019, Proceedings, Ausgabe 11660, 2019, Seite(n) 65-76, ISBN 978-3-030-30858-2
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-30859-9_6

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

Autoren: Stylianos Monogios, Konstantinos Limniotis, Nicholas Kolokotronis, Stavros Shiaeles
Veröffentlicht in: E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age - 8th International Conference, e-Democracy 2019, Athens, Greece, December 12-13, 2019, Proceedings, Ausgabe 1111, 2020, Seite(n) 34-48, ISBN 978-3-030-37544-7
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-37545-4_3

SoMIAP: Social Media Images Analysis and Prediction Framework
Autoren: Yonghao Shi, Gueltoum Bendiab, Stavros Shiaeles, Nick Savage
Veröffentlicht in: Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 20th International Conference, NEW2AN 2020, and 13th Conference, ruSMART 2020, St. Petersburg, Russia, August 26–28, 2020, Proceedings, Part I, Ausgabe 12525, 2020, Seite(n) 205-216, ISBN 978-3-030-65725-3
Herausgeber: Springer International Publishing
DOI: 10.1007/978-3-030-65726-0_19

Peer reviewed articles (7)

inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence
Autoren: Paris Koloveas, Thanasis Chantzios, Sofia Alevizopoulou, Spiros Skiadopoulos , Christos Tryfonopoulos
Veröffentlicht in: Electronics, Ausgabe 10/7, 2021, Seite(n) 818, ISSN 2079-9292
Herausgeber: MDPI
DOI: 10.3390/electronics10070818

A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages
Autoren: Andrew Ramsdale, Stavros Shiaeles, Nicholas Kolokotronis
Veröffentlicht in: Electronics, Ausgabe 9/5, 2020, Seite(n) 824, ISSN 2079-9292
Herausgeber: MDPI
DOI: 10.3390/electronics9050824

On the Design of IoT Security: Analysis of Software Vulnerabilities for Smart Grids
Autoren: Christos-Minas Mathas, Costas Vassilakis, Nicholas Kolokotronis, Charilaos C. Zarakovitis, Michail-Alexandros Kourtis
Veröffentlicht in: Energies, Ausgabe 14/10, 2021, Seite(n) 2818, ISSN 1996-1073

Herausgeber: Multidisciplinary Digital Publishing Institute (MDPI)
DOI: 10.3390/en14102818

Blockchain technologies for leveraging security and privacy
Autoren: Costas Vassilakis
Veröffentlicht in: Homo Virtualis, Ausgabe 2/1, 2019, Seite(n) 7, ISSN 2585-3899
Herausgeber: Virtual Reality, Internet Research and Learning Laboratory (Department of Psychology, Panteion University)
DOI: 10.12681/homvir.20188

Secured by Blockchain: Safeguarding Internet of Things Devices
Autoren: Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Romain Griffiths
Veröffentlicht in: IEEE Consumer Electronics Magazine, Ausgabe 8/3, 2019, Seite(n) 28-34, ISSN 2162-2256
Herausgeber: Institute of Electrical and Electronics Engineers Inc.
DOI: 10.1109/mce.2019.2892221

On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance
Autoren: Sotirios Brotsis, Konstantinos Limniotis, Gueltoum Bendiab, Nicholas Kolokotronis, Stavros Shiaeles
Veröffentlicht in: Computer Networks, Ausgabe 191, 2021, Seite(n) 108005, ISSN 1389-1286
Herausgeber: Elsevier BV
DOI: 10.1016/j.comnet.2021.108005

A proactive malicious software identification approach for digital forensic examiners
Autoren: Muhammad Ali, Stavros Shiaeles, Nathan Clarke, Dimitrios Kontogeorgis
Veröffentlicht in: Journal of Information Security and Applications, Ausgabe 47, 2019, Seite(n) 139-155, ISSN 2214-2126
Herausgeber: Elsevier
DOI: 10.1016/j.jisa.2019.04.013

Monographic books (1)

Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation
Autoren: Edited by Gohar Sargsyan, CGI, The Netherlands | Dimitrios Kavallieros, KEMEA, Greece | Nicholas E. Kolokotronis, University of

Peloponnese, Greece
Veröffentlicht in: 2021, ISBN 978-1-68083-835-0
Herausgeber: now publishers inc.
DOI: 10.1561/9781680838350

Letzte Aktualisierung: 26 Mai 2022

Permalink: https://cordis.europa.eu/project/id/786698/results/de