ARCADIAN-IoT

Newsletter 6

February 2022

EU-made cybersecurity for safe, resilient and trustworthy applications and services

In recent years, the development and increasing adoption of a large variety of Internet of Things (IoT) technologies, devices and solutions have disrupted many industries and modified many aspects of our everyday life, generating a huge impact on businesses, consumers and governments. This has huge implications regarding security and privacy. New technologies will tend to further intensify cybersecurity issues and put in evidence the need for trust and secure solutions for current and future digital services powered by IoT systems.

The European Commission selected several projects that directly address the cybersecurity needs of EU industry and public. Each project has concrete applications which focus on different verticals/application domains: education, energy, healthcare, manufacturing mobility, 5G and 6G networks, emergency and vigilance or smart cities.

This workshop, jointly organised by **ARCADIAN-IoT, ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SENTINEL, SPATIAL**, **TRUST aWARE** projects, will provide an overview on how novel solutions can

protect the complex ICT infrastructures and create a stronger, more innovative and resilient European industry.

The EU-made cybersecurity workshop is designed to provide attendees with the knowledge to create safe, resilient, and trustworthy applications and services. The online workshop will cover a range of topics related to cybersecurity, including:

- Challenges faced by security-agnostic and security-aware IoT service providers
- Best practices for designing and building secure applications and services
- Techniques for identifying and mitigating cybersecurity risks
- Strategies for ensuring the resilience of applications and services in the face of cyber threats

Agenda and registration

LATEST NEWS

Harnessing Cyber Threat Intelligence for a secure IoT ecosystem

Cyber Threat Intelligence (CTI) is a crucial component of the ARCADIAN-IoT framework. The objective of the CTI component is to gather, produce, analyze, and share information related to cyber threats and attacks in the Internet of

Things (IoT) domain, where end devices might be severely impacted. The information is generally presented in the form of Indicator of Compromise (IoC), which can be used by different organizations to detect similar attacks, or to analyze new security incidents.

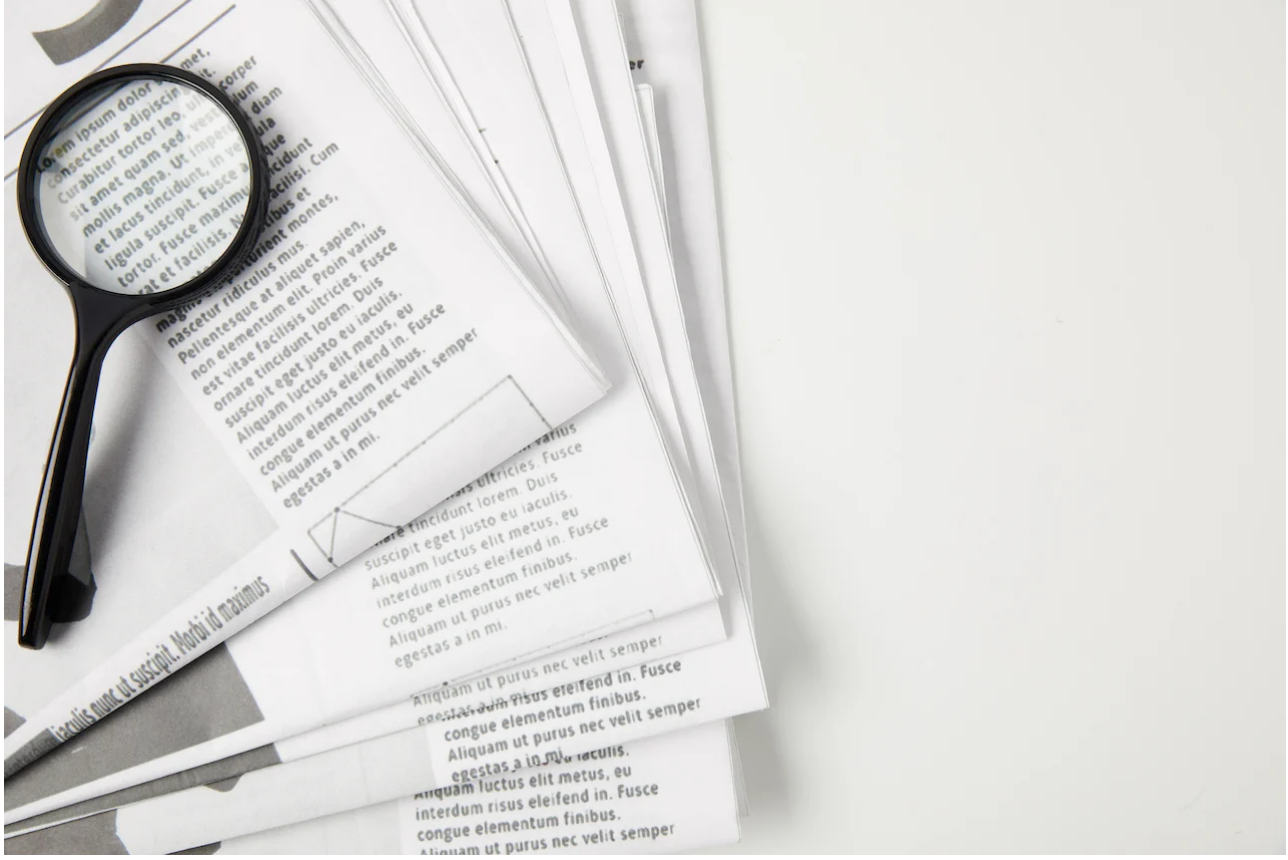
Read more

Enhancing data security with Hardened Encryption

Hardened Encryption is an ARCADIAN-IoT component that is responsible for securing the data at rest or in transit produced by the devices/persons participating in the platform.

Read more

PUBLICATIONS



Enabling Autonomous Trust, Security and Privacy Management for IoT +

This paper presents ARCADIAN-IoT, a framework aimed at holistically enabling trust, security, privacy and recovery in IoT systems, and enabling a Chain of Trust between the different IoT entities (persons, objects and services). It builds on features such as federated AI for effective and privacy-preserving cybersecurity, distributed ledger technologies for decentralized management of trust, or transparent, user-controllable and decentralized privacy.

Illumination-aware image fusion for around-the-clock human detection in adverse environments from Unmanned Aerial Vehicle +

This study proposes a novel illumination-aware image fusion technique and a Convolutional Neural Network (CNN) called BlendNet to significantly enhance the robustness and real-time performance of small human objects detection from Unmanned Aerial Vehicles (UAVs) in harsh and adverse operation environments.

XDP-Based SmartNIC Hardware Performance Acceleration for Next-Generation Networks +

This work presents a novel framework that leverages extended Berkeley

Packet Filter (eBPF) and eXpress Data Path (XDP) to offload network functions to reduce unnecessary overhead in the backbone infrastructure.

An Intelligent Mechanism for Monitoring and Detecting Intrusions in IoT Devices +

This work aims to present research about Host Intrusion Detection that could be applied for IoT devices, and additionally how Federated Learning can be applied in these instances for privacy preservation.

Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks +

This paper proposes a new cognitive closed loop system to offer distributed dual-layer self-protection capabilities to battle against Distributed Denial of Service (DDoS) attacks.

Read more

VIDEOS

Medical IoT

This ARCADIAN-IoT domanin is based on IoT medical sensors (single or combined), which interoperate with a secure communication channel. ARCADIAN-IoT will work in a platform that helps to obtain a more “technology-focused” healthcare system in order to ease the action plans under these situations by making accessible the patient data from everywhere and by providing a decision support system for helping in critical situations.

Watch the video

Emergency and vigilance using drones and IoT

ARCADIAN-IoT will accelerate the development towards decentralized, transparent and user controllable privacy in three real domains (use cases). One of them is Emergency and vigilance using drones and IoT which aims to demonstrate the contribution of the Arcadian-IoT platform to the emergency and vigilance scenarios. This domain of implementation covers trust, security, and privacy challenges.

Watch the video

SYNERGIES

The ARCADIAN-IoT project has fruitful collaborations with other EU-funded projects! Here you can find news from other projects.

Meet projects funded under the same call

TRUST aWARE project
Enhancing digital security, privacy and trust in software

ERATOSTHENES project
IoT trust and Identity management framework

IDUNN project
A cognitive detection system for cybersecure operational technologies

IRIS project
Artificial Intelligence threat reporting and incident response system

SOTERIA project
User-friendly digital secured personal data and prIvacy platform

KRAKEN project
Brokerage and market platform for personal data

SENTINEL project
Bridging the security, privacy and data protection gap for smaller enterprises in Europe

SPATIAL project
Achieving trustworthy, transparent and explainable AI for cybersecurity solutions

Funded by the EU's Horizon2020 programme under agreement n° 101020259.