IoTWeek | Dublin
June 20-23, 2022

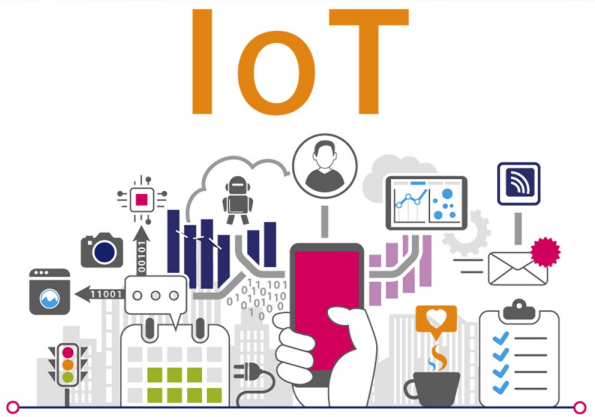
IoTWeek 2022 – Workshop on: *"Identity, trust and privacy in an intelligent, smart IoT World. Challenges and outcomes"*

ERATOSTHENES

Secure Management Of IoT Devices Lifecycle Through Identities, Trust And Distributed Ledgers

Konstantinos Loupos
R&D Director
INLECOM INNOVATION

konstantinos.loupos@inlecomsystems.com



inlecom

INLECOM

- Founded: 1996
- Athens (GR), Dublin (IE), Brussels (BE), London (UK)
- Currently participating in >35 research projects, coordinating 7

- Main Expertise:
  - AI/ML, Digital Twins, Knowledge Graphs
  - Distributed and Blockchain Ledgers
  - Cybersecurity and IoT
  - Natural Language Processing (NLP)
  - ICT Technologies and Integration Platforms
  - Project Management/Coordination and Horizontal Activities
  - Proposal writing and Coordination

- Website: http://www.inlecom.eu/

Technology Application per HE Cluster

Cluster 1 – Health
- Large-scale Data Modelling and Simulations
- Predictive Modelling, Analytics and Simulations

Cluster 2 - Culture, creativity and inclusive society
- Defect Detection and Surface Level Analysis
- Digital Twins Physical Assets Simulations

Cluster 3 - Civil Security for Society
- DLT-based Digital Identity and Trust Management
- Predictive Modelling and Cascading Effects Simulations

Cluster 4 - Digital, Industry and Space
- AI/ML Predictive Modelling, Process Analytics
- Digital Twins Physical Assets Simulations
- Computer Vision for Inspection and Maintenance

Cluster 5 - Climate, Energy and Mobility
- AI/ML for Logistics, Planning and Transport Operations
- Digital Twins Network Simulations and Global Sustainability
- AI/ML-based Decision Support, Modelling and Simulations

Cluster 6 - Food, Bioeconomy, Natural Resources, Agriculture and Environment
- Predictive Modelling, Analytics and Simulations
- Digital Twins Physical Assets Simulations

Background

- Internet of Things (IoT) allowing quotidian devices to connect to the Internet and collect/share information
- Devices intended to improve people's daily life and business environments, by gathering and sharing massive amounts of data
- Number of connected devices 26.66b (2019)
- Prediction for 74.44b devices (2025)

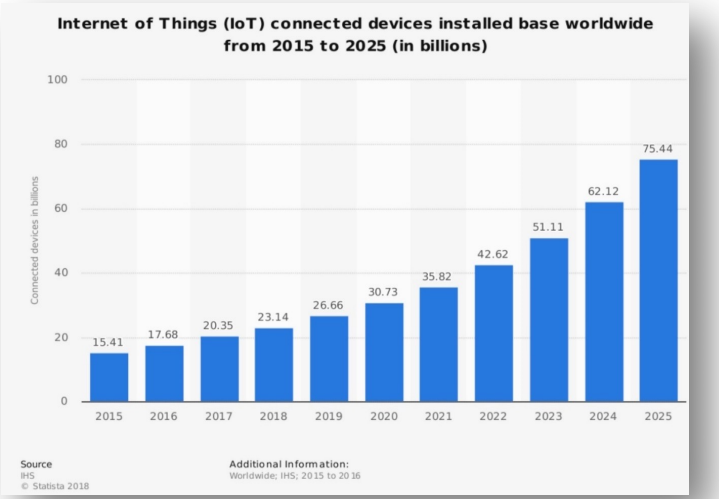
- High penetration of IoT devices in every aspect of human life will lead to:
  - huge attack surface
  - increased security and privacy risks

- Daily reporting of cybersecurity attacks against devices, from toys to medical devices (e.g. Mirai IoT botnet (Oct 2016)
  - Several devices used to perform a DDoS attack against big platforms (i.e., Amazon, Spotify) causing interruption of their services for hours, with high monetary losses
- Based on the Mirai IoT Botnet, different variations were implemented (Torii, Hajime or BrickerBot).

- Current literature identified challenges:
  - confidentiality
  - access control
  - privacy for users and things
  - devices' trustworthiness
  - compliance

Background and IoT Challenges

- **Dynamic orchestration of security mechanisms** (authentication and connectivity)
- **Trustworthy interactions** between unknown devices
- Huge **number of connected devices** (scalability)
- **Fully distributed** network dynamicity
- **Intelligent processing at device level** (threat and opportunity)
- **Heterogeneity** – interaction between different networks and device manufacturers
- **Federated learning and Artificial Intelligence**



ERATOSTHENES Project

Topic: **SU-DS02-2020:** Intelligent security and privacy management

(d) Distributed trust management and digital identity solutions

Full name: **Secure Management Of IoT Devices Lifecycle Through Identities, Trust And Distributed Ledgers**

GA No: *101020416*

Start date: *1 October 2021 (link)*

Duration: *42 months*

Partners: *14*

Countries: *8*

Consortium

No	Name	Short name	Country
1	INLECOM INNOVATION ASTIKI MI KERDOSKOPIKI ETAIREIA	INLE	Greece
2	UNIVERSIDAD DE MURCIA	UMU	Spain
3	ATOS IT SOLUTIONS AND SERVICES IBERIA SL	ATOS	Spain
4	SINTEF AS	SINTEF	Norway
5	AIRBUS CYBERSECURITY SAS	AIRBUS	France
6	ENGINEERING - INGEGNERIA INFORMATICA SPA	ENG	Italy
7	KATHOLIEKE UNIVERSITEIT LEUVEN	KUL	Belgium
8	TECHNISCHE UNIVERSITAET GRAZ	TUG	Austria
9	UNIVERSITY OF PIRAEUS RESEARCH CENTER	UPRC	Greece
10	IDIADA AUTOMOTIVE TECHNOLOGY SA	IDIADA	Spain
11	DIGITAL WORX GMBH	DWG	Germany
12	TELLU IOT AS	TEL	Norway
13	EULAMBIA ADVANCED TECHNOLOGIES MONOPROSOPI ETAIRIA PERIORISMENIS EFTHINIS	EUL	Greece
14	DBC EUROPE	DBC	Belgium

<u>14 Partners</u>

- 6 SMEs
- 5 Academic
- 3 Large

ERATOSTHENES IoT Challenges and Focus

- **Lack of security visibility (**main precursor to security incidents). Security gaps are extremely hard to be detected, to remediate and to address on time
- Lack **of effective information sharing** between organisations and availability of tools to the CERTs/CSIRTs
- **Heterogeneity of IoT devices** extremely challenging to establish a trustworthy environment among objects and persons.
- Lack of a **common trust enforcement mechanism and relevant standards**. Available mechanisms address only security and privacy aspects and rely on centralised authorities while remain vulnerable to threats
  - Trust revolves around assurance and confidence that people, data, information, or processes will function or behave in expected ways
  - Not that easy in an artificial society such as IoT
  - Important to **quantify "trust" such that it can be understood by the artificial agents**
- **Firmware and security updates are infrequent** and **difficult** or even **impossible**, especially in large networks
- **Lack of a transparent identity and privacy framework** to allow the users to maintain full control of their identity and data at the device level, without being forced to transmit them to intermediary or centralised authorities
- **Lacking security training and security protocols' adoption for** persons and devices, one of the most critical challenges as humans are the weakest point in the lifecycle chain, as they build, test, deploy and use IoT

Objectives

- Obj.1: Design a **Trust Framework and a Reference Architecture** to ensure end-to-end trust and identity management in distributed IoT networks, suited for resource-restricted environments, critical and industrial applications

- Obj.2: Design and development of a **lightweight, distributed, and dynamic Trust Manager** to enhance the trust in large-scale distributed networks of heterogeneous IoT devices covering each layer and cross-layer of the network

- Obj3: Design of a **decentralised, scalable, efficient and privacy preserving IoT identity management** to conciliate the requirements of self-sovereignty and privacy preservation in a distributed, interoperable and transparent trust model, including self-encryption/decryption schemes and IoT identity recovery

- Obj4: Build the **lifecycle management** and the **overall governance layer of the trust network** on novel Distributed Ledger Technologies and a hybrid consensus protocol. Implement **Smart Contracts** for enforcing **access policies and sharing trustworthiness** within the network guaranteeing their transparency, integrity, authenticity, and authority. Design of **Inter-ledger Cyber-Threat Information Sharing,** and automated **Recovery Solutions based on a multi-layer approach**

- Obj5: **Integrate and Validate** the approach through **real-world pilots** to assess its effectiveness and organize hands-on training through realistic **cybersecurity exercises**

- Obj6: Deliver knowledge via **dissemination and capacity building**, supporting the enforcement of the Cybersecurity Act and **standardization activities** and **build a robust exploitation plan and market positioning**

Overall Vision

ERATOSTHENES will devise, implement and evaluate a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework to:

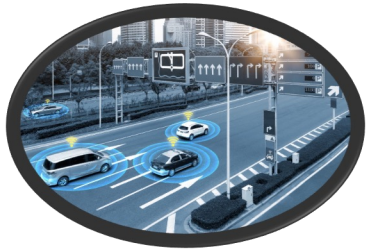
- dynamically and holistically manage the lifecycle of IoT devices,
- strengthening trust, identities, privacy and resilience in the entire IoT ecosystem,
- supporting the enforcement of the NIS directive, GDPR and Cybersecurity Act

"…to provide core cybersecurity features to be adopted by IoT solution providers and manufacturers as baseline certification elements in the production of devices and throughout their entire lifecycle"

Technical Outcomes and Expected Results

- First-ever enclosure of cybersecurity features in IoT devices through deployment of **Trust Agents** and **continuous trust evaluation**
- **Decentralised identity management** mechanisms to conciliate requirements of self-sovereignty and privacy preservation in a distributed/transparent trust model
- **Self-encryption/decryption at device-level** with a whole system **automated recovery** process
- **Threat-analysis models** based on federated learning and edge execution
- **Collaborative IoT threat intelligence** sharing across ledgers to adapt detection/defence mechanisms
- **Integration of Physical Unclonable Functions** in trust framework and distributed ledgers
- Support **enforcement of the NIS directive** information sharing based on inter-ledger technologies

Validation Pilots and Use Cases



- Connected Vehicles
  - Interaction with vehicle (V2V) and road infrastructure (traffic lights)
  - Software updates

- Smart Health
  - Zero-contact enrolment of users and devices.
  - Integrate with third-party services
  - Extending the platform with private devices
  - Emergency situations
  - Continuous monitoring and lifecycle management of services

- Disposal IDs in Industry 4.0
  - Implementation of resilient and secure Asset Identification
  - Distributed Disposable ID service
  - Trust and permission service
  - Open Source and 3rd party integration
  - Scalability testing

Current Status and Upcoming Steps

- System requirements gathering and analysis finalized
- First version of system architecture
- All technical WPs started
  - Technical developments started
  - Technical interfaces and flows testing
- Deployment preparation for our first use-case (automotive)
- First PoC ready by the end of 2022

- <u>Upcoming events:</u>
  - 2nd International Workshop on Advances on Privacy-Preserving Technologies and Solutions (IWAPS 2022) (Aug. 2022, Vienna)

IoTWeek | Dublin
June 20-23, 2022

IoTWeek 2022 – Workshop on: *"Identity, trust and privacy in an intelligent, smart IoT World. Challenges and outcomes"*

Thank you for your attention!

Konstantinos Loupos

R&D Director

INLECOM INNOVATION

konstantinos.loupos@inlecomsystems.com

inlecom

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020416