Overview and Accomplishment of the H2020 IoT Security/Privacy Cluster Projects

John Soldatos, Athens Information Technology

E-Mail: jsol@ait.gr
Twitter: @jsoldatos

All the presented projects have received funding from the European Union’s Horizon 2020 research and innovation programme
<table>
<thead>
<tr>
<th>Project</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brain-IoT</td>
<td>Eight (8) EC Funded Projects</td>
</tr>
<tr>
<td>ENACT</td>
<td>Successful in the H2020 IoT-03-2017 Call for Proposals “R&amp;I on IoT integration and platforms”</td>
</tr>
<tr>
<td>CHARIOT</td>
<td>Timeframe: 01/01/2018-31/12/2020 (36 months)</td>
</tr>
<tr>
<td>IoTcrawler</td>
<td>Focal Area: Solutions for Federation, Interoperability, Security and Privacy</td>
</tr>
<tr>
<td>SecureIoT</td>
<td>Total Budget ~ 37.000.000 EUR (IoT-03-2017 Call Budget)</td>
</tr>
<tr>
<td>SemIoTics</td>
<td></td>
</tr>
<tr>
<td>SerIoT</td>
<td></td>
</tr>
<tr>
<td>SOFIE</td>
<td></td>
</tr>
</tbody>
</table>
Common Innovation Drivers & Motivation

"Third Generation" of IoT Systems
- From Distributed Sensing & Massive IoT/Cloud Systems to Smart Objects with (Semi)Autonomous Behavior
- From Passive Data Analytics to Field Actuation and Cyber-Physical Systems (CPS)

IoT Platforms Interoperability (incl. Security Interoperability)
- Cross-Platform Interoperability Scenarios (e.g., Supply Chain Management)

Alignment to On-Going Evolution and Regulatory Compliance
- Artificial Intelligence, Distributed Ledger Technologies (DLT)
- GDPR into force as of May 2018

Foundation for Dynamic Massively Scalable & Autonomous IoT Systems
- Supporting Industry 4.0
- Leveraging AI and Blockchain Technologies

IoT Platforms Interoperability (incl. Security Interoperability)
- Cross-Platform Interoperability Scenarios (e.g., Supply Chain Management)
Brain-IoT: Model-Based Framework for Dependable Sensing & Actuation in Intelligent Decentralized IoT Systems

Objectives, Scope, Validation

• Interoperability & Dynamic Platforms Federations (Shared Semantic Models linked dynamically to IoT devices)
• Smart Cooperative Behaviours based on AI features
• Dynamic AAA
• Embedded Privacy & Privacy Control
• Dynamic Commissioning & Reconfiguration (edge/cloud deployment & balancing)
• Validation Settings: Robotics, Critical Water Infrastructures, H2020 LSP Projects (Smart Cities, Healthcare, Wearables..)
ENACT: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems

Objectives, Scope, Validation

- Enablers for continuous development and operation of trustworthy IoT systems
- Risk-driven and agile development and delivery
- Continuous evolution to keep the smart IoT system trustworthy despite internal threats
- Address security, privacy, safety, resilience, and reliability.
- Deal with software updates, new security strategies, new user profiles, policies changes.
- Validation: Rail, Healthcare, Smart Building

https://www.enact-project.eu
CHARIOT: Cognitive Heterogeneous Architecture for Industrial IoT

Objectives, Scope, Validation

- Open Cognitive IoT Architecture and Platform for safety critical systems and IoT systems interaction in a secure manner
- Runtime IoT Privacy, Security and Safety Supervision Engine (IPSE)
  - Privacy Engine based on PKI and Blockchain technologies
  - Firmware Security integrity checking
  - IoT Safety Supervision Engine (ISSE)
- Analytics Prediction and Dashboard
- Validation: Trenitalia (Italy) & Athens International Airport (Greece), IBM Campus (Ireland)
IoTCrawler: Search Engine for the Internet of Things

Objectives, Scope, Validation

- Search engines that support crawling, discovery and integration of IoT data.
- Adaptive and dynamic solutions for resource ranking and selection.
- Distributed crawling and indexing mechanisms to enable near real-time discovery and search of massive real world (IoT) data streams in a secure and privacy- and trust-aware framework.
- Enablers for security-, privacy and trust-aware discovery and access to IoT resources in constrained IoT environments
- New applications and services that rely on ad-hoc and dynamic data/service query and access.
- Validation: Smart City, Social IoT, Smart Energy, Industry 4.0
SecureIoT: Predictive Security for IoT Platforms and Networks of Smart Objects

Objectives, Scope, Validation

- End-to-End Security Monitoring for Predictive (AI-based Security)
- Security Interoperability across IoT Platforms
- Cross-Platform & Cross-Vertical
- Validation: Socially Assistive Robots, Smart Manufacturing, Connected Car & Self-Driving

https://secureiot.eu/
SemIoTics: Smart End-to-end Massive IoT Interoperability, Connectivity and Security

Objectives, Scope, Validation

- Patterns for security, privacy, dependability and interoperability
- Semantic interoperability mechanisms
- Dynamically and self-adaptable monitoring
- Embedded intelligence and adaptation
- Programmable networking with SDN/NFV
- SEMIoTICS open architecture prototype
- Promote the adoption of EU technology offerings internationally
- Validation: Wind Energy, Healthcare, Smart Sensing

https://www.semiotics-project.eu/
SerIoT: Secure & Safe Internet of Things

Objectives, Scope, Validation

- Design a Cognitive Packet Network that interconnects distributed IoT subsystems based on SDN technology
- Use “Smart Packets” (SP) to search for secure multi-hop routes having good quality of service & energy efficiency.
- Use Random Neural Networks for routing decisions and overall network performance improvements – “Security Aware” routing
- Validation: ITS & Smart Cities, Surveillance, Flexible Manufacturing, Food Chain

https://seriot-project.eu
Objectives & Scope

- Secure open federation to enable interoperability between existing IoT platforms
- Utilizes multiple distributed ledger technologies (DLTs) in parallel
- Creation of IoT business platforms Enables open data markets

Validation

- Energy - Electrical vehicle charging, allows optimizing electricity generation and grid load
- Energy - laboratory pilot with smart meter data
- Food chain - from field to fork, precise tracking of the whole agricultural supply chain
- Mixed-reality mobile gaming, allows gamers to interact with real-world

SOFIE: Secure Open Federation for Internet Everywhere

https://www.sofie-iot.eu/
Cross Cutting Activities & Joint Results

**Joint Standardization Efforts**
- Specify/Standardize Common Tools for risk assessment and threat analysis
- Explore existing standards in lifecycle management for security and trust

**Knowledge & Experience Sharing**
- Blockchain & DLT Deployment, Operation and Use
- Joint “Thematic” workshops on Blockchain

**IoT Platforms Interoperability and Integration**
- Emphasis on Data-Driven Security Monitoring
- Streamlining with other EU Efforts (e.g., IoT-EPI)

**Joint Dissemination and Policy Contributions**
- Common workshops and conferences – Joint participation in exhibitions
- Collaborative contributions to policies (e.g., GDPR compliance, inputs to ECSO)
Tentative Release Roadmap & Outlook

- Sep ’18: Architectures & Use Cases Detailed
- Mar ’19: Initial Platform Releases
- June ’19: First Results of Joint Standardization & Dissemination Efforts
- Dec ’19: Results Validated (Technical Validation) – Planning of Business Validation