H2020 Project Clustering Workshop

Friday, 20th of April 2018, Athens, Greece

H2020 PROJECT CLUSTERING TECHNICAL WORKSHOP

Venue
CIVITEL Attik
Olimpias 11, Athens
151 24

Organized by
ReCRED Project
www.recred.eu

About

This workshop is organized by the ReCRED project aiming at pilot demonstrations from relative H2020 projects in the field of privacy and cybersecurity.

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 653417

Pilot Demonstrations

Booth	Project Title	Description
1	**ReCRED** - From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control	ReCRED is a European project (H2020 program) that aims to design and implement mechanisms that anchor all access control (AC) needs to mobile devices that users habitually use and carry. It aims to build integrated next generation access control (AC) solution that: i) solves the following problems that stem from the weaknesses of the current authentication methods, ii) is aligned with current technological trends and capabilities, iii) offers a unifying access control framework that is suitable for a multitude of use cases that involve online and physical authentication and authorization via an off-the-shelf mobile device and iv) is attainable and feasible to implement in the existing products under the scope and timeframe of the project.
	Project Representative	**Christos Xenakis** (UPRC) xenakis@unipi.gr
2	**OPERANDO** – Online Privacy Enforcement, Rights Assurance and Optimization	The goal of the OPERANDO project is to specify, implement, field-test, validate and exploit an innovative privacy enforcement platform that will enable the Privacy as a Service (PaaS) business paradigm and the market for online privacy services. The OPERANDO project will integrate and extend the state of the art to create a platform that will used by independent Privacy Service Providers (PSPs) to provide comprehensive user privacy enforcement in the form of a dedicated online service, called "Privacy Authority". The OPERANDO platform will support flexible and viable business models, including targeting of individual market segments such as public administration, social networks and Internet of Things.
	Project Representative	**Constantinos Patsakis** (UPRC) kpatsak@unipi.gr
3	**FutureTrust** – Future Trust Services for Trustworthy Global Transactions	The core objective of the FutureTrust project is to support the practical implementation of the eIDAS regulation (2014/910/EU) on electronic identification (eID) and trusted services for electronic transactions in the internal market and ease the utilization and proliferation of trustworthy eID and electronic signature technology in Europe and beyond in order to enable legally significant electronic transactions around the globe. For this purpose the FutureTrust project will build upon results developed within previous research and large scale pilot projects and integrate existing trust services, which are mostly related to qualified certificates, electronic signatures and time stamps, with the forthcoming eID interoperability framework and conduct research, design innovative solutions and provide Open Source implementations for the recently introduced trust services related to the validation, preservation and mobile creation of qualified electronic signatures and seals.
	Project Representative	**Jon Shamah** (EEMA) jshamah@ejconsultants.eu
4	**LIGHTEST** – Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes	The objective of LIGHTest is to create a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions. By querying different trust authorities' world-wide and combining trust aspects related to identity, business, reputation etc. it will become possible to conduct domain-specific trust decisions. This is achieved by reusing existing governance, organization, infrastructure, standards, software, community, and know-how of the existing Domain Name System, combined with new innovative building blocks. This approach allows an efficient global rollout of a solution that assists decision makers in their trust decisions. By integrating mobile identities into the scheme, LIGHTest also enables domain-specific assessments on Levels of Assurance for these identities.
	Project Representative	**Jon Shamah** (EEMA) jshamah@ejconsultants.eu

5

PaaSword – A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications

PaaSword

PaaSword extends the Cloud Security Alliance's cloud security principles by capitalizing on recent innovations in virtual database middleware technologies that introduce a scalable secure cloud database abstraction layer with sophisticated data distribution and encryption methods. The implementation of enterprise security governance in cloud environments is supported by a novel approach towards context-aware access control mechanisms that incorporate dynamically changing contextual information into access control policies and context-dependent access rights to data stored in the cloud. Finally, PaaSword supports developers of cloud applications through code annotation techniques that allow specifying an appropriate level of protection for the application's data. Applicability, usability, effectiveness and value of the PaaSword concepts are proven through their integration in industrial, real-life services and applications.

Project Representative

Panagiotis Gouvas (UBITECH)
pgouvas@ubitech.eu

6

KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services

KONFIDO

KONFIDO is a H2020 project, that aims to leverage proven tools and procedures, as well as novel approaches and cutting-edge technology, in view of creating= a scalable and holistic paradigm for secure inner- and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European levels. The KONFIDO project aims to advance the state-of-the-art of eHealth technology with respect to the four key dimensions of digital security: data preservation, data access and modification, data exchange and interoperability and compliance. KONFIDO's implementation approach is based upon six technology pillars:

1. The new security extensions provided by some of the main CPU vendors;
2. Physical Unclonable Function (PUF)-based security solutions that are based on photonic technologies;
3. Homomorphic encryption mechanisms;
4. Customized extensions of the selected Security Information and Event Management (SIEM) solutions;
5. A set of disruptive logging and auditing mechanisms developed in other technology sectors – such as blockchain – and transferred to the healthcare domain;
6. A customized eIDAS-compliant eID implementation.

Project Representative

John Avramidis (EUL)
john.avramidis@eulambia.com

7

SAINT – Systemic Analyzer In Network Threats

SAINT

SAINT proposes to analyze and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. Analysis of the ecosystems of cybercriminal activity, associated markets and revenues will drive the development of a framework of business models appropriate for the fighting of cybercrime. The role of regulatory approaches as a cost benefit in cybercrime reduction will be explored within a concept of greater collaboration in order to gain optimal attrition of cybercriminal activities. Experimental economics will aid SAINT in designing new methodologies for the development of an ongoing and searchable public database of cybersecurity indicators and open source intelligence. Comparative analysis of cybercrime victims and stakeholders within a framework of qualitative social science methodologies will deliver valuable evidences and advance knowledge on privacy issues and Deep Web practices. Equally, comparative analysis of the failures of current cybersecurity solutions, products and models will underpin a model for greater effectiveness of applications and improved cost-benefits within the information security industry.

Project Representatives

Sotiris Nikoletseas (CTI)
nikole@cti.gr

8

SHIELD – Securing Against Intruders and Other Threats Through a NFV-enabled Environment

SHIELD

SHIELD project proposes a universal solution for dynamically establishing and deploying virtual security infrastructures into ISP and corporate networks. SHIELD builds on the huge momentum of Network Functions Virtualisation (NFV), as currently standardised by ETSI, in order to virtualise security appliances into virtual Network Security Functions (vNSFs), to be instantiated within the network infrastructure using NFV technologies and concepts, effectively monitoring and filtering network traffic in a distributed manner. Logs and metrics from vNSFs are aggregated into an information-driven Data Analysis and Remediation Engine (DARE), which leverages state-of-the-art big data storage and analytics in order to predict specific vulnerabilities and attacks by analysing the network and understanding the adversary possibilities, behaviour and intent.

The SHIELD virtual security infrastructure can either used by the ISP internally for network monitoring and protection, but it can also be offered as-a-service to ISP customers; for this purpose, SHIELD establishes a "vNSF Store", i.e. a repository of available virtual security functions (firewalls, DPIs, content filters etc.) from which the ISP customers can select the ones which best match their needs and deploy them to protect their infrastructure

Project Representative

Georgios Gardikis (SPACE) ggar@space.gr
Kostas Tzoulas (SPACE) ktzoulas@space.gr
Dimitris Katsianis (INCITES) dkats@incites.eu

DOGANA - Advanced Social Engineering And Vulnerability Assessment Framework

9

The advent of Social Networks has made both companies and public bodies tremendously exposed to the so-called Social Engineering 2.0, and thus prone to targeted cyber-attacks. Unfortunately, there is currently no solution available on the market that allows neither the comprehensive assessment of Social Vulnerabilities nor the management and reduction of the associated risk. DOGANA aims to fill this gap by developing a framework that delivers "aDvanced sOcial enGineering And vulNerability Assessment". The underlying concept of DOGANA is that Social Driven Vulnerabilities Assessments (SDVAs), when regularly performed with the help of an efficient framework, help deploy effective mitigation strategies and lead to reducing the risk created by modern Social Engineering 2.0 attack techniques. Two relevant features of the proposed framework are:
- The presence of the "awareness" component within the framework as the cornerstone of the mitigation activities;
- The legal compliance by design of the whole framework, that will be ensured by a partner and a work package explicitly devoted to this task.

Project Representative

Angelo Consoli (SUPSI)
angelo.consoli@supsi.ch

Project Presentations

Time	Project Title
09:00 – 09:10	**ReCRED** – From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control **Project Representative**: **Christos Xenakis** (UPRC) xenakis@unipi.gr
09:10 – 09:20	**FutureTrust** – Future Trust Services for Trustworthy Global Transactions **Project Representative**: **Jon Shamah** (EEMA) jshamah@ejconsultants.eu
09:20 –09:30	**LIGHTEST** – Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes **Project Representative**: **Jon Shamah** (EEMA) jshamah@ejconsultants.eu
09:40 – 09:50	**PaaSword** – A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications **Project Representative**: **Panagiotis Gouvas** (UBITECH) pgouvas@ubitech.eu
09:50 – 10:00	**KONFIDO** - Secure and Trusted Paradigm for Interoperable eHealth Services **Project Representative**: **John Avramidis** (EUL) john.avramidis@eulambia.com
10:00 – 10:10	**SAINT** – Systemic Analyzer In Network Threats **Project Representative(s)**: **Sotiris Nikoletseas** nikole@cti.gr; **Vasileios Vlachos** vsvlachos@gmail.com; **Stamatiou Iwannis** stamatiu@ceid.upatras.gr; **John Bothos** jbothos@iit.demokritos.gr; **Eirini Papadopoulou** ipapadopoulou@iit.demokritos.gr; **Andreas Zalonis** azalonis@iit.demokritos.gr
10:10 – 10:20	**SHIELD** – Securing Against Intruders and Other Threats Through a NFV-enabled Environment **Project Representative**: **Georgios Gardikis** (SPACE) ggar@space.gr
10:20 – 10:30	**DOGANA** - Advanced Social Engineering And Vulnerability Assessment Framework **Project Representative**: **Angelo Consoli** (SUPSI) angelo.consoli@supsi.ch