



European
Commission

Horizon 2020
European Union funding
for research & innovation

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

ReCRED

H2020 Project Clustering Workshop

Athens, 31st of January 2018



H2020 PROJECT CLUSTERING WORKSHOP

About

This workshop is organized by the ReCRED project aiming at establishing tight connections with relative H2020 projects in the field of privacy and security.

H2020 Project Clustering Workshop

**Wednesday 31st of
January 2018,
Athens, Greece**

Venue
NEW Hotel
Filellinon 16, Athens
Greece, 105 57

Organized by
ReCRED Project
www.recred.eu



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

SESSION 1 – Access Control

Time	Project Title	Description
09:00 – 09:20	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
09:20 – 09:40	AMBER – “enhAnced Mobile BiomEtRics”	AMBER (“enhAnced Mobile BiomEtRics”) is a Marie Skłodowska-Curie Innovative Training Network addressing a range of current issues facing biometric solutions on mobile devices. AMBER will comprise ten integrated Marie Skłodowska-Curie Early Stage Researcher (ESR) projects across five EU universities. The Network has the direct support of seven Industrial Partners. The aim of the Network is to collate Europe-wide complementary academic and industrial expertise, train and equip the next generation of researchers to define, investigate and implement solutions, and develop solutions and theory to ensure secure, ubiquitous and efficient authentication whilst protecting privacy of citizens.
		
	Project Representative	Richard Guest (UoK) r.m.guest@kent.ac.uk
09:40 – 10:00	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 be 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
10:00 – 10:20	TYPES – Towards transparentY and Privacy in the onlinE advertising business	The lack of transparency regarding tracking techniques in the online advertising system and the type of information companies collect about users, is creating increasing concerns in society. TYPES is a European project (H2020 program) that aims to cope with this challenge by defining, implementing, and validating in pre-market status a holistic framework of technologies and tools that guarantees both transparency and privacy preservation, gives the end user control upon the amount of information he/she is willing to share, and defines privacy-by-design solutions. In particular, these tools should enable the end user: i) to configure the privacy settings so that only the information allowed by the end-user is collected by online advertising platforms; ii) to understand the flow of their information within the online advertising ecosystem and how it is being used; iii) to detect episodes of information collection occurring without consent and identify the offender; iv) to know the value of their data. TYPES will demonstrate solutions that protect user's privacy while empowering them to control how their data is used by service providers for advertising purposes. At the same time, TYPES will make it easier to verify whether users' online rights are respected and if personal data is exchanged for a reasonable value-added to users.
		
	Project Representative	Vangelis Bagiatis (UPCOM) vbagiatis@upcom.eu

10:20 – 10:40 **PRIVACY FLAG** – Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments



PRIVACY FLAG

Project Representative

The Privacy Flag project is a European research project on personal data protection. Its experts in law and ICT have developed an innovative methodology – the Universal Privacy Risk Area Assessment Methodology (UPRAAM) – to assess the compliance of applications, websites, and Internet of Things deployments with the European Union's General Data Protection Regulation (GDPR) and Swiss Data Protection law. Using the UPRAAM, Privacy Flag is developing a set of tools to enable citizens to check whether their rights as data subjects are being respected, and tools and services to help companies comply with personal data protection requirements. Privacy Flag is co-financed by the European Commission and the Swiss State Secretariat for Education, Research, and Innovation.

Ioannis Chochliouros (OTE)
ichochliouros@oteresearch.gr

10:40 – 11:00

Coffee Break

11:00 – **ARIES** – Reliable European Identity Ecosystem



Project Representative

ARIES will set up a comprehensive framework of technologies, processes and security features for physical and virtual identity management contributing to further establish a European electronic ID ecosystem, trustworthy for the citizens, that supports law enforcement agencies identity management capabilities and addresses the new threats in cybersecurity.

ARIES delivers new ways to enhance electronic document security and identity document management aligned with the Security Union /EU Agenda on Security objectives related to the establishment of clear rules to ensure that data protection principles are respected in full, while law enforcement gains access to the data it needs to protect the privacy of citizens against cybercrime and identity theft.

Jorge Bernal Bernabé (UoM)
jorgebernal@um.es

11:20 – **CREDENTIAL** – Secure Cloud Identity Wallet



Project Representative

CREDENTIAL is an EU funded research project developing, testing and showcasing innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security than other current solutions.

The main idea and ambition of CREDENTIAL is to enable end-to-end security and improved privacy in cloud identity management services for managing secure access control. This is achieved by advancing novel cryptographic technologies and improving strong authentication mechanisms.

Ioannis Chochliouros (OTE)
ichochliouros@oteresearch.gr

SESSION 2 – Trust eServices

Time Project Title

11:40 – 12:00 **FutureTrust** – Future Trust Services for Trustworthy Global Transactions



FutureTrust

Description

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

12:00 – 12:20 **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

12:20 – 12:40 **PaaSword** – A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications



Jon Shamah (EEMA)
ishamah@ejconsultants.eu

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

12:40 – 13:00 **KONFIDO** - Secure and Trusted Paradigm for Interoperable eHealth Services



Panagiotis Gouvas (UBITECH)
pgouvas@ubitech.eu

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

13:00 – 13:20 **PANORAMIX** - Privacy and Accountability in Networks via Optimized Randomized Mix-nets



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

PANORAMIX is an EU H2020 project on privacy innovation aimed at providing privacy via mix-networks (mix-nets). The objective of PANORAMIX is the development of a multipurpose infrastructure for privacy-preserving communications based on mix-nets and its integration into high-value applications that can be exploited by European businesses.

The three applications targeted in the project are e-Voting, privacy-preserving statistics and messaging. Mix-nets protect not only the content of communications from third parties, but also obscure the exact identity of the senders or receivers of messages, through the use of cryptographic relays. Mix-nets are absolutely necessary for implementing strong privacy-preserving systems and protocols.

Project Representative

Aggelos Kiayias (UoE)
akiayias@inf.ed.ac.uk

SESSION 3 – Cyber Security in IoT

Time	Project Title	Description
14:00 – 14:20	GHOST – Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control	<p> The main objective set forth by GHOST is to develop a user-friendly application to improve security and privacy in a Digital Home connected to Internet of Things (IoT), using the most advanced technologies available for this purpose. In this way, Ghost will contribute to boost European IoT home market, bringing next-generation security systems for domestic applications (based on technologies like Blockchain or deep packet inspection) to all users, independently of their previous knowledge. With minimal effort, consumers will become aware and understand the Cybersecurity risks (threats and vulnerabilities), and will take informative decisions affecting their cyber-physical security and privacy. GHOST is supported by the EU Framework Programme for Research and Innovation Horizon 2020 (specifically in the topic DS-02-2016, under Grant Agreement number GA-740923). Ten companies, organizations and universities from six countries are part of the project, led by Televes.</p>
	Project Representative	Miltiadis Dimas (OBR) m.dimas@obrela.com
14:20 – 14:40	FORTIKA - Cyber Security Accelerator for trusted SMEs IT Ecosystems	<p></p> <p>The FORTIKA project aims to provide SMEs with an embedded, smart and robust hardware security layer enhanced with an adaptive security service management ecosystem (FORTIKA marketplace). The project will explore the capabilities of the secure-by-design FPGA SoC platform, as a CPU enhancement module. The long-term goal of the FORTIKA project is to provide a low-cost, dynamic, security layer for small and medium-sized businesses, individually tailored to meet each beneficiary's requirements.</p>
	Project Representative	Nikolaos Zotos (FINT) nzotos@f-in.co.uk
14:40 – 15:00	ANASTACIA - Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures	<p></p> <p>The main objective of the ANASTACIA project is to address cyber-security concerns by researching, developing and demonstrating a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and Cloud architectures. ANASTACIA will develop a trustworthy-by-design security framework which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools.</p>
	Project Representative	Panagiotis Gouvas (UBITECH) pgouvas@ubitech.eu
15:00 – 15:20	CIPSEC – Enhancing Critical Infrastructure Protection with innovative SECurity framework	<p></p> <p>The main aim of CIPSEC is to create a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology) and OT (operational technology) departments of CIs. As part of this framework CIPSEC will offer a complete security ecosystem of additional services that can support the proposed technical solutions to work reliably and at professional quality. These services include vulnerability tests and recommendations, key personnel training courses, public-private partnerships (PPPs) forensics analysis, standardization and protection against cascading effects. All solutions and services will be validated in three pilots performed in three different CI environments (transportation, health, and environment). CIPSEC will also develop a marketing strategy for optimal positioning of its solutions in the CI security market.</p>
	Project Representative	Ilias Spais (AEGIS) hspais@aegisresearch.eu
15:20 – 15:40	ARMOUR – Large-Scale IoT Security & Trust Experiments	<p>The ARMOUR is a European project (H2020 program) that aims to address Security and Trust issues on Internet of Things by providing duly tested, benchmarked and certified Security & Trust technological solutions for large-scale IoT using upgraded FIRE large-scale IoT/Cloud testbeds properly-equipped for Security & Trust experimentations. ARMOUR identified 3 goals that define the approach being used to achieve the proposed Security and Trust solutions:</p> <ul style="list-style-type: none"> • Enhance two outstanding FIRE testbeds with the ARMOUR experimentation toolbox for enabling large-scale IoT Security & Trust experiments;



ARMOUR

Project Representative

15:40 – 16:00 **EUSEC** - European Security Certification Framework



Elizabeta Fournieret (ST)
elizabeta.fournieret@smartesting.com
Panos Karkazis (SYN)
pkarkazis@synelixis.com

The European Security Certification Framework (EU-SEC) strives to address the security, privacy and transparency challenges associated with the greater externalization of IT to Cloud services. EU-SEC will create a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud. It will be tested and validated in pilots involving industrial partners.

Alain Pannetra (CSA)
apannetra@cloudsecurityalliance.org

16:00 – 16:20

Coffee Break

SESSION 4 – Cyber Security in Social Networks

Time	Project Title
16:20 – 16:40	DOGANA - aDvanced sOcial enGineering And vulNerability Assement Framework



ADVANCED SOCIAL ENGINEERING AND VULNERABILITY ASSESSMENT FRAMEWORK

Description

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

16:40 – 17:00 **ENCASE** – EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors



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

The overall aim of the ENCASE project is to leverage the latest advances in usable security and privacy of minors (age 10-18) in order to design and implement a user-centric architecture for the protection of minors from malicious actors in Online Social Networks (OSNs). In order to identify the magnitude of the problem, ENCASE surveys the existing security and privacy enhancing web-based tools and performs research based on the state-of-art cyber security risks and on security in OSNs. Moreover, the project investigates the problem by collecting data from various OSNs. ENCASE aims to design and implement a platform that will be able to protect minors and inform their parents when their children are exposed to the following threats in OSNs:

1. Malicious behaviour, cyberbullying, and sexual grooming
2. False information dissemination, and fake identity and activity
3. Sensitive and nudity content

The architecture comprises three browser add-ons, an intelligent web-proxy service that will be responsible to detect malicious behaviour, fake identities and activity, and sensitive content in OSNs based on sophisticated machine learning detection rules generated by a data analytics software stack, which is the back-end of the architecture.

Project Representative

Michael Sirivianos (CUT)
michael.sirivianos@gmail.com

SESSION 5 – Cyber Security in H2020

Time	Project Title	Description
17:00 – 17:30	cyberwatching.eu – The European watch on cybersecurity privacy	<p>Over the next 48 months, this Observatory will become THE European hub for Cybersecurity and Privacy. We will monitor R&I initiatives throughout EU & Associated Countries while supporting European stakeholders in playing an active role in shaping the global cybersecurity & privacy landscape.</p> <p>Through a combination of clustering activities and Technical and Market Readiness Level Workshops, we will monitor the whole lifecycle from research development and implementation, to validation and market uptake, making it possible for stakeholders to increase their knowledge, raise their awareness and find possible synergies between different initiatives.</p>

Project Representative

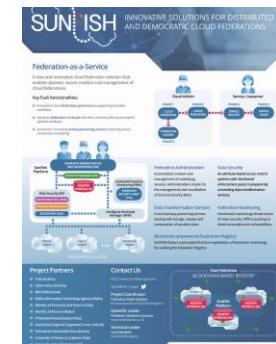
Niccolò Zazzeri (TIT)
n.zazzeri@trust-itservices.com

Poster Session

SUNFISH - SecUre iNformation SHaring in federated heterogeneous private clouds



SUNFISH offers a service to federate private and public clouds, enabling them to exchange data and services in a secure and controlled manner, based on a “democratic” governance model: no federation member rules on others. More in details, SUNFISH conceives designs and implements Federation-as-a-Service (FaaS), a secure-by-design cloud interoperability solution based on blockchain technology. This service is realised via a software platform, named “SUNFISH Platform”, whose forming components represent essential parts of the overall functioning. The SUNFISH Platform is a modular software solution that enables the dynamic and secure creation of cloud federations and their management. Its main functionalities are: a) Dynamic cloud management; b) Democratic governance; c) Data security. The SUNFISH project has developed three concrete deployment examples, through three different use cases



mF2C – Towards an Open, Secure, Decentralized and Coordinated Fog-to-Cloud Management Ecosystem



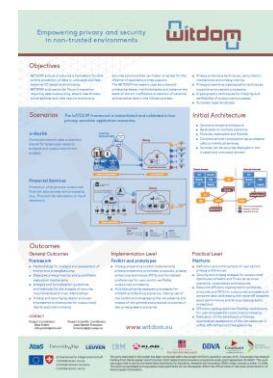
The mF2C sets the goal of designing an open, secure, decentralized, multi-stakeholder management framework, including novel programming models, privacy and security, data storage techniques, service creation, brokerage solutions, SLA policies, and resource orchestration methods. The proposed framework is expected to set the foundations for a novel distributed system architecture, developing a proof-of-concept system and platform, to be tested and validated in real-world use cases, as envisioned by the industrial partners in the consortium with significant interest in rapid innovation in the cloud computing sector.



WITDOM – Empowering Privacy and Security in Non-Trusted Environments



WITDOM is an EU Horizon 2020 funded research project with a duration of 36 months, which started in January 2015. WITDOM focuses on developing innovative solutions for truly efficient and practical privacy enhancing techniques and efficient signal and data processing in the encrypted domain for the increasingly demanded outsourced environments. Actually, the main target WITDOM pursues is to produce a framework for end-to-end protection of data in untrusted and fast evolving ICT-based environments, with a particular focus in data-outsourcing scenarios, where new threats, vulnerabilities and risks due to new uses require end-to-end security solutions that will withstand progress for the lifetime of applications they support.



YAKSHA - Cybersecurity Awareness and Knowledge Systemic High-level Application



YAKSHA aims at reinforcing EU-ASEAN cooperation & building partnerships in the cybersecurity domain by developing a solution tailored to specific user and national needs, leveraging EU Know-How and local expertise. YAKSHA will develop and introduce the innovative concept of honeypots-as-a-service which will greatly enhance the process of gathering threat intelligence. It will enhance cybersecurity readiness levels for end users, help prevent cyber-attacks, mitigate cyber risks and better govern the whole cybersecurity process. YAKSHA is ideally positioned to secure global manufacturing supply chains, given its planned focus on IoT Security. YAKSHA will develop innovative methods for malware detection, collection and analysis, as well as design a specialised ontology to be used for long-term storage and analysis of the information, and deploy standard information formats and interfaces to facilitate interoperability. The YAKSHA software solution will be validated in real-world pilot projects in both regions, focusing on Vietnam & Greece, but with plans to expand the deployments to other countries.