ReCRED

H2020 Project Clustering Workshop

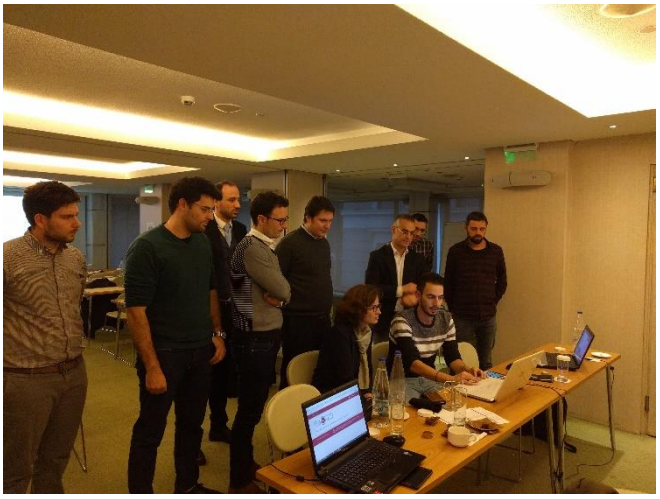
BRUSSELS 2018

IN THIS ISSUE

H2020 Project Clustering Workshop

During our plenary meeting in Athens, on January the 31st, 2018, the ReCRED project organized an H2020 project clustering workshop that brought together more than 25 EU funded project in the domain of cybersecurity. Insightful comments for all the participating projects were made and valuable feedback was received regarding their activities so far.

The opening speech was made by Susanne Butscher, a senior officer in the United Nations High Commissioner for Refugees' (UNHCR's) Identity Management and Registration section, working with a team of professionals on digital identity matters with regards to refugees.

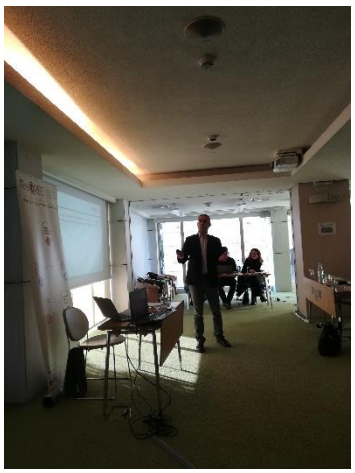


All pilots deployed within ReCRED's framework were showcased in real time and fully operational environment showcasing the reliability of the platform and the high reliability of the proposed application. Technical details regarding the platform architecture were showed to other project representatives that highlighted the reliability of our developed solution and the applicability of the solution in many important everyday domains.

The #H2020PCW event had huge impact in the European community that deals with cybersecurity threats and attacks earning more than 80.000 social media engagements from people around the world. During our next plenary meeting we are planning of hosting the same event but this time demo exhibitions will be made by the participating projects to a wider audience of influencers in the specific domain highlighting the importance of such activities and showing in practice the efficient collaboration between projects and people working for them.

For more information regarding the event visit our website https://www.recred.eu/basic-page/169/synergies where you can find out more about each project that participated in the event and take a close look at the presentations made by each project representative. Many details are also in our social media, Facebook https://www.facebook.com/ReCREDH2020/ and Twitter https://twitter.com/ReCRED_H2020 . A video of the event can also be found at our YouTube channel https://www.youtube.com/channel/UClVzn8b6g_vE3dxzV1sliog

Christos Xenakis from UPRC showed the ReCRED video and described the innovative solutions developed within the project based on real life problems.



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. www.recred.eu

Vangelis Bagiatis from UPCOM described how the project tackles the lack of transparency regarding tracking techniques focusing on how they have raised raising users' awareness, monitor the data collection and thus safeguard their privacy.



Towards transparencY and Privacy in the onlinE advertising business

TYPES demonstrated solutions that protect individuals' privacy while empowering the users to control how their data is used by service providers for advertising purposes. At the same time, TYPES made it easier to verify whether users' online rights are respected and if personal data is exchanged for a reasonable value-added to users. The project has received funding from the European Union's Horizon 2020 Research and Innovation Programme. It was launched in May 2015 and was scheduled to run for 30 months. Its main mission was to define, implement and validate in pre-market status a holistic framework of technologies and tools that guarantees both transparency and privacy preservation by giving the end user control upon the information he/she is willing to share.

Richard Guest from University of Kent described the objectives of this Marie Curie Innovation Training Network pointing out the collaboration between experts from universities and industries across Europe to address the issues related to biometrics on mobile devices. They have already identified some issues regarding usability and reliability, vulnerability, continuous vs. instantaneous authentication, privacy and data protection.



enhAnced Mobile BiomEtRics

AMBER 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.

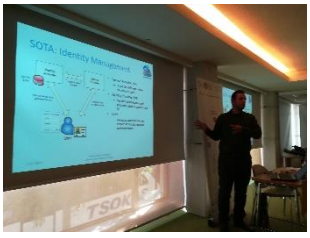
Constantinos Patsakis from UPRC pointed out the main issues related to privacy from end-users' point of view. He described the design concept and the G2C and B2C scenarios. The privacy enforcement framework presented, aims to raise the users' awareness towards the use of data, and it allows users to define privacy settings when they use web services.



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.

Alexandros Kostopoulos from OTE presented the CREDENTIAL project and highlighted the use of a cloud wallet, one of the innovations of the traditional ecosystem of identity management. In addition, he showcased the functionalities developed within the project's framework for both the end-users and the service providers together with the physical architecture and its main components.


Secure Cloud Identity Wallet

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.

Jorge Bernal Bernabé from University of Murcia gave a presentation about the reliable identity ecosystem developed within ARIES' framework, by taking advantage of technologies to ensure high levels of secure credentials.



Reliable European Identity Ecosystem

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.

Alexandros Kostopoulos from OTE described the main advantages of the project that aims to empower the users to set desired level of privacy, monitor and control their privacy. In addition, he showcased a global knowledge database on privacy risks, and the use of crowdsourcing to provide feedback from users.



PRIVACY FLAG

Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments

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 GDPRand 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.

Jon Shamah from EEMA, presented the project's global vision to develop open source components and services complementing the eIDAS ecosystem and to integrate the eIDAS with other trust services worldwide.


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 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.

John Avramidis from EULAMBIA presented the developed solutions for addressing security issues related to storage, processing, dissemination and presentation of e-health data through interoperable services.



KONFIDO

Secure and Trusted Paradigm for Interoperable eHealth Services

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.

Giannis Ledakis from UBITECH showcased the developed solution for cloud security that address security and privacy in a holistic way.



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

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.

Jon Shamah from EEMA, pointed out the trust-related factors that act as barriers for transactions in commerce and presented how the project builds trust transparency by using standard way of publishing trust lists, schemes and formats all over a global trust infrastructure.



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.

Alain Pannetrat from Cloud Security Alliance described the tools and the architecture for multiparty recognition of cloud security certification and continuous auditing-based certification.


European Security Certification Framework

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.

Miltiadis Dimas from OBRELA demonstrate through his presentation the developed application that aims improves significantly the security aspect of a digital connected home.



Safe-Guarding Home IoT Environments with Personalized Real-time Risk Control

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.

Konstantinos Votis from CERTH presented the solutions developed for tackling cybersecurity issues in SMEs and the corresponding financial damages due to these attacks.

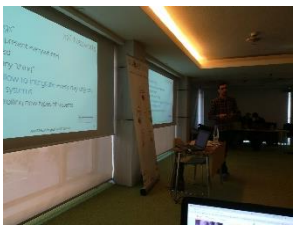


Cyber Security Accelerator for trusted SMEs IT Ecosystems

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.

Giannis Ledakis from UBITECH showcased the innovative solutions developed within the project in order to overcome cybersecurity issues in IoT and the connected devices.





Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures

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.

Ilias Spais from AEGIS presented the unified security framework for the protection of critical infrastructures and enlisted all the services that ensure reliability and quality for end-users.



Enhancing Critical Infrastructure Protection with innovative SECurity framework

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.

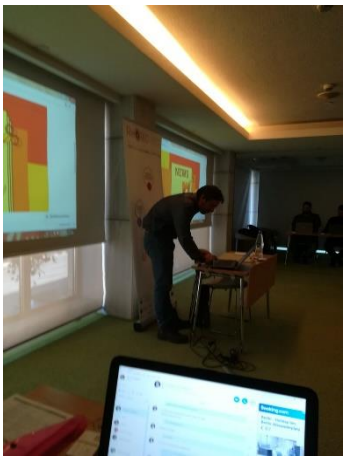
Elizabeta Fourneret from SmarTesting presented one of the outcomes of the project namely the model-based security testing framework that enables IoT labelling and certification



Large-Scale IoT Security & Trust Experiments

The ARMOUR is a European project 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. 1. Enhance two outstanding FIRE testbeds with the ARMOUR experimentation toolbox for enabling large-scale IoT Security & Trust experiments; 2. Deliver six properly experimented, suitably validated and duly benchmarked methods and technologies for enabling Security & Trust in the large-scale IoT; 3. Define a framework to support the design of Secure & Trusted IoT applications as well as establishing a certification scheme for setting confidence on Security & Trust IoT solutions.

Panos Lourodas from GRNET introduced us to the Mix-Net concepts and how they can be used to provide privacy in e-voting, statistics and messaging.



Privacy and Accountability in Networks via Optimized Randomized Mix-nets

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.

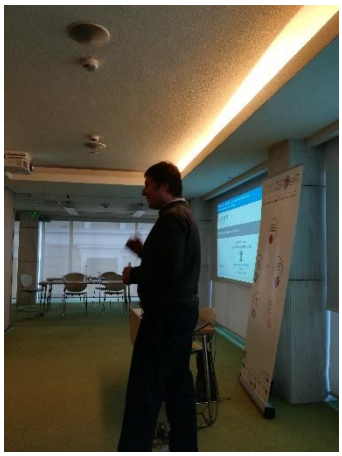
Angelo Consoli from University of Applied Sciences and Arts of Italian Switzerland talked about the framework and the toolsets used to assess the risks within companies and the proposed awareness measures in order to make people more resilient.

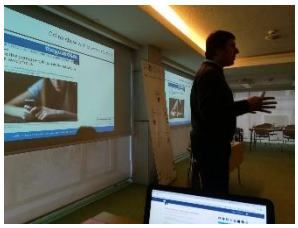


aDvanced sOcial enGineering And vulNerability Assesment Framework

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, 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.

Michael Sirivianos from Cyprus University of Technology showcased how the project aims at protecting the minors in social networks.





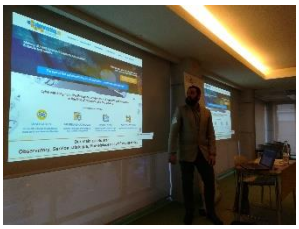
EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors

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.

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.

Niccolò Zazzeri from Trust Services IT gave a presentation demonstrating all the features and services of the developed cybersecurity observatory.





The European watch on cybersecurity privacy

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. 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.

ReCRED in a nutshell

ReCRED's ultimate goal is to promote the user's personal mobile device to the role of a unified authentication and authorization proxy towards the digital world. ReCRED adopts an incre mentally deployable strategy in two complementary directions: extensibility in the type and nature of supported stakeholders and services (from local access control to online service access), as well as flexibility and extensibility in the set of supported authentication and access control techniques; from widely established and traditional ones to emerging authentication and authorization protocols as well as cryptographically advanced attribute-based access control approaches. Simplicity, usability, and users privacy is accomplished by:

i. hiding inside the device all the complexity involved in the aggregation and management of multiple digital identifiers and access control attribute credentials, as well as the relevant interaction with the network infrastructure and with identity consolidation services;

ii. integrating in the device support for widespread identity management standards and their necessary extensions; and

iii. controlling the exposure of user credentials to third party service providers. ReCRED addresses key security and privacy issues such as resilience to device loss, theft and impersonation, via a combination of:

   1. local user-to-device and remote device-to-service secure authentication mechanisms;
   2. multi-factor authentication mechanisms based on behavioral and physiological user signatures not bound to the device;
   3. usable identity management and privacy awareness tools;

iv. usable tools that offer the ability for complex reasoning of authorization policies through advanced learning techniques. ReCRED's viability will be assessed via four large-scale realistic pilots in real-world operational environments. The pilots will demonstrate the integration of the developed components and their suitability for end-users, so as to show their TRL7 readiness.

ReCRED Consortium

UNIVERSITY OF PIRAEUS

Cyprus University of Technology

cnit

institute imdea networks

THE PRODUCTIZERS

verizon

certSIGN

wedia

upcom Bringing business and IT together

EXUS

Telefónica Telefónica I+D

BAKER & MCKENZIE