European Commission

High level Conference on the

EU Cybersecurity Strategy

Project Exhibition Overview

Contents:

1. ABC4Trust - Attribute-based Credentials for Trust

The ABC4Trust research project enables secure login procedures on basis of the data protection principle of data minimisation. The solutions allow the users to reveal only the information necessary for a specific transaction while preserving the trust chain to the issuer of the eID. For scenarios with misuse potential the inspection procedure could be activated transparently and evident to the users prior to login, allowing later the identification of fraudulent users. Core of the ABC4Trust project are the two application pilots which are both on display at this conference. The Swedish school pilot deploys Privacy-ABCs for a communication network within a school. The Greek university pilot uses Privacy-ABCs to allow students anonymous evaluation of lectures.

For further information visit https://abc4trust.eu

2. ACDC

ACDC is a pilot project running from 02/ 2013 to 07/2015 whose aim is to set up a European Advanced Cyber Defence Centre to fight botnets. With 28 partners from 14 countries, ACDC sets up a central data clearing house, open to inputs from ISPs, CERTs and all organisations monitoring attacks across Europe, provides a complete set of solutions accessible online for mitigating on-going attacks, creates national support centres across 8 Member States, fosters extensive sharing of information across Member States to improve the early detection of botnets and creates an open community, a unique opportunity to share information across ISPs, ICT providers, researchers, users, law enforcement organisations etc. Through its networked approach, ACDC paves the way for a consolidated approach to protect organisations from cyber-threats and support mitigation of on-going attacks through easy access to an increasing pool of solutions.

For further information visit www.acdc-project.eu

3. ASPIRE

The core objective of the ASPIRE project is to develop an integrated software security framework that allows developers to add effective software protection to applications automatically. The goal is to establish trustworthy execution of software on mobile client devices that lack generic and open security hardware elements to be exploited, but that have a (persistent or occasional) network connection to a trusted entity at their disposal. We want mobile software security to become trustworthy by leveraging the available network connection and a layered security approach; measurable by developing practical metrics based on validated attack and protection models; cheaper by integrating support into an industrial-strength ASPIRE Framework; more valuable by enabling shorter time-to-markets; more productive by being more widely applicable.

4. ATTPS - Achieving the Trust Paradigm Shift

Trust is an essential prerequisite for connecting people in effective transactions. It builds into the society on elements like security, privacy, transparency, accountability and reputation. European strategy must aim at a strong competitive position in producing trustworthy ICT that bring new attractive ways of living and working that are perceived as trustworthy. ATTPS addresses four pillars,

which include business, legal, social and technical challenges. The paradigm shift requires an environment that enhances simplicity for providers, citizens and government to experiment with solutions that provide trust in real life settings. It will trigger public debates and identify bottlenecks and leads to a balance between trustworthy ICT offered against affordable prices and ICT that is congruent with public expectation of trustworthiness and the generally accepted principles of privacy. ATTPS supports TDL to implement this environment that will be used as public trust platform.

For further information visit: www.trustindigitallife.eu/

5. AU2EU

AU2EU is an EU-funded collaborative research and development project. The project brings together a strong collaboration of leading industry and research organizations from Europe and Australia, determined to increase trust, security and privacy. The project aims at fostering the adoption of security and privacy-by-design technologies in European and global markets. The project will contribute to increased trust, security and privacy, which in turn shall lead to increased adoption of (cloud-based) critical infrastructures and collaborative delivery of services dealing with sensitive data. Central to the AU2EU project is the implementation and demonstration, in a real-life environment an integrated e-Authentication and e-Authorization framework. Two pilots are executed to demonstrate feasibility of our approach for two of the use cases, i.e. for the bio-security incident response use case in Australia and the collaborative services for eHealth and Ambient Assisted Living (AAL) use case in Europe.

For further information visit http://www.au2eu.eu/

6. B-CCENTRE

The Belgian Cybercrime Centre of Excellence for Training, Research and Education is Belgium's central coordination, collaboration and knowledge sharing platform in the fight against cybercrime. Bundling the expertise & forces of several academic research groups, public sector bodies and businesses in Belgium and beyond, the B-CCENTRE coordinates interdisciplinary research on specific cybercrime, cybersecurity & cyberforensics related topics (fundamental & applied research), the development and teaching of basic and advanced trainings for actors involved in the fight against cybercrime from different backgrounds and the organisation of seminars, conferences and awareness raising initiatives for different target audiences. B-CCENTRE is the Belgian node in the European network of Cybercrime Centres of Excellence and collaborates with the main European and international organisations dealing with cybercrime.

For further information visit: www.b-ccentre.be

7. CAPITAL

CAPITAL has been built around two pillars: coordinate European R&D efforts in the cyber security domain and jointly address research and innovation within an Integrated Research & Innovation Agenda. The project will therefore cover two sub-bullets of the call objective. CAPITAL complements the CYSPA project started on October 2012, also coordinated by EOS which aims at defining an overall strategy and creating a community of solution providers, Researchers and end-users to enhance the industrial community to protect itself from cyber-disruptions and support the European elaboration of regulations to enhance the overall protection level.

For further information visit: http://www.eos-eu.com/?page=capital

8. CUMULUS

CUMULUS contributes to cloud technology acceptance by developing an integrated framework of models, processes and tools supporting the certification of security properties of infrastructure (IaaS), platform (PaaS) and software application layer (SaaS) services in cloud. It will define specific cloud service certification models and mechanisms based on evidence coming from service testing results, service monitoring data and trusted computing platform proofs. CUMULUS will also define advanced certification models and mechanisms: to manage security relevant changes at any layer in the cloud stack, so avoiding, as much as possible, to restart each time a cloud service certification from scratch (incremental certification) and to combine in a certificate different types of evidence and certificate (hybrid certification).

For further information visit: http://cumulus-project.eu

9. CYSPA

CYSPA, the European Cyber Security Protection Alliance, is an Alliance of organisations working together to improve protection against cyber disruptions. CYSPA focuses on a sector-by-sector approach to evaluate the impact of cyber risks and to create a community of stakeholders interested in sharing knowledge to improve their level of cyber protection. CYSPA promotes a benefits oriented approach. For providers, benefits include faster time to market for innovative cyber security capabilities. For users, a tailored approach better focused on individual needs. For public authorities, an increased understanding of cyber risks that limit e-government services. The CYSPA Alliance will launch in 2014.

For further information visit: www.cyspa.eu

10. FIRE

FIRE is a collaboration between leading clusters and associations of Information Security companies in Spain, United Kingdom, Germany, Belgium, Czech Republic and Estonia, covering six major parts of Europe. The objective of FIRE is to improve the European industrial competitiveness in markets of trustworthy ICT, by taking into account of the needs of the Security industry in this domain building, on the unique combination of the international participant clusters in information security technologies. The gap between the IT security industry roadmaps and the research activities performed in institutes and academia is currently too wide. FIRE aims to reduce this gap.

For further information visit: www.trustworthyictonfire.com

11. FutureID

The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims. Users of FutureID will benefit from the availability of a ubiquitously usable open source eID client that runs on desktop PCs, tablets and smart phones. Application and service providers will easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments. FutureID will develop

two pilot applications and is open for additional application services who want to use the innovative FutureID technology

For further information visit: www.futureid.eu

12. HINT

For ICT systems with high security requirements, there are growing concerns about counterfeiting or cloning of hardware components and the threat of “Hardware Trojans” or hidden functions in Integrated Circuits. The HINT project addresses these challenges with novel technologies to guarantee that a hardware system is a genuine and non-modified one. The use of authentication schemes based on Physically Unclonable Functions and the detection of Hardware Trojans by Side Channel Analysis shall enable integrated checks of the global integrity for a given system. The project considers two industry-driven application scenarios, a Professional Mobile Radio scenario and an application aiming at an “unclonable” ID card.

For further information visit: www.hint-project.eu/

13. INTER-TRUST

INTER-TRUST's main objective is to support trustworthy applications in heterogeneous networks and devices, developing a new software framework for the enforcement of interoperable and changing security policies. Heterogeneous networks of pervasive ICT devices and services are a key infrastructure for the organisation of modern society, and trust and security are crucial requirements within today’s world. The end-users of INTER-TRUST are the developers, integrators and operators of systems that have to comply with strong security requirements. The INTER-TRUST framework will allow managing, enforcing and negotiating changing security policies, support the verification of the required security level and activate contingency actions

For further information visit: www.inter-trust.lcc.uma.es

14. IPaCSO

IPaCSO is a project and a private consortium by industry representatives and researchers aimed at supporting Privacy and Cyber Security innovations in Europe. Its aim is to support the ICT Security innovators with State of the Art innovation methodologies and best practices in their innovation process. By adapting existing methodologies available in other industries and optimizing the models for the ICT Security and Trustworthy ICT domain, (more particular for cyber security and privacy) and by applying domain specific methods, innovators should be able to obtain a model that can help them in their process. The result is that innovators will be able to find their road to market faster, more effective and more efficient.

For further information visit: www.ipacso.eu

15. MUSES

MUSES will foster corporate security by reducing the risks introduced by user behaviour, taking into account the corporate, technical, legal, social and economic contexts in which their work is done.

For further information visit: www.musesproject.eu

16. NEMESYS

Mobile devices are a key ICT infrastructure for all of our social and economic needs. It is therefore becoming increasingly the object of cyber and network threats and attacks. The EU FP7 project NEMESYS focuses on these threats through a novel security framework for gathering and analysing information about cyber-attacks targeting mobile devices and the core network, for identifying and predicting abnormal behaviours, and taking appropriate countermeasures to understand and block their effect. NEMESYS also aims to understand cyber-criminal operations, and reveal the possible shifts in their attacks on mobile devices through root cause analysis and correlation with known patterns of attack on networks.

For further information visit: www.nemesys-project.eu

17. NESSOS

The Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS) aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. The NESSoS engineering of secure software services is based on the principle of addressing security concerns from the very beginning in system analysis and design, thus contributing to reduce the amount of system and service vulnerabilities and enabling the systematic treatment of security needs through the engineering process. In light of the unique security requirements the Future Internet will expose, new results will be achieved by means of an integrated research, as to improve the necessary assurance level and to address risk and cost during the software development cycle in order to prioritize and manage investments.

For further information visit: http://www.nessos-project.eu

18. PCAS

PCAS aims at providing an innovative, trustworthy, handheld device. The Secured Personal Device (SPD) will allow users to securely store their data, to share it with trusted applications, and to easily and securely authenticate him. The SPD will recognize its user using multiple biometric sensors, including a stress level sensor to detect coercion. Using the same biometric authentication, the SPD will be able to enforce secure communication with servers in the cloud, relieving the user from memorizing passwords. The SPD will take the form of a smartphone add-on that draws power from the smartphone and uses its communication services.

For further information visit: http://www.pcas-project.eu/

19. RASEN

RASEN is a European research project addressing risk assessment, legal compliance, and testing within cyber security. The RASEN project takes the position that cyber security must be understood not just at a technical level, but also at a non-technical level, taking into account the context in which software is used, organizational level assets, and legal issues. The RASEN project will develop a method and a tool box in which risk is used as a basis for communication and decision making, not only within, but across organizational levels.

For further information visit: www.rasenproject.eu.

20. SecCord - CSP Forum

The Cyber Security & Privacy (CSP) Forum (funded via SecCord EU FP7 project), actively coordinates the clustering of the funded EU FP7 trust and security research projects , promoting collaboration, dissemination and networking. CSP Forum through its clustering activities supports enhanced Collaborative Trust and Security Networking, extends the community building and collaborative activities to link with national Trust and security RTD activities, analyses trust & security research results and outputs, supports Impact and dissemination of research results and works to identify trust and security strategic directions.

For further information visit: https://www.cspforum.eu

21. SecFuNet

The goal of the joint EU-Brazil SecFuNet project is to design and develop a coherent security architecture for virtual networks and cloud accesses. The proposed architecture will provide solutions allowing the management of the security of communications for all machines connected to a public cloud using virtual networks.

For further information visit: http://www.secfunet.eu/

22. SECURED

SECURED enables a cybersecurity scenario where end-user protection is uniform and independent of the network connection and terminal she actually uses. This is achieved by off-loading security applications from end-user devices to a secure, trusted and programmable network edge device, the NED, which executes on-demand security applications, configured according to the connected users and their security policies. Use cases include home Internet access, corporate environments, mobile connectivity and Internet-of-Things, with various flavours of NED. SECURED foresees the creation of repositories and marketplaces (for policies and applications) and enables new business models for network service providers and security developers.

For further information visit: http://www.secured-fp7.eu

23. STANCE

The immunity of a system to malicious third parties trying to modify its behaviour (e.g. to perform unauthorized actions) is called security. Ensuring this feature in information and communication technologies is a requirement for establishing a trustworthy Information Society. Several strategies can be explored to deal with this problem. One of them, called program analysis, relies on formal techniques to semi-automatically detect unintended behaviours in software systems. This approach allows the verification and secure exploitation of legacy and commercial-off-the-shelf components. Yet in the domain of security, program analysis techniques are still in infancy. The objective of STANCE is to drive scientific and technological breakthroughs in the domain of software security.

For further information visit: http://www.stance-project.eu/

24. SysSec

SysSec is a Network of Excellence focusing on identifying threats and vulnerabilities for the Future Internet. SysSec coordinates Research and promotes Education in the area of Systems Security in Europe. Over the past few years SysSec has managed to engage more than 100 stakeholders in what is known as a distributed think-tank that has resulted in the "Red Book of Systems Security": a distillation of emerging threats and Grand Challenge problems in the area of Systems Security.

For further information visit: http://www.syssec-project.eu

25. TRESCCA

The TRESCCA project - TRustworthy Embedded Systems for Secure Cloud Computing Applications aims to lay the foundations of a secure and trustable cloud platform by ensuring strong logical and physical security on the edge devices. It will propose and demonstrate hardware/software solutions allowing stakeholders to delegate the processing of their sensitive data to the cloud, opening up whole new field of cloud services and applications. Protecting the system against logical adversaries will rely of virtualization techniques while board-level physical attacks will be prevented by input - outputs encryption and integrity checking.

For further information visit: http://www.trescca.eu/

26. Trust in Digital Life

The Trust in Digital Life (TDL) community, formed by leading industry partners and institutes, considers trust as a priority prerequisite. Trustworthy ICT solutions must become a commodity enforced by citizens and law. The Trust in Digital Life community has capabilities to resolve the issues and will research, pilot and promote innovative trustworthy ICT environments and technologies. TDL community encourages the industry to develop innovative information and communication technologies, enabling consumers and enterprises to judge for themselves if their devices, applications and services are trustworthy enough to protect them from internet threats. Industry has the ambition to provide these technologies for an affordable price to the market.

For further information visit www.trustindigitallife.eu

27. UCD CCI

UCD Centred for Cybersecurity & Cybercrime Investigation has worked closely with EU Law Enforcement since the late 1990's, and have coordinated three DGHOME funded projects, and partnered in a further eight. Recent projects have included Cybercrime Investigation – Developing and Disseminating an Accredited International Training Programme for the Future, 2Centre – Cybercrime Centres of Excellence Network for Training Research & Education and FREETOOL, the development of free or low-cost forensic software tools for the Law Enforcement cybercrime community.

For further information visit: http://www.ucd.ie/cci