TRUST IN THE DIGITAL WORLD 2015

Trusting Big Data

Driving new business without compromising privacy

Executive Summary

25-26 February 2015
Madrid, Spain

EEMA and Trust in Digital Life Present

Trust in the Digital World 2015

Trusting Big Data – Driving new business without compromising privacy

25 - 26 February in Madrid

Conference Highlights

PowerPoint presentations available for download from www.eema.org

Opening Plenary Session

Trusting Big Data - Keynotes

Paul Wang, CTO Global Safety Division, NEC
Jakub Boratynski, Head of Unit Trust and Security, European Commission
Richard Benjamins, Group Director Business Intelligence & Big Data, Telefónica DG
Miguel Iribarren, Director of Cyberintelligence and Information, INDRA

CTO Global Safety Division at NEC Corporation, **Dr Paul Wang** opened Trust in the Digital World 2015 by talking about big data in the context of safe cities, making the observation that trust in the digital and the physical world is coming together.

He explained the challenges of inter-agency data sharing and how this has been achieved in Singapore, with the benefit of faster incident response times and reduced operating costs. For example, surveillance cameras used by the transport authority for traffic management can also be used by other departments to monitor the cleanliness of the streets.

Dr Wang observed the importance of building inter-agency trust in both digital assets (such as surveillance cameras and sensors) as well as digital access to the data. He advised that privacy is an important consideration and that there must be strong access control to data, so that only those with the right permissions are entitled to access what they need.

Big data tells stories commented Group Director Business Intelligence & Big Data at Telefónica DG, **Richard Benjamins**, in his opening address, during which he shared examples of how it is being used creatively, from monitoring the performance of football players during a match, through to 'pay-as-you-drive' initiatives that helps to reduce vehicle insurance for young drivers. He talked about how businesses can take advantage of big data insights, using crowd analytics, whereby mobile devices are 'tracked' in a city giving private and public organisations, access to usable insight regarding where people congregate and when, along with relevant demographic data.

Dr Benjamins also raised the issue of privacy with a quote from 2012 that said "We are living on a privacy time-bomb", before observing that we are now in 2015 and it is yet to explode. He noted that today people are largely unaware of what is going on with their data. However, we are moving to a tomorrow

where consumers will be willing to 'trade-up' and share their data in exchange for services. Finally, he gave a glimpse in to a future in which consumers want organisations to use their data to help improve their lives. He concluded by highlighting the issues of opt-in and opt-out, aggregated and anonymised data, warning that there needs to be an understanding as to what can legally be done with such information, and how companies must be transparent in what data they have and how they are using it.

Head of Unit Trust and Security at the European Commission, **Jakub Boratynski**, began with an overview of what the European Commission means by cybersecurity: 'Cybersecurity is the protection of networks and information systems against human mistakes, natural disasters, technical failures, or malicious attacks.'

Mr Boratynski explained how events in the digital world can have a profound effect in the real world and real life, before warning that we are dealing with a lot of unknowns…

- Who is behind it?
- Is it malicious or not?
- When will the attack come? (All we know is that attacks will happen)

He argued that when it comes to dealing with cybersecurity we are in the equivalent of the 1920s, adding that cybersecurity will never be fully eliminated and it will never be fully solved.

Mr Boratynski discussed proposals for a directive on Network and Information Security (NIS), which it is hoped will be adopted by summer 2015. It aims to make the European Union the leader in cybersecurity, through cooperation and adoption across all member states. He advised that NIS is a major opportunity to nurture more public and private sector cooperation, bringing new market opportunities for cybersecurity products and solutions.

The Director of Cyber Intelligence and Information at INDRA, **Miguel Iribarren**, talked about the challenges in working with structured and unstructured big data, as well as the scale of the information that is being created. He presented a forecast that predicted a Geopybyte of data in existence by 2025. He explained that whilst structured data is still valid, it is taking unstructured data, creating structure from it and in turn creating knowledge and intelligence that is the big issue

top

Industry and Project Demonstrations

Collaborative Mobile Honeypot Ecosystem, Shankar Karuppayah, Doctoral Researcher, CASED/TU Darmstadt
TrustSeed: legal proof eSignature with probative values and strong authentication.
FI-WARE Security Monitoring Generic Enabler Demonstrator, Pascal Bisson, Thales Communications & Security
OPTET (Operational Trustworthiness Enabling Technologies) Sébastian Keller, Thales Communications & Security
n-Auth: Usable, secure and private authentication, Jens Hermans, KU Leuven - COSIC
Data Protection in Distributed Systems Using Cryptographic Enforcement of Policy, Phillips
TaaS4Cloud, CASED/TU Darmstadt
Legal e-Signature with probative value and strong authentication, Sarah Benoudiba, TrustSeed
Identity Assurance Services for Students, Bhardwaj Pulugundia, Verizon

Carolyn Harrison from Aletheia introduced its Trust Framework which provides a seamless and secure method of managing identity and trust in the digital world. With a trusted method of mutually proving a claim of identity and legal role, then the nature of digital business is transformed. This puts contract liability back where it should be – between the contracting parties.

Ecosystem HosTaGe is a collaborative mobile honeypot. It is a lightweight user-friendly security application for mobile devices that aims at the detection of malicious wireless network environments.

Doctoral Researcher at CASED/TU Darmstadt, **Shankar Karuppayah**, explained how this tool is able to inform users whenever malicious activities are detected, whilst utilising a wireless network. In addition, it is capable of learning from other participating users and thus, is able to inform them as to the security health status of a wireless network.

Pascal Bisson from Thales Communications and Security introduced FI-WARE, and discussed the potential of this Security Monitoring Generic Enabler which has been developed as a service suite to secure an ICT system, going far beyond what standard systems today propose.

TrustSeed won the 2014 TDL sprint award for its proposal for a legal proof e-Signature with probative values and strong authentication. The company returned to Trust in the Digital World to demonstrate how it has worked together with Microsoft and its Azure technology to implement a demonstrator to countersign the TDL membership contract. A key innovation of the project is the e-Signature combining four web-services: e-Identification, e-Signature, e-Delivery (time stamping, sealing and storage) and e-Validation of supporting documents.

From KU Leuven, **Jens Hermans** advised delegates to forget about authentication tokens, transferring digits and complex user interactions. He explained that with the n-Auth solution it is possible to authenticate at the 'snap' of a single n-Auth code.

Philips introduced its data protection in cloud storage systems and data protection in distributed systems that uses cryptographic enforcement of policy. The former addresses the concerns surrounding cloud computing, where as soon as the data is stored on the cloud, the owner of the information loses full access control. The solution from Philips encrypts the data before it is stored on the cloud, with the corresponding decryption key (provided only to authorised data requestors) being stored on a different entity than the cloud service.

Classical data protection techniques rely on the enforcement of access policies which state who is authorised to access the data. However, these solutions are only appropriate when the enforcement server is fully trusted in a sense that the access policies are correctly evaluated and enforced. In some cases such trust assumptions would not be valid. To address this problem Philips presents a new technique called Attribute Based Encryption (ABE) whereby the access policies are enforced using cryptographic functionalities without requiring any mediated servers.
top

Panel Sessions

Big Data Security

Tackling big data from a security perspective

Chair: Ghassan Karame, Senior Researcher, NEC Laboratories Europe, Germany
Adrian Perrig, Professor of Computer Science, ETH Zurich
Aljosa Pasic, Business Development Director, ATOS
Josep Román, Senior Manager in IT Security, INDRA
Jose Luis Agundez Dominguez, Data Transparency Lab, Telefónica, Spain

Big Data is gaining increasing attention nowadays both from the industry and from the academia. However, in spite of its advantages, Big Data poses numerous security challenges: What are the security and privacy concerns associated with Big Data? Are these concerns realistic? How can we truly leverage Big Data to analyze security incidents? How can we be protected from Big Data? How can we efficiently perform data analytics and other functions over encrypted data? In this panel, we explored these issues and tackled the Big Data problem from a security perspective with the goal of implementing better corporate policies regarding the collection, use and safeguard of customer data.

Panel -Following a presentation by the chair **Ghassan Karame**, panelist **Jose Luis Agundez Dominguez** provided numerous examples demonstrating how different business models can make use of Big Data in order to provide better service. He outlined the various maturity levels of these models and the associated risks. Among those examples, he showed how Telefónica made use of mobile data to measure the spread of a swine flu in Mexico, and how Telefónica can make use of its logs to help dimensioning emergency services (e.g., in Mexico in 2012). He also commented on the security and privacy basics for handling access to personal data. Namely, a layered framework centered at Data Protection was presented; the suggestion took into account both data security and data quality. Finally, Jose Luis concluded with a university research project sponsored by Telefónica in 2013 that crawled the web, and collected data in order to compare retail prices from different locations. The tool was able to discover 20 retailers that exhibited significant price variations.

Aljosa Pasic emphasised the need for security and privacy for Big Data technologies. Several technologies and tools enabling Big Data were presented. Aljosa remarked that a careful design of security and privacy technologies should be performed for each of the stages of the Big Data value chain: data acquisition, data pre-processing, data analysis, and data usage. The presentation then demonstrated various means to map privacy strategies, such as the *minimize*, *hide*, and *control* strategies to the Big Data chain. Aljosa concluded by looking into possible research topics in the context of security in Big Data, and briefly introduced two research projects, SECCORD and PHEME, which Atos research is involved with.

Adrian Perrig introduced the notion of trusted computing. Trusted computing can enable secure processing over data and resists malicious administrators. Adrian described how trusted computing can enable the construction of an isolated execution environment within an untrusted environment. Two specific systems that leverage trusted computing, Flicker and Trustvisor, were presented. Both systems result in low performance overhead, are readily applicable to current applications with minimum modifications, and are open-source.

The panel concluded with **Josep Román**, who said that Big Data can help in resolving a number of security incidents. More specifically, Josep proposed an architecture which relies on real time analysis of Big Data in order to produce alerts, and issue appropriate reports. Moreover, the proposed architecture leverages machine learning in order to forecast events, and classify new events based on the collected data. Josep remarked that machine learning can only produce results which are based on the quality of collected data, and as such is a tedious process which requires delicate care.
top

Realising eIDAS

The realities of putting Europe's new identity legislation into practice

Chair: David Goodman, Executive Director, EEMA

Neil Clowes, DG CONNECT, European Commission - Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Antonio Lioy, Politecnico di Torino Dip. Automatica e Informatica - STORK as a foundation for eIDAS

Sahra Benoudiba, Strategy & Business Development, TrustSeed SAS

The eIDAS legislation was introduced in July 2014 with the objective of strengthening the EU single market by "boosting trust and convenience in secure and seamless cross-border electronic transactions". This session examined the roadmap for the legislation, how the STORK 2.0 project is contributing to the realisation of this plan and finally raised questions about whether the market would be responsive or seek its own solutions.

Neil Clowes explained the key principles of eID and trust services and that eIDAS plays an important role in realising the Digital Single Market. He showed the timeline for implementation over the next two years

and emphasised that the critical date is 19 September 2018, when subject to certain criteria, the recognition of eID becomes mandatory. He pointed out that legislation doesn't get interpreted by member states, although they do not have to accept a lower level of assurance than currently used.
Although stakeholders will initially be interested in their individual sectors, it is vital that cross-sector take up of eIDAS should be pushed. The conclusion from the first cross-sector stakeholder meeting on 19 November was that, because not enough is known about eIDAS, spreading awareness is critical. The next such meeting will be held in Brussels on 31 March with a calendar of events over the ensuing months

Antonio Lioy revealed that the eIDAS e-ID interoperability framework was based on the STORK architecture that had been in development since 2008 by project partners in 21 member states. He provided an example of how the STORK infrastructure is used in a cross-border scenario involving the collaboration between two member states to share eIDs through national gateways. He went further asserting that there would be more alignment with standards, and increased operational security. Among the technical improvements, he described encrypting assertions to avoid attacks in the browser, including available attributes in gateway metadata (to avoid asking for what is not available), as well as providing sector-specific gateways and the transparent transport of sector-defined attributes. He left the session with some thought-provoking ideas about the usage of eIDAS by the private sector, and the possibility of mixing-and-matching with other e-IDs (private or sector specific).
top

Cloud Security
The many benefits of the Cloud come with new security measures
Chair: Raj Samani, CTO, McAfee
David Barroso, CTO Telefónica Security Division
Steve Purser, Head of Operations, ENISA
Raúl Riesco, Cybersecurity Excellence Program Manager, INCIBE
top

Smart Cities
Many cities across the globe are co-ordinating a wide variety of civic services with new security and privacy concerns
Chair: Daan Velthausz, Senior Manager, Bicore
Asier Abaunza Robles, Counsellor, City of Bilbao
Daniel Villatoro Segura, Senior Data Scientist, BBVA Data & Analytics

Daan Velthausz, gave an introduction to the new security and privacy challenges Smart Cities are facing when dealing with a wide variety of civic services.

Mr Asier Abaunza Robles, Councillor, City of Bilbao, outlined the progress of Bilbao over the last 25 years. From a crisis situation, through transformation Bilbao has become a prosperous city. The transformation covered 25 major projects in urban regeneration, environmental regeneration, heritage and culture, mobility and advanced services. Key lessons from this successful journey are: having a long term vision, strong leadership from the council, public-private partnership, local economy, local technologies, concrete actions, and good governance (including financial management).

In the future Bilbao has six intelligent economic specialization dimensions:
1) Advanced services, 2) Eco technology urban solutions 3) Internet Digital Technology
4) Art & creativity, 5) Tourism and MICE, 6) Health and applied technologies.

Bilbao is becoming a smarter city, not using technology as a starting point but people oriented. The population of the city is aging rapidly and to co-create successful solutions, the concepts of city "hearts of

neighbourhood" (geographical small village regions within the city with decentralized decision making) with active citizen engagement introduced in combination with a living lab approach open to anyone that wants to validate solutions in the Bilbao region. The City focuses on the long term planning: what should be the base and what they want to build in the future. The next step is then to integrate all the systems they have and standardize all data into one interoperable system where all the technology is standardized to be independent of any single vendor. Bilbao has an open big data policy providing access to available data to anyone who wants to use it.

Mr Daniel Villatoro Segura, Senior data scientist of BBVA Data & Analytics spoke about BBVA, the second largest bank in Spain and Southern America, which has embarked on a journey to use all their anonymized daily credit card transactions for data analytics services to be provided commercially outside the bank to third parties.

Transactions of both point of sale, as well as citizens, are used to have a good representation of what is happening. The data is anonymized and aggregated to a certain extent where privacy of individuals is guaranteed: only the location of transactions, amount of transactions, commercial sector of the transactions, county, age and gender of the origin are provided at spatial aggregated level. Visualization experiments have been conducted in Barcelona to validate the relevance of the information for retailers and urban management.

Dr Daniel Villatoro indicated that insight in financial transactions can improve cities operations and planning, e.g.

1) Event impact measurement (sporadic events: congress, festivals; permanent events: opening of new metro line/rural remodelling / legal changes (stores open on Sunday)
2) Tourism analysis (what other cities share the same visitors? Where are the visitors from? What are their main interests? Where do people spend money on lodging? etc).

Based on this kind of data, third parties can develop commercial offerings e.g. for retailers to provide insights like - what do other customers do in the area, what are hot times of day, loyalty rates of customers, or where to set up a particular type of business.

There was some concern in the audience that this might be a sensitive topic for a bank to be involved with, as there have been other examples, e.g. ING bank in Netherlands, where people's perception was negative that the bank is making money from their private transaction information and changed banks on hearing the announcement of the ING bank.
top

Securing Identities & Trust
Today's business world is ever more dependent on securing trusted identities
Chair: Jon Shamah, Chairman EEMA
Enrique Crespo, Director of Professional Services, SafeLayer
Matti van der Gronde, Manager, qKey
Carolyn Harrison, Sales & Marketing Director, Aletheia International

This session looked at various aspects of Trust in an end-to-end identity ecosystem.
Enrique Crespo, from Safelayer**,** showed how the issue of trust elevation, essential when individuals are re-using their credentials in different environments, can be managed and controlled. This was described by using flexible processes and well-designed rule-sets (that were depending on the risk requirements of a particular application) and applying them to incoming transactions and declared Levels of Assurance. Mr Crespo demonstrated the Safelayer methodology and toolkit which was specifically designed to address this in a consistent and appropriate manner.

Matti van der Gronde, from qKey**,** discussed the various Levels of Assurance (LoA) for authentication that could be achieved using mobile devices and second factors such as username-passwords, SMS and other One-Time-Passwords techniques. However it was explained that none of the current techniques could achieve an LoA 4, which signifies a strong authentication, on the same level as smart-cards. Mr van der Gronde, demonstrated and explained how this could be achieved by using a server-based HSM authentication of a mobile client that was in the control of the user and was certified as LoA 4. qKey has already been certified for use at LoA 4 by a national EU eID program.

Carolyn Harrison, from Aletheia International**,** described how a holistic approach to identity management was a major factor in improving the trust and reliability of identity ecosystems. The Aletheia Trust Framework helps companies dramatically reduce cost in areas such as compliance and automating business processes, fraud reduction and simplfying how business is done. It ensures that digital interactions are driven from a 'physical world' viewpoint, and not just the requirements of the technical solutions, thereby increasing trust. There were numerous questions and a lively debate how these three approaches achieved their results.

top

Privacy

Big data and privacy concerns: can they be reconciled?

Chair: Claudia Diaz, Asst Professor KU Leuven
Marit Hansen, ULD
Eleni Kosta, Associate Professor, Tilburg University
Carmela Troncoso, Researcher, Gradiant

This session addressed some of the current challenges in online privacy and data protection. The speakers provided an overview of the main principles of the data protection directive, emphasising some of its problems and limitations. They introduced the expected main changes that will be included in the upcoming data protection regulation, as well as the multi-stage process that the regulation is going through. They further provided an overview of the criteria proposed by the Article 29 working party to assess whether a dataset can be considered anonymous (and thus outside the scope of data protection legislation).

The main challenges discussed by the speakers were:

- The difficulty to ensure that the consent provided by the users of a service is meaningful
- The lack of transparency for data subjects
- The impossibility to ensure that anonymised data cannot be re-identified, particularly in the context of Big Data Analytics, where datasets contain rich information
- The legal uncertainty concerning the validity of data retention laws (that have been ruled invalid by the European Court of Justice) as well as concerning the application of data protection across borders
- Issues of social sorting, discrimination, and manipulation that arise from automated profiling and decision-making in the context of Big Data
- Issues of data integrity and biases in the data that can lead to unfair or problematic decisions and insights.

top

TDL Industry Recommendations

Chair: - Amardeo Sarma, General Manager, NEC Labs, Europe
Volkmar Lotz, Head of Applied Research, Security & Trust, SAP
Pascal Bisson, Thales

Chaired by **Pascal Bisson** from Thales Communications and Security this session outlined the important contribution being made to further engage and better align TDL with the advancement of the Network and Information Security (NIS) directive.
Mr Bisson highlighted TDL's five key recommendations regarding research priorities, which are driven by an observed erosion of trust…

- Economics of trustworthy ICT
- Assurance
- Privacy
- Compliance to new regulation
- Process improvements

TDL has appointed Pascal Bisson, Volkmar Lotz, Svetla Nikov and Eric Blot-Lefevre as champions for each of these recommendations. The aim is to put the TDL SRA views into the perspective of the NIS SRA, providing the NIS WG3 (TDL has three representatives involved in this working group) with actionable recommendations to improve the NIS SRA, as well as clearly demonstrating the commitment of TDL to NIS.

It is planned that the target deliverable of recommendations to NIS will be made by the end of March 2015.
top

Day 2 - Plenary Keynotes

Chair: Ronny Bjones, Director, Cloud Identity & Privacy Services, Microsoft
Márta Nagy-Rothengass, Head of Unit 'Data Value Chain' European Commission
Afonso Ferreira, NIS Project Officer, European Commission

In her keynote entitled 'Towards a data-driven economy in Europe', the Head of Unit 'Data Value Chain' at the European Commission, **Dr. Márta Nagy-Rothengass** stated that data is a top political priority for Europe with European Commission President, Jean-Claude Juncker expressing the importance of digital. She commented that data has become an economic and social asset and the big data market is the biggest growing in the world.

Dr. Nagy-Rothengass explained how data-driven applications represent great opportunities for job creation, to speed up research, create market and economic growth and to solve issues in society. However, the challenge is to set up an accessible but secure ecosystem, and to have the right skills and the necessary capital. She added that trust is a key issue when discussing big data and it is very important to establish a modern, strong and comprehensive data protection framework.

NIS Project Officer at the European Commission, **Alfonso Ferreira** explained in his presentation 'Protecting Big Data and beyond' the context of the European Strategic Research Agenda in Cybersecurity, from a policy-making perspective. Mr Ferreira explained how the EU Cybersecurity Strategy (published in February 2013) is where the Network and Information Security (NIS) directive is hooked. He went on to describe the NIS Platform within the directive that has more than 200 participants across 18 members states and Norway. The objective of the platform is to prepare the ground for the directive, providing guidance on risk management and information sharing and EC recommendations on cybersecurity.

He went on to explain the scope and objectives of the NIS WG3 (a working groups with 180 registered members) set up to address cybersecurity research and innovation in the context of the EU cybersecurity strategy and the NIS Platform. These are…

- Identify challenges and competences
- Promote underpinning research that fosters collaboration
- Exercise ways to increase the uptake and commercial impact of research results in the area of secure ICT.

The next step for the working group is to finalise public versions of the deliverables in March 2015. The deliverables are…

- Secure ICT research landscape
- Business cases and innovation paths
- Snapshot of education and training

Mr Ferreira concluded with a communication from the EC President to Günther Oettinger that expressed the need to develop and implement measures to make Europe more trusted and secure online, so that citizens and businesses can fully reap the benefits of the digital economy.

top

Panel Sessions

eHealth

New opportunities to improve healthcare services depend on taking care of security and privacy

Session Chair: Volkmar Lotz, Head of Product Security Research SAP Labs France
Alberto Sanna, Director eServices Life and Health, Scientific Institute San Raffaele
Ross Little, Secure eID Analyst, Atos
Roberto Sanz Requena, Quiron Hospital
Dominik Bertram, Development Manager, SAP Innovation Center

This session focused on new applications in the e-health sector that exploit the opportunities provided by Big Data analytics, integrated services and the cloud, as well as the discussion of the related security and privacy challenges. Driven by presentations of innovative solutions for medical research and personal health services, the discussions centered on anonymisation, trust establishment and authorization, taking the diversity of stakeholders including patients, researchers, doctors and medical/nursing staff into account.

Alberto Sanna presented an integrated service environment for healthcare and well-being that is operated at the San Raffaele Hospital in Milan, Italy. Based on the view that health can be considered as a state of physical, mental and social well-being, this environment does not only include the medical services, but extends to the daily life and the social environment of the users who do not only include patients, but medical staff, family, and friends as well. This holistic approach, including the physical environment in a smart city, allows gathering big data that facilitates the provision of tailored services to improve prevention and reduce the health risk for everybody, but at the same time requires a high-level of trustworthiness of the provided services and the infrastructure they are running on. San Raffaele is successful in establishing trust in their services by both technical and non-technical means, with the scientific, non-commercial nature of the offer being an important pillar of trust.

Personal Health Records (PHR) and PHR Data-as-a-Service over the cloud provide a new application model for the provision of data for healthcare professionals, users and both for-profit and not-for-profit researchers. **Ross Little** discussed the EU legal environment for this model, which does not only comprise of the EU Data Protection Framework, but also the member states' individual health practice and regulations, which may differ, for instance, on user control / informed consent vs. strict regulations. In the light of these legislations he highlighted the privacy challenges, including anonymisation of data sets, separation of sensitive data, user awareness and federated access control. Given the extended set of entities involved (e.g., cloud and service providers) and the ever larger amount of easily accessible big data, novel concepts that scale to these conditions, for instance, differential privacy, are investigated.

The concept of P4 medicine (personalized, predictive, preventive, and participatory) describes the change of medicine from a reactive science to more integrated diagnostics facilitated by ICT innovation and advanced data processing capabilities. **Roberto Sanz Requena** discussed the opportunities of this change for cloud-based solutions, since data will become so large that they need to be managed in a distributed environment. However, cloud providers need to be compliant with the specific healthcare requirements. Roberto highlighted the related challenges from the end-user perspective, including scalable storage and secure long-term storage of medical data. Potential deficiencies of standard security measure in the healthcare context were exemplified by a discussion of limitations of role based access control for instance based authorization decisions.

Big data helps improving medical research. **Dominik Bertram** illustrated this by example of the increased differentiation of diseases, which imposes a challenge for finding suitable patients for clinical trials. He demonstrated a solution that allows drilling into large distributed datasets to find patients with matching attributes. Such a solution needs to balance the utility of data sets with anonymity. The proposed solution introduces three discrete levels of de-identification adapted to high-level research (access to aggregated data only), clinical trials (individual access to de-identified records) and treatment (individual access to limited number of clear text records). Each level carefully chooses the aggregation of attributes and the consent with respect to the purpose of the task, thus meeting anonymisation requirements while preserving the required by the task at hand.
top

Demonstrating eIDAS-Large Scale Pilots
First steps are already being taken to demonstrate eIDAS in action!
Chair: Roger Dean, Director Special Projects, EEMA
Frédéric Poels, IT Specialist, European Commission
Lefteris Leontaridis, CEO, Netsmart
Linda Strick, Business Developer, Fraunhofer [Cloud for Europe]
Carlos Gómez Muñoz, ICT Civil Servant, MINHAP – Ministry of public Administration.
Alberto Crespo Garcia, Head of Secure Identity Technologies Laboratory, ATOS
Michael Kubach, Senior Scientist, University of Stuttgart

The eIDAS Regulation strengthens the EU Single Market by boosting trust and convenience in secure and seamless cross-border electronic transactions. It provides mutual recognition of eID, electronic trust services and electronic documents

The first steps are already being taken to demonstrate eIDAS in action as illustrated by the speakers below!

Frédéric Poels had adapted his presentation according to the feedback and discussions from the first day. He introduced CEF (Connecting Europe Facility) as the eID and eSignature Digital Service Infrastructures building blocks which are the key enablers to be reused in more complex digital service infrastructures. He described the relationships between eIDAS, STORK, STORK 2.0, CEF, ISA, e-SENS, online dispute resolution (for say Amazon) and UUM&DS (User Management & Digital Signatures), etc. Together with the general concepts of the reference architecture of eIDAS and the implementation provided by CEF (central proxy model and decentralised middleware model) for ECAS (European Commission Authentication Service).

Lefteris Leontaridis described how the e-SENS Large Scale Project is working on the implementation of eID and eSignature building blocks in several business domains such as eProcurement, eHealth, eJustice and Business Lifecycle. The e-SENS pilots will demonstrate how these building blocks will support business processes whilst meeting legal, regulatory and trust/security requirements of the domains and countries involved. e-SENS pilots will re-use the building blocks maintained by the Connecting Europe Facility (CEF)

Programme of the European Commission and provide further input to their evolution towards supporting e-IDAS and its upcoming implementing acts, in cooperation with the piloting Member States, as well as, using their trusted lists of qualified certificates.

Linda Strick is the co-ordinator of the C4E (Cloud for Europe) project funded under the EU 7th Framework programme to get public sector adopting and using unified trusted cloud services in Europe for public eProcurement. C4E will identify the obstacles and challenges and define the services needed for the three phase's for pre-commercial procurement. Some of the challenges include legislation for secure storage in public clouds and the interoperability issues in managing a national federated services brokerage – for example G-Cloud in the UK

Carlos Gómez Muñoz presented Cl@ve, an eID system rolled out by the Spanish national government last year that is aimed to simplify citizens' access to public services. It is the result of a collaborative project, promoted by the CIO of the national government, carried out to unify eID initiatives not based on electronic certificates. It has been built upon the results from STORK, and it has been devised to be fully aligned with the eIDAS regulation, both for allowing recognition of foreign IDs and for matching three authentication assurance levels foreseen in eIDAS, and will be mandatory by the end of 2015.

Alberto Crespo Garcia described the STORK 2.0 Pilots: Bringing citizens, public and private sector closer towards the single European electronic identification & authentication area.

Its focus and purpose is to illustrate, with a number of ground-breaking innovations and real-life cross-border piloting cases, how, with the direct support of the EC and 19 European Member States and Associated Countries, STORK 2.0 Large Scale Pilot is extending the STORK fundamental eID building block and federated eID interoperability platform, to provide governments, citizens and now also businesses across Europe with several of the key trust and convenience elements that are going to be instrumental for realizing the eIDAS regulation vision of a strengthened single digital market based on secure and seamless cross-border electronic transactions. STORK 2.0 pilots are designed to prove how mobility and borderless digital living can be made a reality, in a context of full respect for personal data protection and with user control of data release, for aspects like benefitting from eGovernment services for legal person representatives based electronic mandates, accessing your healthcare record no matter where you are receiving treatment, opening a bank account online in a foreign bank, managing e-Invoices across borders or enabling better e-Learning systems based on the secure retrieval and exchange of academic attributes information and much more.

Michael Kubach, demonstrated e-IDAS from a FutureID perspective. FutureID is an Integration project with 19 partners from 11 countries partially funded under the ICT theme of the Cooperation Programme of the 7th Framework Programme of the EC. FutureID 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.

Michael described the business to business scenario in the automotive industry. A major security-challenge in the automotive industry is to enable the secure and flexible engineering cooperation with changing partners in complex development projects. Therefore an effective inter-organisational, federated identity management is needed to control access to diverse cooperative development platforms. This identity management has to be based on reliable identification of engineers of various partners and suppliers with different credentials. The demo shows a "Cloud-team room for the Automotive Industry". It is adjusted to the specific requirements of the value chains in the automotive industry. Thanks to the FutureID infrastructure, engineers from different partners can access the cloud-team room according to their access rights. For the required strong authentication they can use the credentials that are already available in their company.

top

NIS Platform
Building a European cybersecurity ecosystem – perspectives and views
Chair: Pascal Bisson, Thales
Fabio Martinelli, CNR
Raúl Riesco Granadino, INCIBE
Afonso Ferreira, NIS Project Officer, European Commission
top

Vehicle-to-X
The next generation of talking and networking cars will save money and save lives – but what are the security and privacy implications?
Chair: David Goodman, Executive Director, EEMA
José María de Fuentes, COSEC Lab, Universidad Carlos III de Madrid
Jetzabel Serna-Olvera, Deutsche Telekom Chair of Mobile Business & Multilateral Security, Goethe Universität

V2X security, privacy and trust overview
José María de Fuentes opened by stating that connected cars are part of the smart cities phenomenon and have attracted attention because of the possibilities for increased road safety, efficiency and infotainment. But all stakeholders – the automakers, governments and consumers – are acknowledging that there are security, privacy and trust issues in exposing a mass of data about vehicles as well as their occupants. Despite the recognition of the pitfalls, vehicle-to-X communication is increasing although the standards are still inadequate and the 'normal' procedures relating to security and privacy do not apply particularly over short communication distances and periods.

Requirements from a security perspective are the need for confidentiality and source authentication as well as the avoidance of the hazards associated with illusion attack – the false warning of a crash could cause a crash – and questions of liability in case of accidents.

It was apparent that V2X security, privacy and trust deserve high attention in the near term from industry and research organisations before on-board computing can advance much further.

Cars, freedom and privacy
Jetzabel Serna-Olvera continued on the same theme, remarking that the car is still seen as a symbol of freedom, particularly by young people and that part of the attraction is the sense that once we are inside our car we have all the amenity afforded to us at home. The downside of this is that all the data and personal information that we manage securely at home is also available in the car but now it is very public. A lot can be learnt from this data and consequently there are many positive opportunities for service providers to offer consumers who on the other hand are also at risk of having their privacy compromised. The challenge for privacy experts is to review the requirements and to assess whether the architectural and procedural approaches are fitting.

Ultimately, a number of open questions remain, foremost of which is whether the collection, processing, or transmission of data really needed for a real improvement in the driving situation – and, if so, whether this advantage is worth the additional privacy risks. A further question is whether stakeholders are in a position to make that judgement call or have any control over their own data. As with the security issues, a lot more work has to be carried out before we can be comfortable with sitting in our connected cars and to fully understand the relationship between the car and the people in the car.
top

Cybersecurity for SME's

An insight into SME cybersecurity challenges and possible solutions

Chair: Lorraine Spector, LS Consultancy
Antonio Ramos, CEO, LEET Security/VP ISACA Madrid
Christian Schnuck, Fondazione Inuit, University of Rome Tor Vergata
Jon Shamah, Chairman EEMA

With two out of every three employees working for an SME, they form the backbone of the European economy. This session, chaired by Lorraine Spector of LS Consultancy, provided insight into the challenges and opportunities for these organisations. CEO of LEET Security, Antonio Ramos, began by looking at the top ten cybersecurity threats that SMEs face:

1. Ransom ware
2. Malicious HTML email
3. Reckless web surfing by employees
4. Webserver compromise (citing his own experience with WordPress)
5. Mobile data loss
6. Reckless use of wifi hotspots
7. Reckless use of hotel wifi and kiosks
8. Poor configuration leading to compromise
9. Lack of contingency
10. Insider attacks

Mr Ramos explained that SMEs do not pay attention to new vulnerabilities, as they are busy focusing on their business. They lack awareness of the consequences (most do not see IT as being connected to their business strategy), time, money, and have a belief that a cyber-attack isn't going to happen to them.

Christian Schunck of the University of Rome Tor Vergata added that just 20% of small businesses have an ICT policy in place. He endorsed Mr Ramos's comment that there is a need for a 'business-centric' campaign to drive awareness, which concentrates not only on the impact a cyber-attack can have on the value chain, but also the capacity for value creation.

Building on Mr Ramos call to keep it simple for SMEs, Mr Schunck, recommended guidelines and a 'toolkit' to help them limit their exposure. Ms Spector added that any campaign needs to be ideally centralised in Europe and disseminated out across each EU member state, through channels such as trade bodies and the media.

Jon Shamah of EJ Consultants and Chairman of EEMA, responded to Mr Schunck through the introduction of the new COSTAR initiative, a not for profit organisation that originates from TDL, which will ultimately become a CERT for European SMEs, providing a first step in practically helping SMEs to combat cybercrime.

Mr Shamah explained that unprepared SMEs are vulnerable to even the most basic cyber-attack, and just one such incident could put an organisation out of business.

COSTAR will provide a highly automated and intelligent filtering mechanism, offering managed cybersecurity services to SMEs in all member states. The service works by charging subscribers less than five Euros per device per month to monitoring the health of their infrastructure and deliver remedial action to help keep them protected.

top

Closing Plenary Panel Session
Thoughts and perspectives on trusting big data from Trust in Digital World 2015
Chair: Svetla Nikova, KU Leuven
Harm Jan Arendshorst, Verizon
Ronny Bjones, Director of Cloud Identity and Privacy Services, Microsoft
Antonio Skarmeta, Head of Research Group, ANTS, Universidad de Murcia

Harm Jan Arendshorst of Verizon explained how building an EU cybersecurity ecosystem isn't something that can be done overnight, and the key element is the trust framework which starts with sharing information services (cyber intelligence), and requires interoperability. Furthermore, for such an ecosystem to work, the economics needs to be right and a governance system at a European level needs to exist in order to ensure it is sustainable.

Antonio Skarmeta of the Universidad de Murcia in Spain presented 'The impact of Internet of Things and Big Data in Security and Privacy'. He talked of a possible future Internet featuring omnipresent heterogeneous smart devices wirelessly communicating over hybrid and ad-hoc networks of devices, sensors and actuators working in a synergy to improve the quality of life, optimising energy consumption and reducing the ecological impact of a mankind.

Mr Skarmeta also addressed some of the challenges that such a future presents including the lack of economic incentives for data protection, no control over data disclosure, difficulties in implement PET or data protection and the accountability of data provided by the Internet of Things. But he also cast some doubt over this possible future by questioning whether it is indeed possible to connect anything to the Internet? And even if it is, do we want to connect everything to the Internet?

Director of Cloud Identity & Privacy Services at Microsoft, **Ronny Bjones**, concluded Trust in the Digital World by highlighting the importance of the event in bringing together policy-makers, industry and academia. He observed the insight the conference had given regarding the EC cybersecurity agenda and the call to action to participate.

Considering the big data theme for the event Mr Bjones commented how some people are scared of grasping market opportunities that big data presents, due to the Snowden effect. However, he also noted how organisations and services may collect data because it may be possible to monetize it in the future, but he questioned whether the right measures to protect that data are being taken, and in fact if it is really worth storing the data in the first place! He concluded by saying that the big data industry is fragile. Reiterating the comment from Richard Benjamins that an entire industry can be placed at risk from big incidents, citing the impact on the nuclear industry in the USA following Three Mile Island.
top