ENISA activities in the area of Privacy & Trust

Rodica Tirtea

2nd December 2011

@ 1st ISACA Athens Chapter Conference

Overview

- Introduction & context of the work
  - About ENISA activities
- Activities related to privacy & trust
  - 2010 activities on privacy and data protection topics
  - Ongoing activities
  - Future activities
- Final remarks / Instead of conclusions

About ENISA

(European Network and Information Security Agency)

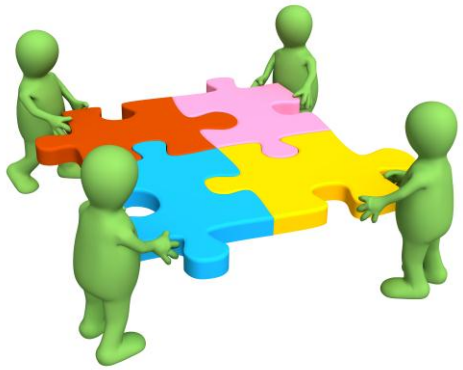
- Created in 2004
- Located in Heraklion / Greece
- Around 30 Experts
  - Centre of expertise
- Supports
  - EU institutions and
  - Member States
- Facilitator of information exchange
  - EU institutions,
  - public sector &
  - private sector
- Has an advisory role
  - the focus is
    - on prevention and preparedness
  - for NIS topics

Activities

- The Agency's principal activities are as follows:
  - Advising and assisting the Commission and the Member States on information security.
  - Collecting and analysing data on security practices in Europe and emerging risks.
  - Promoting risk assessment and risk management methods.
  - Awareness-raising and co-operation between different actors in the information security field.

Work Streams

- The 2011 Work Programme has been structured as three separate work streams.
- These have been chosen so as to ensure continuity between the former MTPs and the Work Streams (WS) of the future strategy.
- These work streams are as follows:
  - WS1 ENISA as a facilitator for improving cooperation
  - WS2 ENISA as a competence centre for securing current & future technology
  - WS3 ENISA as a promoter of privacy, trust and awareness.



WS1 – Improving Cooperation

- The objective is to support EC and the MS in intensifying cooperation between MS in key areas
- The Work Packages in this WS are:
  - Supporting Member States in implementing Article 13a
  - Preparing the next pan-European exercise
  - Reinforcing CERTs in the Member States
  - Supporting CERT cooperation at the European level
  - Good practice for CERTs to address NIS aspects of Cybercrime

WS2 – Securing Technology

- The overall objective of the second Work Stream is to assist the Member States and the Commission in identifying and responding to security issues related to current and future technology
- The Work Packages in this WS are
  - Security & privacy of Future Internet technologies
  - Interdependencies & interconnection
  - Secure architectures & technologies
  - Early warning for NIS

WS3 - Privacy and Trust

- The major objective of the third Work Stream is to promote trust in future information systems by all sections of the population.
- The Work Packages in this WS are:
  - Understanding and analysing economic incentives and barriers to information security.
  - Deploying privacy and trust in operational environments.
  - Supporting the implementation of article 4 of the ePrivacy Directive (2002/58/EC).
  - Promoting the establishment of a European month of network and information security for all.

Privacy, Accountability and Trust – Context

- Internet is open and distributed without authoritative control
- In terms of privacy a number of challenges are posed
  - Data ‘pollution’ - data disseminated without control and is replicated on multiple servers
  - Contrary to humans, data lives forever
    - emails (not only web mail), social networking sites, online collaborative spaces (e.g. Google docs)
- Contradictory positions
  - governments
    - Demand accountability, data protection, data minimization, better privacy protection
    - But also more access control to data, data retention, lawful interception
  - Users
    - Expressing concerns regarding privacy
    - Some users willing to drop the concerns when benefits are offered

Overview of 2010 activities

- 2010 activities on privacy and data protection topics
  - Data Breach Notification in Europe
  - Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments
  - Privacy, Accountability and Trust –Challenges and Opportunities
  - Bittersweet cookies. Some security and privacy considerations

    ➢ http://www.enisa.europa.eu/act/it/library

- Findings and issues to be further addressed

Data Breach Notifications - context

- Review of ePrivacy Directive (2002/58/EC)
- Article 4
  - In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.
- ENISA activities
  - 2010 – Review of current practices among MS
  - 2011 – Consultation workshop on DBN (24th January)
  - 2011 – Technological guidelines for implementation of Art. 4

Data Breach Notifications – technological guidelines (I)

- Target
  - Competent authorities (DPAs and others)
  - Telecom operators (and other sectors players)
- Objectives
  - Practical and usable definition of a breach
  - Criteria for determining a breach
  - National and pan-European approaches
  - Appropriate technological protection measures
  - Identification and assessment of risks of breaches
  - Procedures of notification

Data Breach Notifications – technological guidelines (II)

- ENISA responsibilities
  - Providing advice to EC
  - Collaborating with Art.29 WP, EDPS
- Areas covered by the study
  - Planning and preparations
  - Detection and assessment of data breaches
  - Notification procedures
  - Gathering of evidence, forensics analysis
  - Review and improvement
  - Roles and responsibilities

Survey of mechanisms in online environments. Remarks (I)

- Privacy in online environment; defining personal data given current context of data mining
  - Clear privacy principles and personal data definitions valid in an evolving online environment should be promoted
  - Privacy enhancing technologies and a user centric approach to privacy need to be encouraged. Best practice studies should be prepared and disseminated
- Consent and privacy policies
  - More transparency by organizations on how they handle personal data is needed
  - The way privacy policies are displayed and the issues regarding the changes of policies need further consideration; alternatives to lengthy privacy policies should be available to inform the user
  - Consent provided for a certain privacy policy must not be transferred to another (changed) version of privacy policy without clear understanding and acceptance of the user

Survey of mechanisms in online environments. Remarks (II)

- Profiling and tracking
  - Storage time. Data should not be stored forever
    - Data minimization
- Personal data as a commercial asset; transfer of personal data between providers and outside EU
  - In line with the EU approach, ENISA considers privacy to be a basic Human Right
  - Economic effects of the use of personal data on both consumers and providers
    - and these effects should be analyzed
    - better understanding the effects and the risks could allow for solutions for protecting consumers' privacy
  - The legal framework in 27 EU MS regarding the transfer of personal data should be surveyed; differences in legislation can encourage transfer of personal data to countries where the legal requirements allow for less privacy protection
  - The legal framework for transfer of personal data outside EU should be also analysed; equal treatment and same enforcement should exist for EU users' personal data independent of the location of controllers/processors inside or outside EU

Privacy, Accountability and Trust study. Findings (I)

- Promote technologies and initiatives addressing privacy
  - Data minimization, privacy enhancing technologies and privacy by design concepts should be well understood and promoted in an effort to prevent rather than cure
    - evaluation of existing targeted (constructed on certain assumptions) solutions in the real environment
    - supporting the uptake of research result in the operational environment
  - Research on information accountability technology should be promoted, aimed at the technical ability to hold information processors accountable for their storage, use and dissemination of third-party data
  - Supporting informed user consent in a transparent and user friendly manner i.e. using transparent privacy policies with icons
  - A multidisciplinary approach that considers education, policy legal and technological aspects should be supported

Privacy, Accountability and Trust study. Findings (II)

- Raise the level of awareness and education regarding privacy
  - Concepts such as privacy certification could be supported; this would allow labeling sites and services according to their profiling activity
  - the risks associated to profiling and tracking, i.e. from economic perspective, should be assessed (dissemination of such studies should be supported)
- Support policy initiatives in the field and the revision process of Data protection directive
  - Clear legal provisions limiting behavior tracking and profiling should be promoted.
  - Promoting clear definitions and guidelines in the field, by raise awareness on the data mining techniques and their possibilities to de-anonymize data and profiles (linking this way information that initially are not considered personal data).

Cookies. Some security and privacy considerations

- Cookies, also known as HTTP (Hypertext Transfer Protocol) cookies
  - Useful in the stateless browser –server HTTP interaction to keep the state
  - are generated and modified by the server, stored by the browser and transmitted between browser and server at each interaction.
    - Extensively used
- Privacy concerns
  - Ability to identify and track users
- Security concerns
  - Vulnerabilities i.e. due to setting
- Legal framework
  - Allows for interpretation

- Collection of data from cookies
  - 78% in ENISA survey
    - 73% both persistent and non-persistent cookies
    - 9% only persistent
    - 18% only non-persistent

Overview

- Introduction & context of the work
  - About ENISA
- Activities related to privacy & trust
  - 2010 activities on privacy and data protection topics
    - Data Breach Notification in Europe
    - Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments
    - Privacy, Accountability and Trust –Challenges and Opportunities
    - Bittersweet cookies. Some security and privacy considerations
      - http://www.enisa.europa.eu/act/it/library
  - Ongoing activities
  - Future activities
- Final remarks

Areas of (possible) intervention

- On-line services, applications and transactions can assure benefits and competitive advantage for citizens and EU economy
- The EU requires
  - Advocating and fostering a Pan-European approach to privacy
  - Proposing new models for trust-establishment
  - Developing of guidelines for regulatory review and interpretation
- Areas of (possible) intervention
  - Information/Education - People have to be aware and educated!
  - Policy maker
    - Order to remove contents
    - Promote availability of subscription based services in addition to free
    - Avoid online service providers lock-in by fostering user profile portability
    - Implement Data Breach Notification;
  - Technology
    - Limit data pollution (e.g. minimal disclosure)
    - Limit content's lifetime (e.g. ephemeral communication)
    - Limit data leakage by design (privacy by design)

Privacy & Trust in ENISA 2011 Work Programme

- WPK 3.2 - Deploying Privacy & Trust in Operational Environments
  - ➢ Outcome (Q4 2011)
    - Report on minimal disclosure and other principles supporting privacy and security requirements
    - Report on trust and reputation models. Evaluation and guidelines
    - Study on monetizing privacy
- WPK 3.3 - Supporting the implementation of the ePrivacy Directive (2002/58/EC)
- Activities linked to
  - Digital Agenda
    - ➢ Policy dimension
  - FI Initiative
    - ➢ Research dimension

Some proposal for 2012

- Activities in collaboration with EC (DG JUS, etc), supporting actions of the Digital Agenda for the EU
  - WPK 4.3: Supporting the development of secure, interoperable services
- WPK 4.2 - Security governance
  - Supply Chain Integrity
  - Art 4, DBN continuation
- WPK 4.3 - Supporting the development of secure, interoperable services
  - State of the art of certification schemes in the EU and beyond.
    - ➢ Exploring the feasibility of implementing a pan-European scheme for trustmarks
  - Privacy-by-design, promoting PETs and their possible economic benefits, smart metering and privacy

Privacy is a human right

- "*Everyone has the right to respect for his private and family life, his home and his correspondence*."
  - ➢ Article 8 of The European Convention on Human Rights
    - adopted by states member of The Council of Europe
- "*Everyone has the right to the protection of personal data concerning them*".
  - ➢ Article 16, The Treaty of Lisbon, The Treaty on the Functioning of the European Union states
- *"Everyone has the right to the protection of personal data concerning him or her" [..] "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."*
  - ➢ Article 8, the Charter of Fundamental Rights of the European Union

Contact

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu