Priority Areas and Topics for Call 2015
Action Line for Privacy, Security & Trust (PST)

Jovan Golic

EIT ICT Labs Italy

Partner Event 2014, Berlin, April 11, 2014

Challenge

- Protecting security and privacy of enormous amounts of data being collected, processed, and stored in the cyber space *(cyber security & privacy)* is a big challenge
- Lack of timely technical solutions may endanger the growth of ICT-enabled products and services and may put at risk privacy and liberty of citizens
- Security breaches can have significant negative impact on people' lives, jobs, and property
- *Validation of security properties is a challenge*
- Market share of European companies in industry solutions for data security and privacy (about 16.5%) is considerably lagging behind their global ICT market share (about 25%)
- Targeted markets: general public, enterprise, government, military

Strategy *(Reality or Dream?)*

- Bridge existing gaps between available techniques and practice by innovative solutions following the **‘privacy & security by design’** paradigm
- Support data privacy by practical cryptographic techniques
- Support data protection laws and regulations by certification & auditing procedures
- Raise social awareness about the need for and value of data security and privacy for ordinary people
- Stimulate new ICT products and services implementing data security and privacy, which will become a business opportunity rather than an obstacle
- Widespread adoption and usage of data protection techniques will reduce costs, create economic growth, and improve quality of life in Europe and beyond

Applications

- User profiling
- Social networks
- E-commerce and e-payment
- E-government
- E-voting and e-democracy
- E-health and wellbeing
- Smart spaces, smart cities & communities
- Cyber-physical systems
- Smart energy
- Cloud computing and storage
- Personal data management
- Intellectual property licensing
- Internet of things
- Big data analytics

Priority 1: Secure and Privacy-aware E-authentication and Digital Identity Management (1)

- Widely adopted and deployed innovative solutions for secure and privacy-preserving federated digital e-authentication and e-identification of physical or logical entities (e.g., persons, things, services) via online or wireless communications will create
  - a basis for more secure, authentic and trustworthy products and services, cross-nationally and nationally
  - a springboard for trusted personal data management
  - more trust among people and organizations in Europe

  without violating the privacy of users as citizens!
- Build on existing cross-border projects and initiatives, e.g., STORK, ABC4Trust, GBA, OneAPI, EEMA, Kantara

Priority 1: Secure and Privacy-aware E-authentication and Digital Identity Management (2)

- ***Relevant techniques include***
  - Strong, multi-factor authentication (beyond password-only)
  - Privacy-preserving biometric authentication of persons and physical authentication of things (e.g., biometric encryption)
  - Cryptographic authentication protocols
  - Credentials & certificates
  - Privacy-aware identity federation and attribute sharing
  - Secret sharing and shared access control
  - Trust & liability models
- ***Relevant technologies include***
  - Hardware & software security tokens, biometrics, PUFs, mobile devices, SIM cards, physically embedded digital signatures, NFC, QR codes, monitoring & anti-fraud technologies

Priority 2: Protection of Data Privacy in Online and Mobile Applications, Services and Communications (1)

- Data privacy essentially means that user controls usage of related sensitive data during its whole life cycle, with the minimality principle guiding the balance with usability
- Privacy = security & control of sensitive data
- Data are in principle easy to copy
- Support by legislation or regulation is necessary, but is difficult to correctly implement in practice
- *Current practice is unsatisfactory, especially for ordinary people and with respect to sophisticated adversaries!*
- **Paradigm promoted:** support data privacy by appropriately validated technical & technological means wherever practically possible

Priority 2: Protection of Data Privacy in Online and Mobile Applications, Services and Communications (2)

- ***Relevant cryptographic techniques include***
  - Anonymization & pseudonymization
  - Anonymity protocols
  - Privacy-preserving data mining and profiling
  - Secret sharing and shared control
  - Secure multiparty computation
  - Practical homomorphic encryption
  - Attribute-based encryption and searchable encryption
  - End-to-end encryption
  - Zero-knowledge protocols

Priority 2: Protection of Data Privacy in Online and Mobile Applications, Services and Communications (3)

- ***Relevant technologies include***
  - Hardware security tokens
  - Hardware and software solutions for end-to-end security
  - Distributed databases and servers
  - Privacy-aware operating systems and software platforms
  - Virtualization
  - Secure hardware platforms
  - Cost-effective certification & auditing procedures

Priority 3: Mobile Cyber-Security, Addressing Malicious Software in Mobile and Online Applications (1)

- Privacy-preserving intrusion detection & prevention and protection against malicious software (malware) on computing devices (e.g., smartphone, tablet, PC) is an aspect of cyber security and privacy of ever increasing importance, especially in mobile scenarios
- Smart mobile devices typically contain both personal data and sensitive business-related data
- Malicious or potentially dangerous apps for mobile devices rapidly multiply and evolve
- Existing solutions are partial and fragmented and do not appear to be sufficiently effective, especially with respect to sophisticated attackers and on mobile platforms

Priority 3: Mobile Cyber-Security, Addressing Malicious Software in Mobile and Online Applications (2)

- ***Relevant techniques include***
  - Privacy-preserving intrusion detection/prevention
  - Kernel-level anti-malware protection
  - Detection/prevention of advanced persistent threats
  - Sandboxing
  - Behaviour-based malware detection
  - Combined client-based and cloud-based solutions for malware detection on mobile devices
  - Privacy-aware process monitoring on computing devices
  - Trustworthy apps
  - Machine learning techniques for sophisticated intrusion detection

Priority 3: Mobile Cyber-Security, Addressing Malicious Software in Mobile and Online Applications (3)

- ***Relevant technologies include***
  - Privacy-aware operating systems
  - Virtualization and virtual machines
  - Secure microkernels and hypervisors
  - Multiple operating systems
  - Trusted hardware platforms, secure elements, and trusted execution environment
  - Secure graphical user interfaces
  - Dedicated memory encryption
  - Sensitive data protection in case of device stealing
  - Hardware security tokens

Priority-related Additional Activities

- Feasibility study of currently available cryptographic techniques for privacy protection
- Feasibility study of end-to-end security techniques with respect to data protection laws in EU
- Organization of international contest regarding the effectiveness of anti-malware techniques
- Organization of original events aiming at raising social awareness about the need for and the value of data security and privacy in digital society