Towards More Security and Privacy in Digital World

Jovan Golic

jovan.golic@eitdigital.eu

Action Line Leader for Privacy, Security & Trust (PST)

5G ENSURE Workshop, Sophia Antipolis, June 16, 2016

Data Security and Data Privacy

- **Cyber security** − Data security in cyberspace
- **Cyber privacy** − Data privacy in cyberspace
- ***Data security:*** *Data confidentiality, data integrity, data availability, entity authentication/identification*
- ***Data privacy:*** *User's control + Security of sensitive data*
  - About citizens, private or public companies, institutions, and organizations (**personal**, financial, industrial etc.)
  - During the whole life cycle of data
  - Minimal disclosure principle
  - Minimal trust principle
  - Addressed by privacy policies and cryptographic techniques
- **Cyber surveillance** is useful for government agencies and law enforcement to detect & investigate social threats and crimes in cyberspace and physical world

Challenges

- *Attacks in cyberspace multiply rapidly and evolve dramatically and traditional reactive approaches are insufficient to deal with them effectively*
- *Uncontrolled mass user/citizen profiling by online service providers and abuses of surveillance practices by government agencies are a great threat to data privacy*
- *How to reconcile cyber privacy with cyber surveillance?*
- *Great market opportunities, but EU ICT security market is fragmented along national borders and constrained to high-security military and government segments, without much business prospects*
- ***Data protection laws and regulations in EU do not match the challenges***

Name of the Game

- *Tradeoff:* Privacy ↔ Security in physical space
- ***No tradeoff:*** Cyber privacy ↔ Cyber security
  - Unlike common belief
  - *No cyber privacy → Sensitive data exposed to attacks & abuses → No cyber security*
- ***Tradeoff:*** Cyber privacy ↔ Cyber surveillance
- ***Blocking factor for cyber privacy and business!***
- *Cyber surveillance is not cyber security!*
- *Cyber monitoring can be used for cyber security, but requires trusted parties*
- ***How to enforce cyber privacy with focused & lawful cyber surveillance?***

Cyber Surveillance

- **Mass surveillance collides with human freedom**
- Focused & lawful exceptional access to data for cyber investigation is needed
- Refers to metadata and/or content
- *Difficult to trust entities, as data are easy to copy*
- Security chain is as strong as its weakest link

  humans → crypto algo & prot → keys → SW → HW
- *Backdoors or trapdoors, used in practice for cyber investigation, lead to mass surveillance & abuses*
- Best achieved through keys (key escrow)
- *Focus on data source, time, but also data type!*
- **Status quo can only worsen the situation!**

User/Citizen Profiling

- User profiling means collecting, processing, and modelling of user data over a period of time
- User profiling is useful for:
  - **Personalized and targeted** information, advertising, services, social contacts etc.
  - **Security:** authentication by behavior-based anomaly detection
- Mass user profiling becomes mass citizen profiling if user identity attributes are associated with user profiles!
- Mass user/citizen profiling collides with human freedom
- **User profiling for targeted advertising can be done locally (regulations and practices need to be changed)**
- **Big data analytics should be based on appropriately anonymized data**

Strategy of PST Action Line

- **Address cyber security and privacy proactively, by deploying trustworthy and transparent innovative technologies bridging the gaps between available techniques and practice**
- **Promote security-by-design and privacy-by-design paradigms**
- Foster both cyber privacy and cyber security
- *Develop and put into practice cost-effective certification & auditing procedures (e.g., for SW and HW)*
- *In synergy with other EU organizations, influence EU legislation authorities to improve data protection laws*
- Enable lawful & focused cyber investigation
- **Let data security and privacy become business opportunity rather than obstacle**

Advanced Crypto Techniques for Privacy

- ***Secret sharing*** *(no single points of trust and failure)*
- ***Secure multiparty computation*** *(joint computation of functions without disclosing own data, e.g., end2end)*
- ***Practical homomorphic encryption*** *(processing of encrypted data, e.g., in the cloud)*
- ***Privacy-preserving profiling*** *(without revealing user data, not only pseudonymization and data aggregation)*
- ***Anonymity protocols*** *(e.g., anonymous credentials)*
- ***Revocable anonymity*** *(if needed)*
- ***Attribute-based encryption*** *(cloud data sharing by applying access policies on encrypted data)*
- ***Searchable encryption*** *(search over encrypted data)*
- ***End2end encryption*** *(key escrow with secret sharing for lawful interception, if needed)*

Key Escrow with Forward & Backward Secrecy

- **Master key escrow via secret sharing and session key recovery via shared decryption (in SW or HW)**
- *Session key is encrypted by master public key and appended to message encrypted by session key, for a given user*
- Secret master decryption key is shared-escrowed among independent agents, but never recovered, using the property that decryption function is homomorphic in this key
- Escrow agents compute partial decryption functions on their shares and then combine them into the session key *(threshold cryptography)*
- Cooperation of agents needed for each session key
- Forward & backward secrecy satisfied
- Focus easy to implement

Privacy & Security in the Internet of Things

- Things relate to objects such as various sensors, meters, actuators, and controllers placed in embedded computing devices and connected to the Internet; power and connectivity constraints
- Sensitive data need to be protected by design (e.g., e-health, smart home, smart energy)
- Lightweight encryption and MACs: secure, but with shorter keys and smaller security margins in the design
- Fully homomorphic encryption via trans-encryption!
- Use of backend servers for scalable and practical authentication and authorization
- Use of Physical Unclonable Functions (PUFs) on embedded chips for identification of things – analog of biometric templates
- Use of attribute-based encryption for data sharing, where access policies are enforced on encrypted data without decryption

Attribute-Based Encryption

- **Shared access to encrypted data:** One public encryption key and multiple private decryption keys; only users whose private keys satisfy the access structure can decrypt
  - Access policy/structure is a predicate over attributes, e.g., containing conjunctions, disjunctions, and (k,n)-threshold gates
  - E.g., for attributes {A,B,C,D}, an access policy is A∨(B∧C)
- ***Collusion resistance:*** By pooling their private decryption keys, users cannot get any advantage
- **In ciphertext-policy case,** the access policy is built in the ciphertext and the subsets of attributes are built in private decryption keys of the users
  - E.g., for A∨(B∧C), user with {A,B} can decrypt, while user with {B} cannot
- **In key-policy case,** the set of attributes is built in the ciphertext and the access policies in private decryption keys of the users
  - E.g., for {A,B,C,D}, user with A∨B can decrypt, while user with D∨F cannot

Privacy and 5G-ENSURE

- Privacy is a challenge in 5G network
- 5G-ENSURE project considers privacy a key enabler for 5G
- Some privacy enablers have been identified and specified during the first period of the project . Some of them take into account the suggestions and expertises coming from the PST AL.
  - A mechanism for user identity protection based on the KP-ABE has been proposed
  - A mechanism based on the key escrow approach is also under investigation for providing an end-to-end encryption service with lawful interception when needed.

5G-Ensure

5G Enablers for network and system security and resilience

5G-ENSURE: http://www.5gensure.eu

contact@5gensure.eu

@5GEnsure

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 – October 2017

The 5G Infrastructure Public Private Partnership (SG PPP)