Towards Privacy, Security & Trust in Cloud Services

Jovan Golić

Chip-to-Cloud Security Forum 2014

EIT ICT Labs

- EIT ICT Labs is one of the first Knowledge and Innovation Communities set up in 2010 by the European Institute of Innovation and Technology (EIT), as an initiative of the European Union
- There is an urgent need to strengthen the ICT competence in Europe
- EIT ICT Labs' mission is to drive European leadership in ICT innovation for economic growth and quality of life, through Co-location centers, network of partners, and business development accelerator
- This is achieved by linking Education, Research & Business and by funding finalization stages of research aiming at bringing to market innovative ICT products and services, through 1-year projects conducted by the partners
- 8 thematic action lines

http://www.eitictlabs.eu

Data Security

- **Data integrity** – tag for detection of unauthorized changes
- **Data confidentiality** – reversible transformation of data
- **Data availability** – redundancy, dynamic testing, recovery
- **Entity authentication and identification** – verification of real-world physical/logical attributes, time of communication, protocols

- **Security is relative to attacks** – types, objectives, impact, scale
- **Security is relative to attackers** – skills, sophistication, resources
- **Security has a cost** – widespread usage reduces the costs and enables security-by-design

- **Security as a business opportunity rather than an obstacle**

Digital Trust

- ***Level of confidence that a product or service or process in digital world is functioning accordingly*** – relative, conditional, time dependent
- **Has a subjective component and an objective component, which can be called trustworthiness**
- **Best practices and reputation are fundamental**
- **The problem is that data security is complex, relative, conditional, difficult to verify**
- **Trust + Distrust + Uncertainty = 1**
- Increase trust directly or by decreasing distrust or uncertainty
- **Factors:** *policies and agreements, liability, reputation, best practices, assurance levels, technical and technological assurance, transparence, verifiability, auditing, cost-effective certification, information sharing, awareness, knowledge*

Software Security

- *Standardized cryptographic algorithms and protocols used for data security are subject to public scrutiny and trustworthy*
- *Many proprietary ones turned out to be weak after being exposed*
- **Software products (operating systems, middleware, applications) are frequently proprietary and obfuscated; trustworthiness w.r.t. data security is then not well anchored**
- **SW and SW updates can be authenticated/certified by digital signatures issued by using trusted public keys, possibly associated with trusted entities**
- **Untrusted applications can be separated from the trusted ones, by using trusted execution environment or virtualization**
- Detection of malicious applications and intrusions by signature-based or anomaly-based techniques, centralized or distributed, possibly in sandboxing environment, is fundamental for data security; their effectiveness needs to be improved

Virtualization Security

- **Virtualization is fundamental for cloud services**
- **Hypervisor is SW running on host platform, for generating and supporting guest Virtual Machines (VMs)**
- **Isolation of guest VMs is fundamental for virtualization security**
- **Proving the isolation and other properties of hypervisor by formal security analysis is a challenge**
- **Hypervisor can be transparent and open for verification or certified; this can significantly improve trustworthiness**
- Assuming that the host platform is trusted, security of guest VMs and distributed middleware (intrusion and anti-malware protection including APTs) can be efficiently controlled by the monitoring SW process running on the host
- Virtual monitoring and IDS can be introduced on the network level
- **Insider security:** *traceable system administrator interventions, integrity of logs and audit trails, strong authentication, shared access & control, separation of duties*

Hardware Security

- **The cloud system can be secure on SW level, but insecure on HW level**
- **Strong HW platforms and architectures (including self-checking circuits) are important, especially w.r.t. sophisticated attackers**
- **Transparent and auditable HW fabrication facilities are preferable, but difficult to implement**
- HW devices connected to the cloud, such as smart meters and various sensors, especially if they generate sensitive data, need to be strongly authenticated/identified by using cryptographic keys or chip templates such as Physical Unclonable Functions (PUFs)
- **Such devices should better be run on open or standardized OS guided by the simplicity and security principles**
- **Secure key generation & management (HSM, secure element)**
- **Usage of HW security tokens (HST) for strong user-to-HST-to-cloud authentication**
- *HW/SW implementations of cryptographic algorithms and protocols running on sensitive data should be resistant to side-channel attacks*

Data Privacy - 1

- **Data privacy is about the security of personal data and of any sensitive data regarding citizens, private or public companies, institutions, and organizations**
- **Data privacy is also about the user's control of sensitive data according to the minimality principle**
- **Minimality principle:** *Sensitive data should be controlled by the user during the whole lifecycle and disclosed to the lowest possible extent for a minimum period of time only to entities and for purposes authorized by the user. Ideally, this principle should guide the balance between data disclosure and usability. Rarely applied in practice.*
- **One reason** is massive user profiling by online service providers, since user data has market value. **Another reason** is the surveillance and lawful interception by government agencies and law enforcement authorities to help detect and monitor social threats, and detect, track, and investigate criminal or terrorist activities.
- **Alert:** *Massive user profiling becomes massive citizen profiling if identity attributes are associated with user profiles*

Data Privacy - 2

- **Privacy of sensitive data (e.g., personal data, IoT data, and industrial secrets) w.r.t. to system administrators appears to be the biggest risk of the cloud business, in view of the fact that data protection laws are relative to the physical location of data**
- **Privacy paradigm shift:**
  - *Support data privacy by practical advanced cryptographic techniques, including privacy-preserving data mining and profiling, secure multiparty computation, practical homomorphic encryption, secret sharing, threshold cryptography, anonymization, anonymity protocols, anonymous credentials, attribute-based encryption, format- and syntax-preserving encryption, searchable encryption, end-to-end encryption, and SW obfuscation, in addition to traditional techniques*
  - *Enforce the minimality principle*
  - *Address accountability by techniques for revocable anonymity*
- **Protection of sensitive data requires privacy-aware security platforms and mechanisms in both software and hardware**

Business Opportunities

- **ICT business at risk:** The worldwide ICT security technology and services market is growing more than 11% annually, to reach €92 billion in 2017. By 2020, it is estimated that €440 billion of the added value is at risk if the leveraged data are not appropriately protected.
- **Significant market opportunities:** Market share of European companies in industry solutions for data security and privacy (≈16.5%) is lagging behind their global ICT market share (≈25%).
- *This is possibly due to fragmented national regulations and government control, as cyber security and privacy are considered to be matters of national security and safety. European technology solutions in this area potentially have a comparative advantage with respect to trustworthiness.*
- In after-Snowden era, enterprises, institutions, and organizations hesitate to send their sensitive data to the cloud. This implies that the business opportunities for deploying innovative solutions offering higher assurance for data privacy are significant.

Action Line for Privacy, Security & Trust

- **Mission:** Support users and businesses in protecting their digital assets and transactions, promoting robust and safe products and services that realize data privacy and security
- **Market opportunities:** Great and unexploited
- **Privacy:** *Security & User's Control of sensitive data*
- **Minimality principle:** Disclose sensitive data to a minimum extent
- **Misconception:** *Cyber security is possible without privacy*
- **Strategy:** *Address cyber security and privacy by using more secure, trustworthy, and transparent innovative technologies bridging the gaps between available techniques and practice; promote* ***«security & privacy by design»*** *paradigm; raise social awareness*
- **Focus 2014-2016:**
  - Privacy-aware federated ID management & strong authentication
  - Data privacy in online/mobile applications, services & communications
  - Protection against malicious software & intrusion detection/prevention on computing devices, especially on mobile platforms

EIT ICT Labs

IDEA CHALLENGE

8 topics. 8 cities. One challenge.

CYBER SECURITY AND PRIVACY

Action Line for Privacy, Security & Trust

What it is:

A business ideas contest to support early stage startups and young innovators and researchers

Who can apply:

- At least one EU28 citizen (or legal resident) per team
- Applying startups have to come from EU28

Winners will get:

1st Prize: **40 k€**
2nd Prize: **25 k€**
3rd Prize: **15 k€**

+

- **Coaching and mentoring** from the EIT ICT Labs experts
- **Office space for up to 6 months** in one Co-location Center
- **Integration into pan-European partner network** and future EIT ICT Labs activities

Applications are open from 1st to 30th of September

http://ideachallenge.eitictlabs.eu