PRIPARE

PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Best Practices at Research Level

Hisain Elshaafi

Telecommunications Software and Systems Group (TSSG)

Waterford Institute of Technology, Ireland

Outline

- Aspects of Best Practices
- Research of Privacy Best Practices
- Best Practices for the Cloud
- Best Practices in Mobile Services
- Privacy Best Practices in Research Projects
- Conclusion

Aspects of Best Practices

1. Privacy best practices in research projects
   - Part of research **ethics**
   - E.g. health, education, market research
2. Privacy(-related) best practices
   - Privacy Impact Assessment (**PIA**)
   - Privacy and security **patterns**
   - OASIS Privacy Management Reference Model (**PMRM**)
   - Privacy & security best practices e.g. **OWASP** Privacy Protection Cheat Sheet, ISO/IEC 2700x
   - National and International guidelines e.g. **OECD** privacy principles, **CNIL** privacy risk guidelines

Research of Privacy Best Practices

- **General** privacy and related best practices and guidelines
  - Coding best practices
  - Data minimisation and management in relation to limitation of data quantity, time, sensitivity
- **Domain** specific
  - Mobile services
  - Cloud
  - Social media
  - Smart grid
  - RFID
  - Healthcare systems

Best Practices for the Cloud

- Policy
  - Defines privacy-related rules and states reasons
  - Varies in scope between IaaS, PaaS and SaaS
- Risk management
  - Guidelines on assessing, addressing and reducing risks
- Data encryption
  - Key and certificate management
- Data storage
  - Encrypted data and user data isolation
- Event auditing and reporting
  - Levels of logging, confidentiality agreements, secure archiving, etc.

Best Practices for the Cloud

- Vulnerability scanning
  - Vulnerability and penetration testing, compensation.
- Identity and access management
  - Identity management, personnel access, least privilege principle, granularity, RBAC, Separation of Duties
- Configuration management and change control
  - well-defined, govern changes, identify consequences, assurance
- Network security, Transparency, Monitoring and traceability,...

Best Practices for Cloud Consumers

- Selection based on CSPs'
  - Current **security practices and controls**
  - **Transparency** into security and privacy practices
  - Security **needs** inline with CSP security
  - **Data encryption** (at rest/in motion)
  - Monitoring CSP Infrastructure and policy **changes**

Best Practices in Mobile Services

- App **developers**
  - E.g. policies, PII collection limitation
- App **platform** providers
  - E.g. user education guidelines, reporting tools for privacy violations, app developer education
- **OS** developers
  - E.g. global privacy settings, OS vulnerabilities
- Marketing and **advertising** networks
  - E.g. ad access rights to user services, ad context
- Mobile **operators**
  - E.g. customer and parent mobile privacy education

Evaluation of Best Practices

- Ease of use
  - requires **completeness** of description e.g. context and problem **not only** techniques
- Sufficiency
  - **Distribution** of **types** of best practices and patterns -> attack and misuse patterns, countermeasures, security specifications
  - **Lifecycle** phases -> requirements, design, implementation
- Effectiveness
  - measure using security or privacy **metrics** e.g. frequency of violations

Privacy Best Practices in Research

- Justification of **data requirements**
  - In relation to research objectives and scope
  - Defined purposes
- **Minimisation** of personal data
  - collection, identifiability, sensitivity, anonymisation
- **Consent**
  - For collection, use and disclosure
  - practicality, forms of consent (opt-in, opt-out)
  - documentation and management of consent
- **Informing** participants
  - e.g. understandable language, enough time

Privacy Best Practices in Research

- Protection of personal data and **access** control
  - Institutional, physical and technological measures
  - Risk assessment
- Limit on data **retention**, **use** and **disclosure**
  - As long as necessary
  - Plan on publication of results
  - Sharing for research purposes
- **Accountability** and **transparency** in data management
  - Clearly defined roles and responsibilities of individuals
  - Open policies and practices
  - Dialogue with community

Conclusion

- Privacy related **guidelines**, policies, patterns, models and templates
- **Custom best practices** for cloud, mobile, etc
- Best practices for different **stakeholders**
- **Ethics** in research

PRIPARE

PReparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **RE**search

Questions?

Email: helshaafi@tssg.org