PrimeLife

Reference Group Meeting

March 23 – 24, 2009

Activity 2: Mechanisms

A research project funded by the European Commission's 7th Framework Programme

Problem statement

Huge amount of data about individuals is collected, processed, shared, and communicated

- Growing concerns and demand for privacy by users
- Requires techniques addressing the different issues and threats that can put privacy at risk in the different stages of the information lifecycle

$\Longrightarrow$ Need to invest on research to fill the gap between needs for privacy and what today's technologies provide

Objectives

Perform research for better understanding the open problems and providing novel solutions to their satisfaction

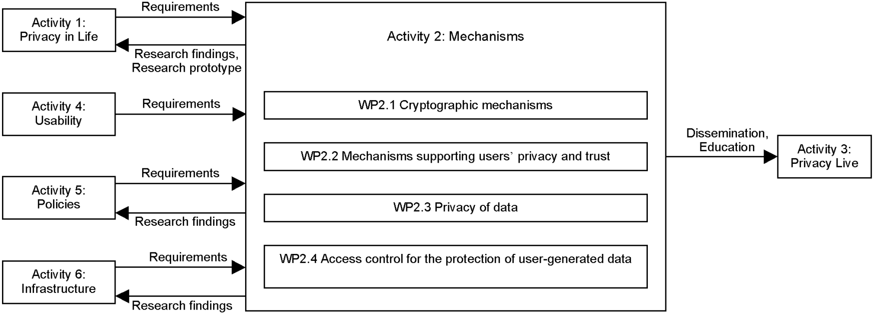
- Provide state of the art foundations
- Provide rigorous scientific analysis of privacy requirements and threats
- Provide novel techniques solving open problems
- Produce proof-of-concepts prototypal tools

Work packages in Activity 2

Broad in scope touching different aspects of the complex privacy problem

- Cryptographic mechanisms (WP2.1)
- Mechanisms supporting users' privacy and trust (WP2.2)
- Privacy of data (WP2.3)
- Access control for the protection of user-generated data (WP2.4)

Relationships with other activities



Cryptographic mechanisms (1)

Goal: research on cryptographic techniques for the support of privacy and trust

- The scenarios of Activity 1 raise a number of open cryptographic problems for which no solutions exist
- Cryptographic mechanisms for privacy and trust
  - anonymous credentials, delegation of credentials, searchable encryption, oblivious service
- Trusted wallet that allows users to securely manage their cryptographic key materials

Cryptographic mechanisms (2)

Research results: improvements of the state of the art in different areas

- Advancement in the area of anonymous credential systems
- Investigation of how to incorporate privacy friendly service selection and payment protocols into systems supporting private service access
- Delegation of anonymous credentials
- Selective access control in social networks
- Trusted wallet, focusing on high security compartment
- Biometries: Match on card

Supporting users' privacy and trust (1)

Goal: study different approaches that help to preserve or even control the users' privacy and to support interaction and collaboration of group/community members

- Transparency tools
- Privacy measurement
- Privacy-respecting establishment of collaborative groups
- Trust management by interoperable reputation systems
- Privacy awareness

Supporting users' privacy and trust (2)

Research results: investigation of privacy requirements individuals and communities have when interacting with each other

- Survey on transparency tools and categorization
- Investigation of techniques of privacy measurements
- Analysis of collaborative groups and identification of privacy issues
- Jason reputation system
- Analysis of the requirements on tools to support privacy awareness

Privacy of data (1)

Goal: investigation of novel solutions and tools for guaranteeing the privacy of potentially large collection of data referred to individuals

- Privacy assessment and privacy metrics to be able to talk about the privacy protection enjoyed by a data collection
- Techniques for enforcing data privacy and possible constraints that must be guaranteed on the data themselves
- Efficient organization and access to privacy-preserving data collections

Privacy of data (2)

Research results: novel solutions for enforcing privacy constraints in mobile networks and privacy requirements/constraints within business applications

- Analysis of privacy metrics
- k-anonymity privacy metric and multi-path communications for protecting the users's privacy
- Definition and management of privacy constraints capturing the protection needs of cooperating parties

Access control for protecting data (1)

Goal: design new solutions for defining and enforcing access control restrictions on user-generated data stored on external servers

- Dissemination control and secondary use restrictions
- Access control to confidential data stored at external services
- User-managed access control to personal data stored in trusted services

Access control for protecting data (2)

Research results: definition of techniques and models for protecting the personal information of users when it is stored on external servers

- Analysis of the requirements and current solutions for supporting user-controlled information dissemination
- Confidentiality of the privacy policies
- Protection of personal information derived from human biometric traits
- Analysis of dynamic access control mechanisms that can be driven by users for providing access to their data

Publications

First results presented at different leading international conferences, including:

- ACM CCS, the flagship conference of ACM SIGSAC
- IEEE ICDCS
- ASIACRYPT
- ACSAC

Future plans

- Exploit proposed solutions in other activities
- Continue investigation of the issues within the different WPs; also considering requirements coming from other activities
  - expand on proposed solutions
  - investigate new open issues
- Develop prototypes of some of the proposed solutions