Integrating novel cryptographic mechanisms into existing Identity Management Systems

Advisor(s): Felix Hörandner

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Current research activities are investigating the use of novel cryptographic mechanisms such as proxy re-encryption or malleable signatures in identity management systems. Especially, conditional proxy re-encryption and redactable signatures are promising.

Proxy Re-Encryption (PRE) extends asymmetric encryption, by enabling a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext encrypted for another user, without learning the underlying plaintext in an intermediate step. Conditional PRE further extends this, by only allowing this re-encryption operation, for data and keys that fulfill related conditions. This cryptographic concept enables secure end-to-end data sharing.

Redactable Signatures allow to redact (or black out) parts of a signed document, while the signature can still be verified on the remaining parts. With this cryptographic primitive, only a desired subset of a document can be disclosed to a receiver, while still ensuring the data's authenticity.

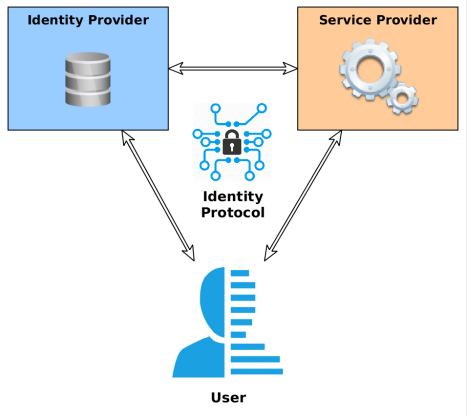
Both technologies offer very desirable features for an identity protocol. In such a protocol, the user is prompted to authenticate against an identity provider, which then releases attributes about the user to a service provider. During this data sharing process, the novel cryptographic mechanisms could be integrated. Therefore, in this project the feasibility of integrating novel cryptographic mechanisms into existing identity management systems should be demonstrated. This is done by extending an existing service provider and identity provider.

This topic is scalable from bachelor's to master's thesis. We can arrange and adjust the scope according to your scheduled effort, interests, and ideas.

Goals and Tasks

- Demonstrator of an identity management system using novel cryptographic mechanisms

Figure



Literature

- M Blaze, G Bleuner, and M Strauss
  Divertible protocols and atomic proxy cryptography
  EUROCRYPT 1998

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in identity management
- Interest in novel cryptography
- Programming skills

Advisor / Contact

felix.hoerandner@iaik.tugraz.at