Multi-Device Key Management and Recover

Advisor(s): Felix Hörandner

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

Motivation

Secure applications employing cryptography require users to use and store key material. As this key material has to be protected, it is often bound to the users' devices via Trusted Platform Modules (TPM). However, these devices (and keys) might get lost or stolen. Even in those events, users obviously do not want to lose all their encrypted data or allow someone to decrypt their data using stolen key material.

Additionally, users nowadays often own multiple devices (a PC, a phone, and a tablet), which all might have individual keys. Therefore, a user is not anymore associated with only one key. This results in the problem that data encrypted for one key can only be decrypted with the corresponding device, resulting in a usability nightmare.

To overcome these challenges, we could employ multi-hop proxy re-encryption. 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.

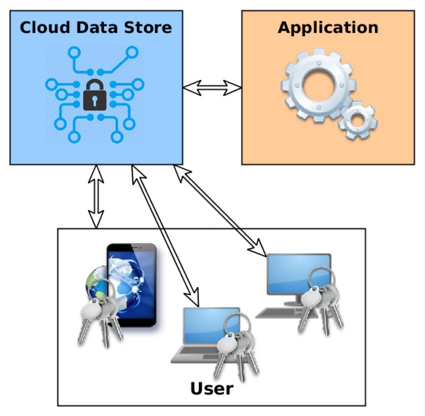
The goal of this project is to apply PRE in a cloud-based data sharing platform to achieve a user-friendly key recovery solution. There, we can build a chain of re-encryption operations to share data from one user's device over possibly multiple intermediate steps with another user's device. By modifying this chain, when individual links (devices) break, we can still securely access the data.

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

- Create and analyze concepts for key management
- Implement re-useable core libraries
- Implement a prototype app and cloud-service

Figure



Literature

- H.-Y. Lin
  Secure Content Distribution Using Multi-hop Proxy Re-encryption
  Wireless Personal Communications 2015

Deliverables

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

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in modern and user friendly IT security
- Programming skills

Advisor / Contact

felix.hoerandner@iaik.tugraz.at

Bachelor or Master Thesis Cloud and eIdentity