Semester- or Diploma Thesis

"Usage Control" in a secure messaging environment.

Institution: ETHZ

Supervisor: David Basin, Ralf Hauser

Team: t.b.d.

Background:

Increasing amounts of information are available, which support our lives in many beneficial ways. However, data is collected with ever increasing granularity and this can also threaten their “owning” individuals or subjects. Data protection laws were an early attempt to address these problems on a legal basis. Technically, so called “mandatory access control” (MAC) has existed since decades in highly structured institutions such as defense and secret service. The rigidity and inflexibility inherent to such systems, however limited the pervasiveness of their use significantly. Recently, some industries concerned with illegitimate consumption of protected assets (with intellectual property rights, e.g., music) have become interested in controlling the usage of such assets and mandate systems known under the term “digital rights management” (DRM) that attempts to further develop the kinds of copy protection mechanism to prevent software privacy that we remember from the 80ies and early 90ies. Such systems are often disliked, and thus the source of conceptual objections such as “fair use” arguments; moreover they are subject to the relentless searches for conceptual flaws and reverse engineering attempts by large global communities.

Ongoing research has, however, come up with promising frameworks to effectively model usage control with full acknowledgement of their limited enforceability. These frameworks allows data providers to formulate realistic usage control policies based on feasible provisions and consumer obligations and they can be complemented with effective observation and compensation strategies for detected violations in case a high-level policy is not fully enforceable.

The field of secure messaging is a prime candidate to prototype usage control architectures because, on the one hand, many basic ingredients to usage control such as authentication mechanisms at various levels, confidentiality- and integrity-methods are in daily use. On the other hand, users of such systems normally entrust it data with higher value to them and thus have an interest in adopting additional security measures such as "usage control". Therefore, they are more likely to accept the additional efforts required and adopt the process changes needed to implement some usage control, at least on the server side, as well as to accept possible convenience impacts on the client side.

Goal/Challenges:

- Define key use cases for high-level usage control policies that show high synergies with secure messaging.
- Determine a set of realistic provisions and obligations that can be implemented, predominantly on the server side.
- Define a set of low-level policies, enforcement and compensation mechanisms. (for certain data, only 2+ factor authentication, or not download only web-bitmaps, or higher minimum session key strengths, or limit viewability of certain documents to some locations, …)
- Design and implement on a secure messaging platform that realise usage control concepts.
- Test these prototyped usage control use cases with selected user communities.
- ...

General Requirements

- use a version control system (recommendation: svn)
- use an open source license
- use a modern, platform independent implementation technology (e.g. Java) / Java Skills
- use a modern quality assurance tool (justify if anything other than BugZilla)

PrivaSphere Role

- be a tutor; as well as a design, architecture, and technology discussion partner
- provide its secure messaging platform as a building ground for usage control architectures.
- provide space for a project- "product" in our BugZilla for quality assurance service and temporary SVN server space

If this is chosen as a diploma thesis, then both a more detailed analysis and a more complete implementation will be required.