Entwicklung eines Schlüssel-Management-Servers für Cloud-Dienste

Bachelorarbeit/Masterarbeit

BETREUER

Dennis Felsch, Paul Rösler

BESCHREIBUNG

Heutige Cloud-Dienste sind meist nicht mehr auf einzelne Geräte beschränkt: Man beginnt ein Dokument am PC, beendet es mit dem Tablet und verschickt es mit dem Smartphone. Das funktioniert, weil das eigentliche Dokument auf dem Server des Anbieters liegt, z.B. *Google Docs* oder *Microsoft Office Online*. Doch bei diesen Diensten haben die Anbieter Zugriff auf die Klartext-Dokumente und könnten diese offenlegen (durch einen Angriff oder staatlichen Zugriff / Gerichtsurteil, etc.).

Nutzt man Verschlüsselung, so verhindert man zwar den unbefugten Zugriff auf die Dokumente, jedoch steht man vor dem Problem, wie man allen seinen Geräten die notwendigen Schlüssel sicher zur Verfügung stellt. Im Rahmen des Forschungsprojekts *SyncEnc* [1] wurde ein Konzept entwickelt, wie private und öffentliche Nutzerschlüssel so an die Nutzer und ihre Geräte verteilt werden können, dass das Kompromittieren des Schlüssel-Servers nicht alle Schlüssel offenlegt.

Im Rahmen dieser Arbeit soll das Konzept implementiert werden und an einen Single-Sign-On-Dienst angebunden werden. Es existieren bereits Vorarbeiten, wie z.B. eine Datenbank-Struktur für die Nutzerverwaltung, die für die Arbeit genutzt werden können.

WARUM IST DIESE ARBEIT SPANNEND?

- Du arbeitest direkt an einem aktuellen Forschungsprojekt des Lehrstuhls mit
- Im Rahmen des Projekts sind bereits Anknüpfungspunkte gegeben

ANFORDERUNGEN

- Programmiererfahrung in Java & Javascript sind hilfreich
- Wissen über Single Sign-On (z.B. aus *XML- und Webservice-Sicherheit*) erleichtert den Einstieg

[1] http://syncenc.de