28. März 2022 Studie · Privatsphäre & Krypto · Web & Cloud

Kryptographischer Zugriffsschutz: Transformation von Interaktiver zu Nicht-Interaktiver Proxy Re-Encryption

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Stand 2022-03-25
Quelle https://technology2.a-sit.at/veroeffentlichungen/kryptographischer-zugriffsschutz-mit-proxy-re-encryption/

Verschiedene kryptographische Mechanismen können eingesetzt werden um Daten sicher an ausgewählte Empfänger zu übertragen, entweder direkt oder nach Zwischenspeicherung in der Cloud. Proxy Re-Encryption ist ein solcher Mechanismus, der es zusätzlich erlaubt verschlüsselte Daten auch nachträglich für einen neuen Empfänger umzuverschlüsseln und somit zu teilen. Proxy Re-Encryption wurde auch erweitert um fein-granulare Zugriffskontrolle auf kryptographischer Ebene durchzuführen. Daten werden beim Verschlüsseln mit einer Liste von Attributen versehen. Über eine Policy basierend auf diesen Attributen kann die BesitzerIn der Daten festlegen, welche Ciphertexte umverschlüsselt werden können.

Proxy Re-Encryption kann durch Schemen realisiert werden, die entweder interaktiv oder nicht-interaktiv sind. Um die Umverschlüsselung zu ermöglichen, dh. einen Re-Encryption Key zu erzeugen, müssen bei interaktiven Schemen die privaten Schlüssel von Sender sowie Empfänger involviert sein. Dazu müssen Sender und Empfänger entweder ihre privaten Schlüssel an einen Teilnehmer offenbaren, oder zusammen Berechnungsschritte durchführen. Nicht-Interaktive Schemen benötigen zum Erstellen eines Re-Encryption Keys (um die Umverschlüsselung zu ermöglichen) neben dem privaten Schlüssel des Senders lediglich den öffentlichen Schlüssel des Empfängers. Dadurch sind nicht-interaktive Schemen eindeutig zu bevorzugen.

Ziel dieses Projekts ist es einen generischen Transformationsmechanismus zu entwickeln mit dem interaktive Proxy Re-Encryption Verfahren in nicht-interaktive Verfahren umgewandelt werden können. Diese Transformation soll nicht nur für klassiche Proxy Re-Encryption, sonder auch für Proxy Re-Encryption mit fein-granularer Zugriffskontrolle anwendbar sein.