Format Preserving Encryption

Fachgebiet: IT-Security
Betreuer: Prof. Dr. Reto Koenig
Experte: Stefan Berner (Diso AG)

Die nachträgliche Verschlüsselung von Daten kann eine grosse Herausforderung darstellen. Alle Applikationen, welche auf diese zugreifen, müssen aufwändig umgeschrieben werden, um mit den verschlüsselten Daten umgehen zu können. Auch ist oft eine Neugestaltung der Datenbank notwendig. Für solche Anwendungsfälle, in denen es nützlich wäre, wenn das Format von verschlüsselten Daten demjenigen des Klartextes entspricht, wurden Format Preserving Encryption Techniken entwickelt.

Ausgangslage

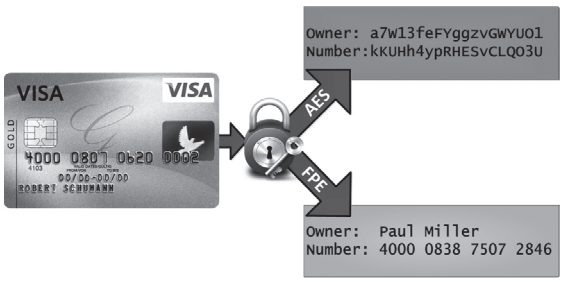
Für gängige Verschlüsselungsschemen wie AES spielt das Format der Verschlüsselung keine Rolle. Der resultierende Geheimtext ist ein Byte-Wert, dessen Format keinen Zusammenhang mehr mit dem ursprünglichen Klartext hat. Grundsätzlich ist dies auch erwünscht, denn man soll von einem Geheimtext keine Rückschlüsse auf dessen Klartext ziehen können.

In gewissen Anwendungsfällen wäre es jedoch praktisch, wenn der verschlüsselte Wert das gleiche Format aufweist wie der Klartext. Also das beispielsweise eine Kreditkartennummer wieder in eine gültige Kreditkartennummer verschlüsselt wird.

Mit solchen Szenarien beschäftigt sich Format Preserving Encryption (FPE). Eine Verschlüsselungstechnik, die in der Kryptographie aktuell (noch) ein Schattendasein fristet.

Ziele

Ein Ziel unserer Bachelorarbeit war die Entwicklung einer Java-Bibliothek, die es erlaubt, FPE-Verschlüsselung einfach in eine bestehende (oder auch neue) Applikation zu integrieren. Um die bestmöglichen Algorithmen für unsere Bibliothek zu finden, haben wir im Vorfeld verschiedene Varianten von FPE-Techniken studiert und dokumentiert. Damit wir als nächsten Schritt anhand eines Tutorials den Einsatz von FPE an einem realitätsnahen Beispiel aufzeigen konnten, entwickelten wir anschliessend eine kleine Webapplikation, die eine e-Banking-Plattform simuliert und erweiterten diese mit einer FPE-Verschlüsselung. Als letztes Ziel integrierten wir unsere Java-Bibliothek in eine bestehende Android Applikation.



Unterschiedliche Verschlüsselung einer Kreditkarte mit AES und FPE

Android App

Die Integration der Verschlüsselung in eine bestehende Umgebung haben wir anhand der Open-Source-Android-App «OwnTracks» aufgezeigt. OwnTracks ist eine Tracking-App, die es erlaubt, GPS-Koordinaten mit anderen Benutzern zu teilen. Da auf öffentlichen Servern jeder Benutzer alle Standorte sehen kann, ist die Implementierung einer Verschlüsselung sinnvoll. So können nur noch ausgewählte Personen, die im Besitz des Kennwortes jenes Benutzers sind, dessen Standort entschlüsseln. Würde für diese Daten eine normale AES-Verschlüsselung verwendet, so würden ältere Versionen der App die verschlüsselten Koordinaten nicht interpretieren können und abstürzen. Mit Hilfe von FPE können nun einzelne Koordinaten aber wieder in gültige Koordinaten verschlüsselt werden.

Fazit

Als Fazit können wir sagen, dass FPE eine interessante Technologie ist, der bis jetzt vielleicht noch zu wenig Beachtung geschenkt wurde. In manchen Anwendungsgebieten würde ein Einsatz ein erhebliches Sicherheitspotential schaffen. Anhand von zwei praktischen Beispielen konnten wir aufzeigen, dass eine nachträgliche Integration einer Verschlüsselung nicht unmöglich, im Gegenteil mit FPE sogar verhältnismässig einfach realisiert werden kann.

Matthias Liechti
matthiasliechti@hotmail.com

Rizja Elias Schmid
rizja.schmid@gmail.com