Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

Schlüsselmanagement und Verschlüsselung für Multicast-TV-Streams

BA21_neut_04

BetreuerInnen: Stephan Neuhaus, neut
Fachgebiete: Information Security (IS)

Studiengang: IT
Zuordnung: Institut für angewandte Informationstechnologie (InIT)
Industriepartner: Init7 (Schweiz) AG (8406 Winterthur)

Gruppengrösse: 3

Kurzbeschreibung:
Kunden von init7 erhalten TV direkt per Multicast-Signal oder per HLS (sowohl Live- als auch Replay-TV). Diese Streams sind soweit unverschlüsselt und können vom Kunden relativ einfach aufgezeichnet werden. Gewisse Privatfernsehsender verlangen aber für die Ausstrahlung in HD einen Kopierschutz bzw. eine Verschlüsselung der Streams.

In dieser Arbeit soll eine Komponente für das Multicast-System konzeptioniert und umgesetzt werden, welche diese Verschlüsselung macht. Eine besondere Herausforderung und das Kernstück der Atbeit wird dabei das Schlüsselmanagement sein.

In Scope sind:

* Eine Beschreibung der bestehenden Architektur * Eine Beschreibung der Anforderungen an das zu erstellende System - Welche Streams sollen verchlüsselt werden

- Welche Streams sollen verchlüsselt werden - Wozu soll die Verschlüsselung dienen? (Absicherung des Transports, Verhinderung einer Aufzeichnung, ...) * Ein Threat Modeling der vorgeschlagenen Lösung als Teil des Requirement Engineering (mit DFD/STRIDE und/oder attack trees) * Eine Übersicht über bestehende Technologien zum Verschlüsseln von Videostreams * Klärung der Frage, wer welche Schlüssel besitzen muss, wie die da hin kommen und wie die auf den Zielsystemen geschützt werden können und müssen. Das wird der theoretische Hauptteil der Arbeit sein. * Prototypische Implementation des Schlüsselmanagements. Das kann der praktische Hauptteil sein.

Out of Scope sind:

* Prodktive Implementationen (wenn die Prototypen auch produktiv einsetzbar sind, umso besser, aber muss nicht) * Anbindung an oder Implementation von Standards wie FairPlay. Hier reichen gemockte Interfaces. Grund: FairPlay ist vermutlich sehr kompliziert und würde die Arbeit unzulässig verkomplizieren.

Unklar:

* Muss die Lösung mit bestehenden Systemen wie FairPlay kompatibel sein?

Voraussetzungen:
- Kenntnisse in Kryptogaphie

Die Arbeit ist vereinbart mit:
Nicolas Da Mutten (damutnic)
Daniela Egli (eglida03)
Andreas Meier (meiera25)