Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

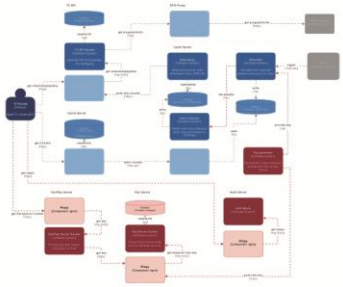
InIT Institut für angewandte Informationstechnologie

Schlüsselmanagement und Verschlüsselung für Live-Videostreams

Diplomierende
Nicolas Da Mutten
Daniela Egli
Andreas Meier

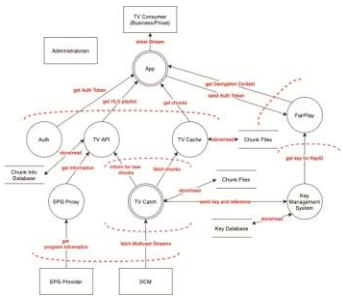
Dozent
Gürkan Gür

Obwohl Streaming-Dienste immer mehr an Bedeutung gewinnen, sind Liveübertragungen für Telekommunikationsanbieter weiterhin ein wichtiges Thema. Denn gerade bei Sport und Reality-TV ist die Lizenzierung von Streaming-Material essenziell, da mit diesen Übertragungen viel Geld erwirtschaftet wird. Es gibt aktuell viele kommerzielle Digital Rights Management (DRM)-Lösungen, aber keine modularen, quelloffenen Systeme und sehr wenig wissenschaftliche Literatur dazu. Deshalb war das Ziel dieser Arbeit, einen Architekturentwurf für ein modulares Key Management System zu entwickeln. Ausserdem sollte ein Prototyp dieser Architektur umgesetzt werden. Dazu wurden zuerst Literaturrecherchen durchgeführt. Anschliessend wurde nach dem Security Development Lifecycle vorgegangen. Dabei wurde eine Bedrohungs-analyse erstellt, welche beim Entwerfen der Architektur verwendet wurde. Der Entwurf sieht zur einfachen Skalierbarkeit des Systems den Einsatz von Microservices vor. Durch diese modulare Architektur können in Zukunft auch andere DRM-Systeme und Verschlüsselungsarten einfacher in die Lösung integriert werden. Auf dieser Basis wurde entschieden, dass der Prototypmit FFmpeg als Transmuxer, Apple FairPlay Streaming (FPS) als DRM-System und AES-128 als Verschlüsselungsalgorithmus umgesetzt wird. Anhand des Architekturentwurfes wurde ein Key Generator entwickelt, welcher pro Kanal Schlüssel generiert und diese an die Key Serversendet. Die Key Server speichern die Schlüssel in einer zentralen Datenbank und stellen diese den DRM-Systemen zur Verfügung. Der FPS Server holt die Schlüssel beim Key Server ab und stellt diese dem Client per FPS-Schlüsselaustausch zur Verfügung.



Architekturentwurf für ein modulares Key Management System

Die entworfene Architektur zeigte sich als solide und zweckmässige Lösung. Doch gerade in puncto Skalierbarkeit und Ausfallsicherheit hat er noch Potenzial. Beispielsweise ist die Schlüsseldatenbank nicht redundant und stört bei einem Ausfall den Betrieb des gesamten Systems. Weiter können bei der aktuellen Architektur die Schlüssel nicht bereits im Vorfeld an die Clients verteilt werden. Dies kann zu Überlastung und Ausfall des Systems führen. Der Prototypwurde gemäss Architekturentwurf umgesetzt und getestet. Jedoch funktioniert die Wiedergabe der verschlüsselten Streams nicht, da FFmpeg kein Sample-AES unterstützt und das für FPS benötigt wird. Anhand des Datenstroms und des Schlüsselaustauschs wurde bestätigt, dass die restlichen Funktionen des Prototyps wie gewollt funktionieren.



Data Flow Diagramm der entworfenen Architektur