Internet and Web Applications, Übung 8

Henry Haustein

Aufgabe 1: Multicast Communication on the Internet

Weaknesses:

- only for live events, not for video on demand
- client software must be deployed, managed and updated
- slower start times/delays duw to push architecture
- network switches and wireless access points must be multicast enabled
- network locations not multicast enables will not benefit

https://www.rampecdn.com/enterprise/what-is-multicast/

Aufgabe 2: Streaming on Video-on-Demand Portals

Netflix nutzt MPEG-DASH und CDNs um seinen Content zu verteilen
https://ieeexplore.ieee.org/document/6195531

Aufgabe 3: Digital Rights Management (DRM)

Google Widevine ist eine proprietäre Technologie zur digitalen Rechteverwaltung (DRM) von Google, welche von den Webbrowsern Google Chrome und Mozilla Firefox, einigen Derivaten dieser Browser sowie Google Android MediaDRM, Android TV und anderen Geräten der Unterhaltungselektronik verwendet wird. Sie unterstützt verschiedene Schemata zur Verschlüsselung und Hardware-Sicherung, um den Zugriff auf verteilte Videodaten durch Endverbraucher nach den Regeln von Content-Eigentümern zu beschränken. In der Hauptsache bietet Widevine ein Content Decryption Module (CDM) als einen Client für Google Chrome und andere Browser und Geräte an. Von Inhalteanbietern kann Widevine kostenlos verwendet werden, da der Hersteller keine Lizenzgebühren für die Integration erhebt, auch nicht für die Integration in Geräten.
Die drei Sicherheitsniveaus von Widevine sind:

- L1 - keine Beschränkung auf die Auflösung oder HDR; höchste Stufe des Schutzes. Sowohl Kryptografie als auch Medienverarbeitung finden in einer vertrauenswürdigen Ausführungsumgebung (TEE) statt.
- L2 - (typischerweise) 540p Auflösungsbegrenzung. Nur die kryptografischen Operationen werden in einer TEE ausgeführt, die Medienverarbeitung nicht.
- L3 - (typischerweise) 480p Auflösungsbegrenzung. Nur softwarebasiertes DRM ohne Hardwarebeschränkung.

Widevine DRM wird mit Chromium-basierten proprietären Webbrowsern und auf Android benutzt. Es verwendet dynamisches adaptives Streaming über HTTP und HTTP Live Streaming. Widevine gehört zu

den DRM-Systemen, die in einem Browser von den Encrypted Media Extensions und den Media Source Extensions Gebrauch machen. Über dreißig Chipsets, sechs größere Desktop- und mobile Betriebssysteme, sowie Google-Produkte wie Chromecast und Android TV verwenden Widevine.
Konzerne wie Amazon Prime Video, BBC, Hulu, Netflix, Spotify und Disney+ verwenden Widevine DRM, um die Verteilung ihrer Inhalte zu verwalten.
Ebenfalls wird es von Mozilla Firefox seit seiner Version 47 im Jahr 2016 verwendet, und unter Microsoft Windows standardmäßig aktiviert. Unter Linux-Systemen wird dem Benutzer die Aktivierung von Widevine im Browser angeboten; dort kann er sie auch abstellen und deinstallieren. Vor der Einführung von Widevine verwendete Mozilla das Produkt Primetime DRM von Adobe für einige Versionen. Vor der Markteinführung der dafür notwendigen Hardwarevoraussetzungen in jeden multimediafähigen Computer wurden vor allem softwarebasierte DRM-Lösungen auf der Basis von proprietären Browser-Plug-ins wie Microsoft Silverlight oder Adobe Flash verwendet.
https://de.wikipedia.org/wiki/Widevine

Die Stufe L3 ist öffentlich gebrochen, es gibt ein Writeup dafür (https://github.com/tomer8007/widevine-l3-decryptor/wiki/Reversing-the-old-Widevine-Content-Decryption-Module). Die anderen Stufen sind auch entschlüsselbar, allerdings sind die Schlüssel nicht öffentlich verfügbar. Raubkopiergruppen müssen aber in Besitz dieser Schlüssel sein, anders ist es nicht erklärbar, dass wenige Minuten nach der Veröffentlichung einer Serie bereits Kopien existieren.