Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

A summary of Widevine

Widevine is a digital rights managment provider which is used by streaming services e.g. Netflix Spotify [1,2].
The Widevine Content Decryption Module (CDM) is embedded into all major browser to ensure compatibility with major streaming services.
Widevine was already attacks with the aid of a differential fault attack [3].
Also, ideas exist to attack Widevine running in a secure enclave [4].
Inside Widevine a white box implementation is used to decrypt and encrypt data [5].

[1] https://www.widevine.com/
[2] https://websites.fraunhofer.de/video-dev/enabling-hardware-drm-on-android-chrome-using-the-encrypte
[3] https://twitter.com/david3141593/status/1080606827384131590
[4] https://www.blackhat.com/docs/eu-17/materials/eu-17-Tang-Clkscrew-Exposing-The-Perils-Of-Security-
[5] https://www.matthieurivain.com/files/slides-cardis17.pdf

Contact

Request Topic

Advisors

Michael Gruber