Sujet de stage M2
Analyse formelle de sécurité de protocoles DRM

Laboratoire & institution : IRISA, CNRS & Univ Rennes, France
Équipe : SPICY – https://spicy.irisa.fr
Encadrants :

— Stéphanie Delaune (DR CNRS), stephanie.delaune@irisa.fr
— Joseph Lallemand (CR CNRS), joseph.lallemand@irisa.fr

Contexte général : Le monde du divertissement évolue rapidement. Les plateformes telles que Netflix, Amazon Prime Video et Disney+, ont révolutionné la manière dont nous consommons du contenu multimédia. La large distribution des médias dans des appareils contrôlés par l'utilisateur pose des problèmes à ces plateformes qui souhaitent éviter le piratage de leurs données.

Pour ce faire, ces plateformes s'appuient sur la gestion des droits numériques (DRM), une technologie qui vise à protéger les médias contre le piratage. Les systèmes modernes expédient les contenus sous une forme chiffrée, et contrôlent leur déchiffrement par le biais de modules autorisés sur les appareils des utilisateurs. La condition préalable au déchiffrement est le traitement de la licence correspondante. Une licence DRM décrit l'accord entre les fournisseurs de contenu, et le consommateur. Elle contient la clé de déchiffrement, les droits d'utilisation associés et les politiques de consommation que le module DRM est autorisé à appliquer. Compte tenu de leur caractère sensible, les licences sont protégées lorsqu'elles sont livrées au module DRM du client. Les mécanismes de protection sous-jacents sont propriétaires et uniques pour chaque système DRM. Il existe ainsi non pas un protocole de protection, mais une variété de tels protocoles [Pat23].

Compte tenu de l'importance et des difficultés inhérentes à la conception de protocoles sécurisés, la communauté de chercheurs s'est efforcée de fournir des fondements et des outils mathématiques solides pour la vérification assistée par ordinateur de ces protocoles. Depuis le début des années 1980, différentes techniques ont vu le jour, et il existe à l'heure actuelle des outils, *e.g.* Tamarin [BCDS22], ProVerif, permettant de réaliser des analyses formelles symboliques de protocoles cryptographiques [CK14]. Malgré les progrès récents, modéliser et mener à bien des preuves de protocoles déployés reste quelque chose de difficile et nécessitant une bonne expertise.

Une première étude formelle du DRM Widevine à l'aide de l'outil Tamarin a été menée et publiée à la conférence USENIX en 2024 [DLP+24]. Cette étude a permi de définir des objectifs de sécurité qu'un tel système doit satisfaire, de mettre au jour une vulnérabilité sur le système existant, et également de proposer un fix pour y remédier. Cet article servira de base au travail proposé dans ce stage.

Objectif du stage : Un premier objectif pour le stage consistera à étudier l'article publié à USENIX 2024 afin de comprendre les objectifs de sécurité qu'un système DRM doit satisfaire, et également comprendre le fonctionnement du protocole Widevine. L'étudiant ou étudiante devra également se familiariser avec l'outil de vérification Tamarin [1] qui sera utilisé au cours de son stage.

1. Outil Tamarin : https://tamarin-prover.com

L'analyse proposée dans l'article publié à USENIX 2024 comporte plusieurs limitations et ce stage a pour but de lever tout ou partie d'entre elles.

1. L'analyse de sécurité a été menée en supposant que les participants du protocole, et en particulier la plateforme, étaient de confiance. Or, il serait préférable de s'assurer que la sécurité du protocole ne repose pas sur cette supposition. Autrement dit, les médias proposés par la plateforme Netflix ne doivent pas pouvoir être consommés illégalement, et ce même si une autre plateforme distribuant des contenus est défaillante.
2. L'analyse de sécurité a par ailleurs été réalisée sur l'implémentation Widevine du protocole EME et ne tient pas compte du fait que d'autres fonctionnalités (hors du flux normal du protocole EME) peuvent être exploitées par un agent malveillant pour tenter de casser le protocole.
3. L'analyse existante ne prend pas en compte la modélisation du protocole permettant de distribuer et d'initialiser les clefs nécessaires au fonctionnement du protocole Widevine. Or des clefs initialement mal distribuées peuvent compromettre la bon fonctionnement du protocole.

Pour prendre en compte ces nouveaux aspects, les modèles Tamarin existants devront être adaptés et retravaillés, et l'analyse de sécurité devra être refaite sur ces nouveaux modèles.

Compétences attendues

L'étudiant ou l'étudiante devra avoir des bases solides en informatique fondamentale (*e.g.* logique). Des connaissances en sécurité seront utiles, mais ne sont pas nécessaires, et pourront être acquises pendant le stage.

Pour aller plus loin

Nous avons choisi Widevine en raison de sa prédominance, mais d'autres systèmes de DRM, tels que PlayReady et FairPlay, méritent bien sûr d'être analysés et pourront être étudiés pendant ce stage ou lors d'un travail de thèse qui s'effectuerait dans la continuité de ce stage. Un financement de thèse sur des projets de recherche en cours dans l'équipe, notamment le projet SVP du PEPR Cybersécurité [2], est disponible pour la poursuite de ce travail.

Références

[BCDS22] David Basin, Cas Cremers, Jannik Dreier, and Ralf Sasse. Tamarin : Verification of Large-Scale, Real World, Cryptographic Protocols. *IEEE Security and Privacy Magazine*, 2022.

[CK14] Véronique Cortier and Steve Kremer. Formal models and techniques for analyzing security protocols : A tutorial. *Found. Trends Program. Lang.*, 1(3) :151–267, 2014.

[DLP+24] Stéphanie Delaune, Joseph Lallemand, Gwendal Patat, Florian Roudot, and Mohamed Sabt. Formal Security Analysis of Widevine through the W3C EME Standard. In Davide Balzarotti and Wenyuan Xu, editors, *Proceedings of the 33rd USENIX Security Symposium, (USENIX'24)*, Philadelphia, PA, USA, 2024. USENIX Association.

[Pat23] Gwendal Patat. *Briser la confiance : dissection et analyse des impacts sécurité et vie privée du DRM widevine. (Bust the trust : dissect and analyze the security and privacy impacts of the widevine DRM).* PhD thesis, University of Rennes 1, France, 2023.

2. Site web du projet SVP : https://pepr-cyber-svp.cnrs.fr

[PSF23] Gwendal Patat, Mohamed Sabt, and Pierre-Alain Fouque. Your DRM Can Watch You Too : Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME. *Proc. 23rd International Conference on Privacy Enhancing Technologies (PETS'23)*, 2023(4) :306–321, 2023.