Extending MitMproxy for HTTP/2

ACRONYME	HTTP, HTTP/2, TLS, TCP
MANDANT	HEIA-FR
ÉTUDIANT-E-S	Josué Tille
PROFESSEUR-E-S	Rudolf Scheurer – Philippe Joye
EXPERT-E	Sylvain Luiset
No	B19T09
TYPE	Projet de bachelor
CONTACT	Josue.Tille@edu.hefr.ch, rudolf.scheurer@hefr.ch

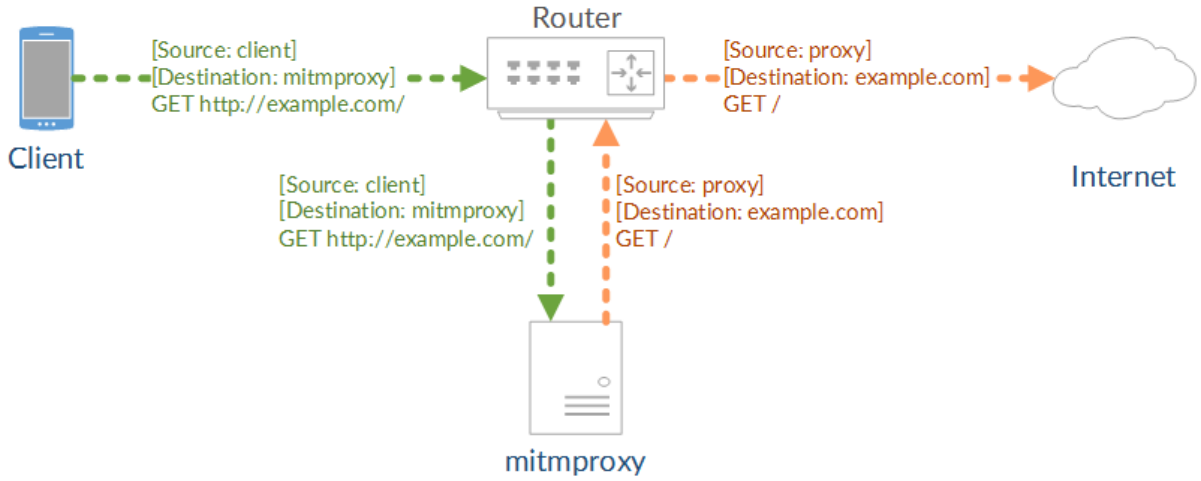
Dans la filière Informatique et télécommunication de la HEIA-FR, le protocole HTTP est enseigné. Afin que les étudiants comprennent le fonctionnement d'un protocole l'analyse de trafic est souvent utilisée.

L'arrivée de la nouvelle version du protocole HTTP (la version 2) a amené beaucoup de nouvelles fonctionnalités intéressantes. La HEIA-FR souhaitant aussi enseigner les nouvelles technologies, le protocole HTTP/2 devra aussi être enseigné. Selon les implémentations actuelles de HTTP/2, le trafic est toujours chiffré par TLS. Par conséquent il n'est pas possible d'analyser simplement les échanges sur le réseau de manière passive.

MitMproxy

MitMproxy est un logiciel libre qui permet d'intercepter du trafic HTTP et HTTPS. Pour le trafic HTTPS (chiffré avec TLS), une attaque Man-in-the-middle est effectuée afin d'intercepter le trafic. MitMproxy permet aussi de traiter des échanges en HTTP/2, cependant les spécificités liées au protocole HTTP/2 ne sont pas visibles.

MitMproxy est composé d'une part d'une partie backend qui permet de gérer le trafic échangé. D'autre part une partie frontend permet de gérer les échanges en les affichant ou en les sauvegardant.



Protocole HTTP/2

Le protocole HTTP/1.1 ayant plusieurs limitations une nouvelle version de ce protocole s'est imposée afin de résoudre ces lacunes. Le protocole HTTP/2 est une couche entre la couche de transport (TCP ou TLS) et les données textuelles HTTP/1.1 qui contiennent les requêtes GET ou POST. Cette nouvelle version de ce protocole permet notamment :

- le multiplexage des requêtes dans la même connexion TCP
- la compression des HEADER HTTP
- la priorisation du trafic
- au serveur d'envoyer des données qui n'ont pas encore été demandées.

But du projet

Le but de ce projet est d'introduire dans MitMproxy la possibilité de visualiser les échanges au niveau HTTP/2 avec toutes ses spécificités.

Comme on peut le voir dans la figure ci-dessous MitMproxy nous permet de voir le trafic HTTP avec une vue HTTP/1.1 (requêtes et réponses GET, POST, etc). Les échanges au niveau du protocole HTTP/2 ne sont pas visibles. Les informations suivantes ne sont par exemple pas visibles de base dans MitMproxy:

- Les HEADER des frames
- La notion de stream
- Les échanges pour la gestion de la connexion HTTP/2

Ce projet est composé des 3 principales parties suivantes :

- Implémentation d'une partie backend pour extraire les informations sur le trafic HTTP/2.
- Implémentation d'une partie frontend pour l'affichage des échanges
- Création de tests unitaires afin de valider le code implémenté.