IUT des Pays de l'Adour - Dpt RT - BUT2
SAE302 - Développer des applications communicantes

MQTT & Man In The Middle
Python, TCP/IP, Wireshark,...

Manuel Munier

Version 23 septembre 2025 (16:46)

Objectifs

Dans cette SAE vous allez explorer le principe des attaques *Man In The Middle* sur le protocole MQTT sur lequel vous avez déjà travaillé l'an passé.

Consignes du projet

- Le développement se fera en langage Python. Votre code devra impérativement être commenté et être lisible.
- Vous devrez rédiger un court rapport fournissant la description de votre travail à chaque étape (à chaque couche). Il ne s'agit pas de simplement fournir le code commenté ! À vous d'expliquer la logique de vos programmes et ce qu'apporte telle couche par rapport à la précédente. Bref, il vous faudra prendre un peu de recul...
- Une courte présentation ainsi qu'une démo seront exigées en fin de projet.

NB Comme pour toutes les SAE, il s'agit d'un **travail individuel**. Pendant les séances vous pouvez bien évidemment vous entraidez. Mais l'évaluation finale sera faite individuellement.

Évaluation

Vous serez évalués individuellement. À vous de préparer "ce que vous avez à nous montrer" ; il s'agit donc de préparer à l'avance les "scénarii" de votre démonstration afin d'éviter toute improvisation... Nous vous interrogerons bien évidemment sur la manière dont vous aurez réalisé vos programmes, sur le code source de vos programmes, etc. Prenez donc le réflexe de bien commenter vos programmes : ce sera plus agréable pour tout le monde.

Rappel L'objectif d'une SAÉ est "d'apprendre et de comprendre des choses", pas simplement de "nous montrer des programmes récupérés bêtement sur Internet ou chez un copain, voire générés par une IA" ! À bon entendeur...

Travail à réaliser

L'objectif de cette SAE est donc de capturer les trames TCP/IP des messages MQTT, d'en extraire les informations "utiles" (ex : *topic*, *payload*, adresses IP, etc.) puis de forger de nouveaux messages dans le but d'impacter les différents clients MQTT.

Dans une première réflexion nous pouvons décomposer le travail de la sorte :

1. capturer le trafic réseau ; vous pouvez pour cela utiliser des outils que vous maîtrisez déjà de part votre cursus : logiciel `Wireshark`, commande `tcpdump`, etc.
2. filtrer ce trafic, identifier les trames concernant le protocole MQTT, interpréter le codage et en extraire les données "utiles" (manuellement dans un premier temps)
3. automatiser ce travail avec un programme Python avec les librairies adéquates (ex : `Scapy` que vous avez déjà utilisée l'an dernier) ; ce module prendra en entrée un fichier de capture préalablement enregistré
4. en suivant une conception modulaire, écrire un autre programme Python pour automatiser la création et l'injection de nouveaux paquets MQTT dans le trafic
5. proposer une solution pour capturer/modifier/injecter les messages MQTT en temps réel cette fois...
6. étudier, concevoir et tester des "solutions" qui permettraient d'éviter ce genre d'attaques

Document rédigé en LaTeX sous Linux.