Rétro Ingéniérie et analyse d'une application Android

Les applications utilisées sur un téléphone Android ont souvent un comportement obscure : on ne sait pas exactement avec qui elles communiques, ce qu'elles communiques, et quand elles communiques.

Des plateformes comme Exodus Privacy analysent automatiquement les applications android pour y détecter des trackers (en cherchant certaines chaines de caractères telles que "com.google.android.gms.ads.mediation" ou des communications réseaux). Cependant, la détection est souvent passive : l'application est lancée, et aucune intéraction n'est effectuée par le système avec ces applications pour génerer du traffic réseau.

Le but de ce projet est de faire de la rétro ingéniérie sur une ou plusieurs applications android, et d'étudier les données transmises par ces dernières, principalement par l'analyse de trames réseaux.

Ce projet peut être séparé en plusieurs parties, modulables selon les préférences du groupe :

1. Man-In-The-Middle d'application Android à l'aide de mitmproxy (dans machine virtuelle) ;
2. Man-In-The-Middle d'application Android à l'aide de mitmproxy (sur un réseau WiFi) ;
3. Analyse statique d'APKs ;
4. Contournement de protections par le patchage d'applications ;

Références.

- Exodus Privacy : `https://exodus-privacy.eu.org/en/` ;
- Izly, l'appli du Cnous qui géolocalise des étudiants et renseigne des sociétés publicitaires : `https://www.lemonde.fr/pixels/article/2017/10/20/izly-l-appli-du-cnous-qui-geolocalise-5203902_4408996.html` ;
- MitmProxy : `https://mitmproxy.org/` ;
- « Comment Powned une application bancaire en 30 minutes » : `https://data.passageenseine.org/2017/aeris_powned-application-bancaire.pdf` ;

Note : Ce projet peut faire tenir deux groupes, par exemple l'un sur la partie "Android", l'autre sur la partie "ESP32".