Installation du proxy

Télécharger et installer Fiddler sur un PC Windows (https://www.telerik.com/fiddler). L'outil est gratuit.

Avec la configuration par défaut, Fiddler va démarrer un "proxy" sur le port 8888 de la machine Windows qui va tracer tout ce qui lui est envoyé.

Démarrer Fiddler, aller dans le menu Tools/Options puis sur l'onglet « Connections ».

Cocher la case "Allow remote computers to connect" pour permettre la connexion d'un périphérique distant (l'iPhone dans notre cas).

Il est également possible de modifier le port par défaut (8888)

Configuration du proxy sur l'iPhone

Il faut que l'iPhone et la machine hébergeant Fiddler soient sur le même réseau (ou des réseaux communiquant entre eux). Attention aux réseaux « guest » des routeurs qui cloisonnent en général les périphériques qui ne pourront se voir entre eux.

Configurer l'instance Fiddler comme proxy dans les paramètres wifi de l'iPhone :

- Aller dans Réglages / Wi-Fi
- Sélectionnez votre réseau wifi
- Tout en bas, cliquer sur « Configurer le proxy » et choisir « Manuel »
- Entrer l'adresse IP de la machine hébergeant Fiddler/Charles dans le champ « Serveur »
- Entrer le port du proxy dans le champ « Port » (8888)
- Redémarrer Fiddler

Démarrer la capture au niveau du proxy (« File / Capture traffic »).

Lancer une application ou Safari sur l'iPhone et s'assurer que la capture du trafic fonctionne bien.

Le trafic non sécurisé est visible directement. On peut accéder au détail des requêtes en utilisant l'onglet « Inspectors » de Fiddler.

Le trafic sécurisé (https / ssl / tls) est chiffré sur l'IPhone, il n'est donc pas possible de visualiser le contenu des requêtes.

Configuration du certificat SSL

Normalement, le trafic vers les serveurs distants est chiffré avec la clé privée de ce serveur, et ne peut donc être déchiffré que par lui-seul.

Pour pouvoir déchiffrer le trafic SSL/TLS, il va falloir installer sur l'iPhone un certificat unique généré par Fiddler. Le trafic sera alors chiffré avec ce certificat et pourra être visualisé dans Fiddler. Le proxy se chargera ensuite d'encoder la requête avec le certificat normal du site distant.

Le fonctionnement est donc celui d'une attaque « Man-In-The-Middle » ou Fiddler se fait passer pour le site distant du point de vue de l'iPhone. Cela nécessite d'installer ce certificat intermédiaire sur l'iPhone, et d'indiquer à iOS qu'on va faire confiance à ce certificat.

Ce fonctionnement était possible sur Android également, mais avec les dernières versions de l'OS, il n'est plus possible de faire accepter globalement aux applications ce certificat intermédiaire. Les applications ne peuvent plus faire confiance qu'aux certificats qui sont déclarés dans leur propre

configuration (manifest.xml). Il est toujours possible de contourner ce fonctionnement, mais cela nécessite de « décompiler » l'APK de l'application, de modifier le manifest pour autoriser le certificat de Fiddler, de reconstruire et signer l'APK modifié et de réinstaller l'application depuis ce package. Pour l'instant, ça fonctionne toujours sur iOS, jusqu'à ce qu'Apple décide d'implémenter une protection similaire (qui sera moins simple à contourner !)

La manipulation pour installer le certificat est la suivante :

- Dans Fiddler, aller dans le menu Tools / Options et l'onglet HTTPS
- Cocher les cases « Capture HTTPS CONNECTs » et « Decrypt HTTPS traffic »
- Cliquer sur le bouton « Actions » et choisir « Trust Root certificate ». Accepter les « warnings »
- Depuis l'IPhone, naviguer vers http://ipv4.fiddler:8888/
- Sur la page qui s'affiche, cliquer sur le lien « FiddlerRoot certificate »
- Accepter l'installation du « profil de configuration »
- Aller dans Paramètres / Général / Gestion des profils et de l'appareil
- Choisir le certificat « DO_NOT_TRUST_FiddlerRoot"
- Cliquer sur Installer, taper votre code de déverrouillage
- Cliquer une nouvelle fois sur Installer, puis une dernière fois sur le bouton Installer et Ok
- Aller dans Paramètres / Général / Informations, descendre tout en bas et choisir « Réglages des certificats »
- Activer le bouton à côté du certificat « DO_NOT_TRUST_FiddlerRoot » et valider par « Continuer »

Désormais, si vous accédez à un site chiffré (https) depuis Safari, la page doit s'afficher dans erreur.

Dans Fiddler, toutes les requêtes doivent être accessibles.

Capture des requêtes

Supprimer les requêtes déjà capturées dans Fiddler, et démarrer l'application à capturer.

Le détail des requêtes (http request / http response) est accessible via l'onglet « Inspectors » et les vues « RAW » (requête http brute) ou JSON/XML selon les formats échangés.

Les échanges peuvent être enregistrées dans un fichier pour être rechargés par la suite.

Attention, toutes les informations d'authentification sont visibles en clair dans les traces, et ce pour toutes les applications utilisées pendant que le profil est actif. Si vous devez envoyer les traces à quelqu'un d'autre, assurez vous qu'aucune information privée n'est présente. Supprimer les requêtes concernées le cas échéant.