Analyse réseau :
ntercepter le traffic entrant et sortant de l'application, pour détermier quisont les destinataires et comment sont échangés les messages

Objectifs :
• Déterminer les serveurs avec qui l'application échange
• Traffic http : intercepter et lire les échanges
• Traffic https : intercepter, déchiffrer et lire les échanges

Analyse réseau :
• Emulateur avec ProxyDroid : modifie les règles iptables pour s'assurer que l'application passe forcément par le proxy• Wireshark pour analyser les paquets interceptés• JustTrustMe pour desactiver la verification des certificats SSl/TLS

L'analyse réseau

Qu'est ce que l'analyse réseau ?

Intercepter le traffic entrant et sortant de l'application, pour détermier qui sont les destinataires et comment sont échangés les messages

Objectifs :

- Déterminer les échanges effectués par l'application
- Lire le traffic http
- Déchiffrer le traffic https

Environnement utilisé

- Emulateur genymotion avec ProxyDroid
- WireShark (Analyseur de paquet)
- Xposed : JustTrustMe

Client-serveur :

- Les échanges sont chiffrés
- Un certificat permet de s'assurer que le serveur est bien celui que l'on attend

MITM :

- Déchiffrer les échanges réalisés
- JustTrustMe pour empêvher la verification des certificats

L'analyse réseau : Principe

- L'analyse réseau

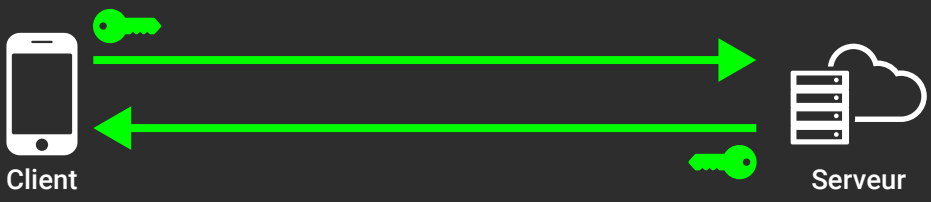

FIGURE – Principe d'une attaque man-in-the-middle

Client-serveur :
- Les échanges sont chiffrés
- Un certificat permet de s'assurer que le serveur est bien celui que l'on attend

MITM :
- Déchiffrer les échanges réalisés
- JustTrustMe pour empêvher la verification des certificats

L'analyse réseau : Principe

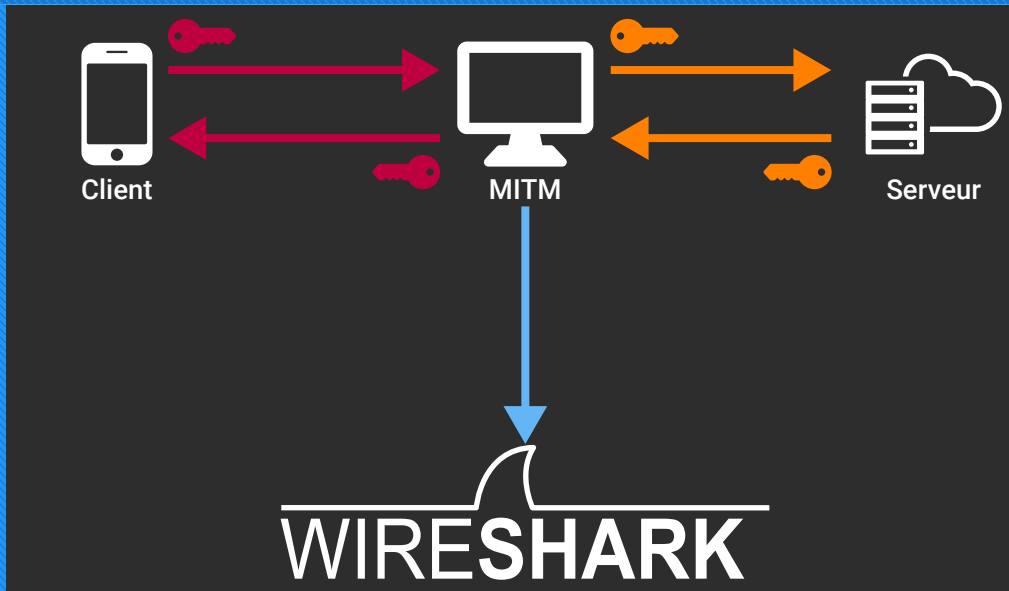

FIGURE – Principe d'une attaque man-in-the-middle