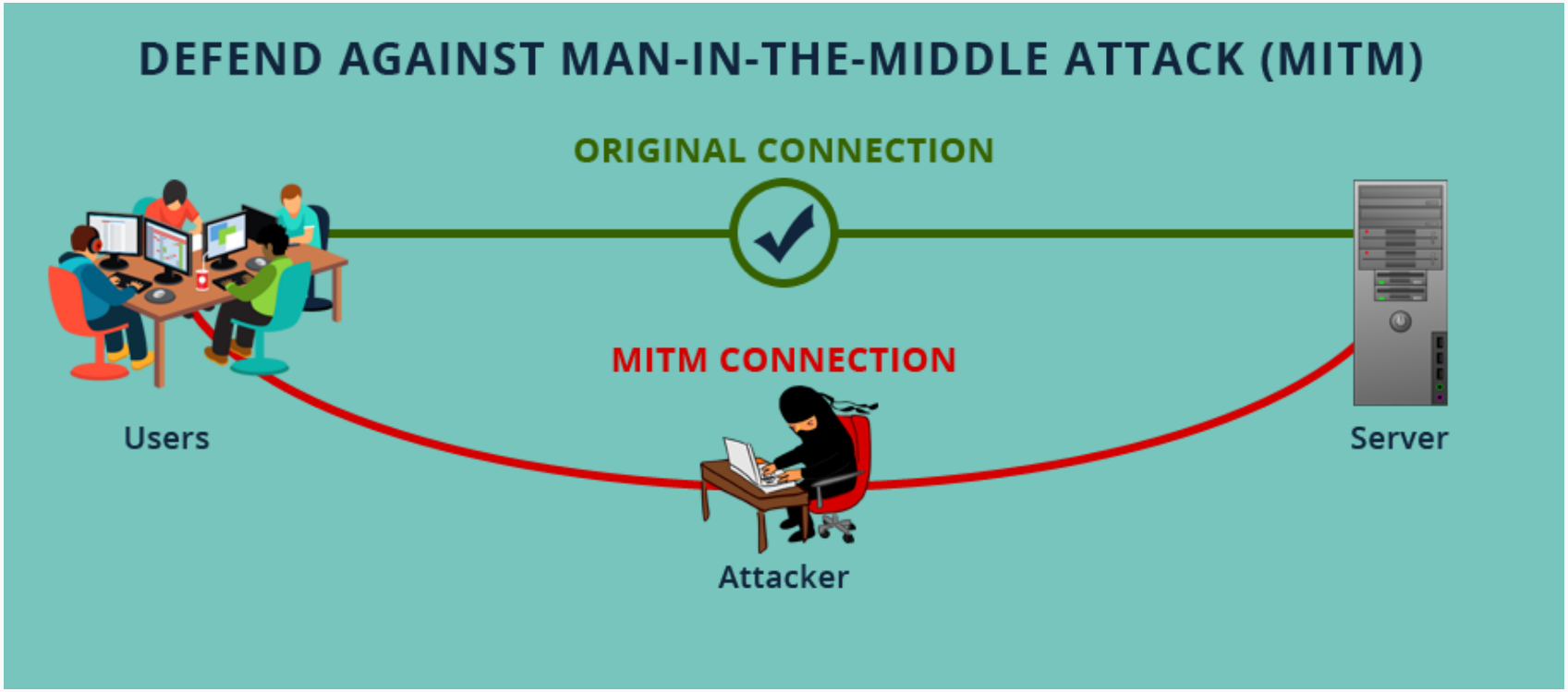
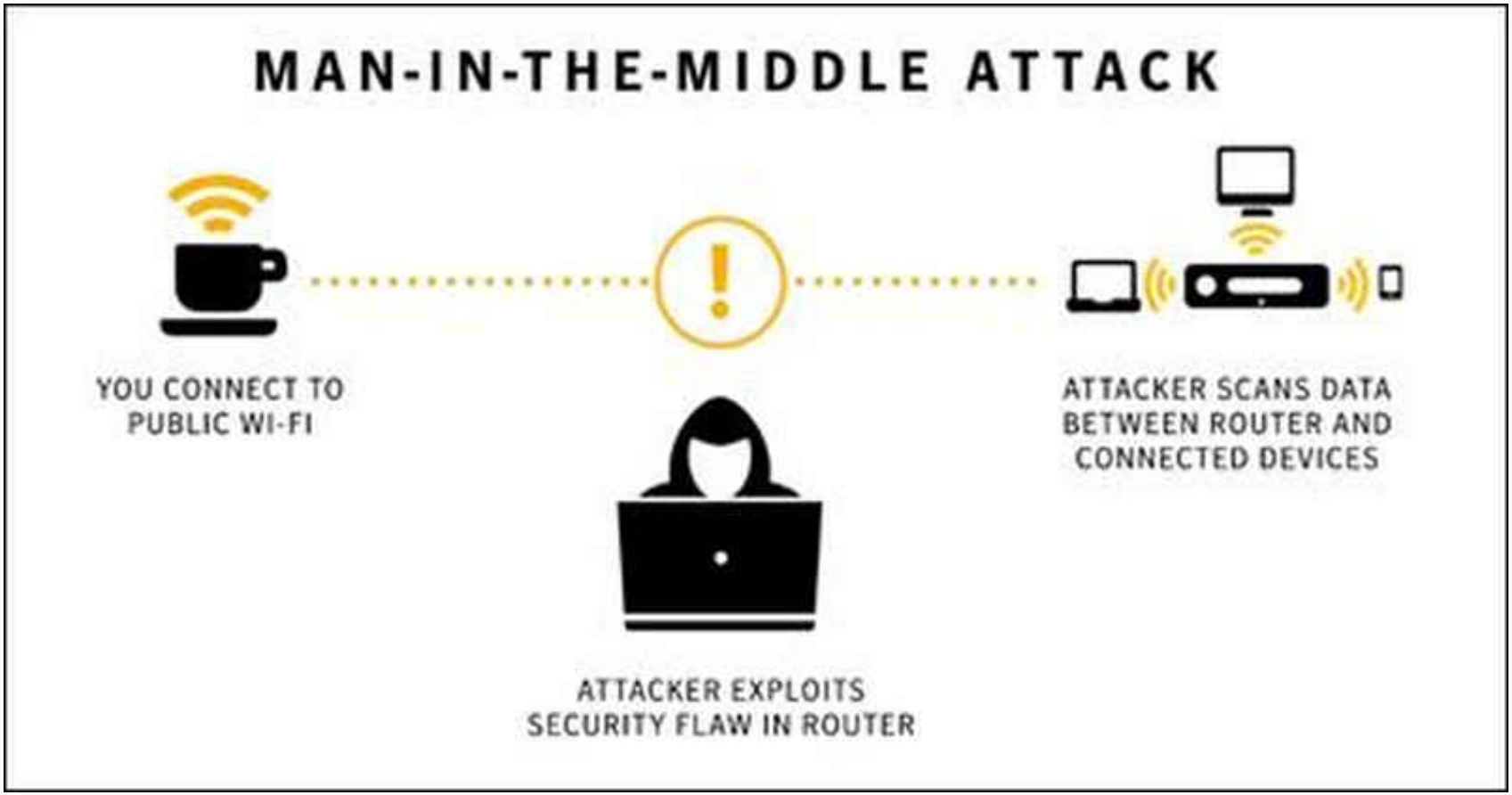
MITM Attack

Une attaque Man In The Middle consiste à intercepter un message qui ne nous est pas destiné.

Il est facile pour un postier de lire une lettre qu'il doit livrer. C'est plus compliqué s'il y a un cadenas.


DEFEND AGAINST MAN-IN-THE-MIDDLE ATTACK (MITM)
ORIGINAL CONNECTION
MITM CONNECTION
Users
Attacker
Server


MAN-IN-THE-MIDDLE ATTACK
YOU CONNECT TO PUBLIC WI-FI
ATTACKER SCANS DATA BETWEEN ROUTER AND CONNECTED DEVICES
ATTACKER EXPLOITS SECURITY FLAW IN ROUTER

Clés asymétriques: Introduction

Au moyen âge, un espion est en mission dans un royaume éloigné à plusieurs jours de marche. Il doit envoyer à son roi des information confidentielles. Si quelqu'un intercepte le message, il se fait décapiter.

Comment procède-t-il ?

Clés asymétriques: Le principe

- Clé publique = cadenas
- Clé privée = clé
- Échange de clés publiques

1. Le client génère un couple de clés
2. Le client envoie sa clé publique au server
3. Le server chiffre un message avec la clé publique
4. Le client déchiffre le message avec la clé privée

Ce principe s'applique aussi lorsque le client veut envoyer un message au server.

HTTPS

- HTTP
- Certificat SSL

mitm-proxy: Introduction

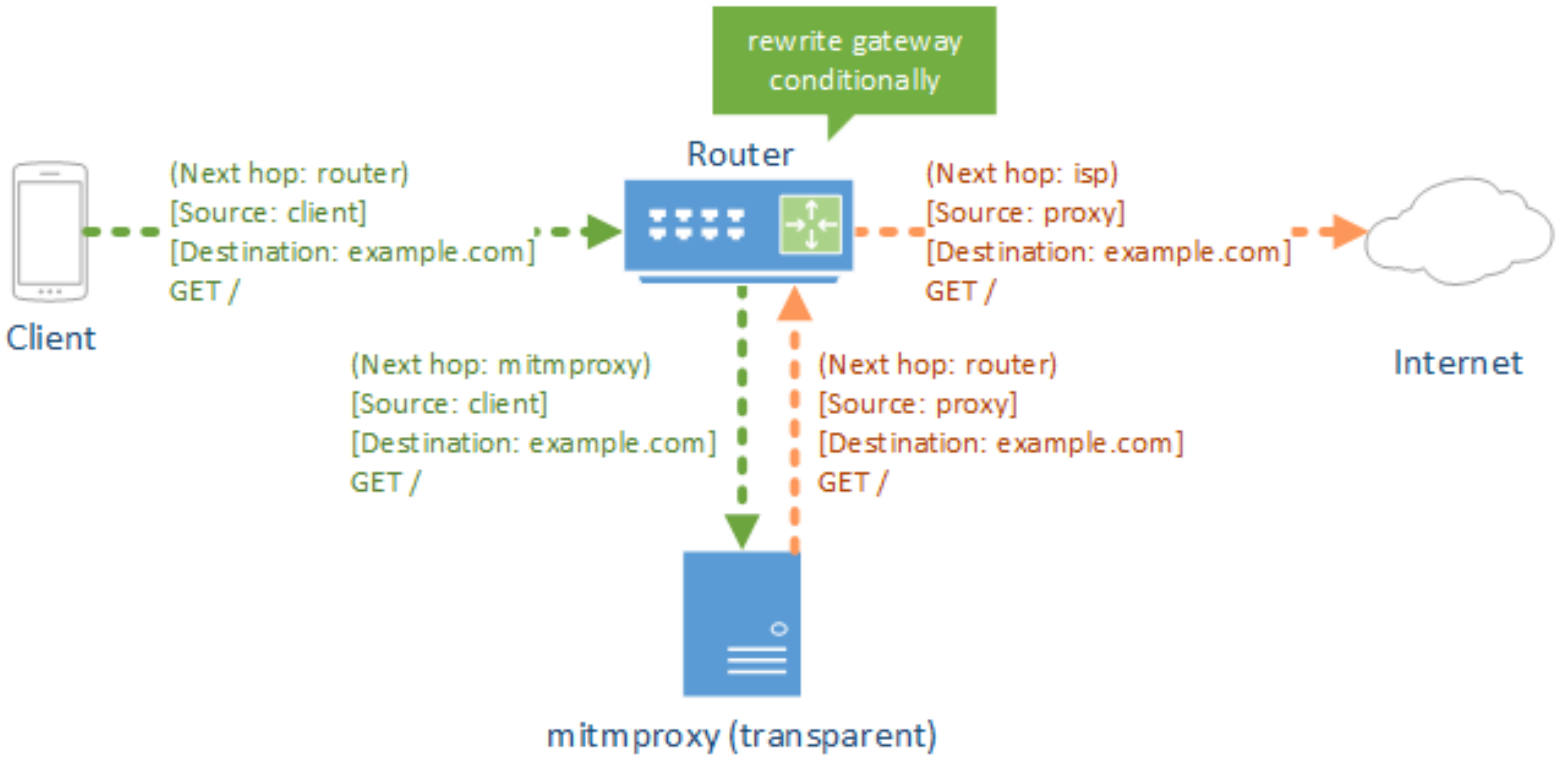
https://mitmproxy.org/

1. mitmproxy
2. mitmweb (beta)
3. mitmdump

Cet outil permet de:

- Intercepter et rediriger le trafic HTTP ou HTTPS
- Générer des certificats SSL à la volée

Transparent Proxy Variant 3: Custom Routing



mitm-proxy: Pourquoi c'est cool ?

- Open Source: https://github.com/mitmproxy/mitmproxy/
- Customizable à travers une API python pour mitmdump

Conclusion

Pas si facile de de faire un MITM sur du https... Mais facile de s'en prémunir !

Comment outrepasser la sécurité des certificats ?

- SSL Strip (protocol downgrade)
- Installer le certificat chez la victime
- Se procurer un certificat pirate valide ($$$)