# Vos données sont en danger ! Protégez votre réseau !

Timothée Simon

*timothee.simon@std.heh.be*

HAUTE ECOLE EN HAINAUT

Campus **technique**

# Sommaire

# Les risques d'un réseau mal sécurisé

## Les risques


- Compromission de données.
- Prise en otage de données.
- Connexion non-autorisée à des services.
- Usurpation d'identité.

# Les risques d'un réseau mal sécurisé

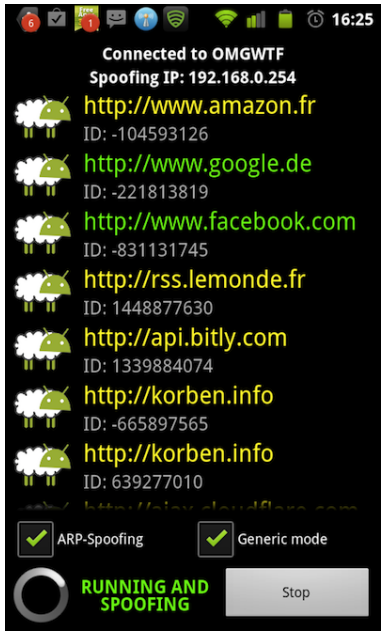
## Qui est le hacker

Un **hacker** est souvent **doué en informatique** mais **pas toujours**

Il est souvent motivé par **l'argent**, en étant payé pour de **l'espionnage industriel** ou en **arnaquant des utilisateurs**.

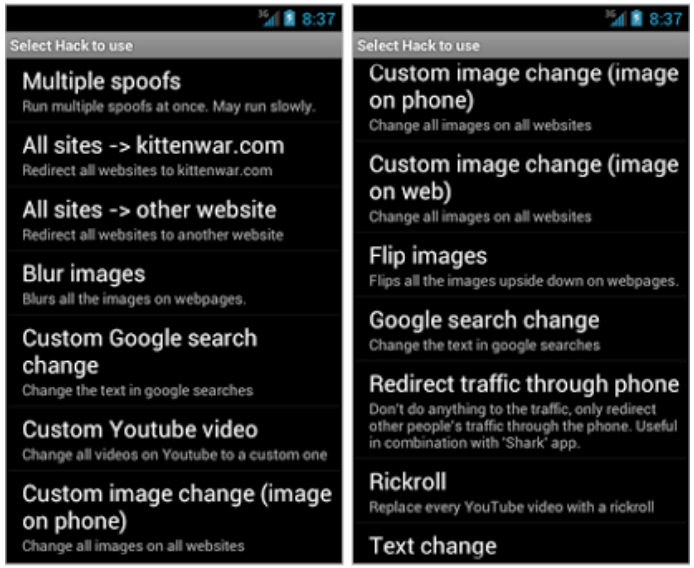
Ses **outils** et ses **techniques** sont beaucoup plus puissant grâce à **Internet**.

# Les risques d'un réseau mal sécurisé




**DroidSheep** est une application pour smartphone permettant de **voler les session** des utilisateurs du même réseau.

# Les risques d'un réseau mal sécurisé




**Network Spoofer** est une application pour smartphone permettant de **jouer des blagues** à ses amis sur le même réseau.

# Les risques d'un réseau mal sécurisé


Figure – Conséquence de Network Spoofer

# Man in the Middle

## Qu'est ce que c'est ?

Un hacker sur votre réseau **intercepte les données** entrante et sortante.

Il peut aussi **modifier** ces **données**.

Le hacker se fait passer pour votre **routeur** et controle toutes les **connexions vers l'extérieur** du réseau.

# Man in the Middle

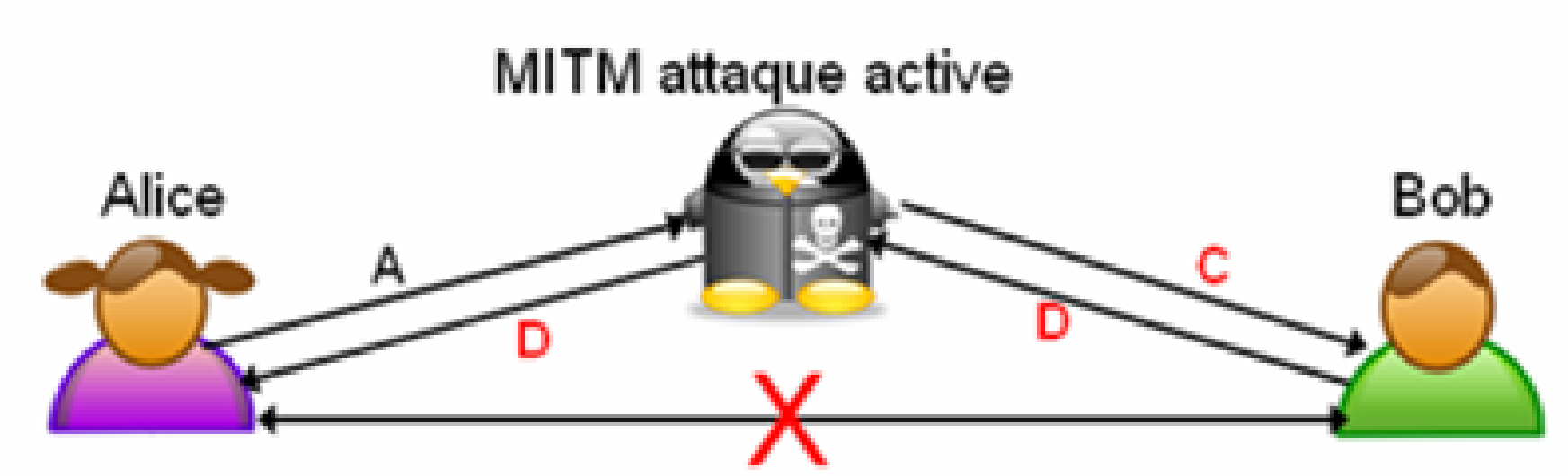



Figure – Attaque par Man in the middle

# Man in the Middle

## Comment s'en protéger ?

- Utilisation d'un **anti-virus** (vous protège des attaques et de leur conséquences).
- Vérification de l'utilisation du **HTTPS** pour les sites sécurisés.


Figure – HTTPS

# Denial of Service

## Qu'est ce que c'est ?

C'est une attaque souvent utilisée en **groupe** par des hacker avec **peu de connaissance en sécurité**.

Elle consiste à **surcharger** un périphérique pour l'**empécher de communiquer** avec les autres périphériques du réseau.

Permet de **ralentir** ou de **bloquer** un appareil.

# Denial of Service

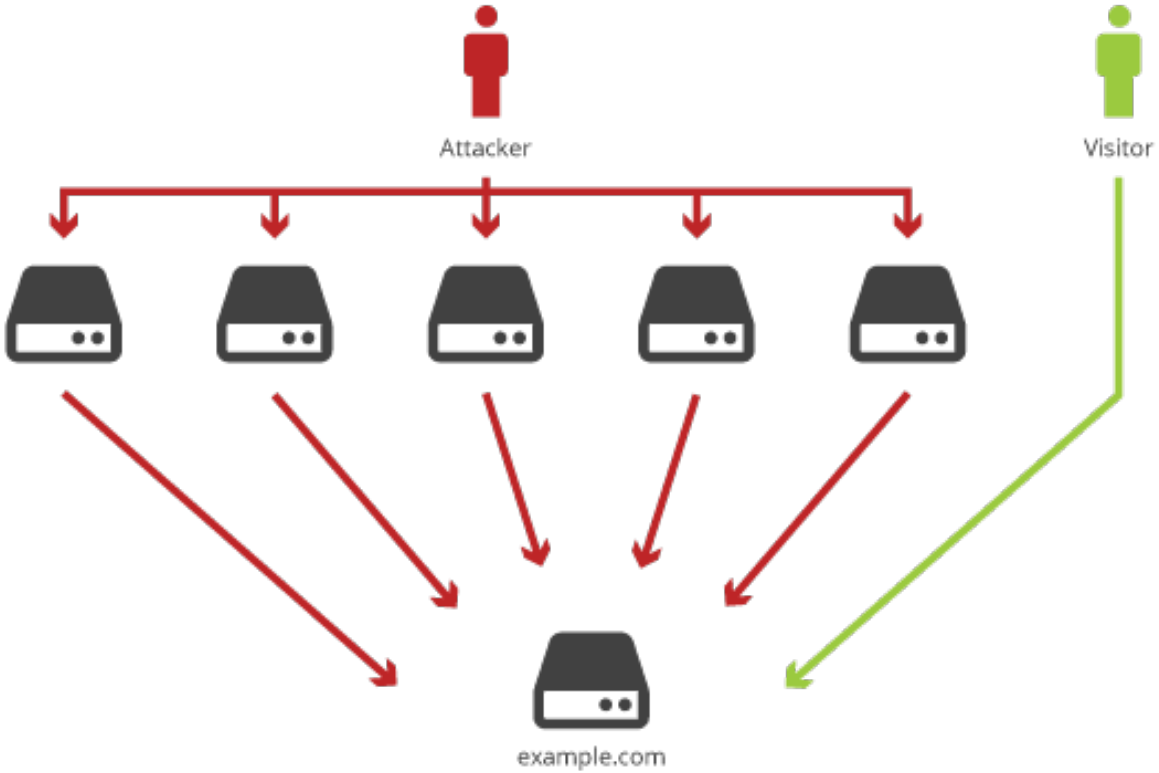



Figure – Attaque par DDOS

# Man in the Middle

## Comment s'en protéger ?

- Utilisation d'un **firewall** (pare-feu).
- Ne pas laisser d'**accès physique** à son réseau **accessible**.

# Brute Force et dictionnaire

## Qu'est ce que c'est ?

Utilisation d'un programme qui **teste toutes les possibilité** pour un mot de passe.

Une variante essaie tout les mots de passe d'un **dictionnaire**.

Les nouveaux programmes utilisent une technique **hybride** combinant les deux précédentes.

# Brute Force et dictionnaire

## Comment s'en protéger ?

Utiliser des mots de passes sécurisés :

- Suffisement **long**.
- Combinaison de **chiffres**, lettres **majuscules** et **minuscules** et de **caractères spéciaux**.
- **Peu commun** (~~Password123~~).

# Utilisation de failles

## Qu'est ce que c'est ?

Utilisation de **moyen détourné** pour pour **accéder** à un système ou un réseau **sécurisé**.

Les failles sont souvent **partagées** entre hackers via **Internet**.

Il est possible d'accéder aux **anciens réseaux Wi-Fi sécurisés** sans mot de passe ou de **prendre le controle** d'une machine sous **Windows 7**.

# Utilisation de failles

## Comment s'en protéger ?

- Toujours **mettre à jour** ses logiciels et son matériel.
- Utilisation d'un **anti-virus** (vous protège des attaques et de leur conséquences).

# Denial of Service


Figure – Ecran d'un utilisateur infecté par WannaCry

# Bonnes pratiques

## Ne pas laisser n'importe qui accéder à votre réseau

HAUTE ECOLE EN HAINAUT

- Utiliser un **mot de passe Wi-Fi sécurisé** et ne le communiquer qu'aux **personnes de confiance**.
- Faire attention lors de l'utilisation d'un **Wi-Fi gratuit**.
- Rester attentif même lorsque vous êtes **chez vous**.
- Protéger l'**accès à votre matériel**.

# Bonnes pratiques

## Protégez vous !

- Installer un **anti-virus** éfficace.
- Toujours **mettre à jour** vous appareils.
- Utiliser des **mots de passe complexes**.
- Vérifiez l'utilisation du **HTTPS**.
- Utiliser un **Firewall**.