Confiance sur Internet

Neutralité du réseau

Romain Tartière <romain@opus-codium.fr>

Opus-Codium

17 septembre 2015

Benjamin Bayart
Photo : Wikipedia

Edward Snowden

Photo : Laura Poitras / Praxis Films

Confiance sur Internet

Plan

Confiance sur Internet

Plan

Un exemple

If you want to be extra safe, check that there's a big block of jumbled characters at the bottom.

Source : `https://xkcd.com/1181/`

Un exemple

```
Date: Fri, 11 Sep 2015 15:35:22 +0200
From: William Durand <william@clermontech.org>
To: clermontech@googlegroups.com
Subject: [Clermont'ech] We Are Back! — APIHour #16 le 17 septembre 2015
à 19h au Centre J. Richepin

[-- La sortie PGP suit (heure courante : dim 13 sep 12:54:12 2015) --]
gpg: Signature faite le ven 11 sep 15:35:22 2015 CEST avec la clef RSA
d'identifiant C1274F3B
gpg: MAUVAISE signature de « William Durand <will@drnd.me> » [inconnu]
[-- Fin de sortie PGP --]

[-- Les données suivantes sont signées --]

Hello!

Comment allez-vous ? La rentrée s'est bien passée ?

Nous, ça va. Bon, on serait bien restés en vacances, mais on a préféré
vous organiser un nouvel API Hour, le 16ème déjà… Le temps passe…

Bref, nous vous proposons de nous rencontrer tous ensembles jeudi
prochain, soit le 17 septembre 2015 à 19h au Centre Jean Richepin,
```

Un exemple

Photo : Wikipedia

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;
- Votre réseau ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;
- Votre réseau ;
- Votre accès à Internet ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;
- Votre réseau ;
- Votre accès à Internet ;
- Internet ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;
- Votre réseau ;
- Votre accès à Internet ;
- Internet ;
- L'hébergeur ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;
- Votre réseau ;
- Votre accès à Internet ;
- Internet ;
- L'hébergeur ;
- Les logiciels du serveur ;

Un exemple

Photo : Wikipedia

Quand vous utilisez Internet, vous êtes seul(e) avec les gens qui conçoivent / opèrent :

- Votre navigateur ;
- Vos extensions ;
- Vos applications ;
- Votre système d'exploitation ;
- Votre réseau ;
- Votre accès à Internet ;
- Internet ;
- L'hébergeur ;
- Les logiciels du serveur ;
- Votre cible.

La tomatina

Photo : Getty Images / Jasper Juinen

Confiance sur Internet

Plan

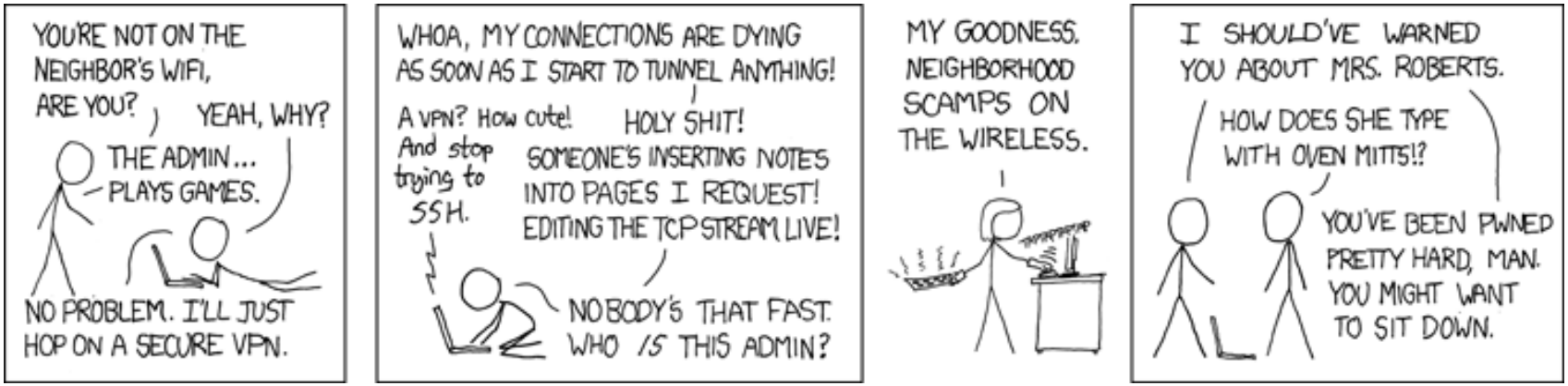
Les menaces : Altérations de contenus

Principe : réécrire le contenu au fur et à mesure qu'il transite.

Les menaces : Altérations de contenus

Principe : réécrire le contenu au fur et à mesure qu'il transite.

Exemples : ajout de publicité (Comcast), Upside-Down-Ternet, …



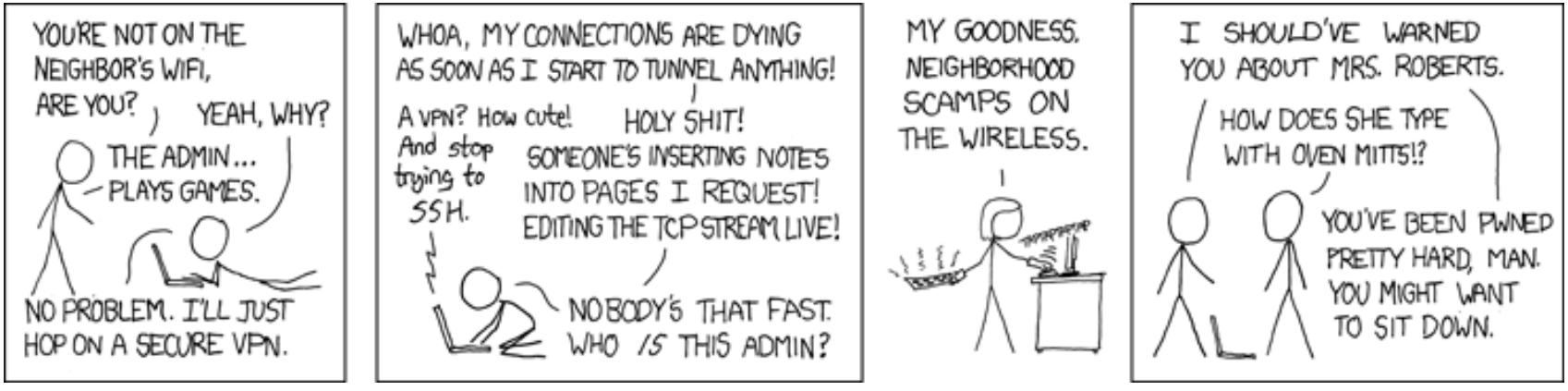
If you're not cool enough to do it manually, you can look up tools like Upside-Down-Ternet for playing games with people on your wifi.

Source : `https://xkcd.com/341/`

Les menaces : Altérations de contenus

Principe : réécrire le contenu au fur et à mesure qu'il transite.

Exemples : ajout de publicité (Comcast), Upside-Down-Ternet, …



If you're not cool enough to do it manually, you can look up tools like Upside-Down-Ternet for playing games with people on your wifi.

Source : `https://xkcd.com/341/`

Contournement : signature / chiffrement des échanges.

CLERMONT'ECH

ASSOCIATION DE DÉVELOPPEURS AUVERGNATS.

L'ASSOCIATION CLERMONT'ECH

Clermont'ech est une association loi 1901 créée le 21 février 2013 à Clermont-Ferrand. Le siège social de l'association est situé 19 rue Rabelais 63100 Clermont-Ferrand.

BUREAU

Le bureau de l'association est composé de :

- *Président : Julien Maupetit*
- *Vice président : Julien Muetton*
- *Trésorier : Pierre Tachoire*
- *Trésorier suppléant : William Durand*
- *Secrétaire : Manuel Raynaud*
- *Secrétaire suppléant : Jean-Philippe Serafin*

STATUTS

Les statuts de l'association sont consultables sur le dépôt GitHub clermontech dans la rubrique documents.

Les menaces : Altérations de contenus

X509, une solution bancale

Ai-je confiance en X509 ?

HTTPS > SSL > OpenSSL > Ai-je patché ?

Les menaces : Altérations de contenus

X509, une solution bancale

Ai-je confiance en X509 ?

HTTPS > SSL > OpenSSL > Ai-je patché ?

Ai-je confiance en mes Autorités de Certification (CA) ?

173 CA (paquet `ca-certificates` dans Debian Jessie).

Les menaces : Altérations de contenus

X509, une solution bancale

Ai-je confiance en X509 ?

HTTPS > SSL > OpenSSL > Ai-je patché ?

Ai-je confiance en mes Autorités de Certification (CA) ?

173 CA (paquet `ca-certificates` dans Debian Jessie).

Ai-je installé d'autres certificats ?

SuperFish sur les ordinateurs Lenovo.

Les menaces : Altérations de contenus

X509, une solution bancale

Ai-je confiance en X509 ?

HTTPS > SSL > OpenSSL > Ai-je patché ?

Ai-je confiance en mes Autorités de Certification (CA) ?

173 CA (paquet `ca-certificates` dans Debian Jessie).

Ai-je installé d'autres certificats ?

SuperFish sur les ordinateurs Lenovo.

Mes CA de confiance n'ont-elles pas été compromises ?

En 2011, DigiNotar émet 531 certificats frauduleux.

Les menaces : DNS menteurs

Principe : Rediriger le trafic d'un domaine vers un autre serveur.

Les menaces : DNS menteurs

Principe : Rediriger le trafic d'un domaine vers un autre serveur.

Exemples : OpenDNS, Comcast, Orange, Free, SFR-Numéricable, Bouygues, ...

```
% host t411.io
t411.io has address 108.162.203.254
t411.io has address 108.162.204.254

% host t411.io
t411.io has address 127.0.0.1
t411.io has IPv6 address ::1
```

Les menaces : DNS menteurs

Principe : Rediriger le trafic d'un domaine vers un autre serveur.

Exemples : OpenDNS, Comcast, Orange, Free, SFR-Numéricable, Bouygues, ...

```
% host t411.io
t411.io has address 108.162.203.254
t411.io has address 108.162.204.254

% host t411.io
t411.io has address 127.0.0.1
t411.io has IPv6 address ::1
```

Contournement trivial : utiliser son propre résolveur DNS.

```
# apt-get install unbound
# echo 'nameserver 127.0.0.1' > /etc/resolv.conf
```

En prime, votre FAI n'a plus un log direct des sites que vous visitez.

Les menaces : Filtrage de contenu

Principe : bloquer l'accès à une ressource.

Les menaces : Filtrage de contenu

Principe : bloquer l'accès à une ressource.

Exemples : SMTP, SIP chez SFR, SRV records chez Bouygues ...

```
% nc mxa.relay.renater.fr 25
nc: connect to mxa.relay.renater.fr port 25 (tcp) failed: Operation
timed out

% nc mxa.relay.renater.fr 25
220 mxb1-1.relay.renater.fr ESMTP asm
```

Les menaces : Filtrage de contenu

Principe : bloquer l'accès à une ressource.

Exemples : SMTP, SIP chez SFR, SRV records chez Bouygues ...

```
% nc mxa.relay.renater.fr 25
nc: connect to mxa.relay.renater.fr port 25 (tcp) failed: Operation
timed out
```

```
% nc mxa.relay.renater.fr 25
220 mxb1-1.relay.renater.fr ESMTP asm
```

Contournement : ne pas être un jambon !

Confiance sur Internet

Plan

Synthèse

Comment garder / regagner le contrôle ?

1. Comprendre ce qu'on fait ;

Synthèse

Comment garder / regagner le contrôle ?

1. Comprendre ce qu'on fait ;
2. Passer par un FAI de confiance ;

Synthèse

Comment garder / regagner le contrôle ?

1. Comprendre ce qu'on fait ;
2. Passer par un FAI de confiance ;
3. Avoir ses propres infrastructures (DNS, modem, routeur, firewall, ...) ;

Synthèse

Comment garder / regagner le contrôle ?

1. Comprendre ce qu'on fait ;
2. Passer par un FAI de confiance ;
3. Avoir ses propres infrastructures (DNS, modem, routeur, firewall, ...) ;
4. Réfléchir avant de créer des CA (CAcert) ;

Synthèse

Comment garder / regagner le contrôle ?

1. Comprendre ce qu'on fait ;
2. Passer par un FAI de confiance ;
3. Avoir ses propres infrastructures (DNS, modem, routeur, firewall, ...) ;
4. Réfléchir avant de créer des CA (CAcert) ;
5. Rester vigilant (bloqueurs de pub, de trackers, ...).

Questions ?