Sécuriser son surf

http S ?

1. **Authenticité** : certificats https = carte d'identité d'un site
2. **Confidentialité** : le trafic entre l'utilisateur et le site est *chiffré*
3. **Intégrité** : personne ne peut modifier les données envoyées https *nécessaire* pour les données sensibles lors d'un accès à internet via une connexion "sale" (wifi public, hôtels etc.)

Casser du https

- Bloquer les connexions https (port 443) et forcer les internautes à utiliser http non sécurisé (port 80)
- Usurper l'identité d'un site https : *Man in the Middle*.
  Alertes de sécurité : exemple
- Voler les papiers d'identité (vol de certificat). ex : août 2011 Diginotar

Solutions

- Désactivez Java
  Kaspersky stats : En 2012, 50% des attaques ont utilisé Java. Adobe Reader arrive juste derrière avec 28%. A titre de comparaison, Microsoft Windows et IE ont été impliqués dans seulement 3% des attaques. via @GRC
- Utilisez Firefox - éventuellement chrome - **pas IE**
- Avec des extensions utiles :
  - https everywhere : pour s'assurer d'utiliser la version https d'un site quand celle-ci est disponible
  - No script : contre XSS et XSRF
  - Pratique : Web of trust
  - Pour les plus paranoïaques : Certificate Patrol