La sécurité

Un sujet TRES vaste !

Qu'est ce qu'un « hacker » ?
Risques pour un utilisateur lambda ?
Comment s'y prennent-ils !?
Comment se protéger ?

Tout ce que cette présentation ne couvre pas...

Les « Hackers »

D'après Wikipedia : « personne qui aime comprendre le fonctionnement interne d'un système, en particulier des ordinateurs et réseaux informatiques. »

Un hacker est un BIDOUILLEUR (au sens large), on peut « hacker » une machine à laver. Analyser et comprendre, afin généralement de créer, et d'assembler « autrement ». CE NE SONT PAS DES « PIRATES INFORMATIQUES »

Les risques

- Perte de ses données
- Monopolisation des ressources par un tiers
- Vol d'informations
- Usurpation de son identité
- Mise sous surveillance de ses activités
- Chantage

Pertes de ses données

- Souvent le résultat d'une erreur humaine
- Parfois à cause d'une panne matérielle
- Ou d'un problème logiciel
- Ou d'un virus
- Ou d'une malveillance
- Etc.

Monopolisation des ressources

- Utilisation des ressources de l'ordinateur
- Essentiellement bande passante et cpu
- Résultat : L'ordinateur « rame »
- Des centaines de millions de gens impactés
- Entre 70 et 90% des mails sont des spams
- Beaucoup de sites illégaux tournent sur des PC « zombies » de particuliers

Vol d'informations

- Documents personnels
- Numéro de carte bleue
- Identifiants à des services en ligne
- Mails etc.

Usurpation de son identité

Avec ces informations, il est facile de se faire passer pour vous auprès de vos collègues, de vos amis. (envoi de « trucs pas cool » etc). Il est aussi possible de modifier les mots de passe de vos services en ligne, de résilier ou de modifier des abonnements etc.

Mise sous surveillance

La technologie permet maintenant une surveillance constante des moindres faits et gestes d'une personne. Localisation GPS avec les smartphone, vidéo avec les webcam intégrées, historique de navigation etc.

Mais la plus grande source d'information vient des utilisateurs eux même ! Aucun dictateur au monde n'aurait jamais pu rêver d'un outil aussi puissant que Facebook :(

Chantages

De nombreux cas de chantages ont étés répertoriés.

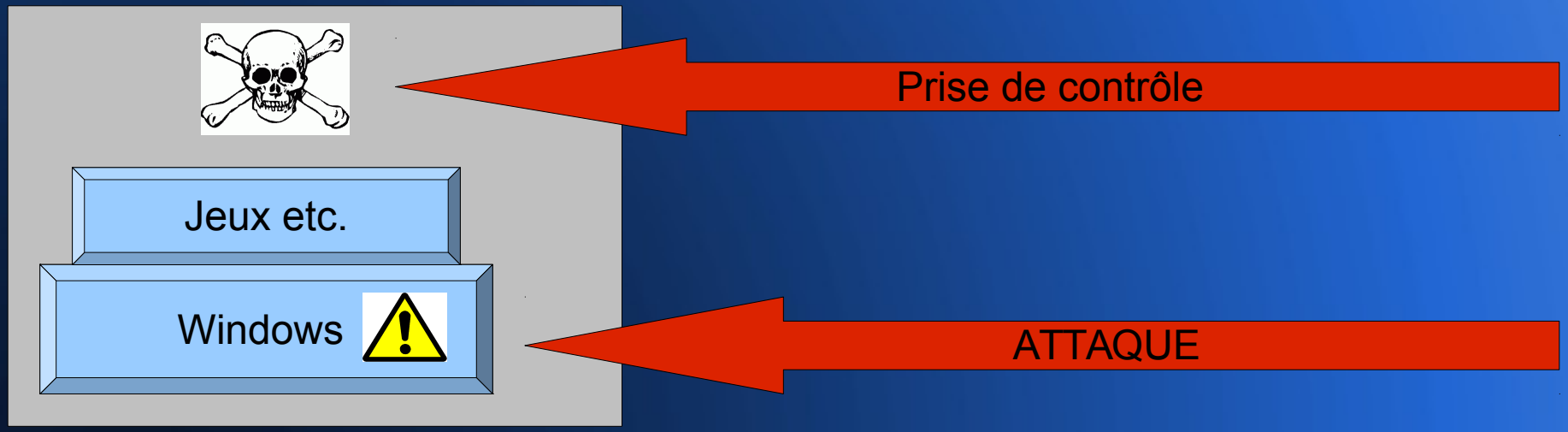
« Paye ou j'envoie cette vidéo compromettante de toi à tous tes amis »

« Paye et tu pourras récupérer tes fichiers qui sont à présent tous chiffrés sur ton ordinateur »

« Paye ou je rends inaccessible le site de ton entreprise »

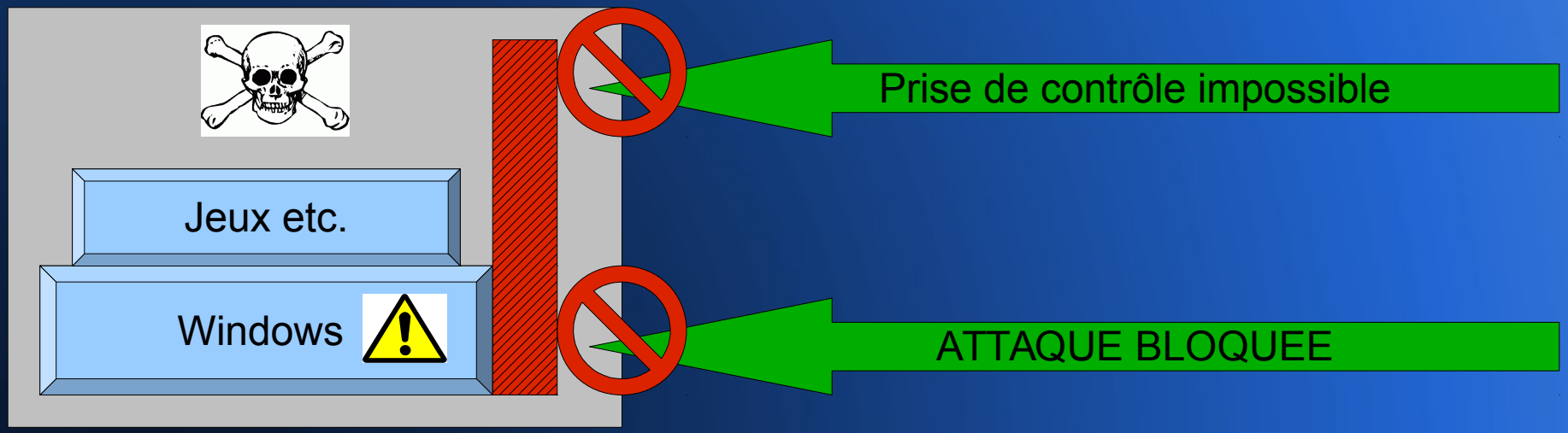
Comprendre les attaques

A la belle époque des modem RTC...



Comprendre les attaques

Le firewall était une solution efficace !



Comprendre les attaques

Mais les techniques ont beaucoup évoluées !

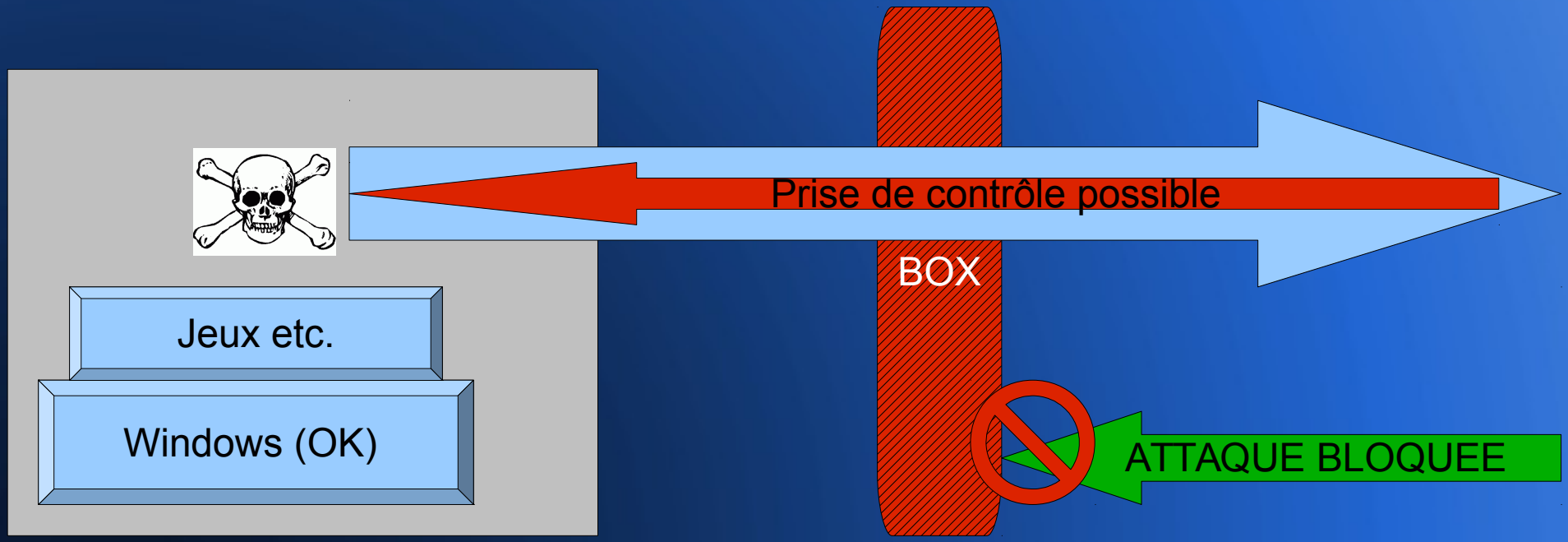
Nous avons déjà tous un firewall.

(Box adsl, cable, fibre...)

Les chances de pouvoir se connecter directement à une machine sont si faibles que plus aucune attaque ne fonctionne de cette façon. C'est toujours la machine « cible » qui effectue la connexion.

Comprendre les attaques

Les connexions sortantes permettent de créer des « tunnels »
Ou plus personne ne peut savoir ce qui se passe à l'intérieur



La « box » totalement impuissante,à empêcher les connexions entrantes une fois la connexion sortante établie.

Comprendre les attaques

- Attaques au niveau TCP et OS
- Envoi de mails « piégés »
- Attaques des applications clientes (navigateur)

  Ces attaques sont aujourd'hui (et de très loin) les plus efficaces et les plus faciles à mettre en œuvre. un Firewall ne sert plus à rien !
- Le SE à l'heure de Facebook

Comment se protéger ?

- Quelques réponses techniques
  - Utilisation des logiciels libres en priorité
  - Toujours avoir un système à jour (XP est mort)
  - Surfer avec des extensions comme WOT
  - Désactiver UPNP sur son routeur
  - Sous Windows : Antivirus indispensable.
    Celui de Microsoft est abandonné*
  - Attention aux extensions de fichier

- *http://www.howtogeek.com/173291/goodbye-microsoft-security-essentials-microsoft-now-recommends-you-use-a-third-party-antivirus/

Comment se protéger ?

- Mais surtout de bonnes pratiques !
  - Bonne gestion DES mots de passe
  - Toujours vérifier les liens dans un mail
  - Vérifier l'url avant d'entrer des identifiants
  - Éviter les réseaux sociaux
  - Ne pas consulter ses mails sur un réseau Wifi non chiffré. (sauf webmail en https)
  - Privilégier l'auto-hébergement.

Tout le reste...

- Les sauvegardes

  (un raid n'est pas une sauvegarde !)
- Le Chiffrement

  Solution contraignante, mais seule protection « physique » efficace.
- L'anonymat

  (proxy, VPN, darknet, navigateur sécurisé...)

Liens

En français :

http://korben.info/interview-black-hat.html
http://www.xmco.fr/article-fast-flux.html
http://www.securite-informatique.gouv.fr/gp_rubrique34.html
http://www.cnetfrance.fr/news/vos-appareils-connectes-n-ont-jamais-ete-aussi-vulnerables-39786799.htm
http://www.01net.com/editorial/571737/le-scandale-des-nouvelles-cartes-bancaires/
http://www.april.org/vie-privee-en-2013-pourquoi-quand-comment-par-werner-koch
http://www.numerama.com/magazine/15288-chantage-au-piratage-deux-avocats-devant-le-conseil-de-discipline.html
http://trends.levif.be/economie/actualite/high-tech/perdre-son-emploi-a-cause-de-facebook-ou-twitter/article-1194712269539.htm
http://www.leparisien.fr/faits-divers/l-ingenieux-systeme-des-escrocs-a-la-carte-bancaire-05-04-2013-2699609.php
http://www.lemondeinformatique.fr/actualites/lire-black-hat-2013-un-faux-chargeur-menace-la-securite-des-terminaux-apple-54593.html
http://fr.wikipedia.org/wiki/Computer_Emergency_Response_Team
http://www.securiteinfo.com/attaques/divers/social.shtml
http://zythom.blogspot.fr/2010/06/perquisition.html

http://www.pcinpact.com/news/81014-en-prison-depuis-4-mois-pour-commentaire-sarcastique-sur-facebook.htm
http://www.radio-canada.ca/regions/saguenay-lac/2009/06/03/005-photo_facebook_congediement.shtml
http://www.usine-digitale.fr/article/six-millions-d-utilisateurs-touches-par-la-fuite-de-donnees-sur-facebook.N199941
http://www.pcinpact.com/news/81929-six-mois-prison-pour-propos-aux-airs-menace-terroriste-sur-tumblr.htm
http://archives-lepost.huffingtonpost.fr/article/2009/04/30/1516052_licenciee-pour-avoir-surfe-sur-facebook-durant-son-arret-maladie.html

En anglais :

http://repo.zenk-security.com/
http://packetstormsecurity.com/
http://www.exploit-db.com/
http://www.securiteam.com/

Questions / Réponses

Questions ?