Sécurité informatique : Sécurité dans un monde en réseau

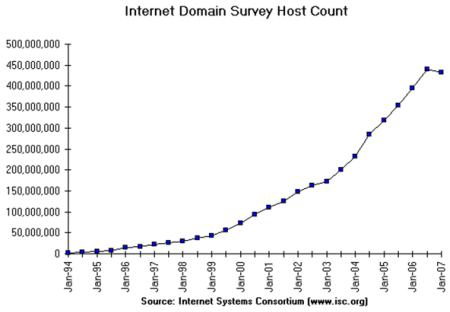
Matthieu Amiguet

2006 – 2007

haute école arc ingénierie
neuchâtel berne jura saint-imier le locle porrentruy

Explosion des connexions à internet 2

- En 1990, environ 320'000 hôtes étaient connectées à internet
- Actuellement, le chiffre a dépassé les 4 millions. . .



. . . Mais c'est pas tout ! 3

- Évidemment, l'explosion du nombre de connexions à l'internet pose de nouveaux problèmes de sécurité. . .
- . . . mais ces dernières années, la mise en réseau devient encore plus systématique et plus pervasive
  - Mise en réseau de la gestion des infrastructures critiques
  - Caméras de surveillance en réseau
  - Téléphones portables, PDA's, . . .
    - Localisation permanente des utilisateurs. . .
    - . . . et failles bluetooth (bluesnarf, bluebug) !
  - Omniprésence des RFID's
  - . . .

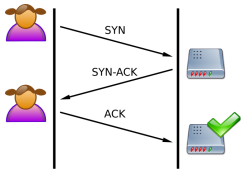
Rappel : les couches réseau 4

OSI	TCP/IP	protocoles
7. Application	Application	HTTP, FTP, SMTP,
6. Présentation		
5. Session		
4. Transport	Transport	TCP, UDP
3. Réseau	Internet	IP, ARP, ICMP
2. Liaison	Accès réseau	
1. Physique		

- Problème : TCP/IP a été conçu pour transporter des données de manière fiables, mais pas de manière sûre !

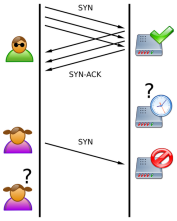
Three-way handshake 5

- Les connexions TCP commencent par un *three-way handshake*



SYN Flood – le principe 6

- Le principe du SYN flood est de saturer le serveur avec des connexions semi-ouvertes



- Ceci empêche donc les connexions “normales” : déni de service.

SYN Flood – protections 7

- Limitation du nombre de connexions depuis la même source ou la même plage d’IP
  - Souvent implémentée, cette protection n’est efficace que contre les attaques “centralisées”. . . mais pas contre un DDoS !
- Libération aléatoire de connexions semi-ouvertes en cas de besoin
- Utilisation de diverses techniques (p.ex. “SYN cookies”) pour n’attribuer des ressources qu’aux connections complètement établies.

Autres “floods” 8

- Le SYN flood constitue la plus connue des attaques de ce genre
- On peut aussi “inonder” au niveau ICMP (ping flood). . .
- . . . ou au niveau applicatif, avec des requêtes “normales”
- Dans ce cas, on ne bloque pas la machine mais on vise de la ralentir suffisamment pour obtenir un DoS
- Ce type d’attaque est encore plus difficile à contrer : comment distinguer le trafic d’attaque du trafic légitime ?
  - Surtout en cas d’attaque distribuée...

IP Spoofing 9

- L'IP spoofing, ou usurpation d'adresses IP, peut servir à deux choses :
  1. Camouflage lors d'une attaque (p.ex. DoS)
  2. Profiter d'une relation de confiance entre 2 machines lorsque celle-ci repose sur l'adresse IP
- L'idée est essentiellement de remplacer l'adresse IP de provenance dans les paquets IP
- L'utilisation 1. ne demande pas de précautions particulière
- L'utilisation 2. montre deux points délicats
  1. prédiction des numéros de séquence TCP
  2. l'attaque est forcément "à l'aveugle"

ARP Poisoning 10

- Fonctionnement d'ARP (en gros !) :
  - La machine A doit contacter la machine B du même sous-réseau
  - Elle broadcaste un
    - Who has 192.168.1.118 ? Tell 192.168.1.27
  - B se reconnaît et répond
    - 192.168.1.118 is at 00 :12 :ff :3d :a6 :15
  - A met la correspondance en cache pour la prochaine fois
- Il n'y a aucun mécanisme de sécurité : tout renseignement ARP est considéré comme valable (même s'il ne répond pas à une question)
- Donc si C dit à A qu'il est B et à B qu'il est A, il peut intercepter tout le trafic !

DNS Spoofing 11

- Le ARP Poisoning est limité au sous-réseau de l'attaquant. . .
- . . . mais on peut utiliser le même principe à plus large échelle en falsifiant des réponses DNS
- Dans ce cas, il s'agit de répondre *avant* le serveur DNS officiel, avec le bon numéro d'identification
- La réponse officielle sera alors ignorée et le cache DNS local contiendra une fausse correspondance
- Peut être utilisé pour obtenir des informations de e-banking, . . .

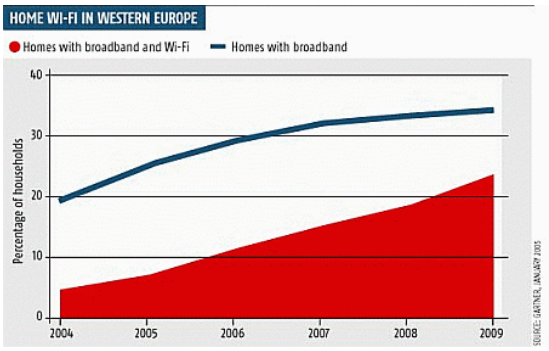
Autres 12

- Les attaques ci-dessus ne donnent qu'une petite idée des possibilités de détournement des technologies de l'internet. . .
- On peut aussi jouer sur
  - La fragmentation des paquets (ping of death, . . .)
  - Les noms de domaines proches, voire indiscernables
  - . . .
- Les attaques les plus efficaces combinent généralement plusieurs de ces techniques
  - En broadcastant un ping depuis une adresse spoofée, on peut faire tomber un serveur DNS dans le but de le remplacer. . .

L'attaque de Mitnick 13

- L'attaque de Kevin Mitnick contre le réseau de Tsutomu Shimomura à Noël 94 est légendaire
- Intéressante du point de vue des techniques qu'elle met en place et de la maîtrise qu'elle témoigne
  - Attaque tout de même assez complexe, depuis plusieurs machine
  - Durée : 29 secondes !
- Plus de détails : cf. article de C. Vincenot, MISC n°18, mars-avril 2005.

Généralisation des réseaux sans fil 14



Interception 15

- Comme dit plus haut, la suite TCP/IP n'est pas conçue avec la sécurité en tête. . .
- . . . mais l'approche traditionnelle de réseau filaire nécessite tout de même une présence physique sur le réseau pour obtenir quelque chose. . .
- La généralisation des réseaux sans fil pose de ce point de vue des problèmes nouveaux !
  - N'importe qui peut écouter la communication (contenu, mots de passe, . . .)
  - N'importe qui peut utiliser la communication à des fins illégales (piratage, contenu illicite, . . .)
  - N'importe qui a un accès au réseau du côté *interne*
  - . . .

WEP 16

- WEP : Wired Equivalent Privacy
- Basé sur RC4
- Contient plusieurs erreurs qui le rendent vulnérable à des attaques cryptanalytiques
  - Si il y a assez de trafic, par simple écoute
  - Dans le cas contraire, on peut même *générer* du trafic !
- Si vous faites encore confiance au WEP : `http://www.tuto-fr.com/tutoriaux/crack-wep/fichiers/videos/video-crack-wep-devine.php`

WPA 17

- WPA : Wi-Fi Protected Access
- Conçu pour remédier aux faiblesses de WEP
- WPA est basé sur RC4
  - Mais les erreurs de WEP ont été évitées, donc les attaques cryptanalytiques classiques ne sont pas possibles
  - Par contre, la solution est basée sur un mot-clé choisi par l'utilisateur… il faut faire attention à sa solidité !
- WPA2, successeur de WPA, est basé sur AES et constitue la solution la plus sûre à ce jour.

Et si on ne veut rien de tout ça ? 18

- Une alternative à WEP/WPA(2) est de laisser le réseau ouvert mais de mettre en place d'autre mécanismes de sécurité
- Identification basée sur l'adresse MAC
  - Attention à la falsification !
  - N'empêche pas le sniffing !
- L'accès au réseau ne permet *rien* tant qu'un VPN n'est pas établi
  - Efficace si bien implémenté !