JSSI 2002

SÉCURITÉ.ORG

Dénis de service et vers
Attaques, détection et protection

"Les services en ligne sont comparables à un château de cartes exposé à tous vents et de surcroît construit sur du sable mouvant"

> Nicolas FISCHBACH

IP Engineering Manager - COLT Telecom

nico@securite.org - http://www.securite.org/nico/

version 1.01

Programme

- **Objectifs des dénis de services et vers**
- **Attaques**
  - > Architectures des attaques
  - > Attaques « mutualisées » et agents
  - > Attaques « réseaux » locales et distantes
- **Détection et Protection**
  - > Au niveau local
  - > Au niveau de l'Internet
- **Conclusion**

Définition (1)

» **Objectif des dénis de services**

> Consommer les ressources (bande passante, CPU, mémoire, etc) pour rendre le service lent ou indisponible :

- Descripteurs de fichiers, sockets, mémoire d'états, PIDs
- Session SSL, chiffrement IPsec
- Pages dynamiques, requêtes SQL, téléchargements, SPAM
- Remplir les journaux (et rendre la recherche plus complexe)

> Rendre le service inopérant en exploitant (continuellement) une faille dans le réseau, le système, le service ou l'application ou en détruisant des informations

> Plus simple pour un *script kiddie* de monter un déni de service que de pénétrer un système :

- Permet de se « venger » et de créer des *netsplits* sur IRC
- Les agents et les systèmes sous contrôle se négocient

Définition (2)

- **Objectif des dénis de services**
  - > Attaque depuis une seule source ou attaque « mutualisée » depuis un grand nombre de sources distribuées
  - > Adresse source manipulée ou utilisation de rebonds (« stepping stone ») pour :
    - Masquer la source
    - Amplifier l'attaque
    - Rendre le filtrage de la source impossible
    - Faire croire qu'un « concurrent » attaque
  - > Malheureusement beaucoup d'attaques sont encore utilisées et possible des mois, voire des années après leur découverte :
    - Intrinsèque au protocole ou à l'infrastructure
    - Solution non-encore disponible ou non déployée

Attaques : architecture (1)

» **Attaque « simple »**

> Quelques noms :

- (win)nuke, ping of death, land, teardrop, jolt, pepsi, bo(i)nk, nestea(2), naptha (et dérivés), 3wahas, stream, fraggle, ou une combinaison de plusieurs « techniques » (targa/rape)

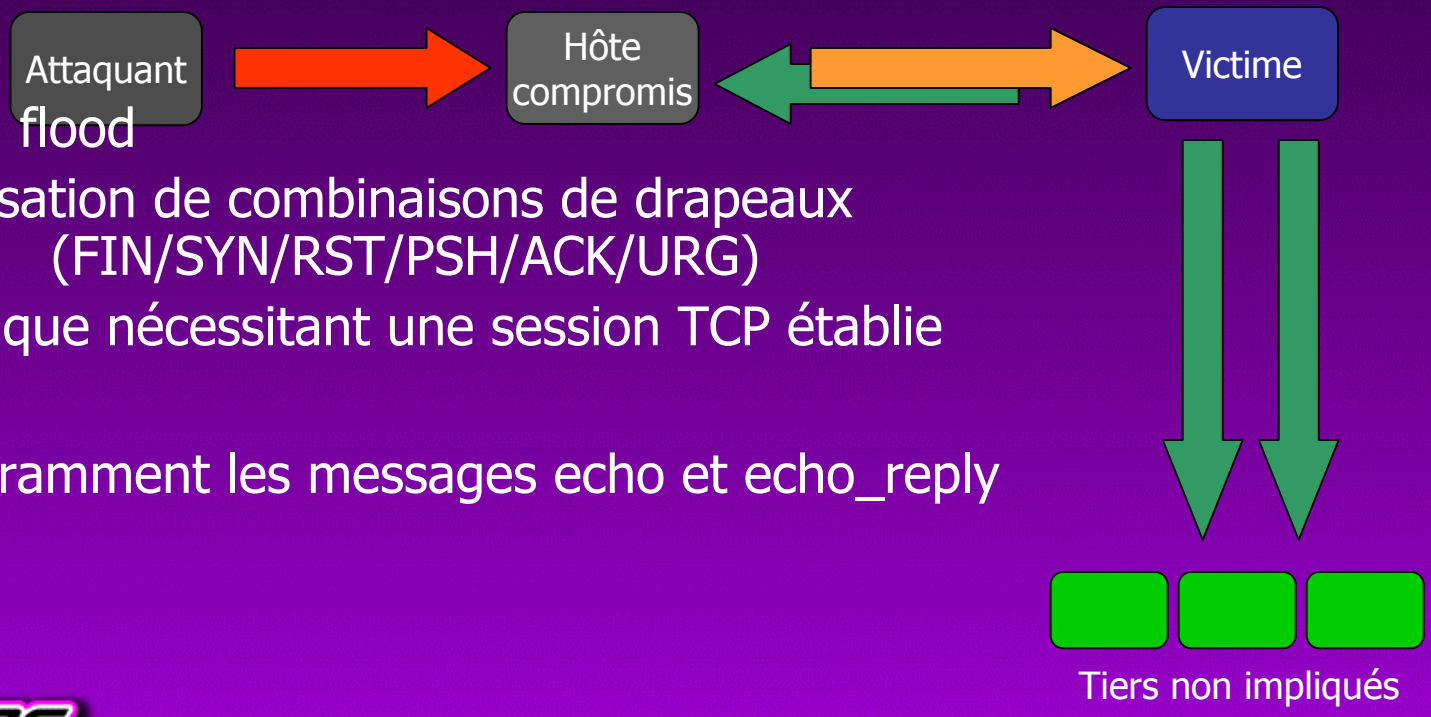
> TCP

- SYN flood
- Utilisation de combinaisons de drapeaux (FIN/SYN/RST/PSH/ACK/URG)
- Attaque nécessitant une session TCP établie

> ICMP

- Couramment les messages echo et echo_reply

> UDP

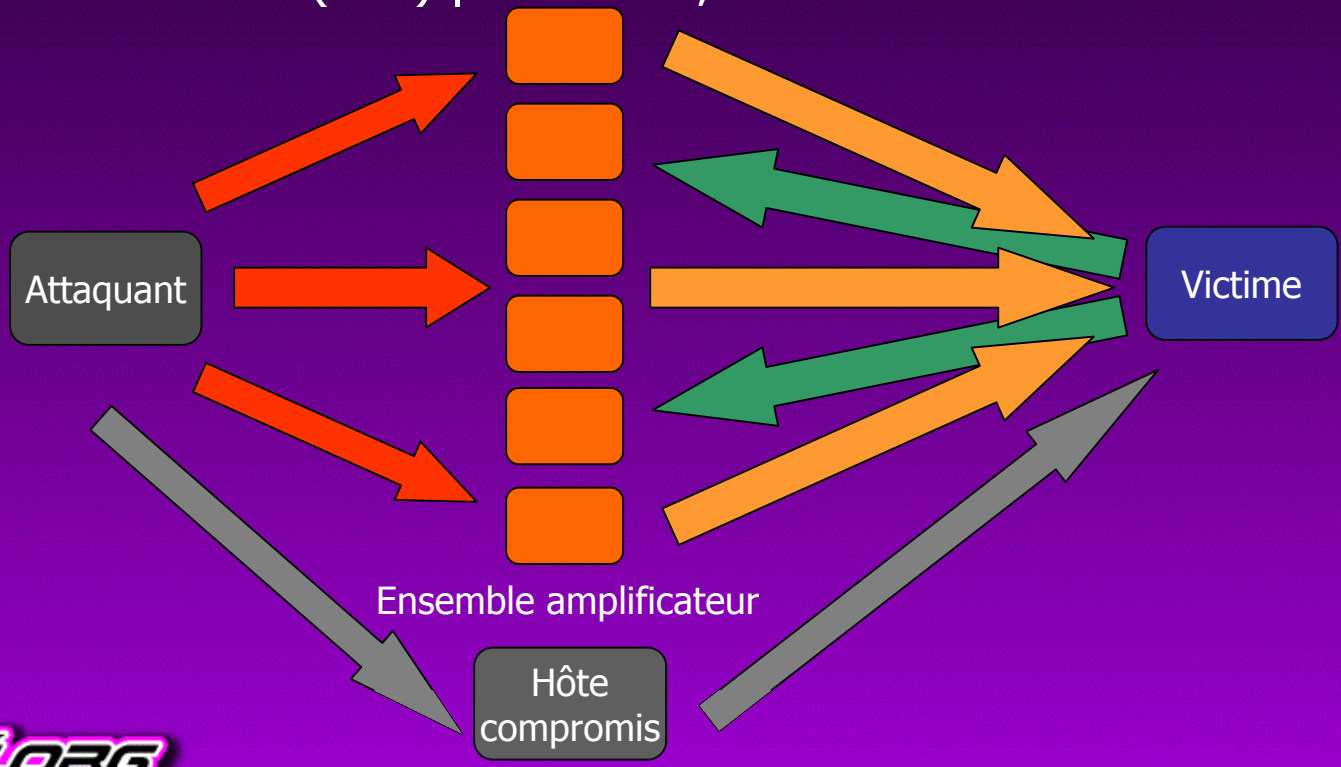


Attaques : architecture (2)

» **Attaque « par amplification » ou « par réflexion »**

> Attaque « simple », mais amplifiée (facteur 10-1000:1) et/ou « par rebond » (facteur 1 pour 1) :

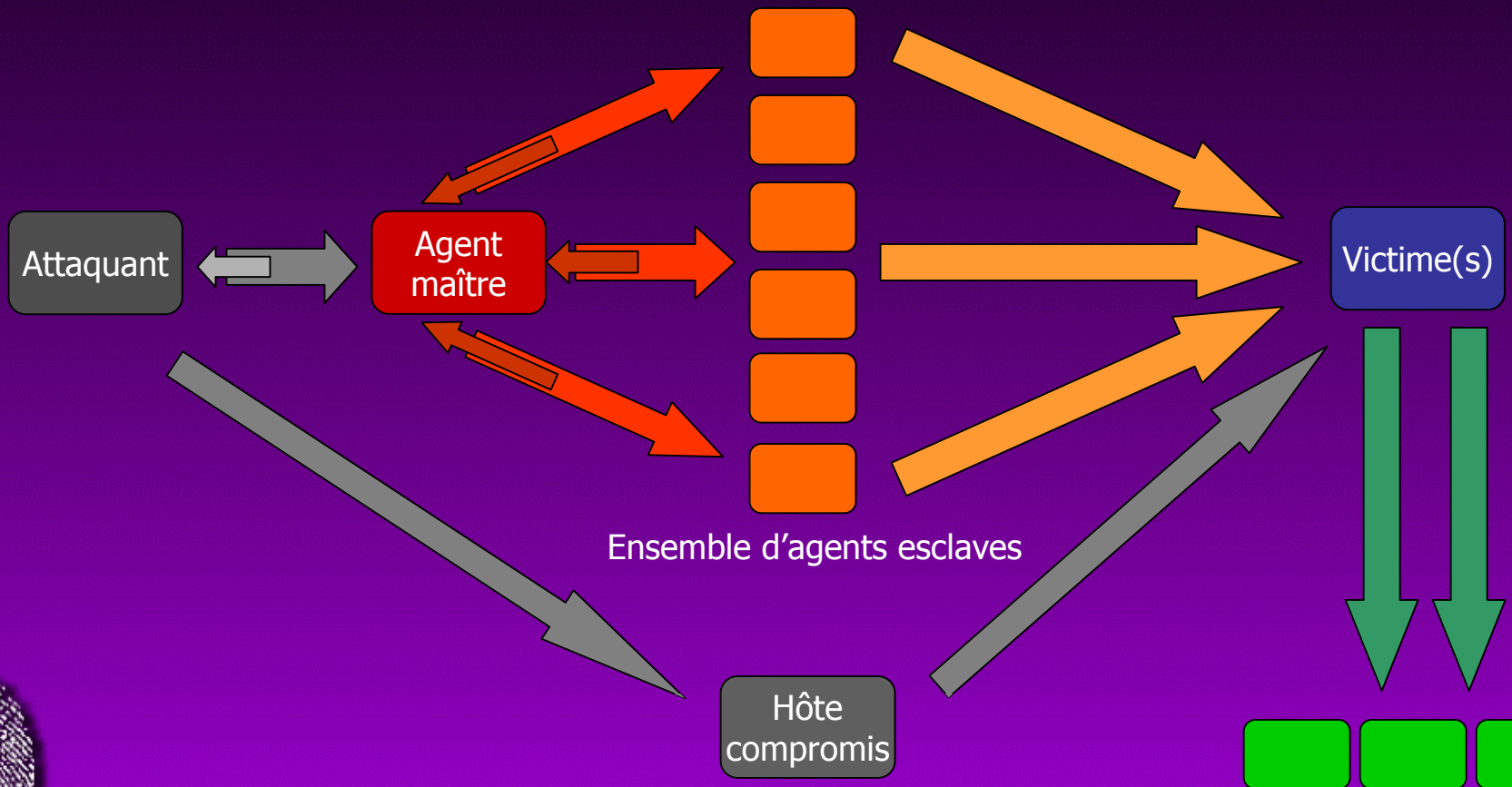
- smurf, clients/serveurs P2P, serveurs DNS, implémentations TCP aux NSI (ISN) prévisibles, etc.



Attaques : architecture (3)

» **Attaque « mutualisée »**

> Fréquemment une seule cible



Attaques : les agents (1)

- **Les agents esclaves**
  - > Serveurs ou services détournés de leur fonctionnement « normal », également des équipements réseaux (routeurs)
  - > Serveurs compromis avec un agent dédié installé :
    - Trinoo, TFN{(2,3)k}, omega, Stacheldrat*, Carko, Trinity, etc.
    - Chevaux de Troie
  - > Outils P2P (peer-to-peer)
- **Répartition des agents**
  - > Même(s) réseau(x) : école, entreprise, ISP, cable/DSL
  - > Même « pays »
  - > Même continent
  - > Même type de réseau : ilôt IPv6, mbone, Internet2
  - > Aléatoirement distribués sur Internet

Attaques : les agents (2)

» **Déploiement des agents et communication**

> « A la main »

> Script automatisé (récupérant des informations sur un serveur central via HTTP/FTP/DCC/etc)

> Agents DDoS installés grâce à un ver ou à un virus et masqués par un *{tool,root}kit* (adore, t0rn, par exemple) :

- Acquisition rapide d'un grand nombre d'hôtes
- Signe précurseur d'une attaque ?
- VBS/*, Win32/*, Code*, Nimda, 1i0n/ramen, etc.
- La (bio)diversité permet de résister à certains vers, mais est source de complexité

> Serveurs FTP « pirates »

> « Fausse » mise à jour pour un programme répandu

> Serveurs IRC, outils P2P, messagerie instantanée, etc.

Attaques : au niveau liaison

» **Les protocoles « sensibles »**

> ARP : détourner le trafic et déni de service

> CDP : déni de service

> STP : création de boucles dans le réseau

> VTP : modifier les VLANs

> DTP : transporter les VLANs (et donc le trafic) sur le réseau

> DHCP/BOOTP : détourner le trafic et déni de service

Attaques : au niveau réseau

» **Attaques « locales »**
  > Protocoles de routage de type IGP (OSPF, (E)IGRP, IS-IS)

» **Attaques « distantes »**
  > Segment TCP avec certains drapeaux
  > Datagrammes UDP (fragmentés)
  > Messages ICMP (divers et fragmentés)
  > Paquet isolé contenant un débordement de tampon, chaîne de format, etc.
  > Injection de routes dans eBGP

Détection (1)

- **Définissez des métriques et modélisez le comportement (a)normal de vos réseaux, systèmes et applications**
- **Au niveau réseau**
  - > De nouveaux flux SMTP et/ou HTTP
  - > Taille et fragmentation des paquets
  - > Distribution protocolaire (TCP/UDP/ICMP)
  - > Charge de la ligne, processeur, mémoire, temps de réponse
  - > Analyse statistique avancée du trafic
- **Au niveau système/applicatif**
  - > Pare-feu, xIDS, NMS
  - > Journaux
  - > Charge processeur, mémoire, temps de réponse
  - > Tables d'état (« état » des sessions TCP par exemple)

Détection (2)

- **Détection par corrélation**
  - Au niveau local en combinant les événements de plusieurs sources : xIDS/pare-feu/ACLs/NMS/« pot(s) de miel »
    - Cela permet de détecter/réduire les faux positifs et/ou les faux négatifs
  - En participant et/ou en payant pour un service qui analyse des journaux pseudo anonymes et vous informe des attaques « en cours »
  - Paquets, transactions, comportements « bizarres » précédant une attaque (résolution DNS, *scan* par nmap/queso/xprobe, etc)
- **Détection des anomalies en s'aidant de l'IA**
  - Encore dans les laboratoires R&D

Détection (3)

» **Comment retrouver la source d'une attaque ?**

> Journaux locaux

> Journaux des relais « mal nettoyés »

> Archives/serveurs publics d'information de routage :

- Dans quel AS était « routé » le préfixe réseau
- Quels serveurs de routes « voyaient » la même chose

> Exports Netflow (ou RMON, mais impact important)

> Traces réseaux :

- Très rarement de traces réseaux (encore moins de traces pour les protocoles de la couche liaison)
- Démarrent souvent après l'attaque
- En fonction de l'architecture la capture de trafic est complexe voire impossible

Protection (1)

» **Quels sont les problèmes ?**

> Adresses IP source falsifiées et diverses

> La source de l'attaque est « loin » au sens réseau

> Vous ne pouvez (souvent) que subir et attendre :

- Vous et votre ISP êtes les derniers de la chaîne
- Les ISPs « source » sont dans la zone APNIC
- Les blocs « routés » ne sont pas alloués et sont éphémères

> Il n'est pas facile d'identifier le type de trafic générant le déni de service : il faut être proactif et non réactif

> Votre réseau est souvent conçu pour être redondant, divisé en domaines et « survivre » à la panne de certains équipements : faites de même pour la protection vis-à-vis des dénis de service.

Protection (2)

» **Quelles sont les solutions ?**

> Il n'y a pas de solution technique qui protége de toutes les attaques :

- Configuration des équipements et architecture du réseau
- Systèmes et applicatifs « à jour », audités et surveillés

> Il est possible de filtrer ces attaques à différents niveaux :

- Commutateurs, routeurs, pare-feux, xIDS « réactifs »
- Equipements dédiés : des solutions commerciales locales et distribuées se développent, mais impliquent (encore/heureusement ?) une décision humaine
- Système/application (décodez et filtrez les paramètres)

> Faut-il « détruire » le trafic ou également répondre ?

- RST en réponse à des SYN ?
- Ne rendez pas la situation plus complexe et plus dramatique

Protection (3)

- **Au niveau liaison de données**
  - Désactivez et filtrez (suivant l'architecture de votre réseau) tous les protocoles « inutiles »
    - CDP, STP, DTP, VTP
  - Surveillez (voire fixez) les caches et les tables ARP de vos équipements et systèmes

Protection (4)

» **Au niveau réseau**

> Bande passante : impliquez, si possible, votre FAI

- Nécessite une coopération forte entre les FAI et/ou des solutions de détection/prévention distribuées dans des points d'échange (IX) et d'interconnection entre FAI : il existe des solutions commerciales
- Pourquoi autoriser plus de 64Kb/s de trafic ICMP et/ou UDP sur votre connexion Internet ? Tenez compte du trafic légitime (DNS et Path MTU Discovery par exemple)
- Si votre bande passante vous est facturée « à l'utilisation » cela à encore un impact de coût supplémentaire

> Filtrez les adresses IP sources et destinations :

- Vos plages d'adresses IP
- Réseaux DSUA (RFC 1918, AutoDHCP, classes D/E, etc)
- Acceptez uniquement les adresses venant de blocs alloués

Protection (5)

- **Au niveau réseau**
  - Ne pas « router » ou accepter certains blocs clairement identifiés comme des sources d'attaques (méthode empirique, comparable à filtrer *@{hotmail, yahoo}.com au niveau SMTP)
  - Si vous annoncez plusieurs plages d'adresses dans votre AS et que celle attaquée est en PI (Provider Independent), arrêtez de l'annoncer durant une certaine durée (1h au minimum). Cette technique est courante pour les serveurs IRC
  - Prévoyez des mécanismes d'administration « out-of-band » pour pouvoir vous connecter sur vos équipements, voire un deuxième FAI (attention au routage, aux plages et à la traduction d'adresses (NAT))

Protection (6)

» **Au niveau réseau**

> « Blacklister » automatiquement (ou de façon sélective) peut vous rendre inaccessible rapidement (caches HTTP et opérateurs DSL/cable).

> En fonction de votre choix de filtrage vous n'aurez même plus de traces :

- Routage dynamique dans Null0/reject sur des routeurs
- Règle « drop » sans journalisation, uRPF
- Filtrage en amont dans le réseau (chez le FAI par exemple)

> Evaluez si vous voulez voir le trafic disparaitre ou si vous voulez uniquement limiter la quantité de trafic, voire le rediriger vers un système prévu à cet effet

> Filtrez en fonction de certaines caractéristiques (TTL, ip.id, ip.length, ISNs, type de message ICMP, ports, etc)

Protection (7)

- **Au niveau transport**
  - > Segments TCP avec le drapeau SYN :
    - Utilisation de « cookies » (idem pour IPsec par exemple)
    - Ouverture de session TCP interceptée par un équipement intermédiaire (routeur, pare-feu, filtre DDoS)
  - > Sessions TCP « ouvertes » :
    - Utilisez des distributeurs de charges pour rediriger une partie du trafic (soit pour ralentir l'attaque, soit vers un trou noir, soit - en fonction de certaines règles - vers un système dédié)
    - Nécéssité d'un équipement/technique qui intercepte ou surveille toute la session TCP ?
- **Au niveau « applicatif »**
  - > Filtrez avec des relais applicatifs
  - > Equipements qui « reconnaissent » et filtrent les flux

Protection (8)

» **Au niveau de l'Internet**

> Propositions techniques (drafts) :

- ICMP traceback (itrace)
  - Le routeur adresse un message ICMP horodaté (et authentifié) à la même destination que celle du datagramme pris au hasard qu'il vient de « router/forwarder ». Ce message contient le saut précédent, le saut suivant ainsi qu'une partie de ce datagramme
  - La probabilité étant faible (1/{1,2}0000), ce concept n'est valide que pour des attaques de taille conséquente
- MULTOPS (Multi-Level Tree for Online Packet Statistics)
  - Une structure de données sur le routeur stocke les flux par préfixes et est analysée par rapport à une heuristique simple (trafic asymétrique) pour détecter mais aussi réagir aux attaques
- IDIP (Intruder Detection and Isolation Protocol)
  - Protocoles, composants et architecture permettant la détection, la corrélation, la centralisation ainsi que la réponse aux intrusions

Protection (9)

» **Au niveau de l'Internet**

> Propositions techniques (drafts) :

- SPIE (Source Path Isolation Engine)
  - . Le router stocke temporairement des informations (hash) sur les datagrammes qui passent par lui. La destination peut interroger les routeurs dans son « domaine » pour obtenir ces informations
  - . Permet de retrouver même un flux isolé
- IP Traceback
  - . Le routeur « marque » (champ ip.id) au hasard des datagrammes IP avec des informations compressées sur les routeurs IPT traversés/d'extrêmités
  - . La probabilité de retrouver des traces est meilleure que pour ICMP Traceback, mais nécessite une modification des datagrammes et les besoins CPU/mémoire sont importants
- Caller Identification System in the Internet Environment
  - . Tentative d'implémentation d'un équivalent du Caller ID (CLID)

Protection (10)

» **Au niveau de l'Internet**

> Propositions techniques (drafts) :

- HIP (Host Identity Payload/Protocol)
  - . Introduit un nouvel espace de nommage (HI, en plus d'IP/DNS) et une authentification à clé publique des hôtes via un échange Diffie Hellman (DH)
  - . HIP n'est pas aussi complet/complexe qu'IKE mais peut être utilisé avec ESP/IPsec (génération automatique d'une SA)
- Pushback
  - . Le routeur qui a détecté un déni de service (par rapport à certaines caractéristiques du trafic) le fait savoir à ses « voisins » pour qu'ils réduisent/limitent la bande passante pour ces préfixes
- CenterTrack
  - . Réseau secondaire (tunnel IP/GRE et routage dynamique) dans lequel sont transférés les datagrammes « intéressants » pour analyse sur un équipement spécialisé/dédié

Protection (11)

» **Au niveau de l'Internet**

> Propositions techniques (conclusion) :

- Véritable challenge technique !
- Implique des changements fondamentaux (architecture, déploiement, opérations, etc)
- Ne reste qu'une partie de la solution et ne permet pas de retrouver systématiquement et facilement la source d'une attaque

> Filtrage {in,e}gress

> Déploiement de S-BGP, IPsec (AH), IPv6, ECN, multicast ?

> Ne pas accepter de trafic de certains FAI (AS/préfixes)

> Les dénis de services légitimes (« Slashdot effect »)

> Evolution des lois (criminalité informatique)

> « Sécuriser tout l'Internet » ;-)

Conclusion

- **Quel futur ?**
  - La recherche dans ce domaine est très active mais peu de publications sont diffusées (offensif / défensif)
  - Utilisation d'équipements pouvant générer beaucoup de trafic (routeurs, commutateurs multiniveau)
  - Agents et vers plus « intelligents »
  - Un nouveau bac à sable : Internet2
  - Introduire « un peu de finesse dans ce monde de brutes » : les attaques sont souvent émotives et peu réfléchies
- **Et vous ?**
  - Analyse post-mortem et procédure de réponse aux incidents
  - Participez à la réduction des dénis de services en sécurisant votre réseau !

That's all folks :-)

- **Dernière version de la présentation**

  < http://www.securite.org/presentations/ddos/ >

- **Présentation « Protection de l'infrastructure réseau en environnement IP »**

  < http://www.securite.org/presentations/secip/ >

- **Questions/Réponses**

Image: http://www.inforamp.net/~dredge/funkycomputercrowd.html

Merci aux membres du groupe eXperts et AC pour la relecture et les commentaires, et à vous pour votre participation.