BGP et DNS: attaques sur les protocoles critiques de l'Internet

Nicolas Dubée – ndubee@secway.fr
Secway / BD Consultants
Mai 2003

Plan de la présentation

- Les infrastructures critiques
- Aperçu de BGP
- Vulnérabilités de BGP
- Risques sous-jacents
- Solutions pour la sécurisation

Infrastructures critiques

- Les infrastructures critiques, un axe à la mode dans la problématique de défense nationale
  - Notion d'infrastructures critiques
  - Notion d'interdépendance des IC
  - Identification des infrastructures critiques
  - Protection de celles-ci
- Depuis récemment, Internet vu comme une infrastructure critique
  - Notamment aux USA
  - Nombreuses réflexions engagées dans la plupart des pays occidentaux

Infrastructures critiques sur Internet (1/2)

- On ne considère pas ici les réseaux physiques, l'électricité…
  - Sont eux-mêmes d'autres infrastructures critiques
- Sont considérés comme critiques pour Internet[2] :
  - DNS
  - BGP
  - La caféine !

Infrastructures critiques sur Internet (2/2)

- “National Strategy to Secure Cyberspace” (17 fév. 2003)
  - Stratégie "***whose goal is to engage and empower Americans, to secure the portions of cyberspace that they own, operate, control, or with which they interact."***
- Plan à 5 ans

Cadre de l'exposé

- Nous nous attacherons dans la suite à BGP uniquement
- Nous verrons les vulnérabilités du protocole BGPv4
- Nous évaluerons les risques associés, au niveau de l'infrastructure

BGP, Internet et nous

- BGP est au cœur du routage sur Internet
  - Assure le partage d'informations de routage entre systèmes (routeurs)
  - Des incidents passés (mauvaises configurations) ont montré les risques liés à BGP : AS7007 en 1997
  - Attention du public importante autour de BGP, nombreuses rumeurs[4]
- BGP est aussi présent là où on ne l'attend pas
  - MBGP utilisé pour propagation de routes pour VPNs sur backbones d'opérateurs en MPLS[3]

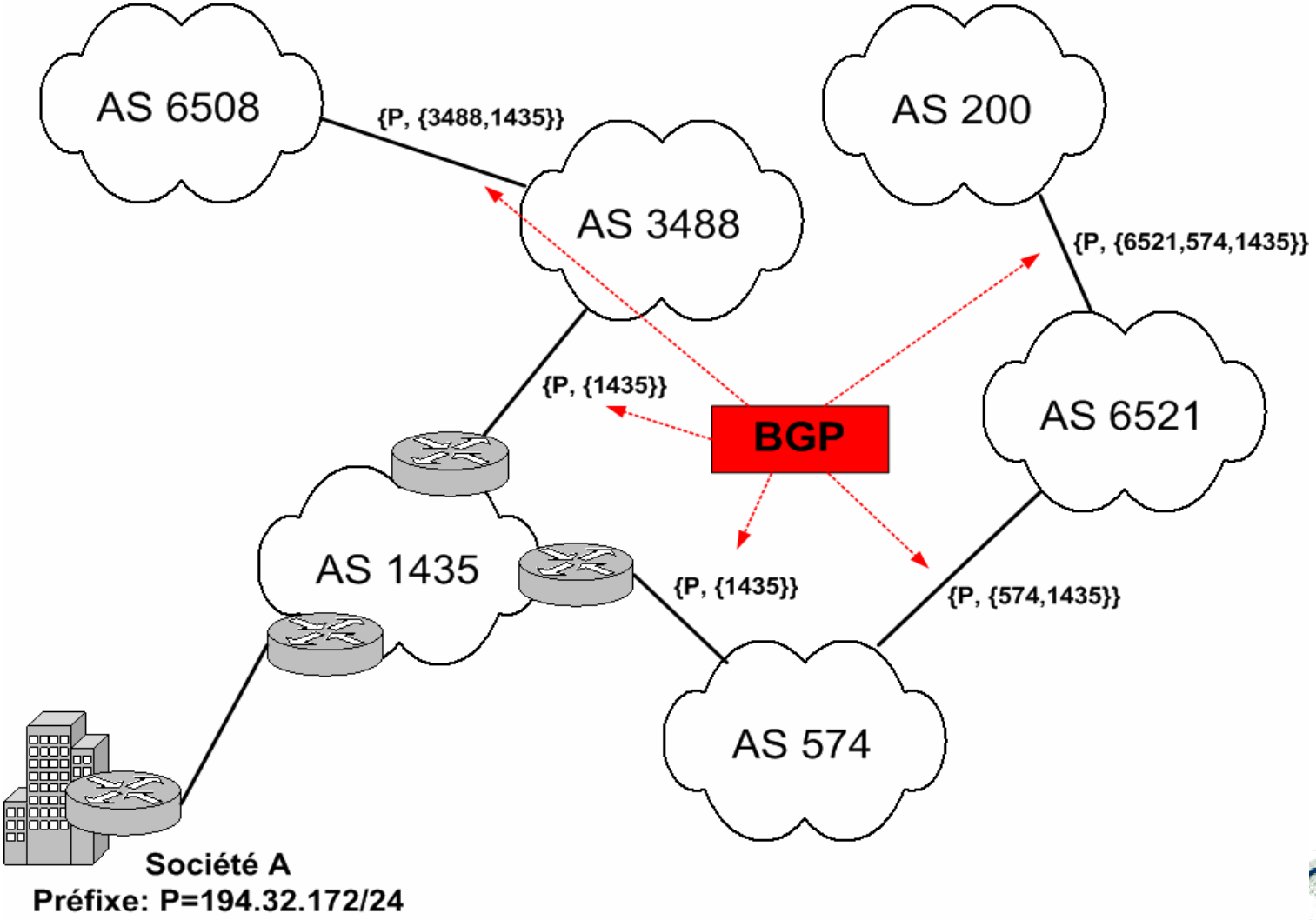
Aperçu de BGP (1)

- Version actuelle 4, définie en 1994 par RFC 1654 et 1771
- Notion d'AS, *Autonomous System*
  - Groupe d'un ou plusieurs préfixes (=réseaux) ayant une politique de routage commune
  - Identifié par un numéro
  - Exemple: 194.51.23.0/24 appartient à l'AS3215 de France Telecom Transpac
- BGP est un protocole permettant l'échange d'informations d'accessibilité entre AS
- Maintien de la *table de routage Internet globale*

Aperçu de BGP (2)

- Construit au dessus de TCP, port 179
  - Donc pas de broadcast/multicast
  - Propagation entre pairs préconfigurés, non forcément adjacents
  - Pas de topologie dans les connexions entre pairs
- Machine à états finis
- Échange de messages simples
  - *Open*
  - *Update*
  - *Notification, Keepalive*
- *AS path* constitué pour chaque préfixe annoncé

Aperçu de BGP (3)



Vulnérabilités

- Pas d'authentification requise des pairs
  - Par défaut la seule barrière est la négociation TCP
  - Authentification MD5 par secret partagé optionnelle
- Pas de validation des informations
  - Nécessité de faire confiance à ses voisins sur les préfixes qu'il annonce
    - Possibilité (très recommandée) de filtrer
    - Mais très difficile quand on se rapproche du cœur du réseau…
  - Impossible de vérifier la validité du message en terme d'insertion, modification, *replay*
- Pas de confidentialité (mais rarement requis)

Dénis de service ciblés

- Le routeur BGP est pris pour cible d'un déni de service classique
  - SYN flood sur port 179
  - Attaque par oscillation, *router flap* et *flap* par ses peers
- Faisabilité
  - Aisée si aucune mesure n'a été prise pour réduire ce trafic parasite et si routeur mal dimensionné

Réinitialisation de sessions (1)

- Spoof d'un RST TCP pour fermer la connexion BGP entre deux routeurs
  - Flush des routes associées au pair en question
  - La session de peering est redémarrée par l'un des pairs
  - Déni de Service efficace si réitéré continuellement

Réinitialisation de sessions (2)

- Faisabilité ?
  - Nécessite d'avoir:
    - IP SRC, Port SRC
    - TCP SEQ dans window
    - IP TTL à 1 (selon les implémentations courantes)
  - En pratique difficilement faisable sans pouvoir sniffer le réseau
    - Ce qui est souvent encore plus difficile !

Hijacking de sessions

- Injection de messages dans un flux BGP établi
  - Donc insertion/retrait de routes, fin de session, …
- Faisabilité ?
  - Nécessite de spoofer tous les paramètres TCP
  - Plus informations propres à la session BGP
  - Très difficile sans sniffer le réseau des peers

Constats

- L'attaque par un tiers hors BGP est très délicate
  - Attention au hack de routeurs cependant !!!
- Les risques sont plus liés aux acteurs de BGP
- La plupart des risques qui vont suivre peuvent être aussi bien des mauvaises configurations que des hacks
  - En BGP, les « oops! » ne pardonnent pas
  - C'est ce qui rend BGP dangereux…

Désagrégation

- Annonce de préfixes plus spécifiques
  - En BGP, les préfixes plus spécifiques prennent précédence
  - Principalement un déni de service important
  - Possibilité de partitionner le réseau cible en préfixes plus longs et annoncer ces préfixes au monde entier
- Faisabilité
  - Forte si l'*upstream* ne filtre pas les annonces reçues du réseau pirate, propagation probablement limitée cependant
  - Incident AS7007, 04/1997, désagrégation de tout Internet

Injection de routes (1)

- Annonce de préfixes pour lequel l'émetteur n'a pas autorité
  - Couplé avec un préfixe plus long
  - Risque de détournement du trafic destiné au réseau victime vers cible arbitraire
  - Soit déni de service (*blackhole*, cible de trafic)
  - Soit hack :
    - Interception de trafic
    - *Takeover* complet de flux par *Man-in-the-Middle*
    - *Masquerade* de serveurs

Injection de routes (2)

- Faisabilité
  - Peu (pas?) de malveillances volontaires connues, plutôt des négligences
  - Théoriquement faisable, nécessite un filtrage laxiste de la part des *upstreams*
  - Possibilité de rebonds : p.e., injections sur les préfixes de *root-servers DNS* plutôt que de la cible…

Injection de routes (3)

- Cas particuliers :
  - Annonce de préfixes non alloués
    - Saturation des tables
    - Couplée à des DDoS classiques, remontée importante d'ICMP Unreach vers les routeurs annonçant
  - Annonce de préfixes DUSA (192.168.0.0/16 par exemple)

Attaques sur les implémentations

- Comme toute implémentation, celle faite de BGP dans les routeurs est sujette à problèmes
- Le parc des core routers est-il suffisamment hétérogène pour éviter une avalanche si bug trouvé dans une implémentation ???
- Exemple des root-servers DNS : remplacement de BIND par NSD surk.root-servers.net (fév. 2003)

Sécurisation (1)

- Un protocole urgent selon certains : S-BGP
  - IPsec pour la communication inter-peers
  - Framework PKI entre tous les participants
  - Autorisations pour annoncer des préfixes
  - RR CA opérés par RIPE, ARIN, APNIC, …
- Extension concurrente : SOBGP (Cisco)

Sécurisation (2)

- Pour l'instant, flux remontant via un ISP
  - Forcer l'authentification MD5 des peers
  - Utiliser un loopback ou une adresse secondaire pour le peering
  - Autoriser les clients à annoncer seulement leurs préfixes
  - Autoriser seulement les préfixes de l'ISP à en sortir

Sécurisation (3)

- Flux descendant des upstreams
  - Forcer l'authentification MD5 des peers
  - Utiliser un *loopback* ou une adresse secondaire pour le peering
  - Valider autant que possible ce qui arrive des peers (difficile…)
  - Filtrer les « bogons » et DUSA
  - Ne pas avoir de route par défaut

Conclusion (1/2)

- Erik Shrek, MCI (NANOG'28)
  - *"To be honest we have never seen any real attacks directed at BGP. There seem to be a lot of people focused on this, but the attacks are relatively hard to do compared to a ton of other attacks that are much easier to do."*

Conclusion (2/2)

- Des vulnérabilités ont été identifiées dans BGPv4
- Risques potentiels allant du déni de service à la redirection de trafic
- Peu de cas de malveillances connus actuellement
- Améliorations du protocole difficilement exploitables
- L'application des BCP devrait cependant limiter l'impact d'attaques BGP

Références

[1] Barry Greene, *BGPv4 Security Risk Assessment*, 06/2002

[2] Barry Greene, *Is the sky falling?*, présentation à NANOG25 – Toronto

[3] E. Rosen, Y. Rekhter, *BGP/MPLS VPNs*, RFC 2547

[4] Robert Lemos, *Expert: Router holes threaten Net*, http://zdnet.com.com/2100-1105-990608.html

[5] Iljitsch van Beijnum, *BGP*, O'Reilly 2002

[6] Y. Rekhter, T. Li, *A Border Gateway Protocol 4 (BGP-4)*, RFC 1771, 03/1995

[7] Stephen Kent, *Transitioning Secure BGP into the Internet*, BBN janv. 2001

[8] James Ng, *Secure Origin BGP (soBGP)*, IETF Internet Draft oct. 2002