BGP enfin pour de bon sécurisé

Stéphane Bortzmeyer
bortzmeyer@nic.fr

Sam Bowne
@sambowne

Suivre

I don't like BGPSEC because it adds too much complexity --David Conrad #InternetSummit

À l'origine en anglais

22:35 - 14 sept. 2017

Le problème

Il est bien connu (RFC 7908) :

Le problème

Il est bien connu (RFC 7908) :

- 2008, Pakistan Telecom annonce le préfixe de YouTube et DoS YouTube,

Le problème

Il est bien connu (RFC 7908) :

- 2008, Pakistan Telecom annonce le préfixe de YouTube et DoS YouTube,
- 2013, un opérateur biélorusse (?) annonce des préfixes et réinjecte (?) le trafic, après espionnage (?),

afnic

Le problème

Il est bien connu (RFC 7908) :

- 2008, Pakistan Telecom annonce le préfixe de YouTube et DoS YouTube,
- 2013, un opérateur biélorusse (?) annonce des préfixes et réinjecte (?) le trafic, après espionnage (?),
- 2015, Telekom Malaysia fuit, mais en respectant l'AS d'origine du chemin (`1.0.208.0/22` annoncé avec le chemin `4788 3491 4651 9737 23969` où 4788 est Telekom Malaysia et 23969 est bien le titulaire du préfixe),

afnic

Le problème

Il est bien connu (RFC 7908) :

- 2008, Pakistan Telecom annonce le préfixe de YouTube et DoS YouTube,
- 2013, un opérateur biélorusse (?) annonce des préfixes et réinjecte (?) le trafic, après espionnage (?),
- 2015, Telekom Malaysia fuit, mais en respectant l'AS d'origine du chemin (`1.0.208.0/22` annoncé avec le chemin `4788 3491 4651 9737 23969` où 4788 est Telekom Malaysia et 23969 est bien le titulaire du préfixe),
- 2017, Google annonce plein de préfixes et coupe l'Internet au Japon.

afnic

Solution zéro : alarmes et coopération

En pratique, ça marche plutôt bien.

Première solution : IRR et filtres

RFC 7682

```
route6:          2a04:cec0::/29
descr:           BOUYGTEL-ISP
origin:          AS5410
mnt-by:          BYTEL-MNT
created:         2016-03-24T00:56:53Z
last-modified:   2016-03-24T00:56:53Z
source:          RIPE
```

afnic

Première solution : IRR et filtres

RFC 7682

```
route6:          2a04:cec0::/29
descr:           BOUYGTEL-ISP
origin:          AS5410
mnt-by:          BYTEL-MNT
created:         2016-03-24T00:56:53Z
last-modified:   2016-03-24T00:56:53Z
source:          RIPE
```

- Les objets route ne sont pas toujours bien maintenus,

afnic

Première solution : IRR et filtres

RFC 7682

```
route6:          2a04:cec0::/29
descr:           BOUYGTEL-ISP
origin:          AS5410
mnt-by:          BYTEL-MNT
created:         2016-03-24T00:56:53Z
last-modified:   2016-03-24T00:56:53Z
source:          RIPE
```

- Les objets route ne sont pas toujours bien maintenus,
- Il faut dire que c'est pénible (relations client-fournisseur compliquées).

afnic

Première solution : IRR et filtres

RFC 7682

```
route6:          2a04:cec0::/29
descr:           BOUYGTEL-ISP
origin:          AS5410
mnt-by:          BYTEL-MNT
created:         2016-03-24T00:56:53Z
last-modified:   2016-03-24T00:56:53Z
source:          RIPE
```

- Les objets route ne sont pas toujours bien maintenus,
- Il faut dire que c'est pénible (relations client-fournisseur compliquées).

[Au passage, n'oublions pas de configurer un nombre maximal de préfixes pour les pairs.]

afnic

Deuxième solution : ROA

ROA = *Route Origin Authorization*. RFC 6482 et 6811

Deuxième solution : ROA

ROA = *Route Origin Authorization*. RFC 6482 et 6811

- Une RPKI (*Resource Public Key Infrastructure*) stocke des certificats pour les ressources Internet (ASN, préfixes. . .),

Deuxième solution : ROA

ROA = *Route Origin Authorization*. RFC 6482 et 6811

- Une RPKI (*Resource Public Key Infrastructure*) stocke des certificats pour les ressources Internet (ASN, préfixes. . .),
- On publie des ROA pour ses préfixes, annonçant « tel AS peut être origine de tel préfixe »,

Deuxième solution : ROA

ROA = *Route Origin Authorization*. RFC 6482 et 6811

- Une RPKI (*Resource Public Key Infrastructure*) stocke des certificats pour les ressources Internet (ASN, préfixes. . .),
- On publie des ROA pour ses préfixes, annonçant « tel AS peut être origine de tel préfixe »,
- Un cache/validateur vérifie les ROA et rejette les invalides,

afnic

Deuxième solution : ROA

ROA = *Route Origin Authorization*. RFC 6482 et 6811

- Une RPKI (*Resource Public Key Infrastructure*) stocke des certificats pour les ressources Internet (ASN, préfixes. . .),
- On publie des ROA pour ses préfixes, annonçant « tel AS peut être origine de tel préfixe »,
- Un cache/validateur vérifie les ROA et rejette les invalides,
- Le routeur récupère cette information en RTR (RFC 6810).

afnic

Limites des ROA

Limites des ROA

- Ne vérifie que l'origine, pas tout le chemin d'AS,

Limites des ROA

- Ne vérifie que l'origine, pas tout le chemin d'AS,
- C'est suffisant pour attraper les erreurs, pas les attaques,

afnic

Limites des ROA

- Ne vérifie que l'origine, pas tout le chemin d'AS,
- C'est suffisant pour attraper les erreurs, pas les attaques,
- Cahier des charges de BGPsec, RFC 7353

afnic

BGPsec

Principes (RFC presque publiés) :

BGPsec

Principes (RFC presque publiés) :

- On utilise la même RPKI que les ROA,

BGPsec

Principes (RFC presque publiés) :

- On utilise la même RPKI que les ROA,
- Chaque routeur de bordure d'AS signe avant de transmettre l'annonce,

BGPsec

Principes (RFC presque publiés) :

- On utilise la même RPKI que les ROA,
- Chaque routeur de bordure d'AS signe avant de transmettre l'annonce,
- Bien plus dynamique que les ROA, donc (et BGPsec ne remplace pas ROA),

BGPsec

Principes (RFC presque publiés) :

- On utilise la même RPKI que les ROA,
- Chaque routeur de bordure d'AS signe avant de transmettre l'annonce,
- Bien plus dynamique que les ROA, donc (et BGPsec ne remplace pas ROA),
- Pour valider, il faut une chaîne continue de routeurs BGPsec.

afnic

Détails techniques

Détails techniques

- Nouvel attribut `BGPsec_Path`, qui remplace `AS_PATH`,

Détails techniques

- Nouvel attribut `BGPsec_Path`, qui remplace `AS_PATH`,
- Les deux pairs doivent le gérer, donc capacité `BGPsec Capability`, sinon, il faut repasser en `AS_PATH`,

Détails techniques

- Nouvel attribut `BGPsec_Path`, qui remplace `AS_PATH`,
- Les deux pairs doivent le gérer, donc capacité `BGPsec Capability`, sinon, il faut repasser en `AS_PATH`,
- Non transitif (il faut le refaire à chaque fois qu'on change d'AS),

Détails techniques

- Nouvel attribut `BGPsec_Path`, qui remplace `AS_PATH`,
- Les deux pairs doivent le gérer, donc capacité `BGPsec Capability`, sinon, il faut repasser en `AS_PATH`,
- Non transitif (il faut le refaire à chaque fois qu'on change d'AS),
- Il contient une liste d'AS, chaque AS signé par un routeur de l'AS,

Détails techniques

- Nouvel attribut `BGPsec_Path`, qui remplace `AS_PATH`,
- Les deux pairs doivent le gérer, donc capacité `BGPsec Capability`, sinon, il faut repasser en `AS_PATH`,
- Non transitif (il faut le refaire à chaque fois qu'on change d'AS),
- Il contient une liste d'AS, chaque AS signé par un routeur de l'AS,
- Chaque routeur sur le chemin doit valider le `BGPsec_Path`,

Détails techniques

- Nouvel attribut `BGPsec_Path`, qui remplace `AS_PATH`,
- Les deux pairs doivent le gérer, donc capacité `BGPsec Capability`, sinon, il faut repasser en `AS_PATH`,
- Non transitif (il faut le refaire à chaque fois qu'on change d'AS),
- Il contient une liste d'AS, chaque AS signé par un routeur de l'AS,
- Chaque routeur sur le chemin doit valider le `BGPsec_Path`,
- Comme avec IRR ou ROA, la décision en cas d'échec de la validation est une décision locale.

afnic

En fait. . .

En fait. . .

- J'ai simplifié l'algorithme,

En fait. . .

- J'ai simplifié l'algorithme,
- L'attribut `BGPsec_Path` contient en fait une liste de segments de chemins d'AS,

En fait. . .

- J'ai simplifié l'algorithme,
- L'attribut `BGPsec_Path` contient en fait une liste de segments de chemins d'AS,
- Un attaquant ne peut donc pas retirer des AS dans le chemin, ni en ajouter au milieu.

Pièges

Pièges

- Les communautés ne sont pas couvertes,

Pièges

- Les communautés ne sont pas couvertes,
- Toutes les manipulations ne sont pas détectées (prolongation d'un chemin légitime...), cf. RFC 7132,

Pièges

- Les communautés ne sont pas couvertes,
- Toutes les manipulations ne sont pas détectées (prolongation d'un chemin légitime. . .), cf. RFC 7132,
- « *The data plane does not always follow the control plane* »,

afnic

Pièges

- Les communautés ne sont pas couvertes,
- Toutes les manipulations ne sont pas détectées (prolongation d'un chemin légitime. . .), cf. RFC 7132,
- « *The data plane does not always follow the control plane* »,
- Les attaques par rejeu restent trop faciles,

afnic

Pièges

- Les communautés ne sont pas couvertes,
- Toutes les manipulations ne sont pas détectées (prolongation d'un chemin légitime. . .), cf. RFC 7132,
- « *The data plane does not always follow the control plane* »,
- Les attaques par rejeu restent trop faciles,
- Si on rejette des annonces invalides, on les verra peut-être venir via un autre pair.

afnic

Mises en œuvre

- BIRD (pas dans la distrib officielle)
- Quagga (idem)

afnic

Déploiement

Déploiement

- La nécessité d'un chemin complètement BGPsec va être un obstacle,

Déploiement

- La nécessité d'un chemin complètement BGPsec va être un obstacle,
- On veut vraiment de la sécurité ?

afnic

Merci !

www.afnic.fr
contact@afnic.fr