

*afnic*

# RPKI + ROA, sécuriser enfin le routage BGP ?

*Stéphane Bortzmeyer*

AFNIC

*bortzmeyer@nic.fr*

*afnic*

Vide, exprès

*afnic*

2 / 30

# Définir le problème

# Définir le problème

- 24 février 2008, Pakistan Telecom prive la planète de YouTube, sans pirater un seul routeur,

# Définir le problème

- 24 février 2008, Pakistan Telecom prive la planète de YouTube, sans pirater un seul routeur,
- 8 avril 2010, China Telecom détourne une partie du trafic (FoxNews dit que c'est grave),

# Définir le problème

- 24 février 2008, Pakistan Telecom prive la planète de YouTube, sans pirater un seul routeur,
- 8 avril 2010, China Telecom détourne une partie du trafic (FoxNews dit que c'est grave),
- 23 juin 2011, Open Transit annonce (entre autres) les routes de l'AFNIC.

# Définir le problème

- 24 février 2008, Pakistan Telecom prive la planète de YouTube, sans pirater un seul routeur,
- 8 avril 2010, China Telecom détourne une partie du trafic (FoxNews dit que c'est grave),
- 23 juin 2011, Open Transit annonce (entre autres) les routes de l'AFNIC.

À noter que, quoi qu'en dise FoxNews, les trois cas étaient des erreurs.

# Rappel BGP



# Rappel BGP

- 1 Le protocole standard d'échange des routes sur l'Internet,

# Rappel BGP

- 1 Le protocole standard d'échange des routes sur l'Internet,
- 2 Réseau de pairs configurés à la main : un pair transmet à son voisin les routes qu'il connaît. Elles sont ensuite retransmises aux autres voisins.

# Rappel BGP

- 1 Le protocole standard d'échange des routes sur l'Internet,
- 2 Réseau de pairs configurés à la main : un pair transmet à son voisin les routes qu'il connaît. Elles sont ensuite retransmises aux autres voisins.
- 3 Une annonce de route comprend un **préfixe** IP et un **chemin d'AS**. L'AS d'**origine** est le plus à droite. (AS = *Autonomous System*, typiquement un opérateur)

# Rappel BGP

- 1 Le protocole standard d'échange des routes sur l'Internet,
- 2 Réseau de pairs configurés à la main : un pair transmet à son voisin les routes qu'il connaît. Elles sont ensuite retransmises aux autres voisins.
- 3 Une annonce de route comprend un **préfixe IP** et un **chemin d'AS**. L'AS d'**origine** est le plus à droite. (AS = *Autonomous System*, typiquement un opérateur)
- 4 Contrairement au DNS, ce n'est pas un arbre mais un graphe (bordélique).

# Principes de la solution

# Principes de la solution

- ① Une infrastructure de distribution de **certificats numériques** prouvant qu'on contrôle un préfixe IP : la **RPKI** (*Resource Public Key Infrastructure*),

# Principes de la solution

- 1 Une infrastructure de distribution de **certificats numériques** prouvant qu'on contrôle un préfixe IP : la **RPKI** (*Resource Public Key Infrastructure*),
- 2 Des objets signés par le titulaire du préfixe, les **ROA** (*Route Origin Authorizations*). Un ROA est une **déclaration authentifiée** disant « Le préfixe `2001:db8:42::/48` peut être originé par l'AS 65584 ».

# Principes de la solution

- 1 Une infrastructure de distribution de **certificats numériques** prouvant qu'on contrôle un préfixe IP : la **RPKI** (*Resource Public Key Infrastructure*),
- 2 Des objets signés par le titulaire du préfixe, les **ROA** (*Route Origin Authorizations*). Un ROA est une **déclaration authentifiée** disant « Le préfixe 2001:db8:42::/48 peut être originé par l'AS 65584 ».

RFC 6480, <http://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>



La *Resource Public Key Infrastructure* est une infrastructure de distribution de :

- Quoi ? Des certificats **X.509**, utilisant les extensions du RFC 3779. Le sujet du certificat n'est pas important, ce qui compte est le `IPAddrBlocks`.

La *Resource Public Key Infrastructure* est une infrastructure de distribution de :

- Quoi ? Des certificats **X.509**, utilisant les extensions du RFC 3779. Le sujet du certificat n'est pas important, ce qui compte est le `IPAddrBlocks`.
- Par qui ? [ IANA ->] RIR -> LIR -> Client (pas les AC traditionnels)

La *Resource Public Key Infrastructure* est une infrastructure de distribution de :

- Quoi ? Des certificats **X.509**, utilisant les extensions du RFC 3779. Le sujet du certificat n'est pas important, ce qui compte est le `IPAddrBlocks`.
- Par qui ? [ IANA ->] RIR -> LIR -> Client (pas les AC traditionnels)
- Comment ? `rsync -av`  
`rsync://rpki.ripe.net/repository /var/RPKI`

# RPKI

La *Resource Public Key Infrastructure* est une infrastructure de distribution de :

- Quoi ? Des certificats **X.509**, utilisant les extensions du RFC 3779. Le sujet du certificat n'est pas important, ce qui compte est le `IPAddrBlocks`.
- Par qui ? [ IANA ->] RIR -> LIR -> Client (pas les AC traditionnels)
- Comment ? `rsync -av`  
`rsync://rpki.ripe.net/repository /var/RPKI`

RFC 6487 et 6481

# ROA

Test pour entretien d'embauche d'un admin' BGP :  
« savez-vous ce qu'est un ROA ? »

Test pour entretien d'embauche d'un admin' BGP :  
« savez-vous ce qu'est un ROA ? »

## *Route Origin Authorizations*

Un fichier CMS signé avec la clé du certificat (ci-dessus), listant les AS qui peuvent être l'**origine** d'un ou plusieurs préfixe(s).

# ROA

Test pour entretien d'embauche d'un admin' BGP :  
« savez-vous ce qu'est un ROA ? »

## *Route Origin Authorizations*

Un fichier CMS signé avec la clé du certificat (ci-dessus), listant les AS qui peuvent être l'**origine** d'un ou plusieurs préfixe(s).

Émis par le titulaire du préfixe.

# ROA

Test pour entretien d'embauche d'un admin' BGP :  
« savez-vous ce qu'est un ROA ? »

## *Route Origin Authorizations*

Un fichier CMS signé avec la clé du certificat (ci-dessus), listant les AS qui peuvent être l'**origine** d'un ou plusieurs préfixe(s).

Émis par le titulaire du préfixe.

RFC 6482



# Le ROA de l'AFNIC

```
% certification-validator --print -f e6Y1dFuFnChdD1ZZ2AcNN_Xqp  
Object Type: Route Origin Authorisation object  
Signing time: 2012-05-02T14:57:28.000Z  
ASN: AS2486  
Prefixes:  
    2001:67c:2160::/48  
    2001:67c:217c::/48
```

# Détails : RTR

## Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.

## Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.

## Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
- 3 On va donc découpler :

## Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
- 3 On va donc découpler :
  - 1 Un **cache/validateur**, typiquement une machine Unix, le **serveur** RTR,

# Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
- 3 On va donc découpler :
  - 1 Un **cache/validateur**, typiquement une machine Unix, le **serveur** RTR,
  - 2 Le routeur, le **client** RTR.

# Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
- 3 On va donc découpler :
  - 1 Un **cache/validateur**, typiquement une machine Unix, le **serveur** RTR,
  - 2 Le routeur, le **client** RTR.

Entre les deux : RTR (*RPKI/Router Protocol*)



# Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
- 3 On va donc découpler :
  - 1 Un **cache/validateur**, typiquement une machine Unix, le **serveur** RTR,
  - 2 Le routeur, le **client** RTR.Entre les deux : RTR (*RPKI/Router Protocol*)
- 4 RFC pas encore publié mais presque.

# Détails : RTR

- 1 Le routeur route, il vaut mieux ne pas trop le charger.
- 2 Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
- 3 On va donc découpler :
  - 1 Un **cache/validateur**, typiquement une machine Unix, le **serveur** RTR,
  - 2 Le routeur, le **client** RTR.

Entre les deux : RTR (*RPKI/Router Protocol*)

- 4 RFC pas encore publié mais presque.
- 5 RTR transmet juste des assertions (« l'AS 2486 peut originer 2001:67c:2160::/48 »), **c'est le routeur qui décide.**

Détails : qui allez-vous appeler ?

# Détails : qui allez-vous appeler ?

- Si on se fie à l'expérience de PGP/X.509/DNSSEC, il y aura des problèmes.

# Détails : qui allez-vous appeler ?

- Si on se fie à l'expérience de PGP/X.509/DNSSEC, il y aura des problèmes.
- Votre routeur rejette une route car signature invalide : *Who you gonna call ?*

# Détails : qui allez-vous appeler ?

- Si on se fie à l'expérience de PGP/X.509/DNSSEC, il y aura des problèmes.
- Votre routeur rejette une route car signature invalide : *Who you gonna call ?*
- whois ? Qualité variable...

# Détails : qui allez-vous appeler ?

- Si on se fie à l'expérience de PGP/X.509/DNSSEC, il y aura des problèmes.
- Votre routeur rejette une route car signature invalide : *Who you gonna call ?*
- whois ? Qualité variable...
- *Ghostbusters !*

# Détails : qui allez-vous appeler ?

- Si on se fie à l'expérience de PGP/X.509/DNSSEC, il y aura des problèmes.
- Votre routeur rejette une route car signature invalide : *Who you gonna call ?*
- whois ? Qualité variable...
- *Ghostbusters !*
- Des vCard dans la RPKI



# Mises en œuvres, gestion des certificats

Mélange de logiciel d'une AC X.509 et d'une solution IPAM.

# Mises en œuvres, gestion des certificats

Mélange de logiciel d'une AC X.509 et d'une solution IPAM.

- Il y en a sur le *cloud* (voir plus loin celui du RIPE-NCC)

# Mises en œuvres, gestion des certificats

Mélange de logiciel d'une AC X.509 et d'une solution IPAM.

- Il y en a sur le *cloud* (voir plus loin celui du RIPE-NCC)
- Au moins deux logiciels libres (pas testés), rcynic et Local Certification Service

# Mises en œuvres, cache/validateur

# Mises en œuvres, cache/validateur

- Solution du RIPE-NCC, en Java, RPKI Validator

# Mises en œuvres, cache/validateur

- Solution du RIPE-NCC, en Java, RPKI Validator
- Solution ISC/ARIN, en C, rcynic

# Mises en œuvres, cache/validateur

- Solution du RIPE-NCC, en Java, RPKI Validator
- Solution ISC/ARIN, en C, rcynic
- D'autres apparaissent (BBN).

# Mises en œuvres, routeur

Rappel : il suffit au routeur d'être client RTR et d'avoir un mécanisme permettant d'utiliser les assertions dans son processus de décision.

Client RTR sur Juniper :

```
rpki@lr1.ham1.de> show validation session
```

Session	State	Flaps	Uptime
195.13.63.18	Up	1015	00:53



# Mises en œuvres, routeur

Rappel : il suffit au routeur d'être client RTR et d'avoir un mécanisme permettant d'utiliser les assertions dans son processus de décision.

- Cisco IOS (publiée avec Classic 15.2(1)S et XE 3.5)

Client RTR sur Juniper :

```
rpki@lr1.ham1.de> show validation session
```

Session	State	Flaps	Upt
195.13.63.18	Up	1015	00:53

# Mises en œuvres, routeur

Rappel : il suffit au routeur d'être client RTR et d'avoir un mécanisme permettant d'utiliser les assertions dans son processus de décision.

- Cisco IOS (publiée avec Classic 15.2(1)S et XE 3.5)
- Juniper (pas officiellement publiée, pour la 12.2 quelque part en 2012 ?)

Client RTR sur Juniper :

```
rpki@lr1.ham1.de> show validation session
```

Session	State	Flaps	Upt
195.13.63.18	Up	1015	00:53

# Mises en œuvres, routeur

Rappel : il suffit au routeur d'être client RTR et d'avoir un mécanisme permettant d'utiliser les assertions dans son processus de décision.

- Cisco IOS (publiée avec Classic 15.2(1)S et XE 3.5)
- Juniper (pas officiellement publiée, pour la 12.2 quelque part en 2012 ?)
- Quagga (patch disponible, nommé BGP-SRX)

Client RTR sur Juniper :

```
rpki@lr1.ham1.de> show validation session
```

Session	State	Flaps	Upt
195.13.63.18	Up	1015	00:53

# Mises en œuvres, routeur

Rappel : il suffit au routeur d'être client RTR et d'avoir un mécanisme permettant d'utiliser les assertions dans son processus de décision.

- Cisco IOS (publiée avec Classic 15.2(1)S et XE 3.5)
- Juniper (pas officiellement publiée, pour la 12.2 quelque part en 2012 ?)
- Quagga (patch disponible, nommé BGP-SRX)
- Bibliothèque cliente RTR libre, RTRlib (utilisée par BIRD)

Client RTR sur Juniper :

```
rpki@lr1.ham1.de> show validation session
```

Session	State	Flaps	Upt
195.13.63.18	Up	1015	00:53

# RTR en action, avec RTRlib

```
2012-05-29T09:07:22Z + 2800:38:: 32 - 128 27808
2012-05-29T09:07:22Z + 2001:67c:2160:: 48 - 48 2486
2012-05-29T09:07:22Z + 2001:1448:: 32 - 32 16245
2012-05-29T09:07:22Z + 2a02:d28:: 32 - 120 5580
2012-05-29T09:07:22Z + 2a00:8640:: 32 - 32 57771
2012-05-29T09:07:22Z + 2001:4190:: 32 - 32 8246
```

# Portail RIPE pour les LIR

File Edit View History Delicious Bookmarks Tools Help

Twitter / Inter... Measurement... Interstices - X... Blog Stéphane... How to Enabl... LIR Portal - ... RPKI Validator... My BGPmon.n...

ripe.net https://certification.ripe.net/certification/public/view-certificate/certic

Most Visited Mon blog DSC AFNIC ExpMainCourante < ... post to del.icio.us my del.icio.us Python Library Refer... Tests de moteurs de...

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

RIPE NCC Resource Management Member Support Training Contact

You are signed in as **bortzmeyer+ripe@nic.fr** - Sign out

[News](#) [My Certified Resources](#) [My ROA Specifications](#) [History](#) [RIPE NCC ROA Repository](#)

## Resource Certificate

[Download »](#)

<b>Serial</b>	210577930
<b>Subject</b>	CN=9f720f631ae5d7d1de8acbad3d7e100b90abb63b
<b>Issuer</b>	CN=u75at9r0D4JbJ3_SFkZXD7C5dmg
<b>Not valid before</b>	2012-02-08T15:47:07.000Z
<b>Not valid after</b>	2013-07-01T00:00:00.000Z
<b>Resources</b>	194.0.9.0/24, 194.0.36.0/24, 2001:678:c::/48, 2001:678:4c::/48, 2001:67c:2160::/48, 2001:67c:217c::/48, 2001:67c:2218::/48
<b>AIA</b>	<a href="#">ca issuer</a>
<b>SIA</b>	<a href="#">ca repository</a> <a href="#">manifest</a>

Feedback

# Portail RIPE pour les LIR, suite

File Edit View History Delicious Bookmarks Tools Help

Twitter / Inter... Measurement... Interstices - X... Blog Stéphane... How to Enabl... LIR Portal - ... RPKI Validator... My BGPmon.n...

ripe.net https://certification.ripe.net/certification/protected/ca/ViewCertificat ghostbusters

Most Visited Mon blog DSC AFNIC ExpMainCourante < ... post to del.icio.us my del.icio.us Python Library Refer... Tests de moteurs de...

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Coordination Data & Tools LIR Services RIPE Community

RIPE  
NCC RIPE NETWORK COORDINATION CENTRE

Site Map | Contact | Help | RIPE Database Search

Search Site Search

About The RIPE NCC Resource Management Member Support Training Contact

You are signed in as **bortzmeyer-ripe@nic.fr** - Sign out

[News](#) [My Certified Resources](#) [My ROA Specifications](#) [History](#) [RIPE NCC ROA Repository](#)

## Certified Resources

<b>Certificate Authority Name</b>	CN=fr.nic 194.0.9.0/24 194.0.36.0/24 2001:678:c::/48
<b>Certified Resources</b>	2001:678:4c::/48 2001:67c:2160::/48 2001:67c:217c::/48 2001:67c:2218::/47

[View Certificate »](#)

Feedback

# Portail RIPE pour les LIR, les ROA

## ROA Specifications

A Route Origin Authorisation (ROA) allows anyone on the Internet to validate that you have authorised the announcements you create. A specification, a ROA is automatically published in the RIPE NCC ROA Repository in the form of a cryptographically signed specification, you state which Autonomous Systems are authorised to originate the prefixes you hold. At all times, your ROA must match your intended BGP routing.

Name	AS number	Prefixes	Not valid before	Not valid after
NIC-FR-DNS-ANYCAST	AS2484	2001:678:c::/48	2012-05-01T00:00:00.000Z	2012-06-30T00:00:00.000Z
NIC-FR-DNS-ANYCAST-PCH	AS42	2001:678:4c::/48	2012-05-01T00:00:00.000Z	2012-06-30T00:00:00.000Z
NIC-FR-DNS-ANYCAST-bis	AS2486	2001:678:c::/48	2012-05-23T00:00:00.000Z	2012-07-24T00:00:00.000Z
NIC-FR-DNS-UNICAST	AS2486	2001:67c:2160::/48, 2001:67c:217c::/48	2012-05-01T00:00:00.000Z	2012-06-30T00:00:00.000Z

[Add ROA Specification »](#)

## Current BGP announcements

These are the current BGP announcements, as seen by the RIPE NCC Remote Route Collectors, that overlap with announcements seen by five or more peers are shown. This data can be up to nine hours old, so recent changes might not be reflected.

Search:

Origin AS	Prefix	Route Validity
AS2484	194.0.9.0/24	UNKNOWN

Feedback



# Outils RIPE

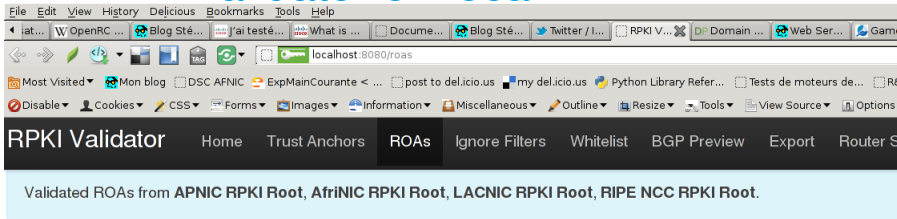
RPKI Validator fournit un cache/validateur, des outils en ligne de commande, une interface Web conviviale-graphique-pour-zutilisateurs...

# Outils RIPE

RPKI Validator fournit un cache/validateur, des outils en ligne de commande, une interface Web conviviale-graphique-pour-zutilisateurs...

Contrairement à tant d'outils en Java, ça semble tourner sur une machine 100 % libre (Debian).

# RIPE RPKI Validator en local



File Edit View History Delicious Bookmarks Tools Help

localhost:8080/roas

Most Visited Mon blog DSC AFNIC ExpMainCourante < ... post to del.icio.us my del.icio.us Python Library Refer... Tests de moteurs de... RE

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

**RIPE Validator** Home Trust Anchors **ROAs** Ignore Filters Whitelist BGP Preview Export Router S

Validated ROAs from APNIC RPKI Root, AfrinIC RPKI Root, LACNIC RPKI Root, RIPE NCC RPKI Root.

Show  entries

Search:

ASN	Prefix	Maximum Length
1	61.45.250.0/23	23
1	61.45.250.0/23	23
	2001:678:3::/48	48
	194.0.42.0/24	24
	2001:678:60::/48	48
42	2001:678:4c::/48	48
42	194.0.17.0/24	24

Feedback

# Routeurs connectés au validateur du RIPE

File Edit View History Delicious Bookmarks Tools Help

Twitter / Interactions RPKI Validator - Router Se... Veille technologique - Gt... Après le désormais célébr... Flame, le cyber-espionna...

localhost:8080/rtr-sessions

Most Visited Mon blog DSC AFNIC ExpMainCourante < ... post to del.icio.us my del.icio.us Python Library Refer... Tests de moteurs de... R

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

**RPKI Validator** Home Trust Anchors ROAs Ignore Filters Whitelist BGP Preview Export Router S

## Router Sessions

See below for a list routers that have connected to this validator. See [here](#) for debug logging of these connections.

Remote Address	State	Last Request from Client	Last Serial
127.0.0.1:45537	11:00:16.135+02:00 <b>CONNECTED</b>	15:55:30.471+02:00 <b>SerialQuery</b>	15:55:30.471
127.0.0.1:45523	10:59:30.412+02:00 <b>DISCONNECTED</b>	10:59:25.999+02:00 <b>ResetQuery</b>	15:11:21.92

Feedback



Copyright ©2009-2012 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights reserved.

# Outil ligne de commande du RIPE

```
% certification-validator --print -f roa-5574190.roa
Content type: 1.2.840.113549.1.9.16.1.24
Signing time: 2011-01-11T19:04:18.000Z
ASN: AS559
Prefixes:
  193.5.26.0/23 [24]
  193.5.152.0/22 [24]
  193.5.168.0/22 [24]
  193.5.22.0/24
  193.5.54.0/23 [24]
  193.5.58.0/24
  193.5.60.0/24
  193.5.80.0/21 [24]
```

## Autre outil, rcynic

rcynic fournit une AC RPKI (pas testée), un cache/validateur, des outils en ligne de commande.

Dépend de OpenSSL : attention sur Debian où le OpenSSL standard n'a toujours pas les extensions du RFC 3779 :-)

# Démos de rcynic

```
% find_roa /var/rcynic 2001:660::/32
ASN 2200 prefix 2001:660::/32 \
    ROA /var/rcynic/data/authenticated.2012-05-02T13:35:03Z

% print_roa /var/rcynic/data/authenticated.2012-05-02T13:35:03Z
...
asID:          2200
...
addressFamily: 2
    IPAddress: 2001:660::/32
```

# Outils génériques

OpenSSL peut gérer les certificats de la RPKI

```
% openssl x509 -inform DER -text \  
  -in ./q3C8zU6hYpb7zVqmpjlVY5BBWE.cer  
...  
  Signature Algorithm: sha256WithRSAEncryption  
  Issuer: CN=5XxoZDVUZvaNYJcVATAgTQ2ifLQ  
  Validity  
    Not Before: Dec 14 15:26:48 2010 GMT  
    Not After : Jul  1 00:00:00 2011 GMT  
...  
  sbgp-ipAddrBlock: critical  
    IPv4:  
      85.118.184.0/21  
      93.175.146.0/23  
    IPv6:  
      2001:7fb:fd02::/47
```



# Outils non locaux

## Le serveur whois de BGPmon

Avant la création du ROA :

```
% whois -h whois.bgpmon.net " --roa 2486 2001:67c:2160::/48"  
1 - Not Found
```

Après :

```
% whois -h whois.bgpmon.net " --roa 2486 2001:67c:2160::/48"  
0 - Valid
```

-----  
ROA Details  
-----

```
Origin ASN:          AS2486  
Not valid Before:    2012-05-01 00:00:00  
Not valid After:     2012-06-30 00:00:00   Expires in 57d17h16m11s  
Trust Anchor:        rpki.ripe.net  
Prefixes:            2001:67c:217c::/48  
                    2001:67c:2160::/48
```

# Looking Glasses, voir la RPKI à distance

- [http://www.labs.lacnic.net/rpkitools/looking\\_glass/](http://www.labs.lacnic.net/rpkitools/looking_glass/)

# Configuration du routeur

Configuration du client RTR sur un Cisco :

```
bgp rpki server tcp 2001:db8:1000:2000::f00d port 8282 refresh

route-map test-rpki permit 10
  match rpki invalid
  set local-preference 50
```

État d'une route sur un Cisco (rappel : le routeur décide de ce qu'on fait d'une route invalide) :

```
rpki-rtr>show ip bgp 62.73.128.0
BGP routing table entry for 62.73.128.0/19, version 1865228
...
 12654 50300 15533
   193.0.4.1 from 193.0.4.28 (193.0.4.28)
     Origin IGP, localpref 110, valid, external, best
     path 58970BAC RPKI State valid
```

# État du déploiement

# État du déploiement

- Tous les RIR sauf ARIN distribuent des certificats et des ROA,

# État du déploiement

- Tous les RIR sauf ARIN distribuent des certificats et des ROA,
- Au 12 mai 2012, dans les 1200 ROAs (bancs de tests exclus), en croissance très rapide dans RIPEland,

# État du déploiement

- Tous les RIR sauf ARIN distribuent des certificats et des ROA,
- Au 12 mai 2012, dans les 1200 ROAs (bancs de tests exclus), en croissance très rapide dans RIPEland,
- Logiciels qui commencent à devenir stables mais peu de clients RPKI dans les images officielles des routeurs,

# État du déploiement

- Tous les RIR sauf ARIN distribuent des certificats et des ROA,
- Au 12 mai 2012, dans les 1200 ROAs (bancs de tests exclus), en croissance très rapide dans RIPEland,
- Logiciels qui commencent à devenir stables mais peu de clients RPKI dans les images officielles des routeurs,
- Quasiment aucun routeur de production ne valide.



# Futur

- 1 Les ROAs n'authentifient que l'**origine**. C'est largement suffisant contre les erreurs.

- 1 Les ROAs n'authentifient que l'**origine**. C'est largement suffisant contre les erreurs.
- 2 Mais un attaquant type Kapela&Pilosov va respecter l'origine et ne sera pas détecté

- 1 Les ROAs n'authentifient que l'**origine**. C'est largement suffisant contre les erreurs.
- 2 Mais un attaquant type Kapela&Pilosov va respecter l'origine et ne sera pas détecté
- 3 Prochaine étape, déjà en cours à l'IETF, utiliser la RPKI et un nouvel attribut BGP pour signer le chemin d'AS complet. Cette fois, cela modifiera BGP.
  - 1 IRR et systèmes d'alerte → BGPbrut
  - 2 RPKI+ROA → BGPdemisec
  - 3 Validation du chemin → BGPsec

# Critiques techniques

# Critiques techniques

- Complexité, et dépendance vis-à-vis de nouvelles infrastructures pas maîtrisées,

# Critiques techniques

- Complexité, et dépendance vis-à-vis de nouvelles infrastructures pas maîtrisées,
- Risques de faux positifs (comme avec les IRR, où beaucoup de routes seraient rejetées si on filtrait),

# Critiques techniques

- Complexité, et dépendance vis-à-vis de nouvelles infrastructures pas maîtrisées,
- Risques de faux positifs (comme avec les IRR, où beaucoup de routes seraient rejetées si on filtrait),
- Les ROA protègent contre les accidents, pas contre les attaques.



# Rover

c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNIC

*afnic*



# Rover

- La RPKI est la solution « officielle » à l'IETF et chez les RIR. Y a-t-il une alternative technique ?

c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNIC

The logo for afnic, featuring the word "afnic" in a stylized, lowercase, black script font. To the right of the logo is a solid blue square.

afnic

# Rover

- La RPKI est la solution « officielle » à l'IETF et chez les RIR. Y a-t-il une alternative technique ?
- ROVER propose de mettre la même information (AS d'origine et, demain, chemin) dans le DNS, signé avec DNSSEC. Même niveau de sécurité que la RPKI. Fini, X.509.

c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNIC

The logo for afnic, featuring the lowercase letters 'afnic' in a black, handwritten-style script font. It is positioned in the bottom right corner of the slide, partially overlapping a solid blue rectangular area.

# Rover

- La RPKI est la solution « officielle » à l'IETF et chez les RIR. Y a-t-il une alternative technique ?
- ROVER propose de mettre la même information (AS d'origine et, demain, chemin) dans le DNS, signé avec DNSSEC. Même niveau de sécurité que la RPKI. Fini, X.509.
- Réutilise logiciels et hiérarchies existantes.

c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNIC

# Rover

- La RPKI est la solution « officielle » à l'IETF et chez les RIR. Y a-t-il une alternative technique ?
- ROVER propose de mettre la même information (AS d'origine et, demain, chemin) dans le DNS, signé avec DNSSEC. Même niveau de sécurité que la RPKI. Fini, X.509.
- Réutilise logiciels et hiérarchies existantes.
- Nettement moins testé et soutenu que la RPKI. Mais plus simple et moins risqué.

c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNIC

# Rover

- La RPKI est la solution « officielle » à l'IETF et chez les RIR. Y a-t-il une alternative technique ?
- ROVER propose de mettre la même information (AS d'origine et, demain, chemin) dans le DNS, signé avec DNSSEC. Même niveau de sécurité que la RPKI. Fini, X.509.
- Réutilise logiciels et hiérarchies existantes.
- Nettement moins testé et soutenu que la RPKI. Mais plus simple et moins risqué.
- Beaucoup de problèmes (risques de faux positifs, problèmes politiques) sont les mêmes avec ROVER et la RPKI.

c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNIC

# Politique

*afnic*



# Politique

- Autrefois, les RIR n'avaient qu'un rôle indicatif : n'importe qui pouvait annoncer n'importe quel préfixe. En criant assez fort, ça passait. Inversement, une annulation d'allocation par un RIR (RBN. . . ) n'avait pas d'importance pratique.



# Politique

- Autrefois, les RIR n'avaient qu'un rôle indicatif : n'importe qui pouvait annoncer n'importe quel préfixe. En criant assez fort, ça passait. Inversement, une annulation d'allocation par un RIR (RBN. . . ) n'avait pas d'importance pratique.
- Si la RPKI+ROA est déployé, avec refus des annonces non ou mal signées, cela sera différent. Une révocation pourrait rendre un préfixe largement inaccessible. **Les RIR auraient gagné un rôle opérationnel.**

# Politique

- Autrefois, les RIR n'avaient qu'un rôle indicatif : n'importe qui pouvait annoncer n'importe quel préfixe. En criant assez fort, ça passait. Inversement, une annulation d'allocation par un RIR (RBN. . . ) n'avait pas d'importance pratique.
- Si la RPKI+ROA est déployé, avec refus des annonces non ou mal signées, cela sera différent. Une révocation pourrait rendre un préfixe largement inaccessible. **Les RIR auraient gagné un rôle opérationnel.**
- Il va falloir réviser son code pénal néerlandais.

# Politique

- Autrefois, les RIR n'avaient qu'un rôle indicatif : n'importe qui pouvait annoncer n'importe quel préfixe. En criant assez fort, ça passait. Inversement, une annulation d'allocation par un RIR (RBN. . . ) n'avait pas d'importance pratique.
- Si la RPKI+ROA est déployé, avec refus des annonces non ou mal signées, cela sera différent. Une révocation pourrait rendre un préfixe largement inaccessible. **Les RIR auraient gagné un rôle opérationnel.**
- Il va falloir réviser son code pénal néerlandais.
- Les discussions politiciennes sur la gouvernance de l'Internet se focalisent sur l'excitant .xxx et oublient les problèmes concrets comme la RPKI.

# Comparaison avec DNSSEC



# Comparaison avec DNSSEC

- 1 Mêmes problèmes des faux positifs (bien plus nombreux que les vrais),



# Comparaison avec DNSSEC

- 1 Mêmes problèmes des faux positifs (bien plus nombreux que les vrais),
- 2 Mêmes optimistes jurant que tout ira bien (tu parles),

# Comparaison avec DNSSEC

- 1 Mêmes problèmes des faux positifs (bien plus nombreux que les vrais),
- 2 Mêmes optimistes jurant que tout ira bien (tu parles),
- 3 Même question fondamentale : « la sécurité vaut-elle une telle dépense ? »,

# Comparaison avec DNSSEC

- 1 Mêmes problèmes des faux positifs (bien plus nombreux que les vrais),
- 2 Mêmes optimistes jurant que tout ira bien (tu parles),
- 3 Même question fondamentale : « la sécurité vaut-elle une telle dépense ? »,
- 4 Même nécessité de montée en compétence et même résultat : éliminer les petits,



# Comparaison avec DNSSEC

- 1 Mêmes problèmes des faux positifs (bien plus nombreux que les vrais),
- 2 Mêmes optimistes jurant que tout ira bien (tu parles),
- 3 Même question fondamentale : « la sécurité vaut-elle une telle dépense ? »,
- 4 Même nécessité de montée en compétence et même résultat : éliminer les petits,
- 5 Moins de problèmes politiques : le DNS était déjà arborescent.

# Observatoire de la résilience de l'Internet

## Concepts :

- 1 appréhender la résilience de l'Internet français ;
- 2 promouvoir les bonnes pratiques ;
- 3 définition et mesures d'indicateurs techniques représentatifs de la résilience.

Rapport 2011 : analyse sur les données BGP & DNS de janvier à novembre 2011

- les co-auteurs sont présents et disponibles ;
- des copies papier peuvent être récupérées.

*Merci !*

*afnic*

[www.afnic.fr](http://www.afnic.fr)  
[contact@afnic.fr](mailto:contact@afnic.fr)  
Twitter : @AFNIC  
Facebook : afnic.fr

*afnic*