Sécuriser le routage sur Internet

Guillaume LUCAS

UFR Mathématique-Informatique
Université de Strasbourg

7 mai 2013

Introduction

- Sécuriser le routage inter-domaine comme sujet de TER
- Routage = cœur de tout réseau
- Importance d'Internet

Rappels -> Allocation des ressources uniques

- Ressources numériques uniques = ASN, préfixe v4, préfixe v6
- Besoin d'unicité globale
- Donc besoin d'une distribution cohérente au niveau mondial

Au commencement (70's - mi-90's)

- SRI NIC (puis d'autres)
- Dès le début des 90's : émergence de l'idée d'un modèle hiérarchique

Mi-90's - aujourd'hui

- Modèle hiérarchique
- IANA -> 5 RIR -> multitude de LIR

Quid des ressources obtenues avant l'apparition du modèle hiérarchique ?

Rappels -> BGP

- Protocole de routage inter-AS
- Meilleure route ? choix subjectif
- Pas d'authentification des annonces

N'importe qui peut faire n'importe quoi ?

- S'annoncer comme l'origine d'un préfixe quelconque
- Relayer/manipuler une annonce

Attaques sur BGP

Deux catégories d'attaques

- Attaquer la communication entre pairs -> en dehors du sujet
- Injecter de fausses annonces

Objectifs

- RFC 4272 « BGP Security Vulnerabilities Analysis »
  - Empêcher ou ralentir l'accès à un préfixe
  - Rediriger des flux de données
  - Attaques actives sur les couches supérieures
- Mauvaise utilisation de ressources (émission de spam, attaques, ...)

Attaques sur BGP

"Historiques"

- Détournement de (sous-)préfixe
- Modification AS-PATH
- Performances : fluctuations, désagrégation, ...

Kapela&Pilosov

- Été 2008
- But : intercepter du trafic de manière plus silencieuse
- Nouvelle méthodologie, combinaison de techniques existantes
- Plus facile

Attaques sur BGP -> IRL

- Des incidents
- 1997 : AS 7007 désagrège tous les préfixes qu'il reçoit en /24
- 2008 : cas d'école Pakistan Télécom/Youtube
- Utilisation du préfixe non alloué 2.0.0.0/12 pour du phishing

Et tous les autres incidents ?

- Les incidents ont tendance à se multiplier ces dernières années
- Ceux jamais publiés comme 42/8, OSIRIS, ...
- Zones d'ombre

Relativiser ?

Facteurs limitants : coût (financier/administratif/technique) de mise en œuvre, réactivité humaine, méthodes plus efficaces, ...

Solutions -> Ce qu'il faut faire

- 2 problèmes = 2 solutions

Validation de l'origine

- « Est-ce que X était bien autorisé à annoncer ce préfixe ? »
- Relativement simple : peu de préfixes au final, normalement enregistrés et de rares changements
- BGPdemisec (Hugo Salgado)

Validation du chemin

- « Est-ce qu'Y avait le droit de relayer cette annonce ? Et Z ? »
- Complexité supérieure : explosion combinatoire, performances, changements fréquents, ...
- Validation de l'origine + validation du chemin = BGPSec (H.S.)

Certaines solutions tentent d'apporter une réponse aux deux problèmes. Les autres sont réalistes.

Solutions historiques

- Systèmes d'alarme : surveiller les annonces BGP
- Passifs, basés sur la réactivité humaine, zones d'ombres

- Best Current Practice : ensemble de bonnes pratiques (filtrer les annonces invalides, limiter le nombre maximal de préfixes, ...)
- Très peu suivies, n'est pas une solution en soi.

- Secure-BGP : BBN, Mi-90's. Pairs + origine + chemin. PKI.
- Complexité en une seule fois, performances ?

- Secure Origin BGP : Cisco, 2003. Origine + chemin. Réseau de confiance.
- Problèmes des réseaux de confiance (expiration ? révocation ?), complexité en une seule fois, modification de BGP.

Solutions historiques

- Pretty Secure BGP : Carleton, 2005. Origine + chemin. Reprendre le meilleur de S-BGP et SoBGP.
- Complexité++ en une seule fois, problèmes habituels des réseaux de confiance (expiration ? révocation ?)

- Pretty Good BGP : New Mexico, 2006. Prendre le temps d'accorder sa confiance aux nouvelles routes.
- Pas de cryptographie, faux positifs, réactivité humaine.

Et tant d'autres papiers de recherche (Listen and Whisper, Reachability Validation Graph, ...)

Solutions actuelles

ROute Origin VERification

- Validation de l'origine en utilisant le DNS
- Nouveaux enregistrements dans les zones reverse (in-addr.arpa / ip6.arpa)
- Avantage : se base sur une infrastructure de confiance existante
- Inconvénient : dépend du DNS et surtout de DNSSEC dont le déploiement débute

RPKI+ROA

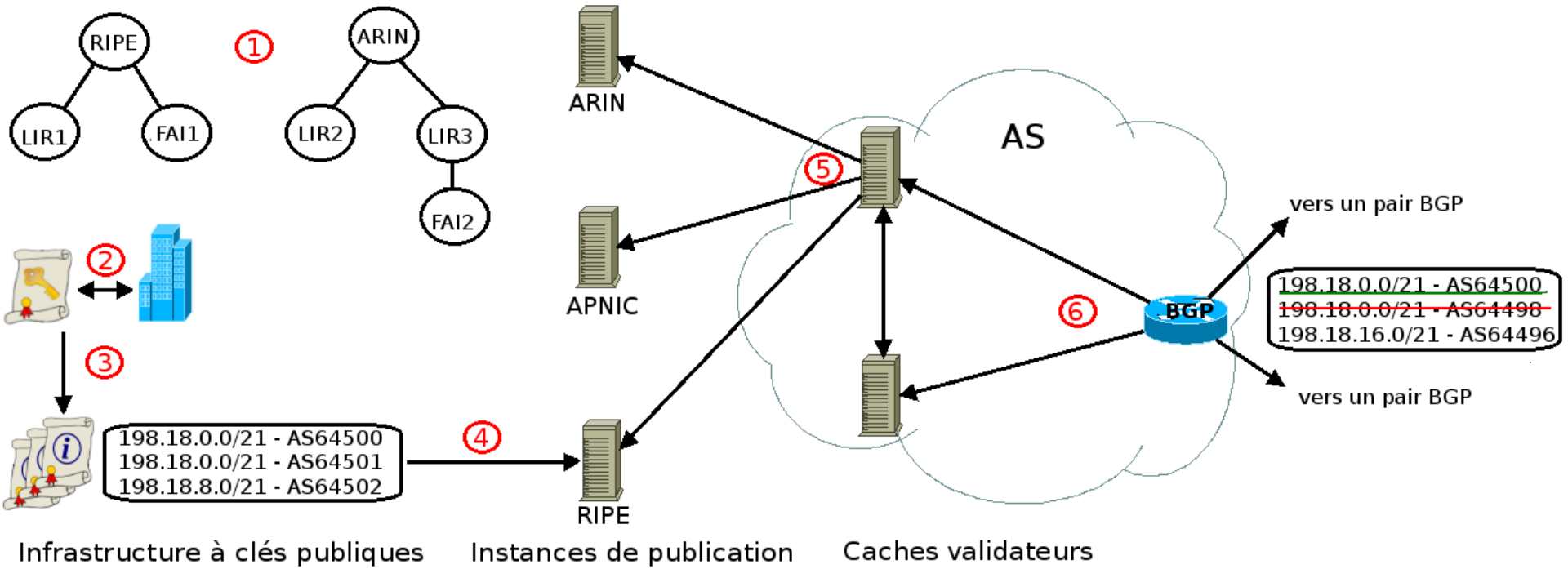
RPKI+ROA -> Généralités

- Janvier 2013 : solution normalisée à l'IETF
- Validation de l'origine
- Cryptographie asymétrique habituelle (paire de clés, certificats x509, ...)
- Ne casse pas BGP

Resource Public Key Infrastructure + Route Origin Authorizations

- Une PKI dédiée à la certification des ressources uniques d'Internet
- Des autorisations signées concernant l'origine d'un préfixe

RPKI+ROA -> Détails



RPKI+ROA -> Limites

- Des manques dans la normalisation (délais, procédures de validation des Manifest, roulement des certificats racines, ...)
- L'infrastructure actuelle est-elle suffisante ? Supportera-t-elle la charge ? Grande inconnue.
- Manque d'intérêt ? 3000 ROA, 4000/467000 préfixes, qui valide ?
- Manque de logiciels libres production-ready ?
- De nouveaux pouvoirs aux RIR ?
- Complexité ?
- Exclusion de réseaux des Internets

Qu'ai-je fait ?

- Me documenter
- Maquette RPKI+ROA
- Rapporter des bugs
  - RPKI tools : bug mineur web UI + impossible de créer des ROA v6. Corrigés (`https://rpki.net/ticket/414`).
  - RIPE RPKI-Validator 2.7 : blocage de la validation si Ghostbusters présent dans un point de publication. Corrigé dans 2.8.
  - BGP-SRX : états de validation fluctuants + support v6 incomplet (?). Toujours en cours.

Conclusion

Bilan RPKI+ROA

- Une solution normalisée
- Des points à améliorer
- Une inertie à prendre (10, 15, 20, 20+ ans ?)
- D'ici là : BGPSec ? Pas simple.

Bilan TER

- Une maquette réalisée
- Prolongement des cours RO et SSR
- Capable de mettre en place une technique récente
- Contribution mineure à l'amélioration des logiciels existants

Any questions ?

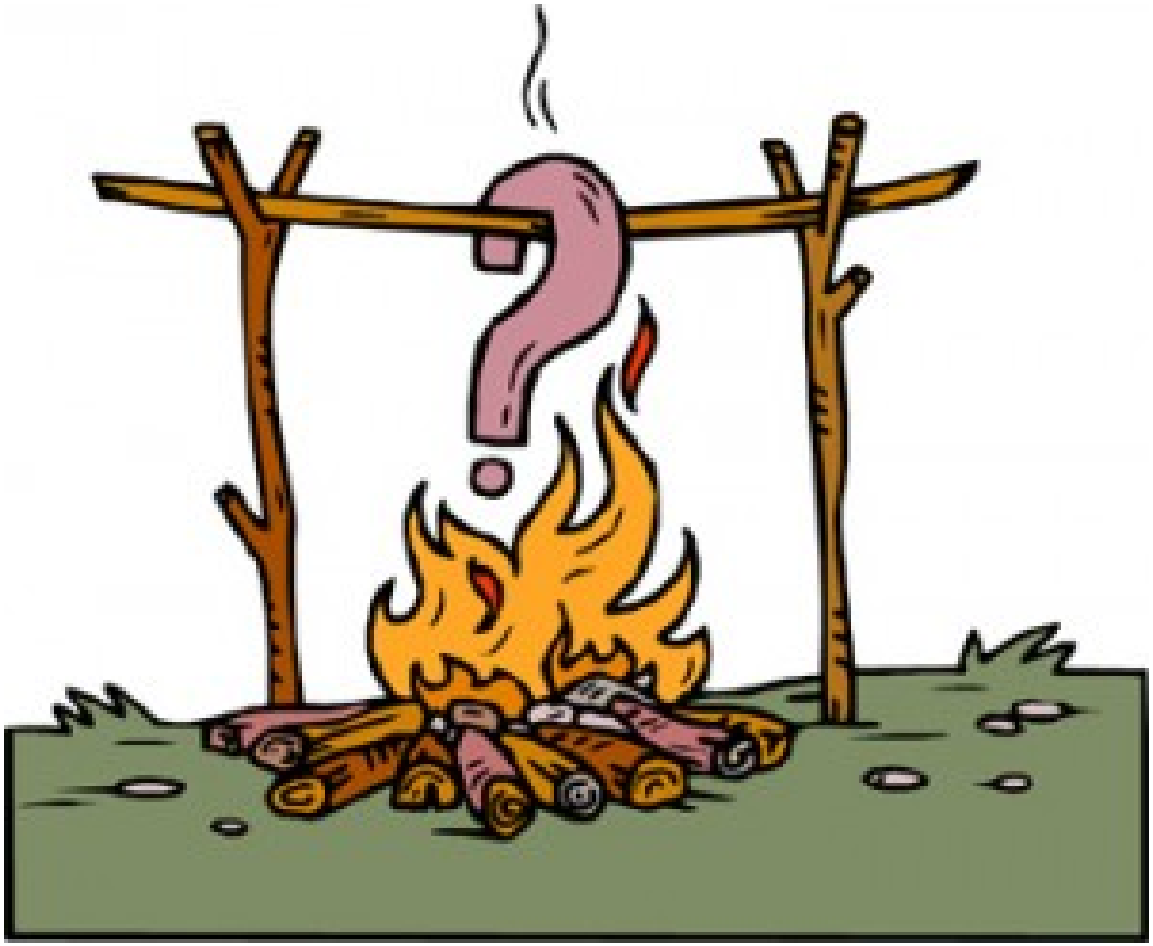


FIGURE : Source :
https ://somkritya.files.wordpress.com/2012/01/burning-question.jpg.