Segurança no roteamento BGP

Italo Valcy <italovalcy@ufba.br>
Salvador – BA, 07/Out/2016

POP-BA

STI
Superintendência de Tecnologia da Informação | UFBA

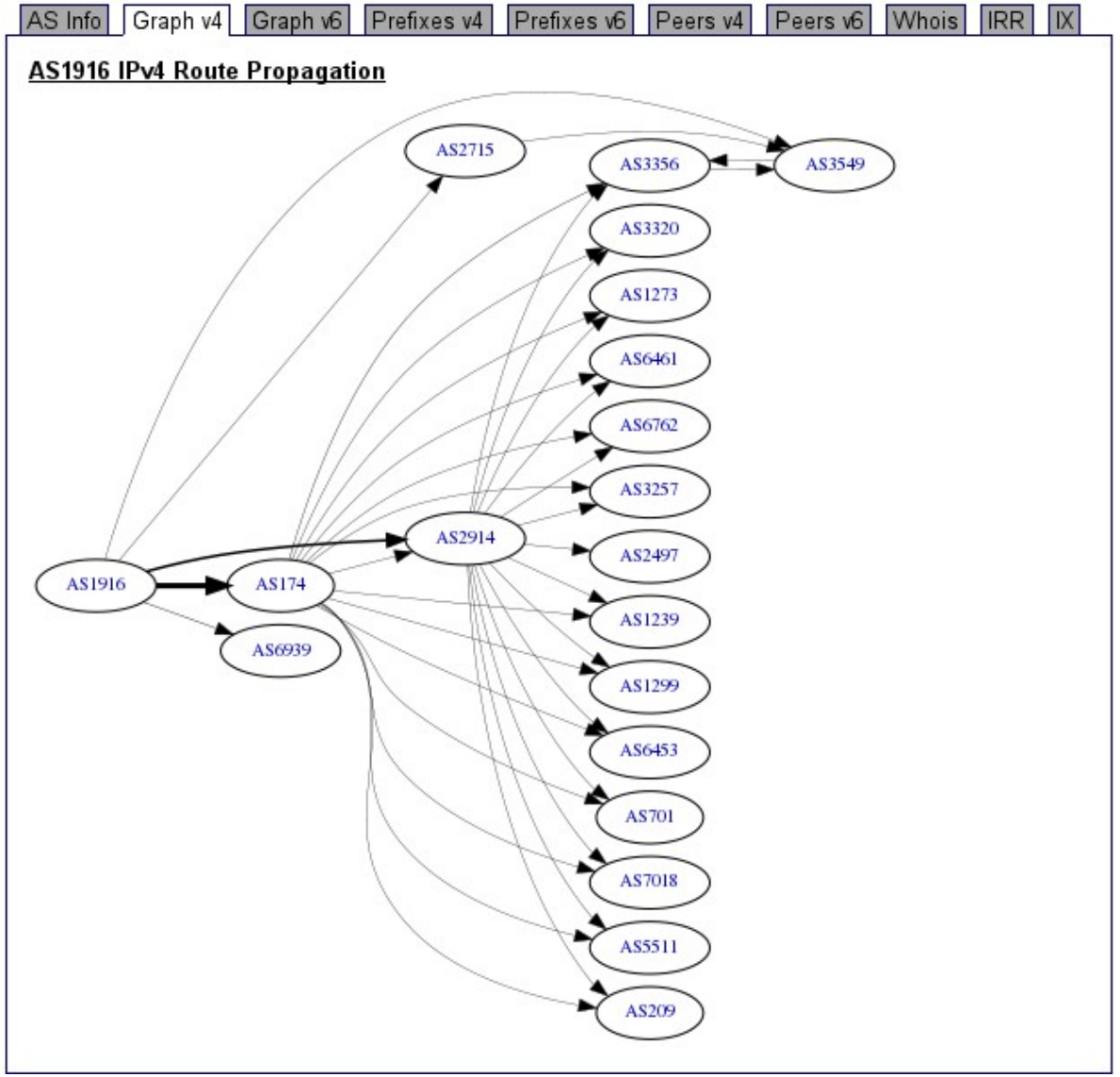
Créditos

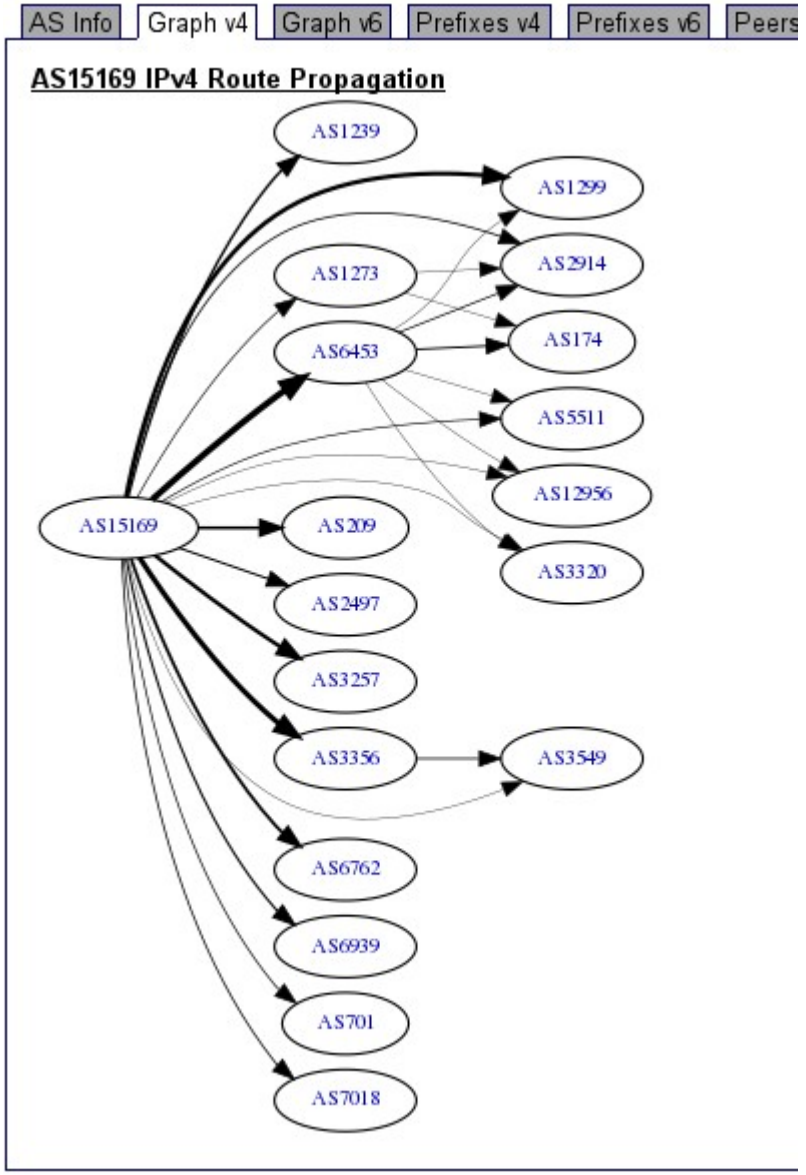
- Curso “Boas práticas para Sistemas Autônomos”, módulo 9, CEPTRO.br/NIC.br
- Palestra “Como a Internet Funciona?”, Netcafé, Jerônimo Bezerra, PoP-BA/RNP
- Curso “BGP Operations and Security”, RIPE NCC
- Jumpstarting BGP Security with Path-End Validation, Cohen et. al., SIGCOMM 2016

O que é BGP

- Protocolo de roteamento para troca de informações de rotas na Internet (rfc4271, ...)
- Sistemas Autônomos identificam unicamente as redes (política de roteamento)
- Capacidade de transportar informações sobre diversos protocolos (ipv4, ipv6, l2vpn, vpnv4)
- Path vector protocol

BGP entre ASes na Internet





Fonte: http://bgp.he.net

Excesso de confiança no BGP

- Excesso de confiança no protocolo BGP
  - Não apenas no BGP, mas em diversos protocolos da Internet
- O BGP funciona com base na “confiança” entre os *peers*
  - Cada *peer* confia nos prefixos enviados pelo outro *peer*
  - *Peers* confiam no caminho anunciado

Notícias relacionadas

YouTube Hijacking: A RIPE NCC RIS case study

Publication date: 17 Mar 2008 — news, ris, internet governance

Introduction

How an Indonesian ISP took down the mighty Google for 30 minutes

Internet's web of trust let a company you never heard of block your Gmail.

by **Sean Gallagher** - Nov 6 2012, 11:07pm SEAST

Google's services went offline for many users for nearly a half-hour on the evening of No

Syria shuts down the Internet

Posted by Andree Toonk - November 29, 2012 - BGP instability - 9 Comments

As of 10:27 UTC this morning the majority of the Internet in Syria is no longe
rest of the world and can be considered as offline. Syria has only one major p
The Syrian Telecommunications Establishment. This provider is government
originates 56 out of 62 Syrian prefixes.

Turkey Hijacking IP addresses for popular Global DNS providers

Posted by Andree Toonk - March 29, 2014 - Hijack, News and Updates - 26 Comments

At BGPmon we see numerous BGP hijacks every single day, some are interesting because of the size and
It all sta
This sta

BGP Hijacker Steals Bitcoins

Researchers at Dell's Secureworks have
covered multiple BGP incidents used to
eal bitcoins. According to Secureworks,
e attacker used a compromised
dministrator account at a yet undisclosed

HIJACKED!

Indonesia Hijacks the World

03 APR, 2014 | 3:09 PM | BY EARL ZMIJEWSKI

Yesterday, Indosat, one of Indonesia's largest telecommunications providers, leaked large portions of the global routing table multiple times over a two-hour period. This means that, in effect, Indosat claimed that it "owned" many of the world's networks. Once someone makes such an assertion, typically via an honest mistake in their routing policy, the only question remaining is how much of the world ends up believing them and hence, what will be the scale of the damage they inflict? Events of this nature, while relatively rare, are certainly not unheard

10 Alleged vDOS Proprietors Arrested in Israel

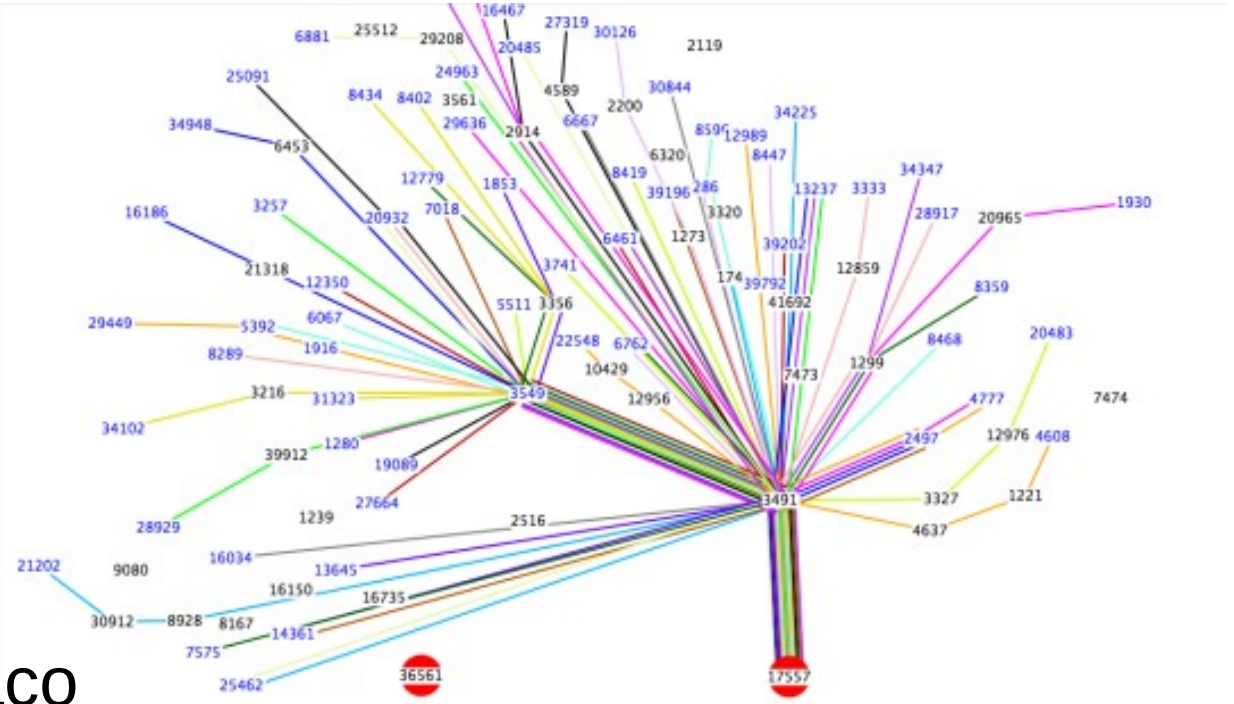
SEP 16

Two young Israeli men alleged to be the co-owners of a popular online attack-for-hire se
were reportedly arrested in Israel on Thursday. The pair were arrested around the same
that KrebsOnSecurity published a story na

"Defensive" BGP hijacking?

Tipos de Incidente de Roteamento

- Má configuração
  - Não intencional
  - Bugs de software
- Maliciosa
  - Concorrência
  - Contestando espaço não utilizado
- Ataques dirigidos
  - Redirecionamento de tráfego
  - Espionagem ou modificação de tráfego



Fonte: www.ripe.net
(youtube-hijacking-a-ripe-ncc-ris-case-study)

Problemas de endereçamento

- Exaustão de endereços – IPv4 vs IPv6
- IP Spoofing
  - Origem não-rastreável ou incorreta
    - Alterada para fins maliciosos??
  - Usada para ataques de negação de serviço
    - Oculta o atacante
    - Ataques de reflexão e amplificação
- Configurações erradas – endereços inválidos
  - Tráfego com IPs incorretos naquele contexto
    - Martians – Endereços privados ou reservados (RFC 1918, RFC 5735, RFC 6598)
    - Bogus – Prefixos IP não alocados pelo IANA

Mitigando IP spoofing

- Adoção de filtros de entrada descritos na BCP38
- Reverse Path Forwarding (*RPF*), RFC3704
  - Automatiza a implantação da BCP38
  - Modo “**strict**” – maior controle (cuidado com tráfego assimétrico e clientes *multihomed*)
  - Modo “**loose**” – mais flexível (cuidado com *allow-default*)

Mitigando endereços inválidos

- BOGON vs FULLBOGON
  - Não são lista estática!
- Como se proteger
  - Filtros manuais
    - Prefix-lists
    - AS-Path
  - Bogon Route Server Project / Team Cymru
    - BGP feed
    - APIs (HTTP, DNS etc.)

Prefix-Lists

- Prefix-list são filtros de rotas para aceitar ou anunciar
- Fácil de configurar porém não escalável
- Criadas manual ou automaticamente
  - RIPE DB ou outros Internet Routing Registry (ex. RADb)
- Ferramentas
  - filtergen.level3.net
  - Bgpq3
  - IRRexplorer

AS Path

- Filtragem de rotas baseada no AS-Path
- Amplamente usada e escalável
- Extensível via expressões regulares

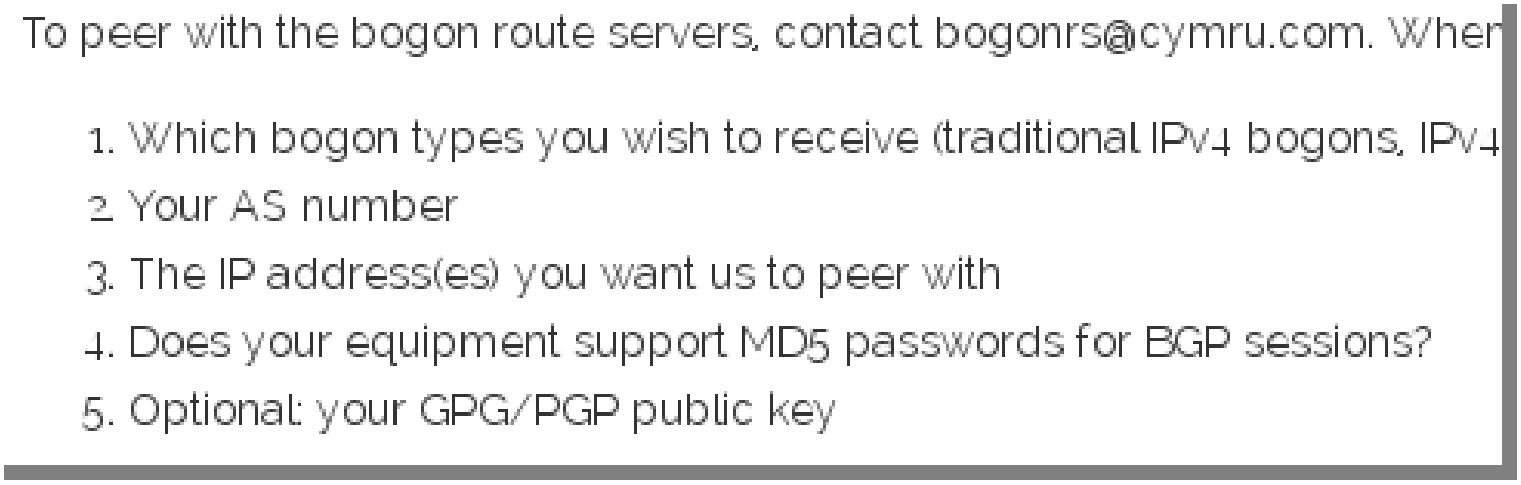
```
router bgp 65564
  network 10.0.0.0 mask 255.255.255.0
  neighbor 172.16.1.1 remote-as 65563
  neighbor 172.16.1.1 filter-list 1 out
  neighbor 172.16.1.1 filter-list 2 in

ip as-path access-list 1 permit ^65564$
ip as-path access-list 2 permit ^65563$
```

Boas práticas de filtragem

- Não aceitar prefixos RFC1918 e demais
- Não aceitar seu próprio prefixo
- Não aceitar rota padrão (a menos que necessário)
- Não aceitar prefixos mais específicos que /25
- Não aceitar prefixos mais específicos que /48

BGP feed

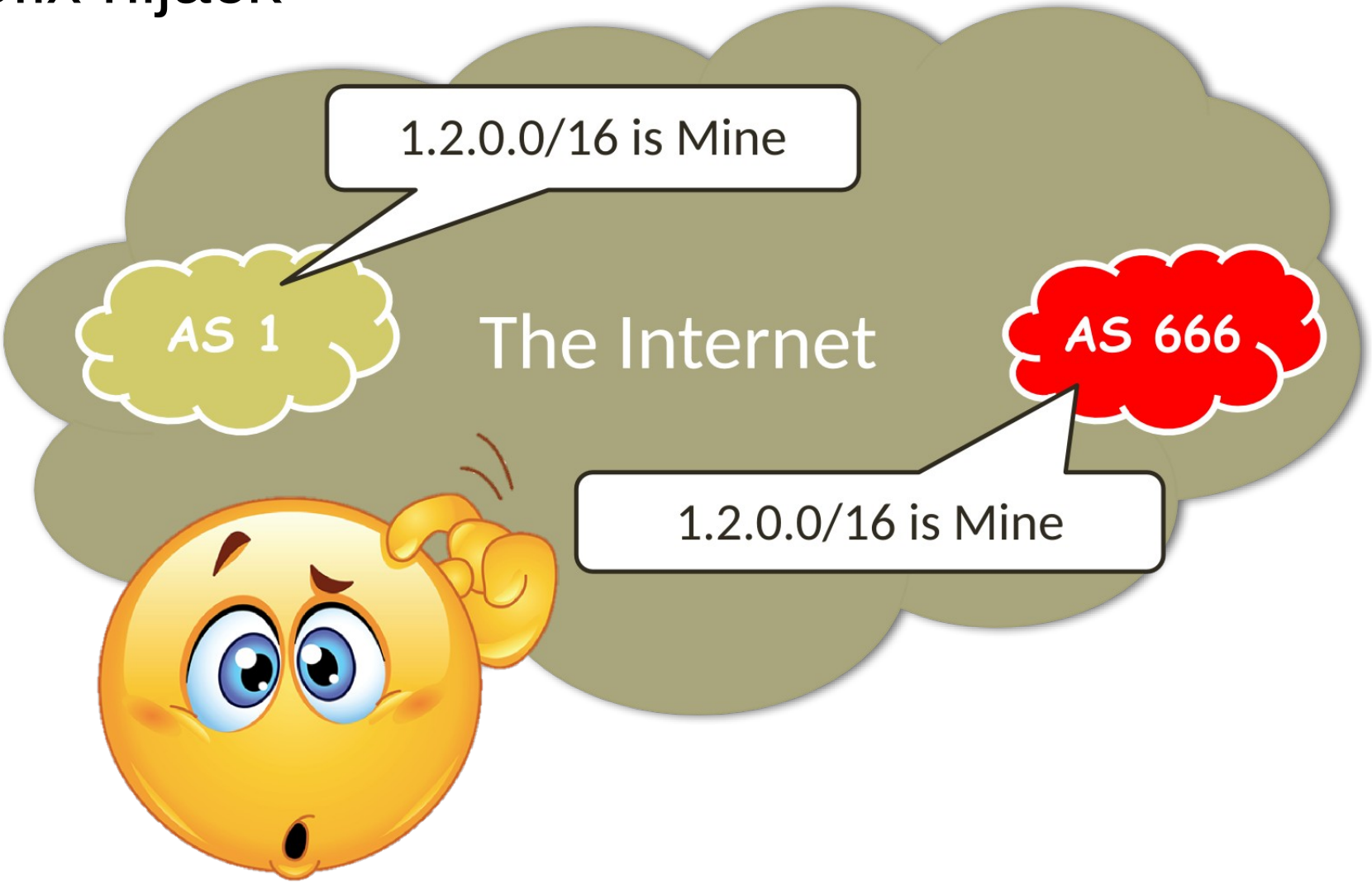
- Automatizar a criação de filtros para bogons e martins
- Team Cymru disponibiliza BGP feed gratuitamente
  - http://www.team-cymru.org/bogon-reference-bgp.html


To peer with the bogon route servers, contact bogonrs@cymru.com. When

1. Which bogon types you wish to receive (traditional IPv4 bogons, IPv4
2. Your AS number
3. The IP address(es) you want us to peer with
4. Does your equipment support MD5 passwords for BGP sessions?
5. Optional: your GPG/PGP public key

Como garantir a origem?

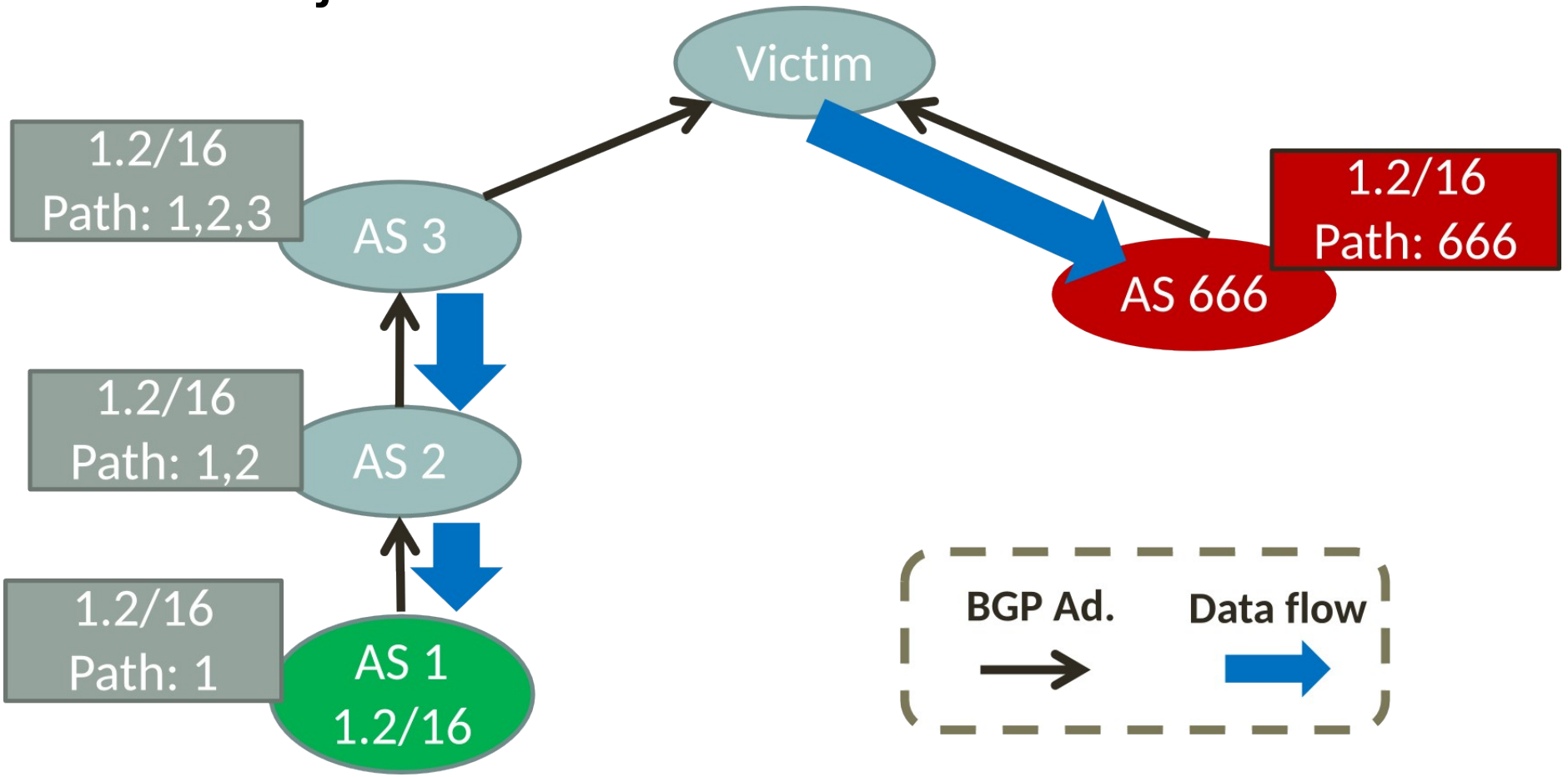
- Prefix hijack



Fonte: Jumpstarting, Avichai, SIGCOMM

Como garantir a origem?

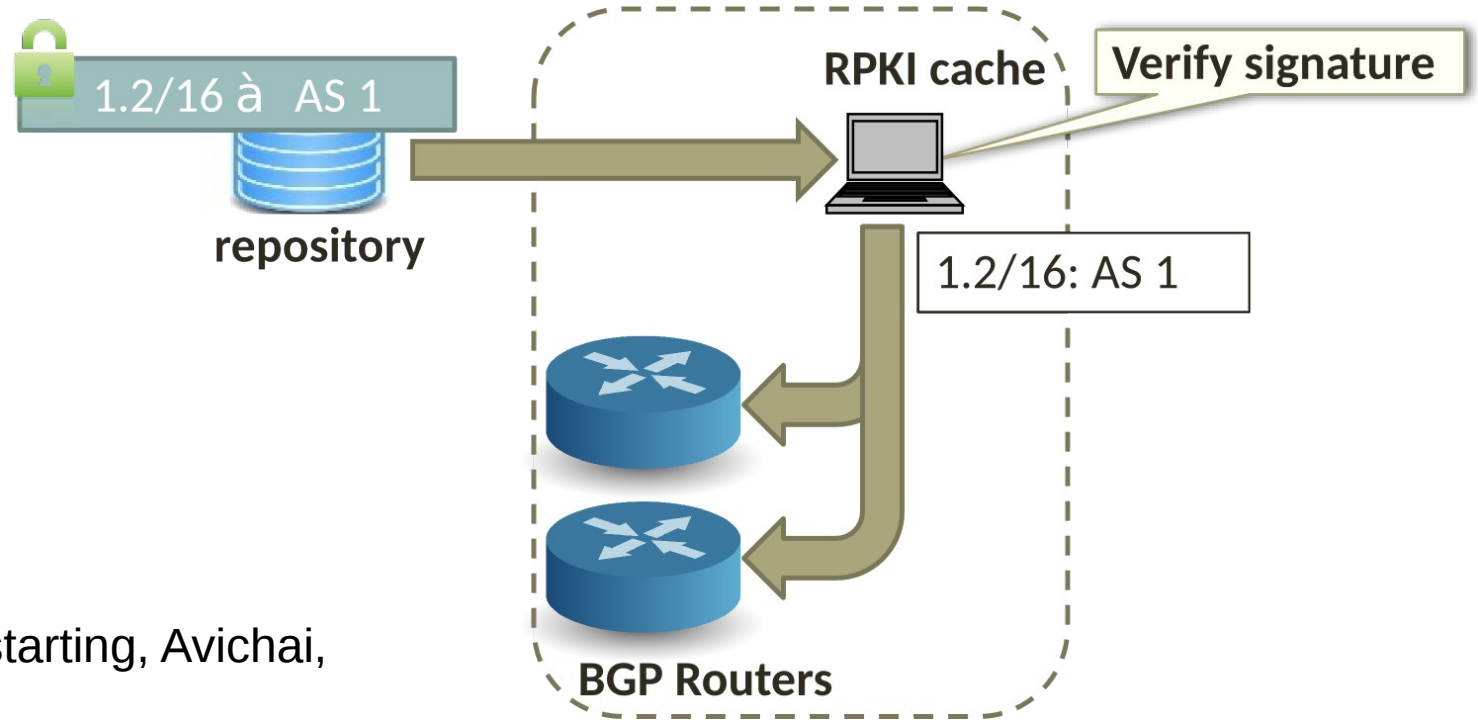
- Prefix hijack



Fonte: Jumpstarting, Avichai, SIGCOMM

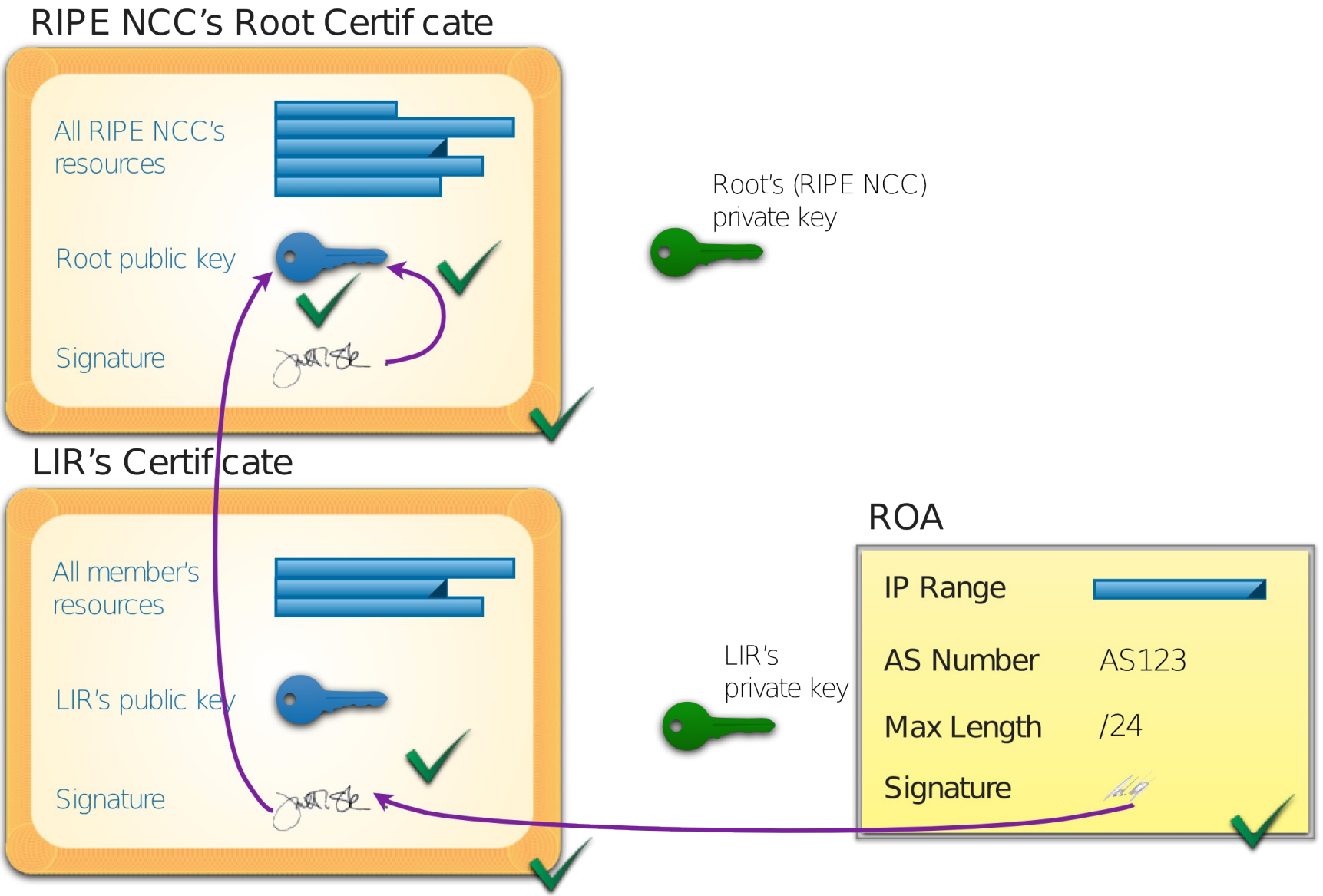
Resource PKI (RPKI)

- Autenticação da origem
  - Protege contra prefix/subprefix hijacking
  - Adiciona certificados digitais a recursos de rede, associando-os com seus proprietários
  - Route Origin Authorisations (ROAs) + Chain of trust



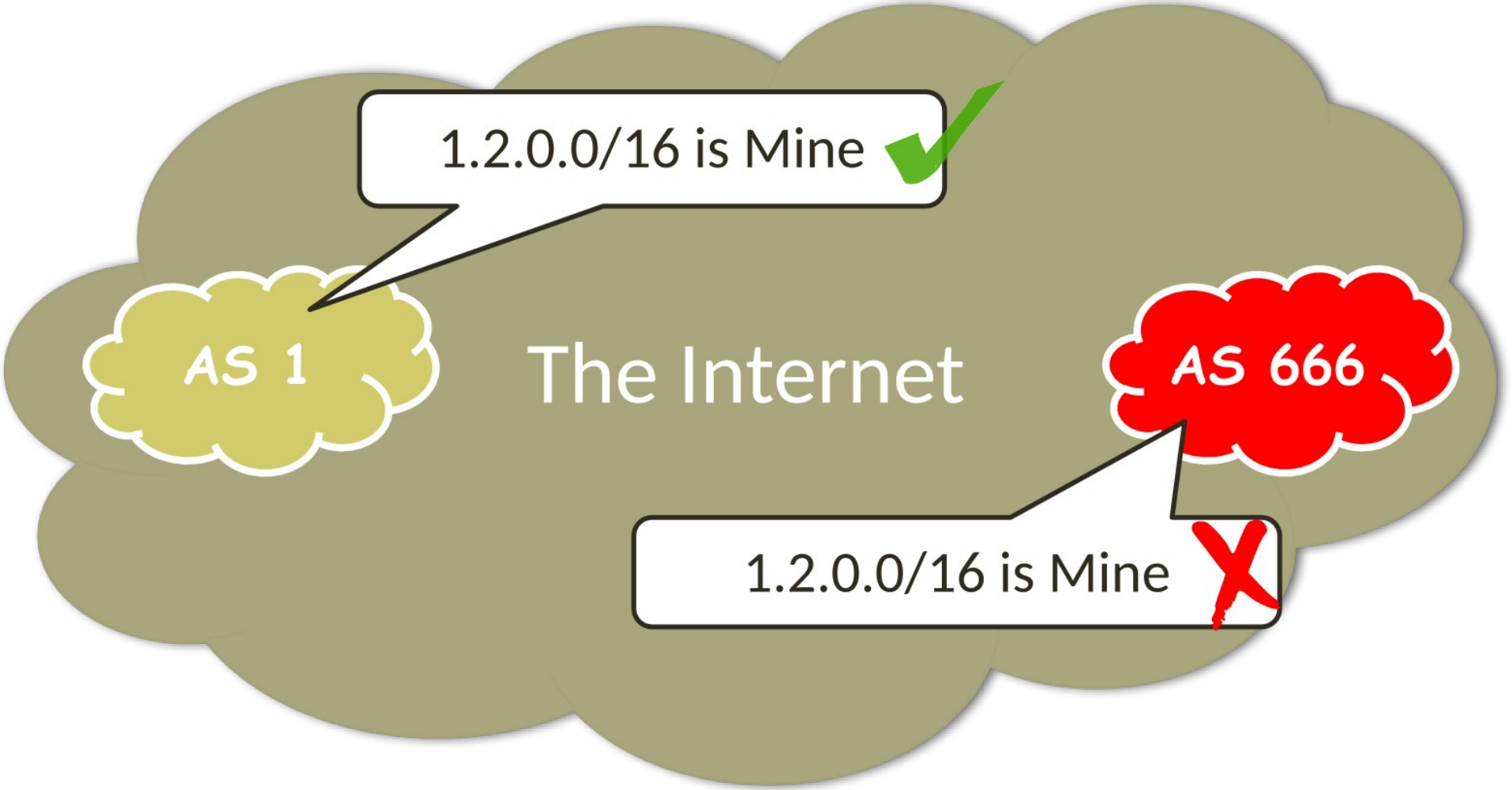
Fonte: Jumpstarting, Avichai, SIGCOMM

ROA + Chain of Trust



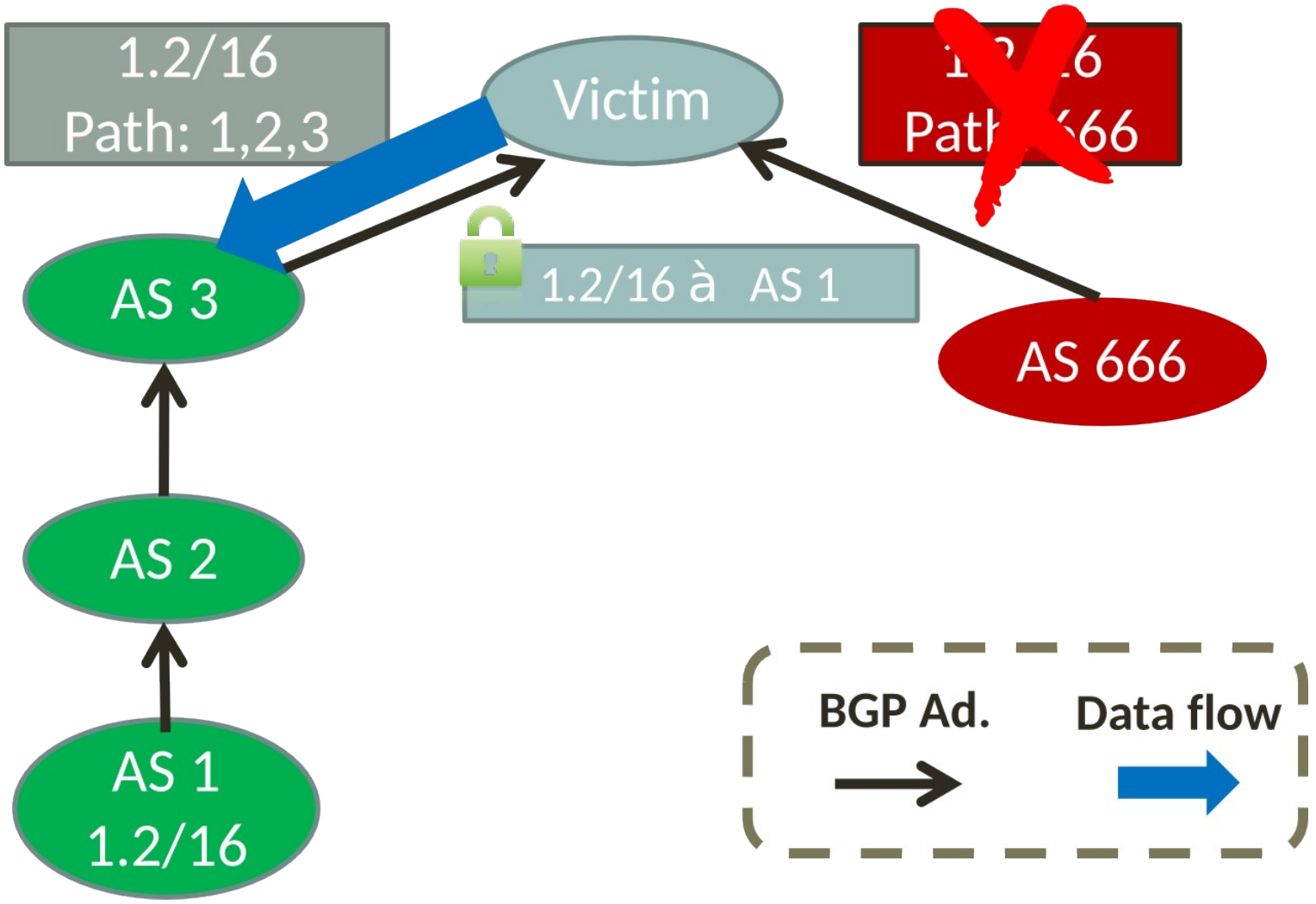
Fonte: bgp-operations-and-security (RIPE)

Resource PKI (RPKI)



Fonte: Jumpstarting, Avichai, SIGCOMM

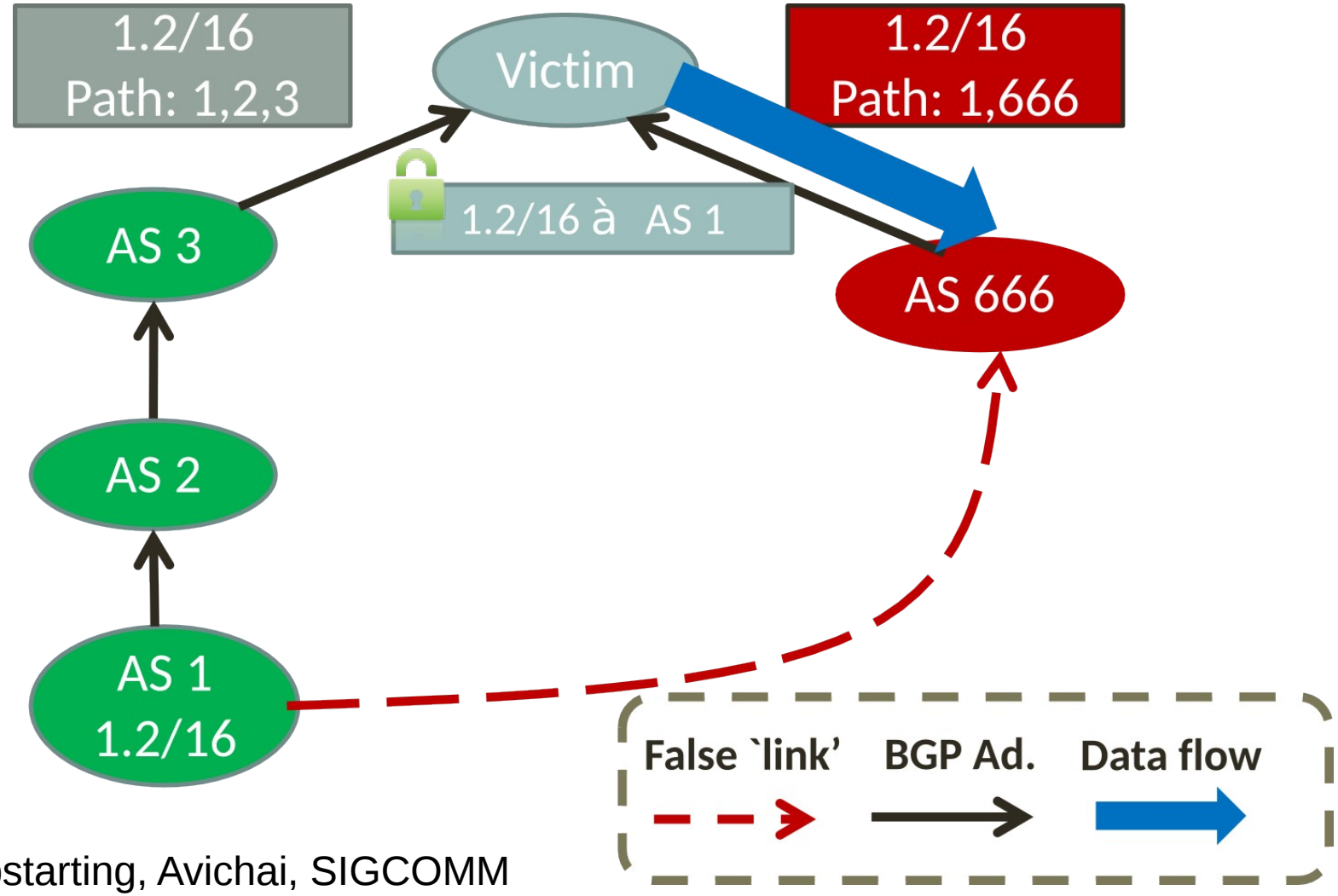
RPKI – prevenção de *prefix hijack*



Fonte: Jumpstarting, Avichai, SIGCOMM

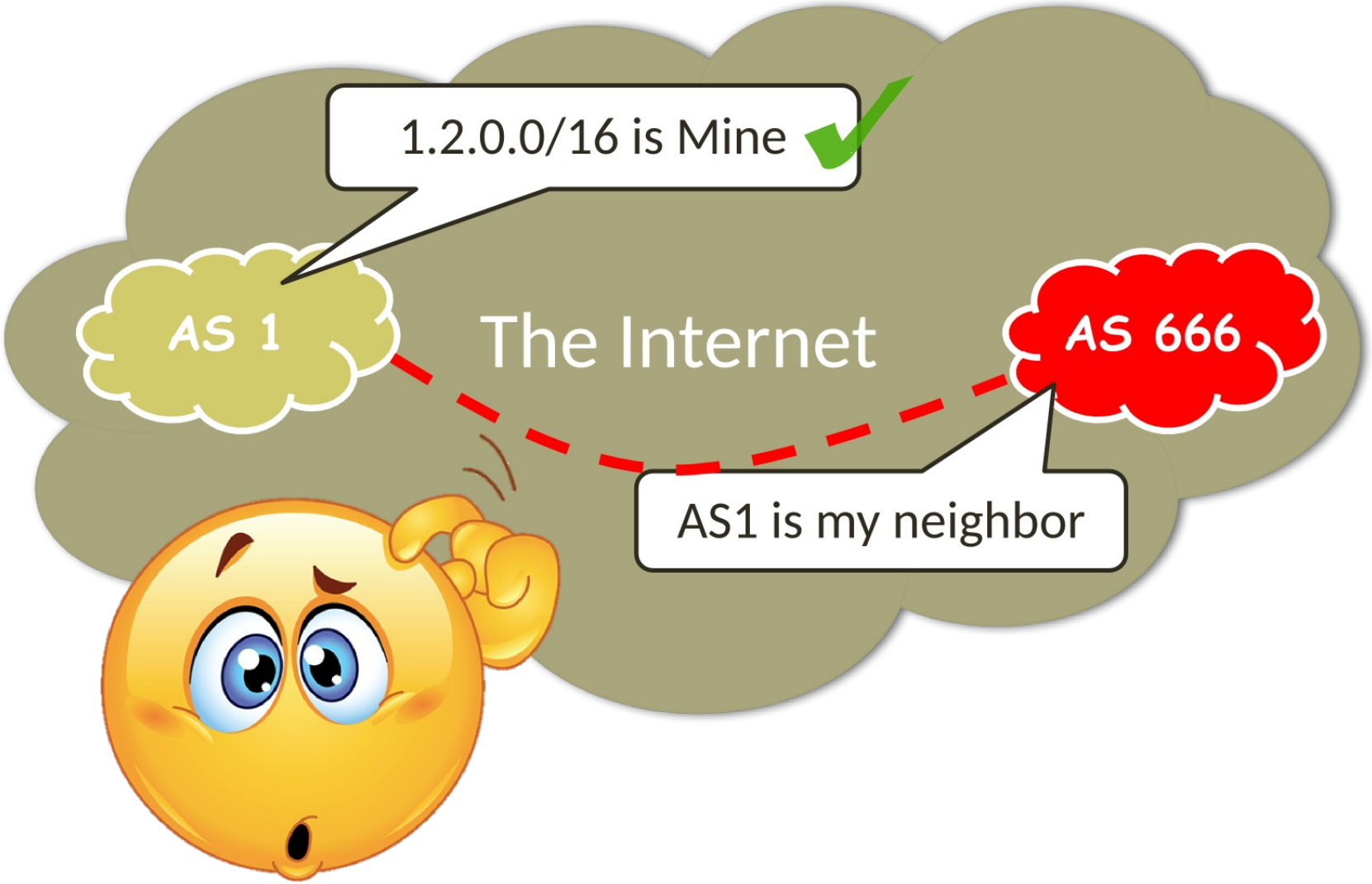
Ataque Next-AS

- RPKI não protege contra roteamento incorreto terminando em origens válidas



Fonte: Jumpstarting, Avichai, SIGCOMM

Ataque Next-AS

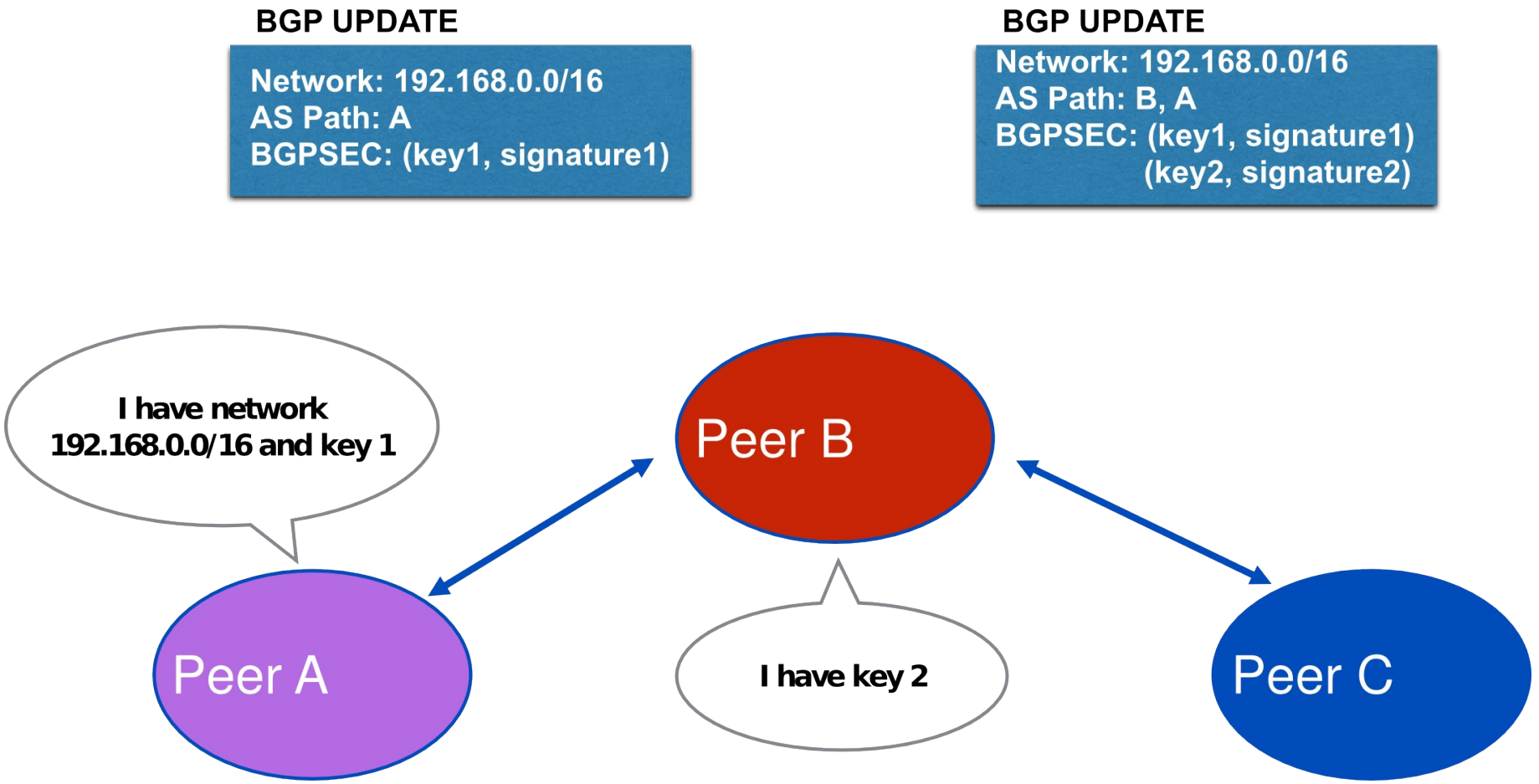


Fonte: Jumpstarting, Avichai, SIGCOMM

BGPSEC

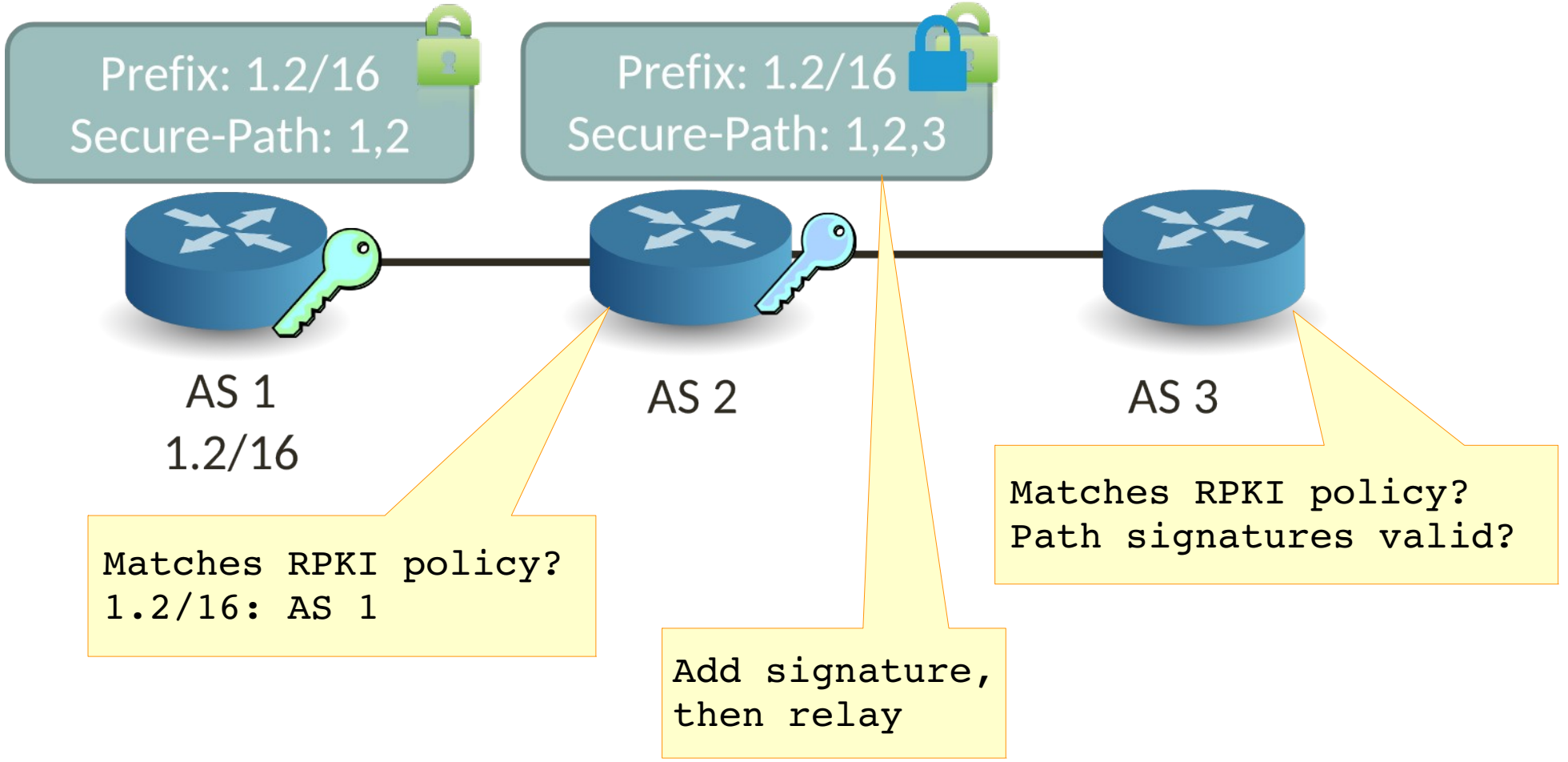
- Novo atributo, opcional, não-transitivo, que carrega assinatura digital de cada AS
- Atributos negociados entre roteadores
- Possibilidade de implementação incremental
- Desafios:
  - IETF Draft
  - Assinatura e validação em tempo real

BGPSEC



Fonte: bgp-operations-and-security (RIPE)

BGPSEC + RPKI



Fonte: Jumpstarting, Avichai, SIGCOMM

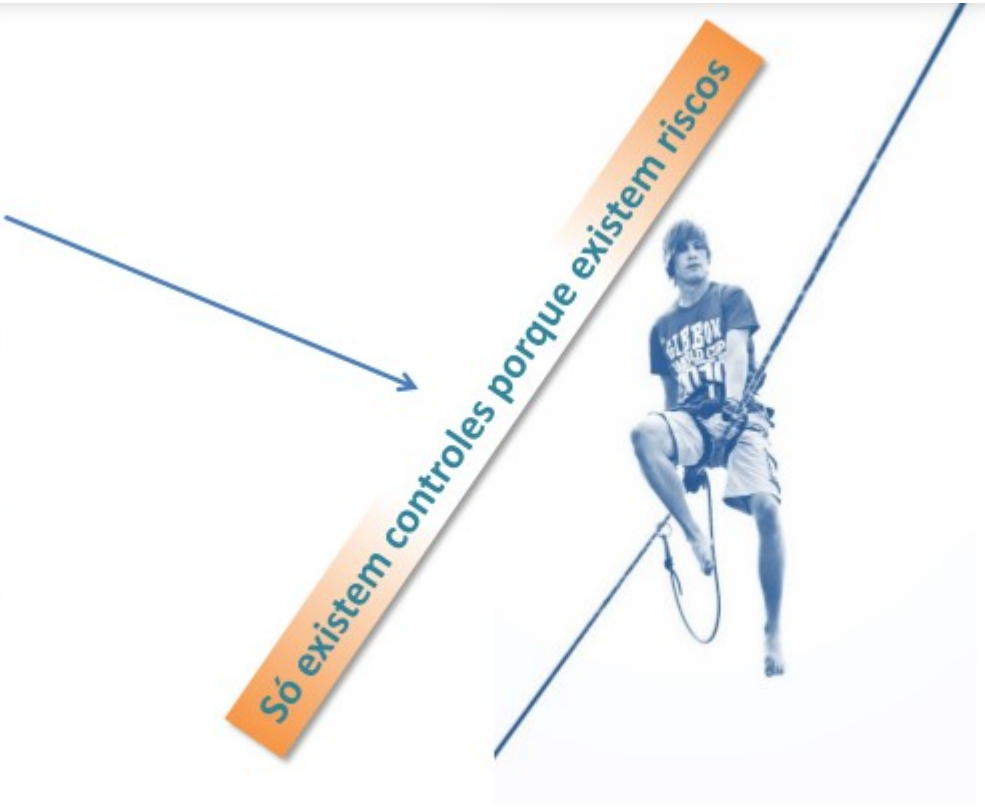
RPKI + BGPSEC Status

- RPKI
  - RPKI é padrão IETF (rfc5280, rfc3779, rfc6481-6493)
  - Os RIRs estão em implantando desde 2011
    - http://certification-stats.ripe.net/
  - Muitos fabricantes já implementam
- BGPSEC
  - Ameaças e requisitos já publicados (rfc7132 e rfc7353)
  - Academia pesquisando carências e alternativas
  - Fabricantes trabalhando em implementações reais

Resumo

- BGP não é seguro por padrão
  - Peers desonestos podem prejudicar a rede
- Existem muitos patches a serem aplicados
  - Não aplicá-los também não resolve
- Segurança BGP pode ser melhorada com:
  - Boas práticas gerais de roteamento e BGP
  - Filtros
  - RPKI + BGPSEC

Gestão de Riscos



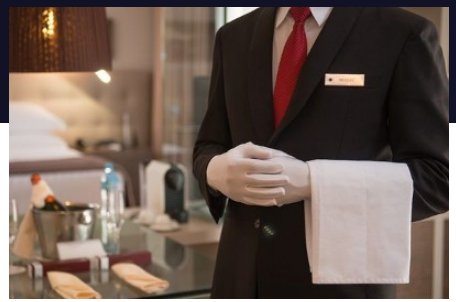
"Tudo na vida é administração de risco, não sua eliminação" (Walter Wiston, ex-presidente do Citicorp).

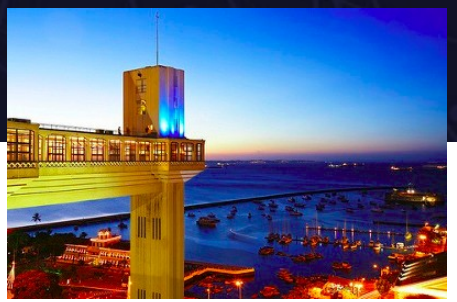
Segurança no Roteamento BGP

ENCONTRO REGIONAL DE
PROVEDORES DE INTERNET DA BAHIA

IX.br - Salvador

Brasil Internet Exchange - Salvador



Italo Valcy
italovalcy@ufba.br