Segurança no roteamento BGP: boas práticas, RPKI e BGPSEC

Italo Valcy <italovalcy@ufba.br>
GTS 29, 26/Mai/2017

POP-BA

STI
Superintendência de Tecnologia da Informação | UFBA

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)
- BGP é usado para divulgar os recursos de numeração de um AS

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 long
only one major
is government

bgpstream @bgpstream · 3h
BGP,HJ,hijacked prefix AS15919 217.75.242.0/24, Servicios de Hosting en Internet S.A.,-,By AS12389 PJSC Rostelecom, bgpstream.com/event/80334

bgpstream @bgpstream · 3h
BGP,HJ,hijacked prefix AS11383 216.150.144.0/24, Xand Corporation,-,By AS12389 PJSC Rostelecom, bgpstream.com/event/80333

bgpstream @bgpstream · 3h
BGP,HJ,hijacked prefix AS26380 216.119.216.0/24, MasterCard Technologies LLC,-,By AS12389 PJSC Rostelecom, bgpstream.com/event/80332

bgpstream @bgpstream · 3h
BGP,HJ,hijacked prefix AS9221 203.112.91.0/24, HSBC HongKong,-,By AS12389 PJSC Rostelecom, bgpstream.com/event/80331

bgpstream @bgpstream · 3h
BGP,HJ,hijacked prefix AS9221 203.112.90.0/24, HSBC HongKong,-,By AS12389 PJSC Rostelecom, bgpstream.com/event/80330

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
ncovered multiple BGP incidents used to
eal bitcoins. According to Secureworks,
e attacker used a compromised
dministrator account at a yet undisclosed

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

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 s
were reportedly arrested in Israel on Thursday. The pair were arrested around the same
that KrebsOnSecurity publ

"Defensive" BGP hijacking?

https://arstechnica.com/security/2017/04/russian-controlled-telecom-hijacks-financial-servic

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

Russian-controlled telecom hijacks financial services' Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/27/2017, 5:20 PM

HURRICANE ELECT
INTERNET SERVI

AS174 Cogent Communications

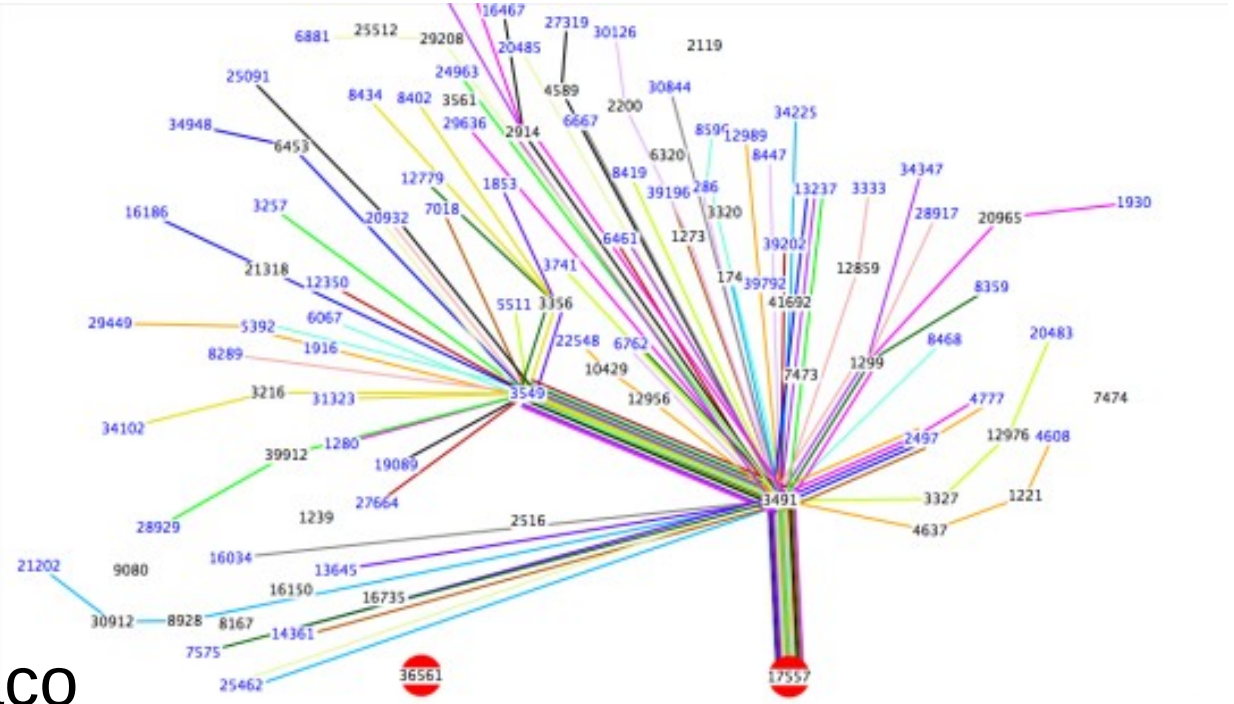
Quick Links
BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Exchange Report
Bogon Routes

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v

AS174 announces bogons.

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 (2008)
(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

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.)

Filtros BGP

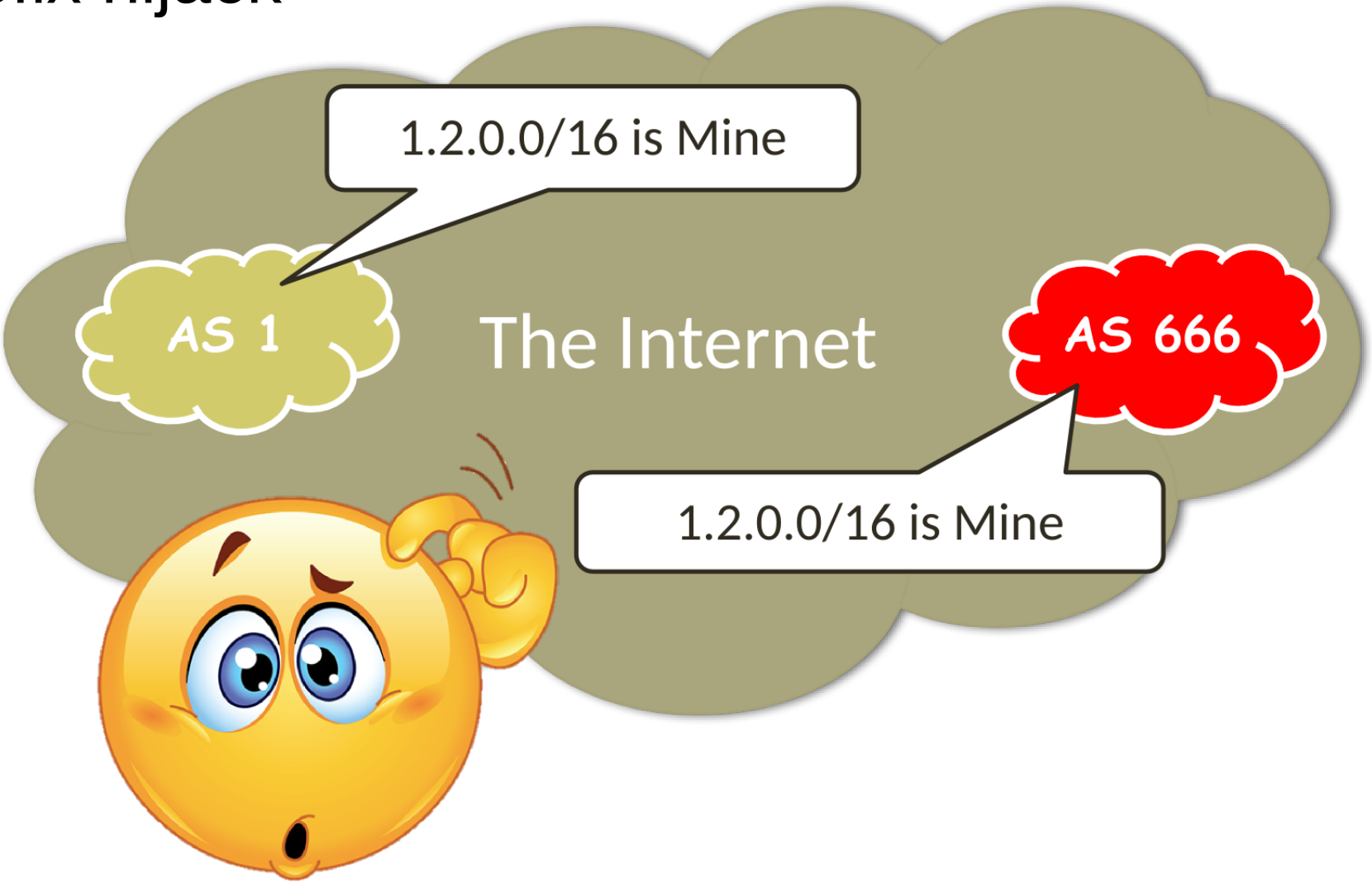
- Prefix-list
  - Filtros de rotas para aceitar ou anunciar
  - Fácil de configurar porém não escalável
  - Criadas manual ou automaticamente
    - RIPE DB e outros IRRs (ex. RADb, PeeringDB, etc)
- AS-Path
  - Filtragem de rotas baseada no AS-Path
  - Amplamente usada e escalável
  - Extensível via expressões regulares

Boas práticas de filtragem

- Não aceitar prefixos RFC1918 e demais
- Não aceitar seu próprio prefixo
- Não aceitar rota padrão (a menos que necessário)
- Validar prefixos de clientes
- Monitorar sempre, agregar ao máximo, engenharia de tráfego quando necessário

Como garantir a origem?

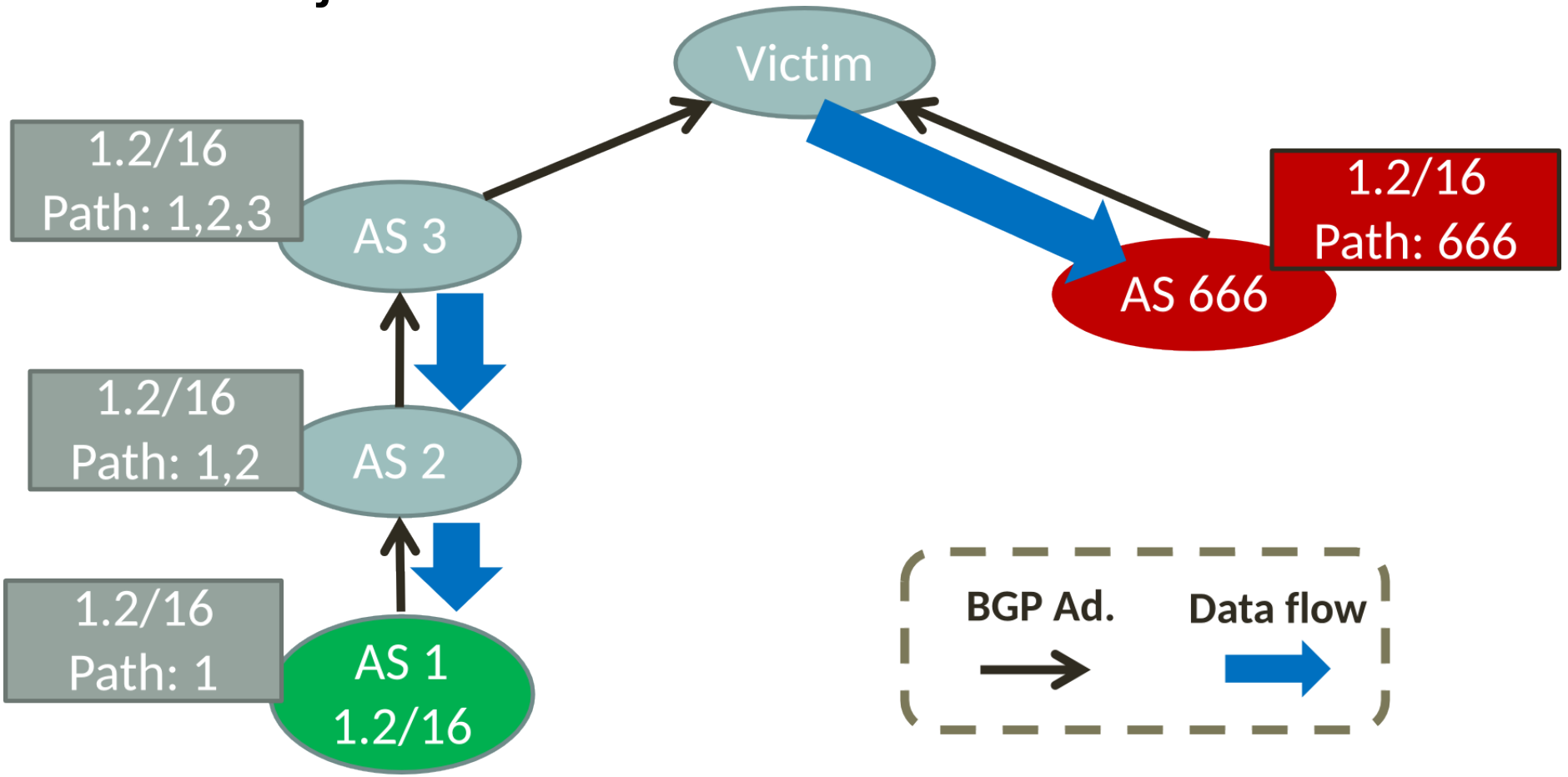
- Prefix hijack



Fonte: Jumpstarting, Avichai, SIGCOMM

Como garantir a origem?

- Prefix hijack



Fonte: Jumpstarting, Avichai, SIGCOMM

Problemas à vista

- Como garantir a autoridade dos prefixos anunciados?
- Como garantir a validade de informações em bases IRR?
- O que fazer com rotas inválidas?
- Como validar o caminho (path) de um prefixo?

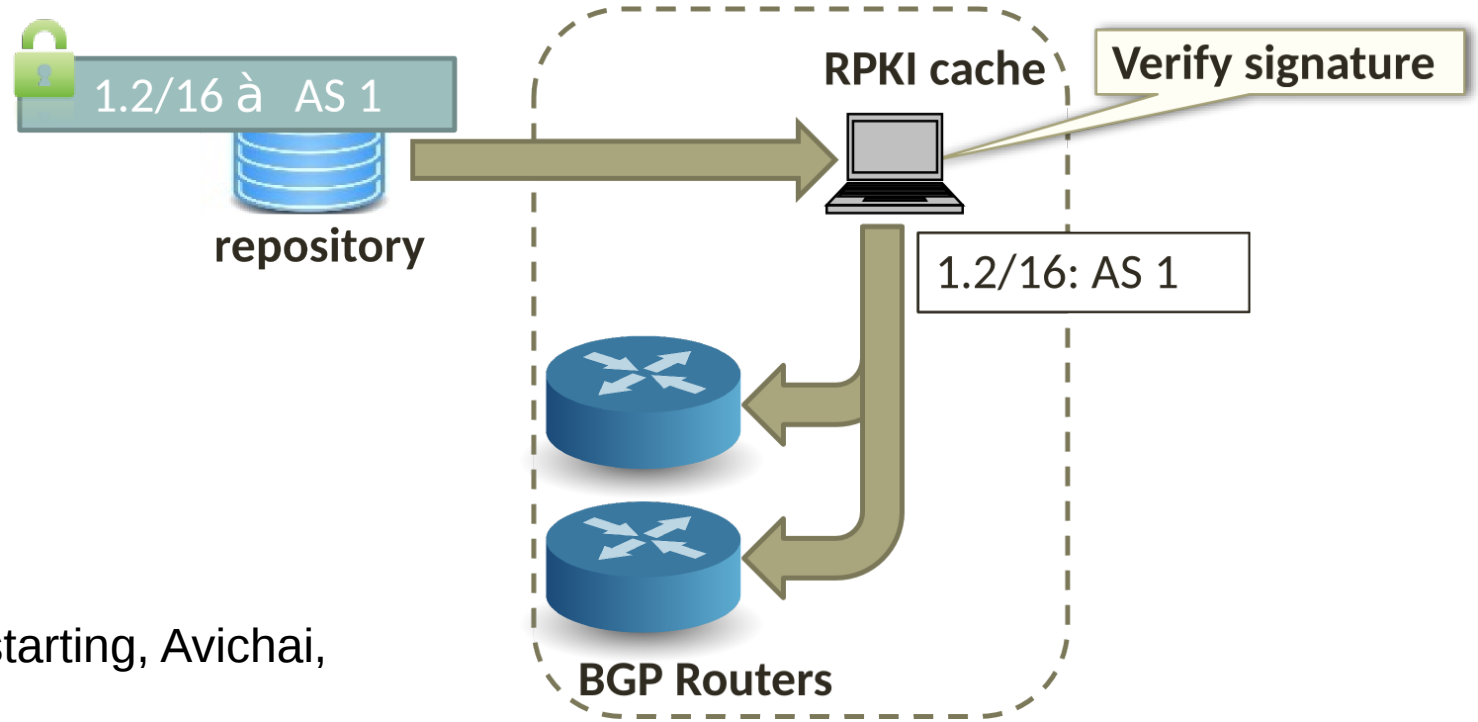
RPKI – Adicionando segurança aos recursos de numeração da Internet

O que é RPKI?

Um framework de **segurança para roteamento na Internet** que provê verificação da associação entre **recursos de Internet** e **proprietários de recursos**

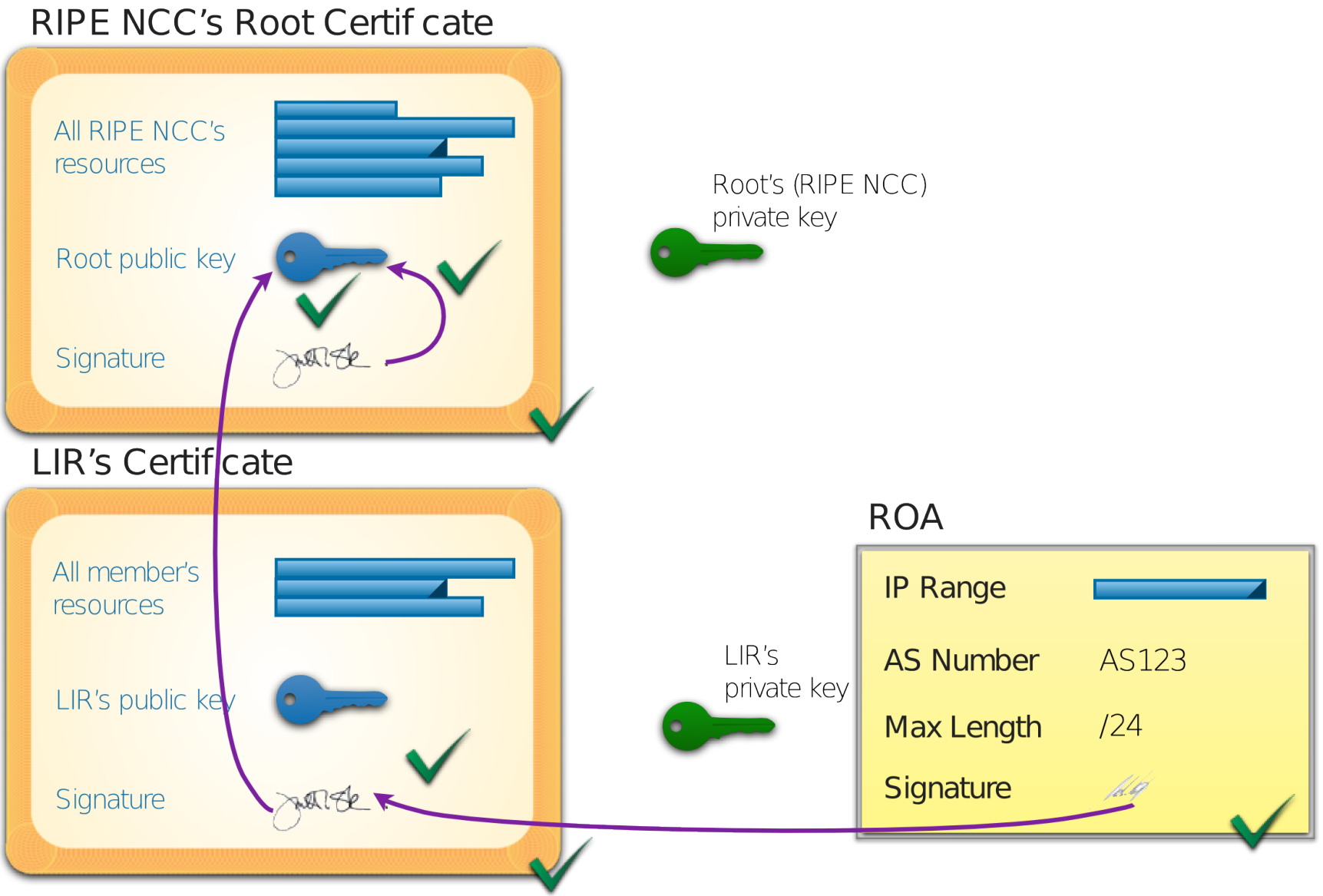
Resource PKI (RPKI)

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



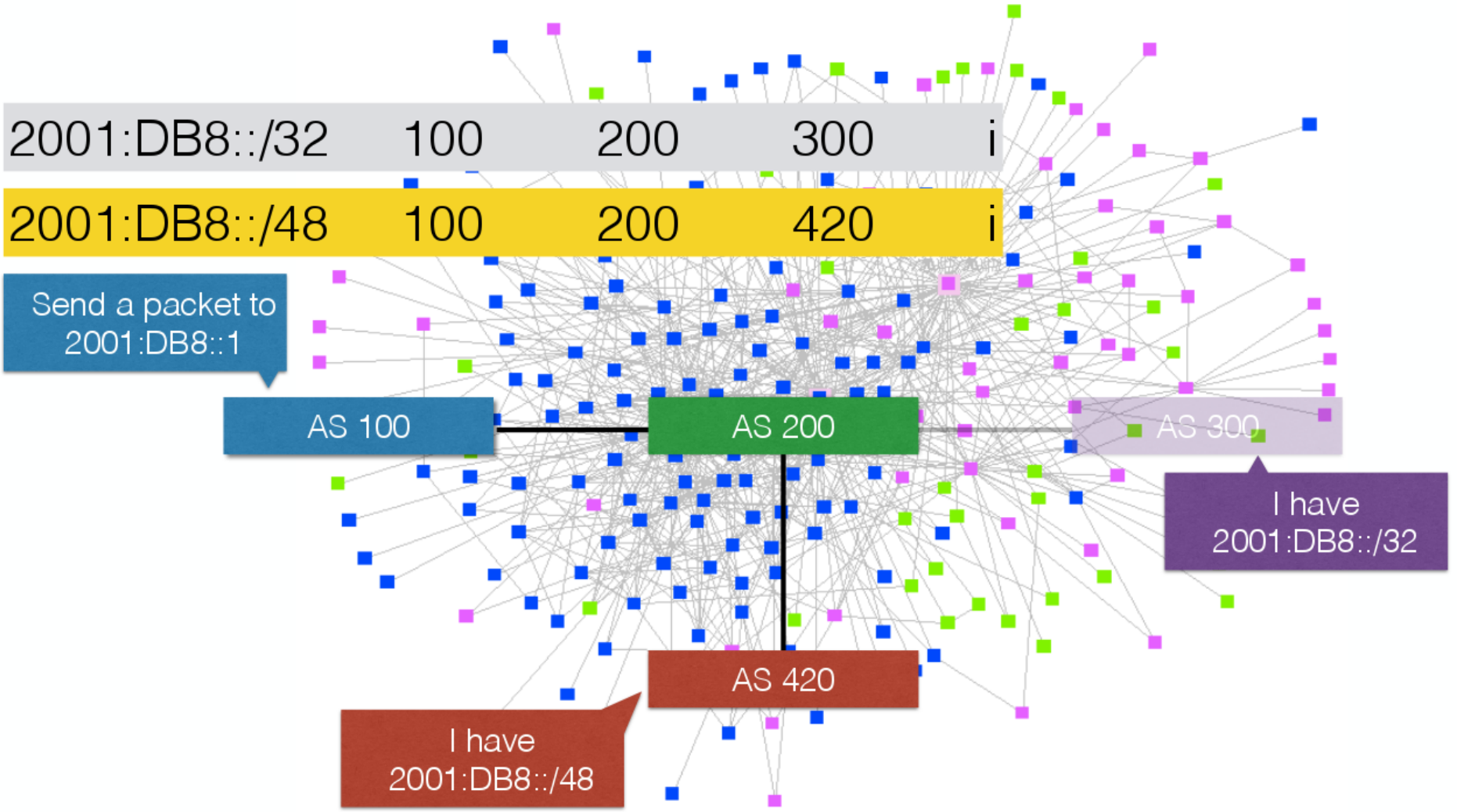
Fonte: Jumpstarting, Avichai, SIGCOMM

ROA + Chain of Trust



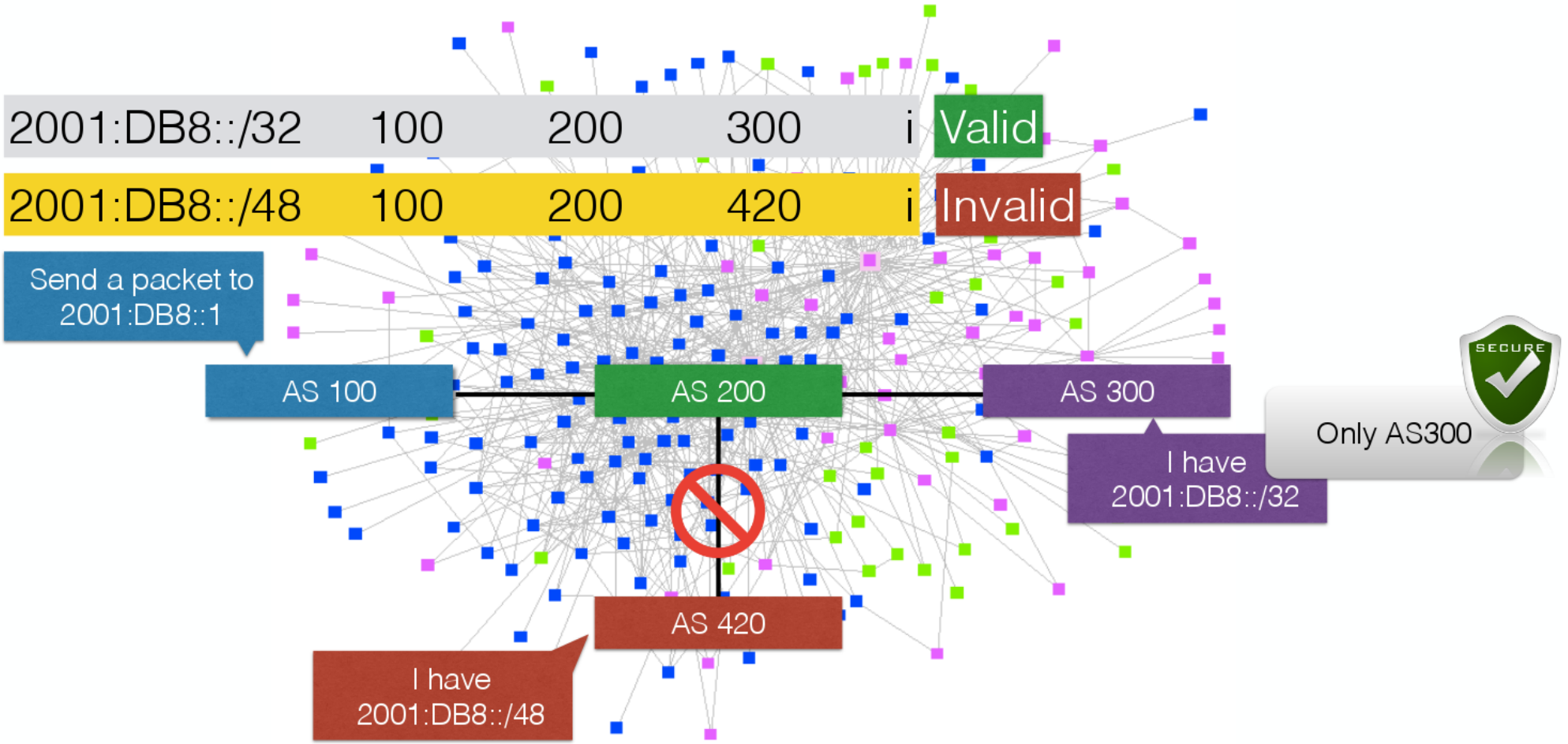
Fonte: bgp-operations-and-security (RIPE)

Exemplo



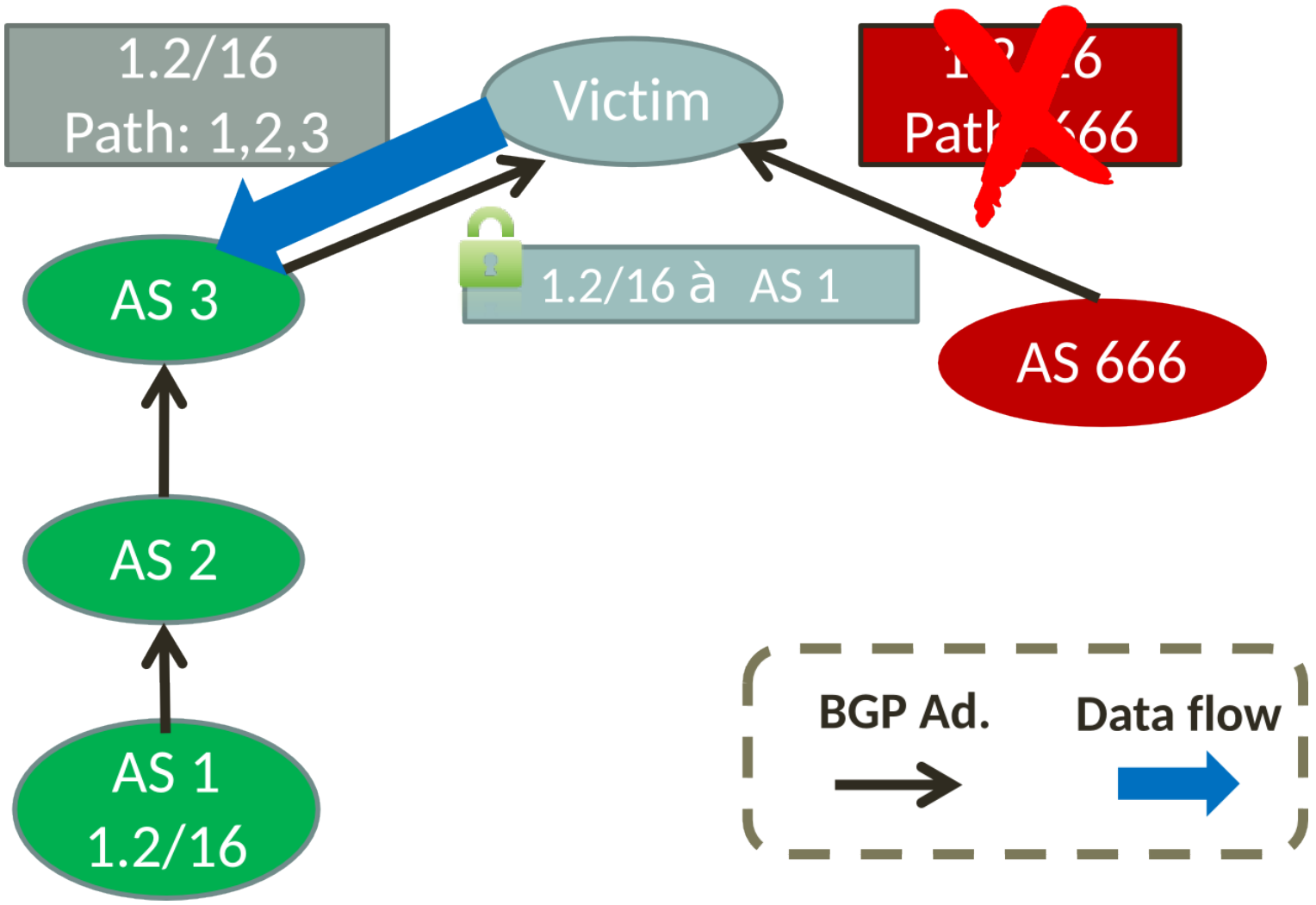
Fonte: RPKI Tutorial, SANOG25

Ex c/ Validação da Origem RPKI



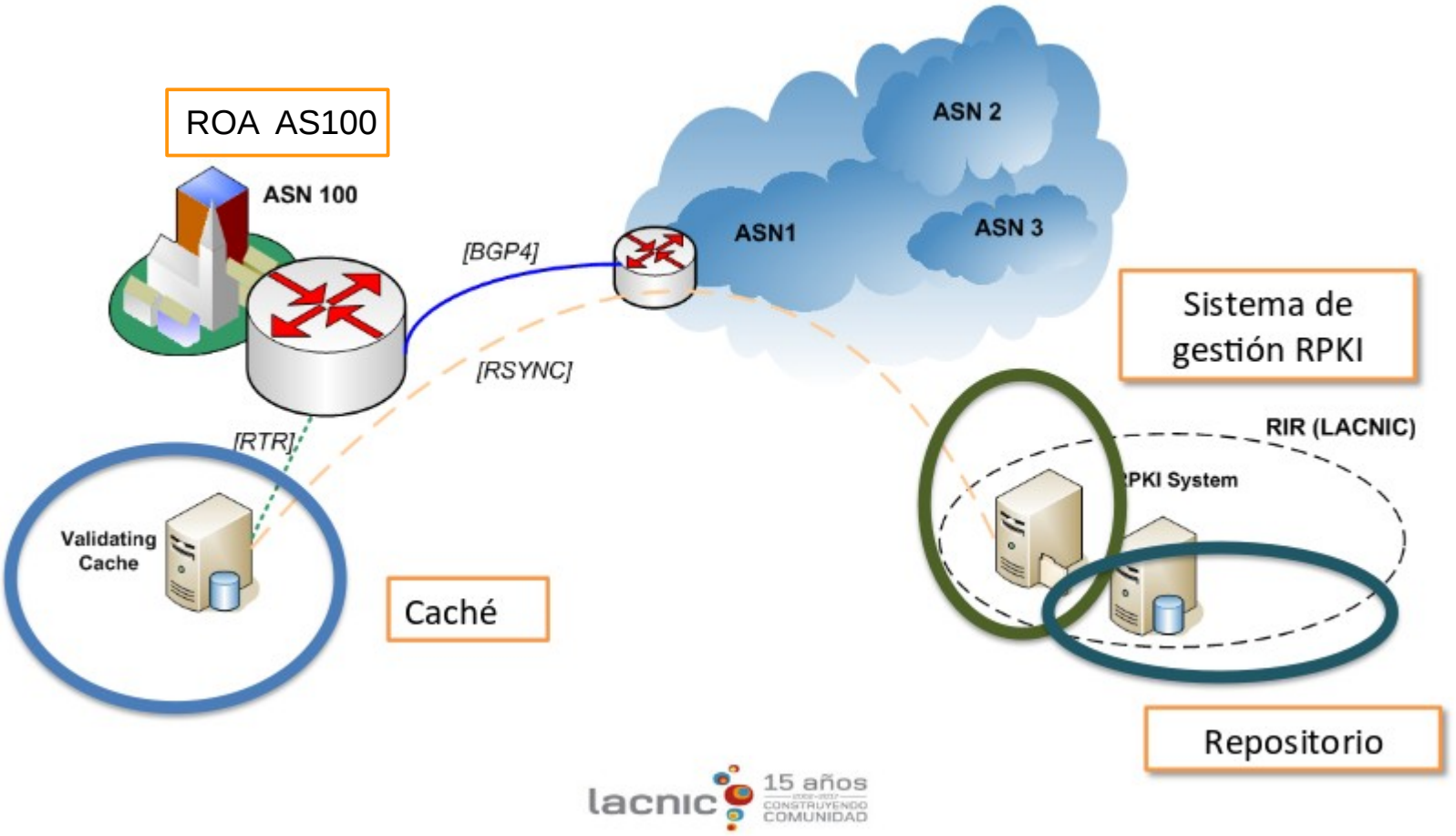
Fonte: RPKI Tutorial, SANOG25

RPKI – prevenção de *prefix hijack*



Fonte: Jumpstarting, Avichai, SIGCOMM

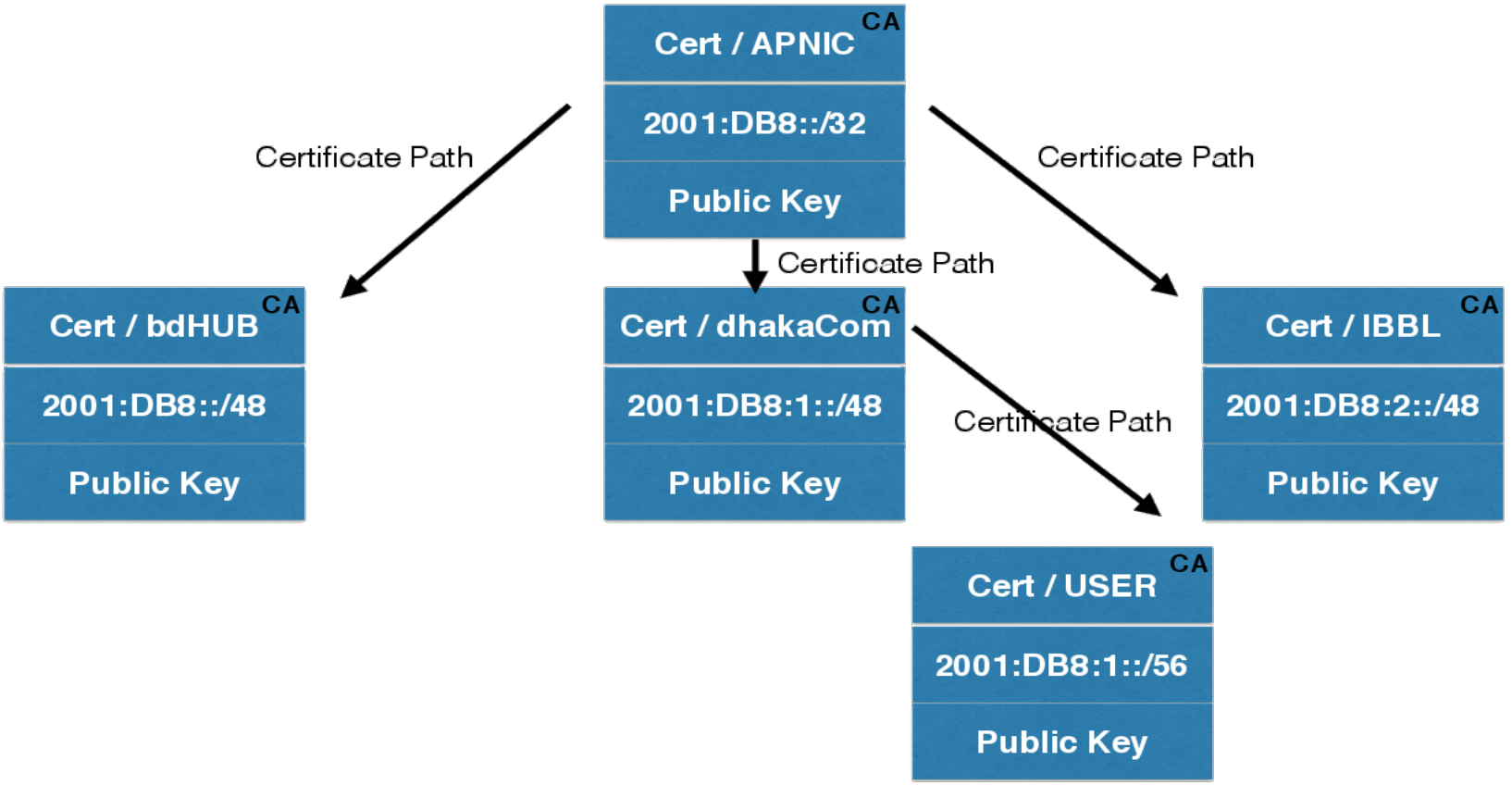
RPKI building blocks



Fonte: Tutorial BGP/RPKI LACNIC27

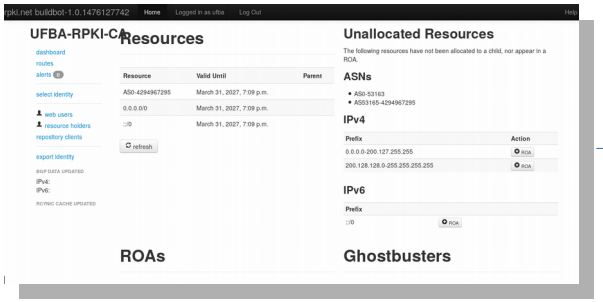
Trust Anchor

- Na estrutura de PKI uma Trust Anchor (ex: CA) é uma entidade em que a **confiança é assumida e não derivada**
  - Tipicamente consiste no certificado raiz

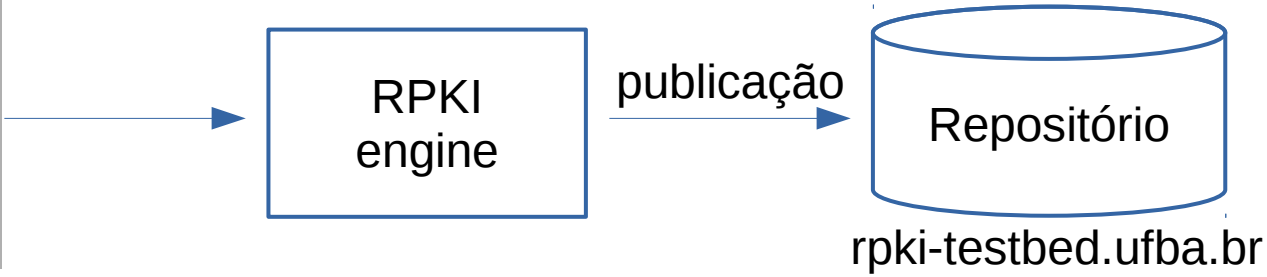


Trust Anchor

- Internet Registries (RIR, NIR, grandes LIRs)
- Atua como AC e AR, emitindo certificados para detentores de recursos
- Geralmente também disponibiliza uma interface para emissão de ROAs
- Publica os ROAs em um repositório

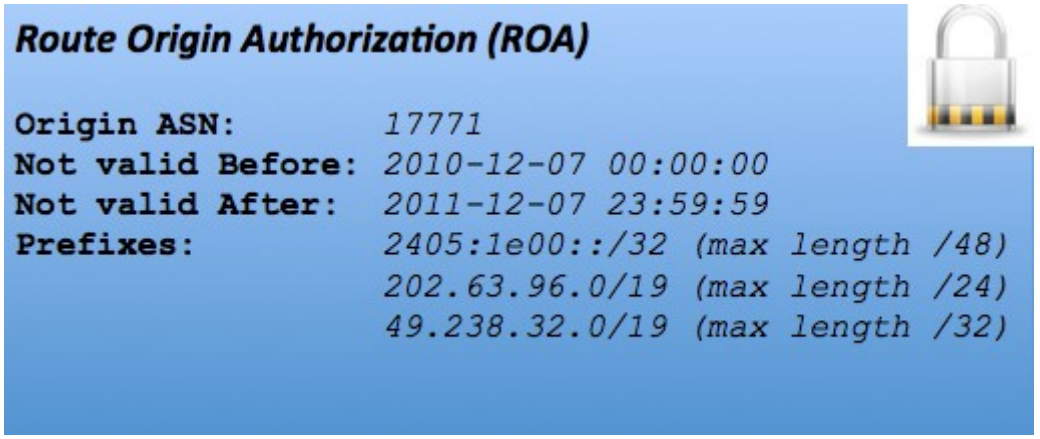


MyRPKI GUI



Route Origination Authorization (ROA)

- Objeto digital assinado que contém uma lista de endereços IP
- É uma autorização emitida pelo proprietário de recursos autorizando um AS a anunciar um ou mais específicos prefixos/rotas



Validators (Relying Party – RP)

- Roteadores que suportam RPKI podem validar os prefixos recebidos através de **Relying Parties / RPKI Cache / Validators**
  - A validação é feita no RP, o roteador apenas se pergunta algo como:

    “Recebi um anuncio para 8.8.8.0/24 com origem no AS 15169, este anuncio é autorizado?”

Resultado da checagem

- **Valid** – Indica que o prefixo e o AS foram encontrados na base RPKI e estão válidos;
- **Invalid** – Indica que o prefixo/AS foram encontrados, porém o AS de origem ou o tamanho do prefixo divergem do que está autorizado na base
- **Not Found / Unknown** – Indica que o prefixo não está na base

Valid > Unknown > Invalid

Exemplo

Prefix: 10.0.0.0/16
ASN: 65420

	Origin AS	Prefix	Max Length
ROA	65420	10.0.0.0/16	/18
VALID	AS65420	10.0.0.0/16	
VALID	AS65420	10.0.128.0/17	
INVALID	AS65421	10.0.0.0/16	
INVALID	AS65420	10.0.10.0/24	
UNKNOWN	AS65430	10.0.0.0/8	

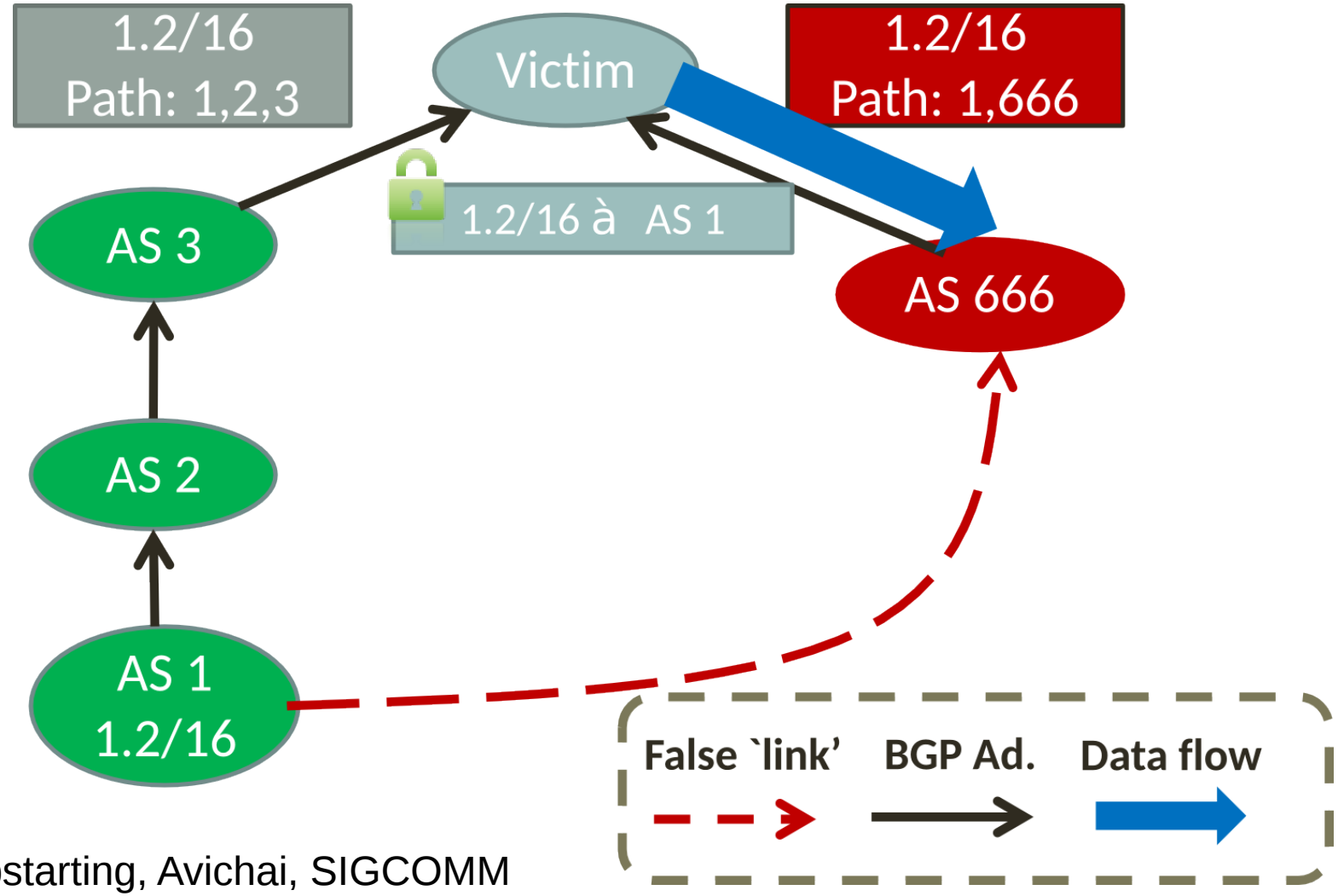
Estamos seguros agora?

Estamos seguros agora?

- RPKI é util para validação da origem ou autorização de anuncio
- Porém, não protege contra spoofing do AS de origem ou modificações não autorizadas no caminho!
  - Ataques de Next-AS

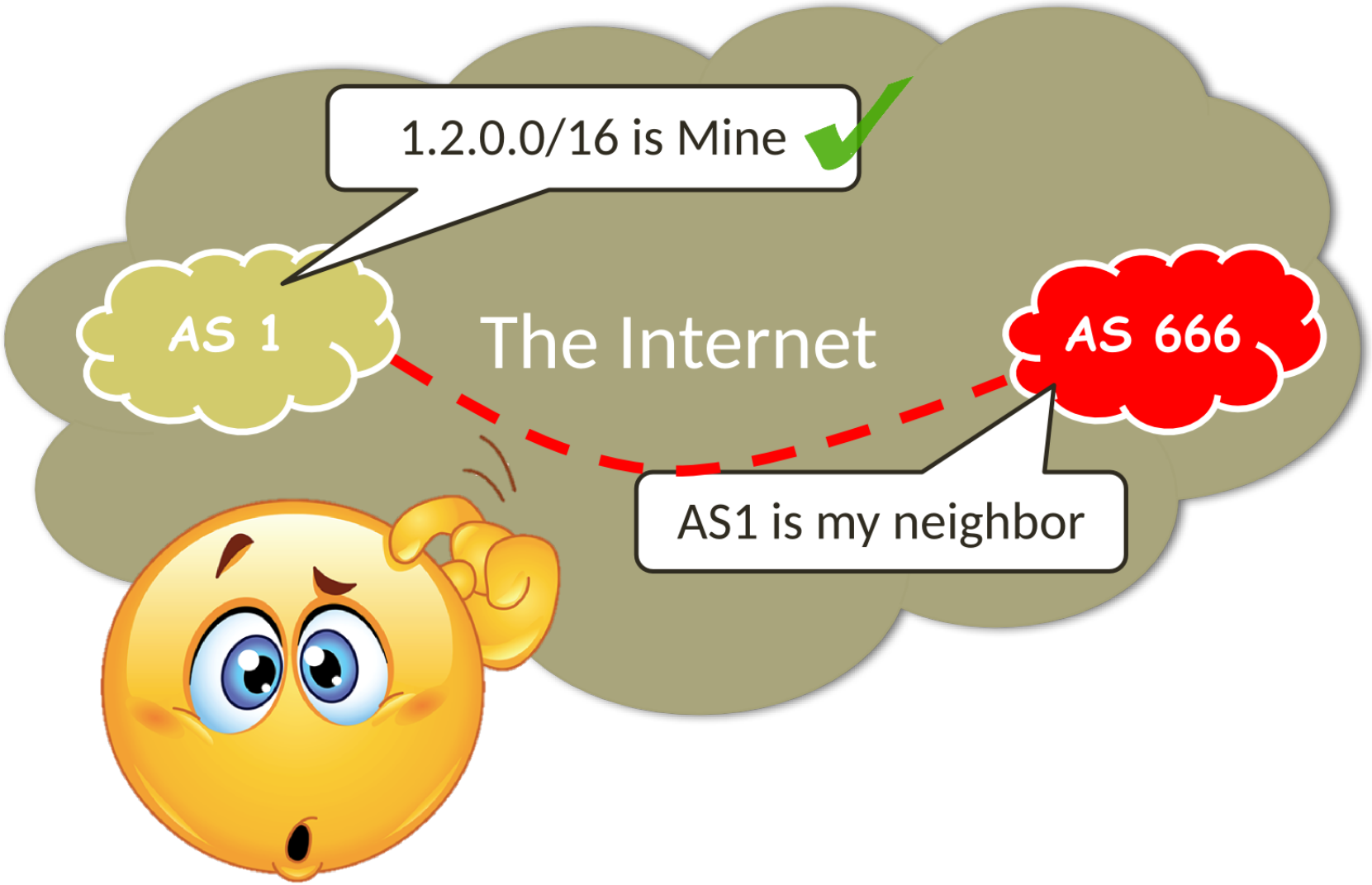
Ataque Next-AS

- RPKI não protege contra roteamento incorreto terminando em origens válidas



Fonte: Jumpstarting, Avichai, SIGCOMM

Ataque Next-AS

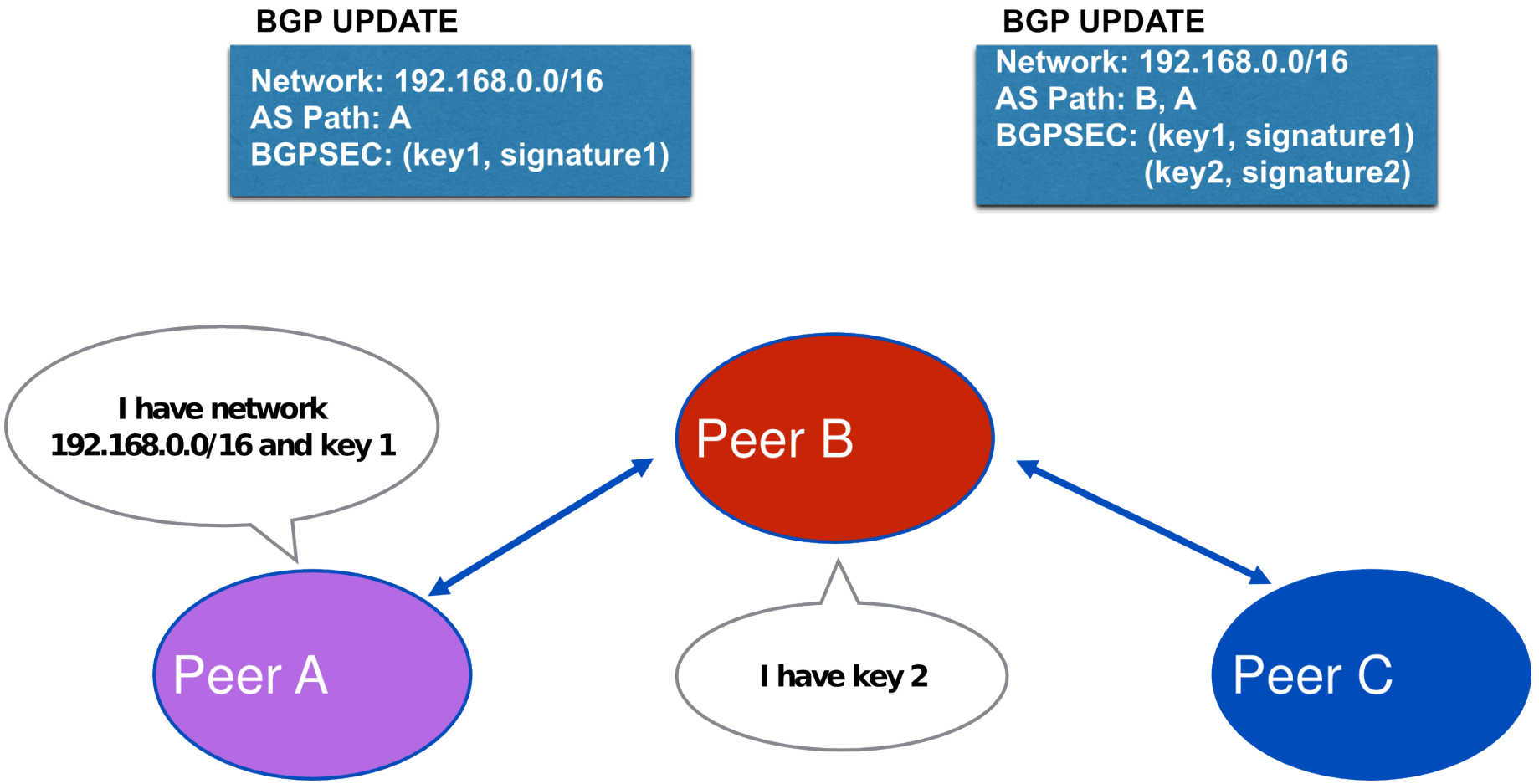


Fonte: Jumpstarting, Avichai, SIGCOMM

BGPSEC

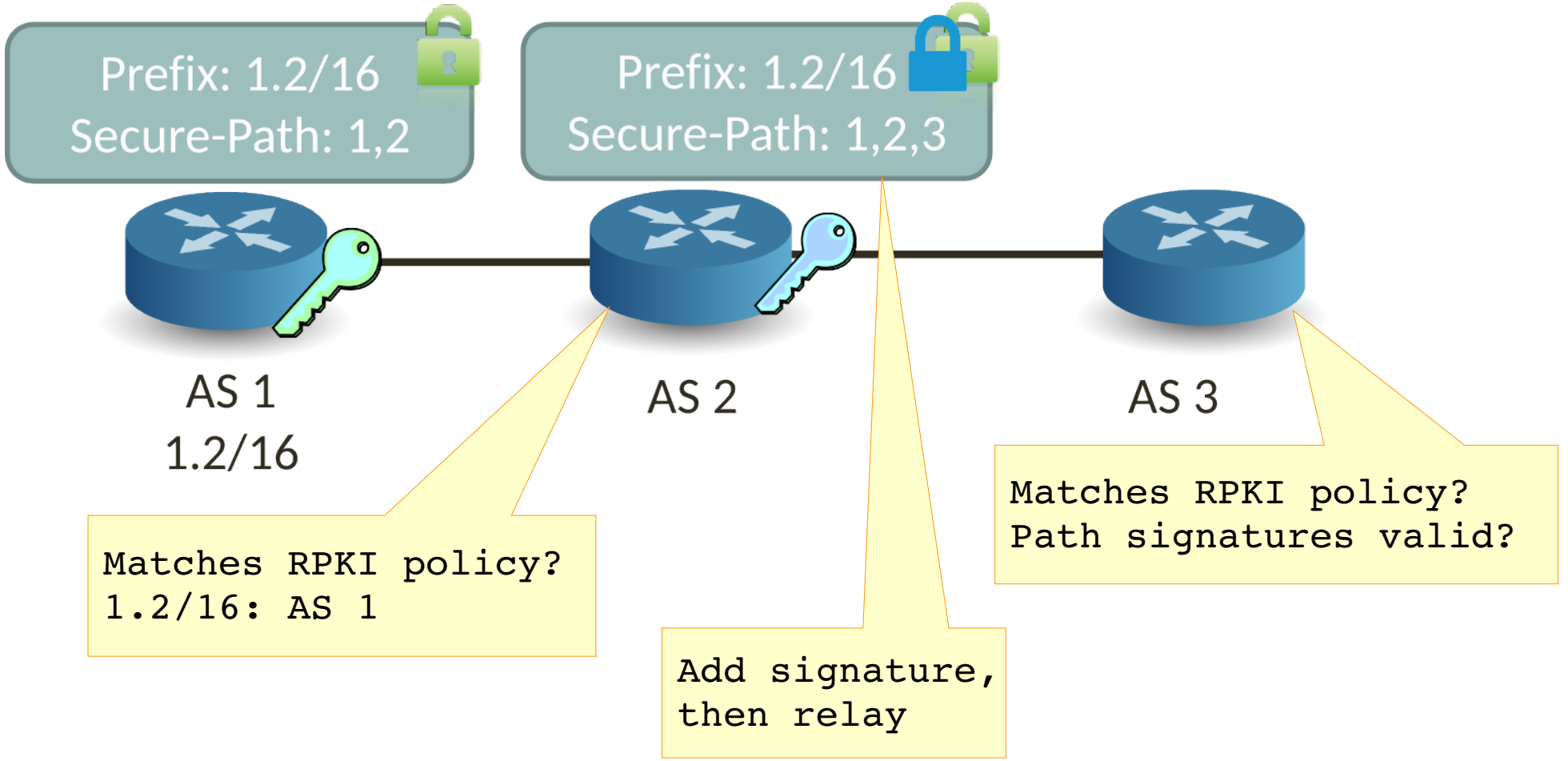
- Novo atributo, opcional, não-transitivo, que carrega assinatura digital de cada AS
- Atributos negociados entre roteadores
- Possibilidade de implementação incremental
- Desafios:
  - IETF Draft
  - Assinatura e validação em tempo real

BGPSEC



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

BGPSEC + RPKI



Fonte: Jumpstarting, Avichai, SIGCOMM

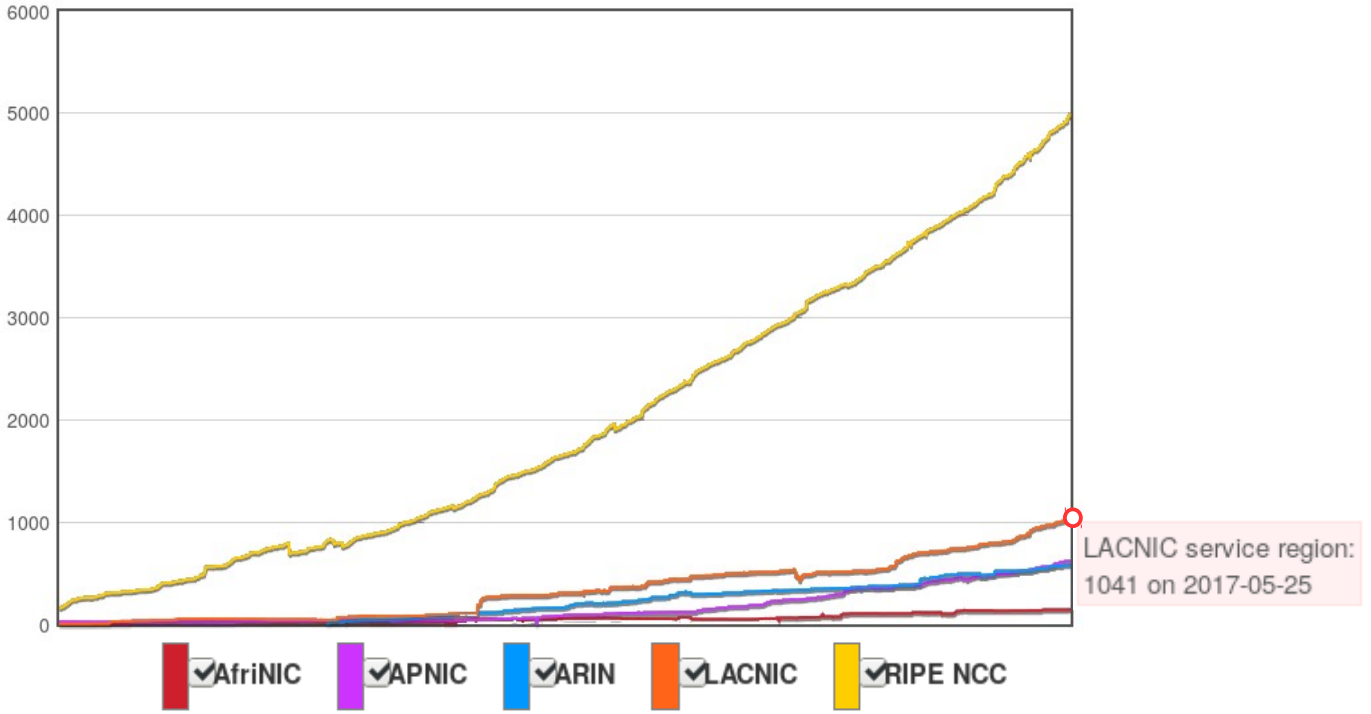
RPKI + BGPSEC Status

- 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
    - Brocade não suporta (no melhor do nosso conhecimento)
    - Possibilidade de implantação via communities
- BGPSEC
  - Ameaças e requisitos já publicados (rfc7132 e rfc7353)
  - Academia pesquisando carências e alternativas
    - Path-End Validation (2016, Avichai et al.)
  - Fabricantes trabalhando em implementações reais

Muitos trabalhos em andamento

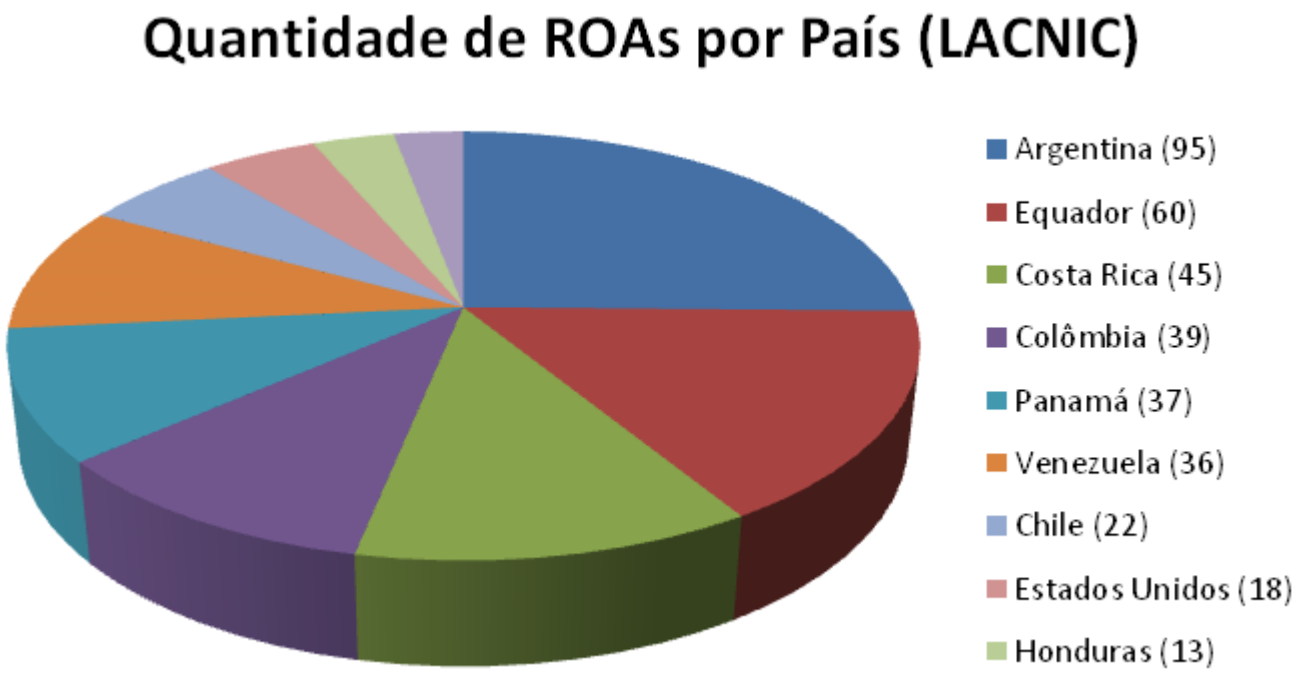
- SIDR Working Group (IETF)
  - Trabalhos em andamento com BGPsec
  - Publicação de chaves
  - …
- Acadêmia
  - Jumpstarting BGP Security with Path-End Validation (SIGCOMM 16)
    - Extensão do RPKI para fazer validação em até 2 hops

Adoção de RPKI nos RIRs



Fonte: RIPE NCC RPKI Statistics

Adoção de RPKI no LACNIC



- 465 ASNs em ROAs
  - Maioria são provedores de acesso
  - 34 universidades/NRENs; alguns provedores de conteúdo
- 2654 rotas protegidas (16% IPv6)
  - 1927 anúncios BGP com RPKI inválido

Erros na validação RPKI

- Indicam anúncios não autorizados de endereços
- Podem indicar também erros de configuração!
- Exemplo LACNIC:
  - 273 Invalid ASN
  - 1654 Invalid Length

AS6xx7
Prefixo: 2001:xxxx::/32
Max-Length: 47

Trabalhos em Andamento

- Co-orientação de TCC: Investigar os benefícios e impactos da implantação de RPKI no BR, bem como desafios operacionais

- Criação de um testbed RPKI na UFBA para provedores interessados
  - Trust Anchor (CA)
  - Validador (RP)

Considerações finais

- Ataques na infraestrutura de rede afetam de forma crítica as organizações
- BGP não é seguro por padrão
  - Peers desonestos podem prejudicar a rede
- Tecnologias como RPKI e BGPSEC são importantes para ajudar a mitigar alguns deles
  - Falta de compatibilidade dos vendors pode atrapalhar
- Adote boas práticas de configuração BGP

Créditos

- Tutorial BGP/RPKI (LACNIC27)
- 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

Segurança no roteamento BGP: boas práticas, RPKI e BGPSEC

Italo Valcy <italovalcy@ufba.br>
GTS 29, 26/Mai/2017

POP-BA

STI
Superintendência de Tecnologia da Informação | UFBA