Ataques a Infraestrutura BGP e medidas de contenção

Leandro M Bertholdo (berthold@penta.ufrgs.br)

PoP-RS/RNP/Ufrgs

Roteiro

- Ataques Teóricos ao BGP
- Ataques Práticos ao BGP
- Mitigação
- Soluções a mais longo prazo

O BGP é "inseguro" porque qualquer AS pode anunciar qualquer rota que desejar a qualquer um de seus vizinhos.

BGP is “insecure” because any AS can announce any path it wants to any subset of its neighbors.

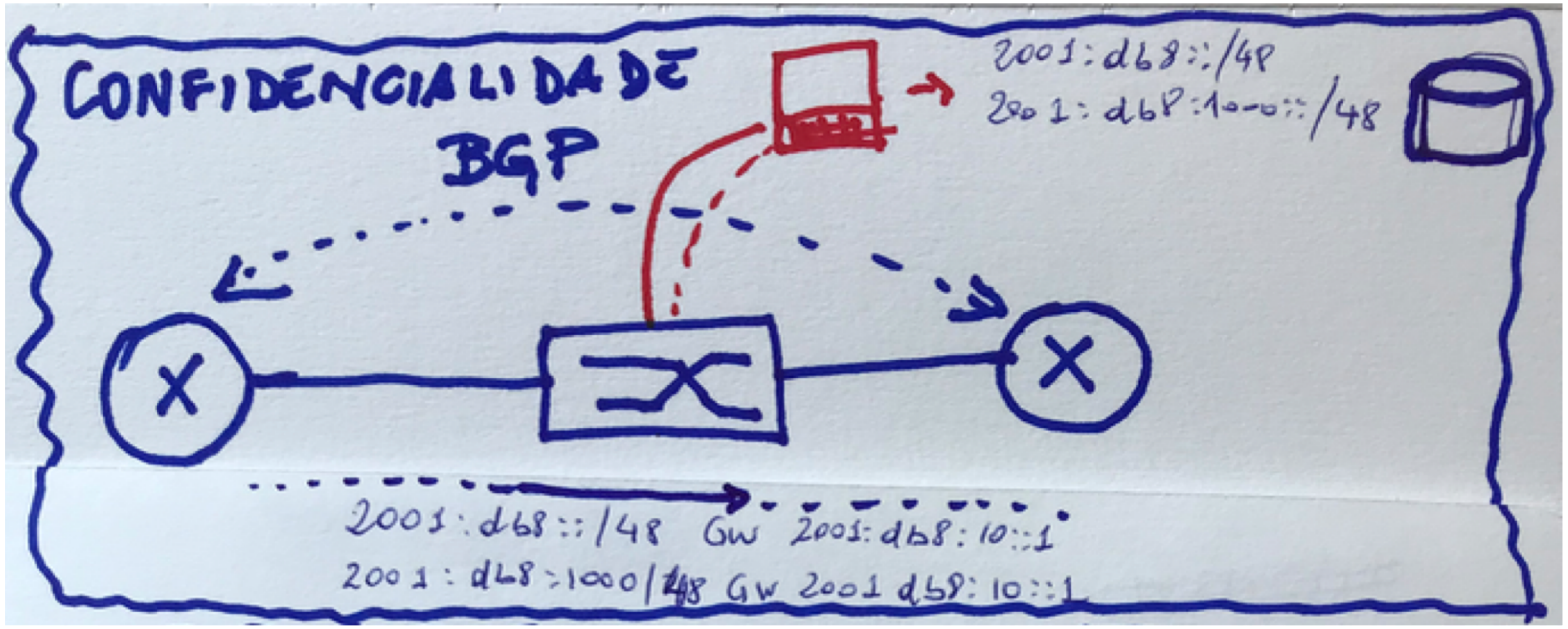
Robert Lychev, Michael Schapira, and Sharon Goldberg. 2016. Rethinking security for internet routing. Commun. ACM 59, 10 (September 2016)

Análise de ataques conhecidos ao protocolo BGP

Violação de Confidencialidade
Reprodução de Mensagem
Inserção de Mensagem
Exclusão de Mensagem
Alteração de Mensagem

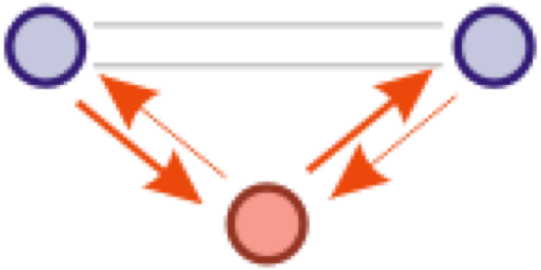
Ataques conhecidos (teóricos)

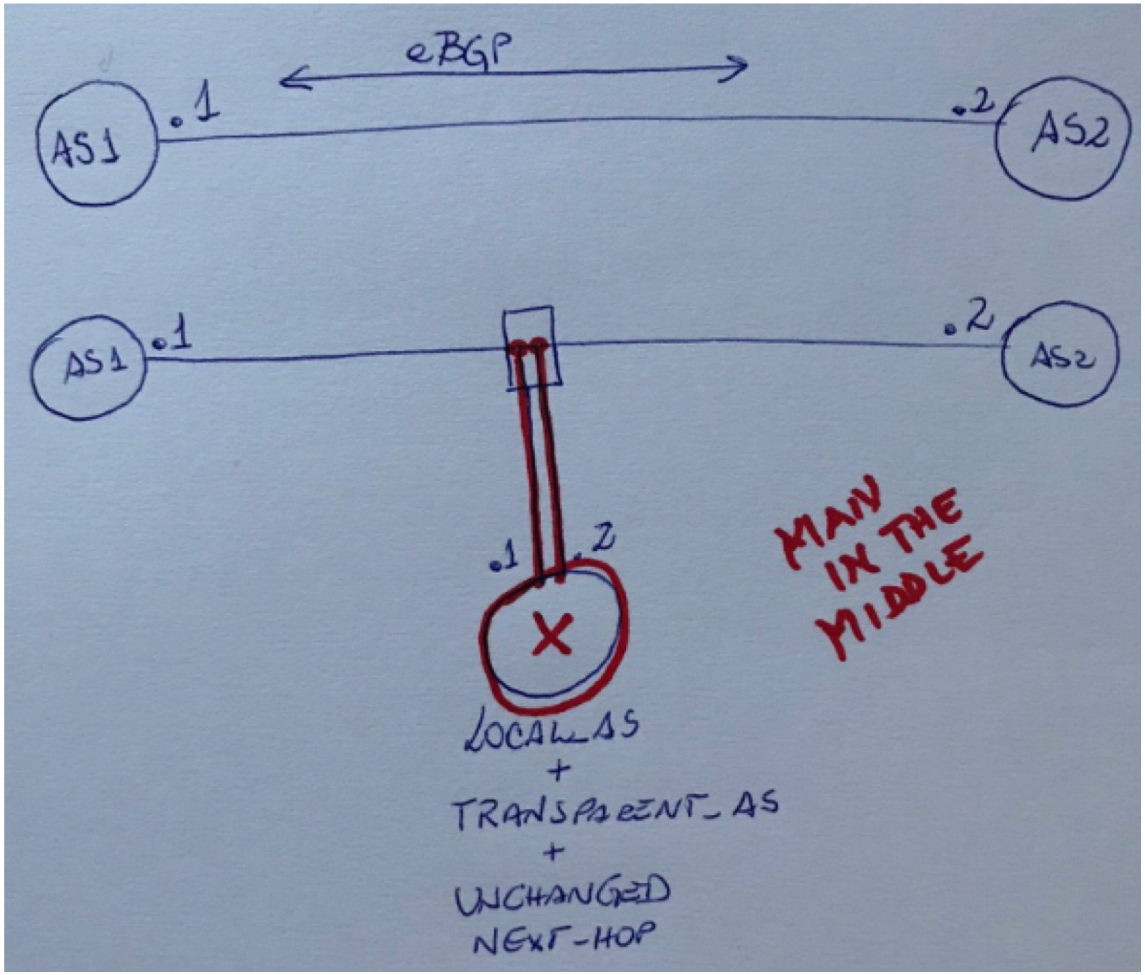
- **Violacao de confidencialidade**
  - Dados do BGP são transportados em texto claro



Ataques conhecidos (práticos)

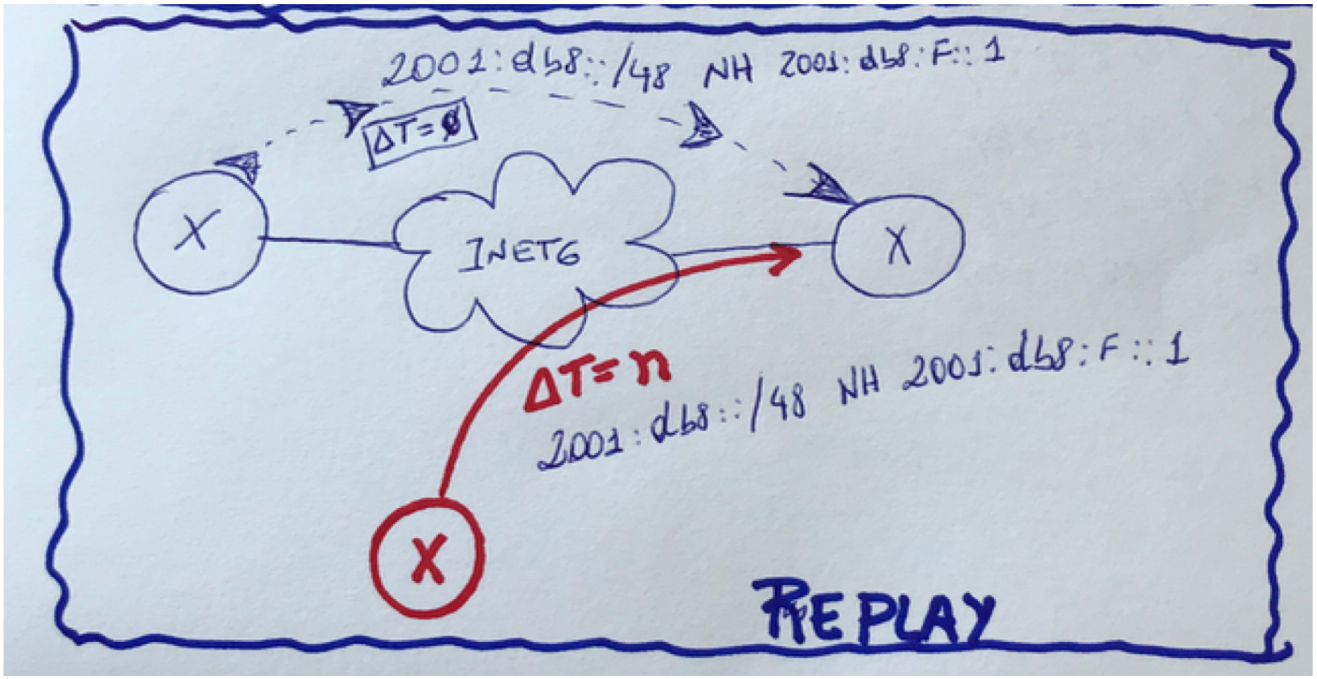
- **Man-in-the-middle**
  - BGP não autentica seus vizinhos
  - Fácil de implementar





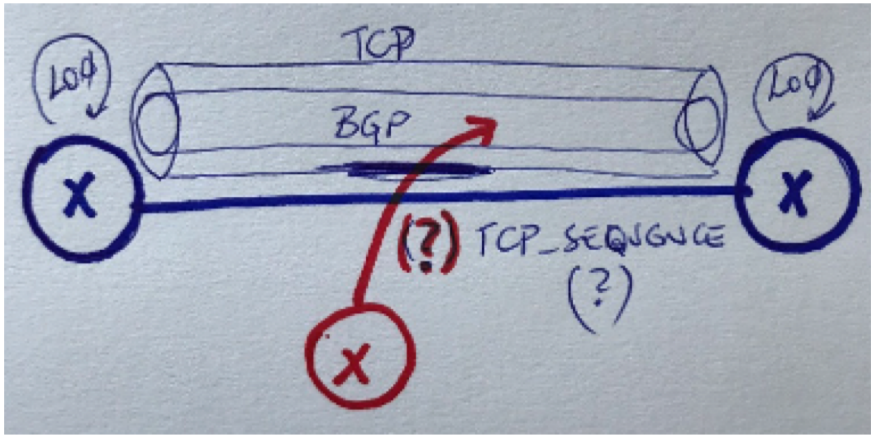
Ataques conhecidos (teóricos)

- **Reprodução de mensagem**
  - O protocolo BGP não tem proteção contra a reprodução de mensagens antigas – **a única proteção é o número de sequencia TCP**



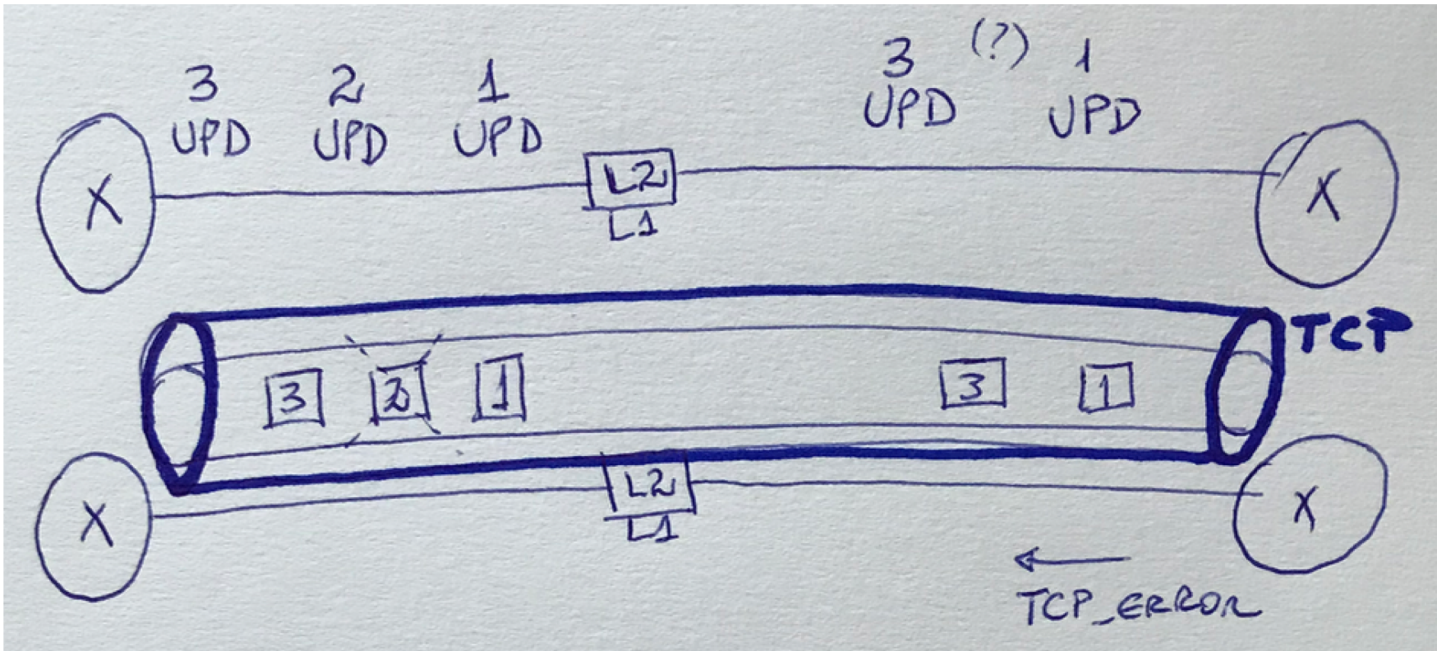
Ataques conhecidos (teóricos)

- **Inserção de mensagem BGP**
  - O BGP não fornece proteção contra inserção de mensagens.
  - Como o BGP usa TCP, para inserir uma mensagens por um estranho é preciso prever o **número de seqüência TCP**.



Ataques conhecidos (teóricos)

- **Exclusão de mensagem**
  - O BGP não fornece proteção contra exclusão de mensagens.
  - O ataque é **difícil** contra uma implementação **TCP madura**

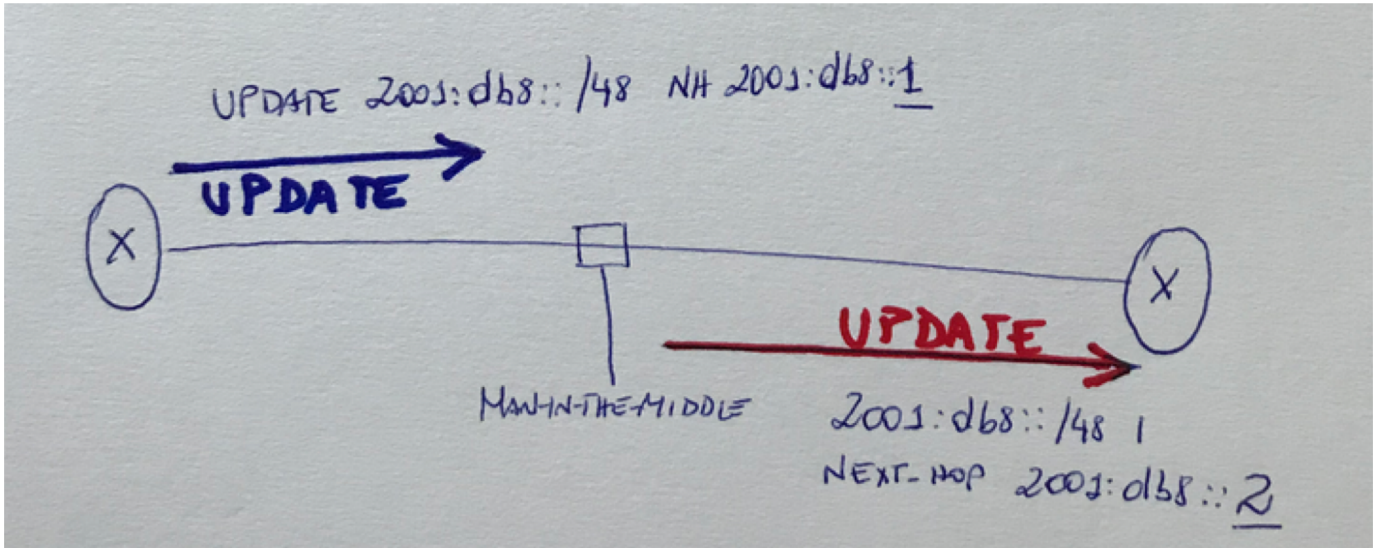


Ataques conhecidos (teóricos)

Transmission Control Protocol (TCP) Header
20-60 bytes

source port number 2 bytes				destination port number 2 bytes
sequence number 4 bytes				
acknowledgement number 4 bytes				
data offset 4 bits	reserved 3 bits		control flags 9 bits	window size 2 bytes
checksum 2 bytes				urgent pointer 2 bytes
optional data 0-40 bytes				

- **Alteração de mensagem**
  - O BGP não fornece proteção contra modificação de mensagens.
  - Uma modificação que estivesse sintaticamente correta e não alterasse o tamanho da carga TCP em geral não seria detectável.
    - Ou que a implementação **TCP ignorasse o Checksum**



ESXi? BGP-EVPN? VXLan?

Linux debian how to disable TCP checksum verification?

0

While trying to open a TCP Port to host B from A, I figure out there's a problem in the 3 way TCP handshake between the two hosts.

Client/Host A send a SYN to host B, Host B send a SYN/ACK, then host A send a RST packet.

I sniffed packets in wireshark, and found that the SYN/ACK packet does not have the same TCP checksum after it has been sent by A and received by B. Otherwise it is the exact same packet. Wireshark mark the packet as "ACKed unseen segment".

I do not have any hops between the two machines. The two hosts are VMs in VMware ESXi hosts . The VMs are in different hosts. They are directly connected in the same VLAN in ESXi. The client VMs is on ESXi v4.1.0. I opened all the firewall for my tests. And finally I totally turned off the TCP checksum offload. I did the same test with a VM that is on the same host, same result. The client

asked 1

viewed 5

BLOG

PRTG NETWO MONIT

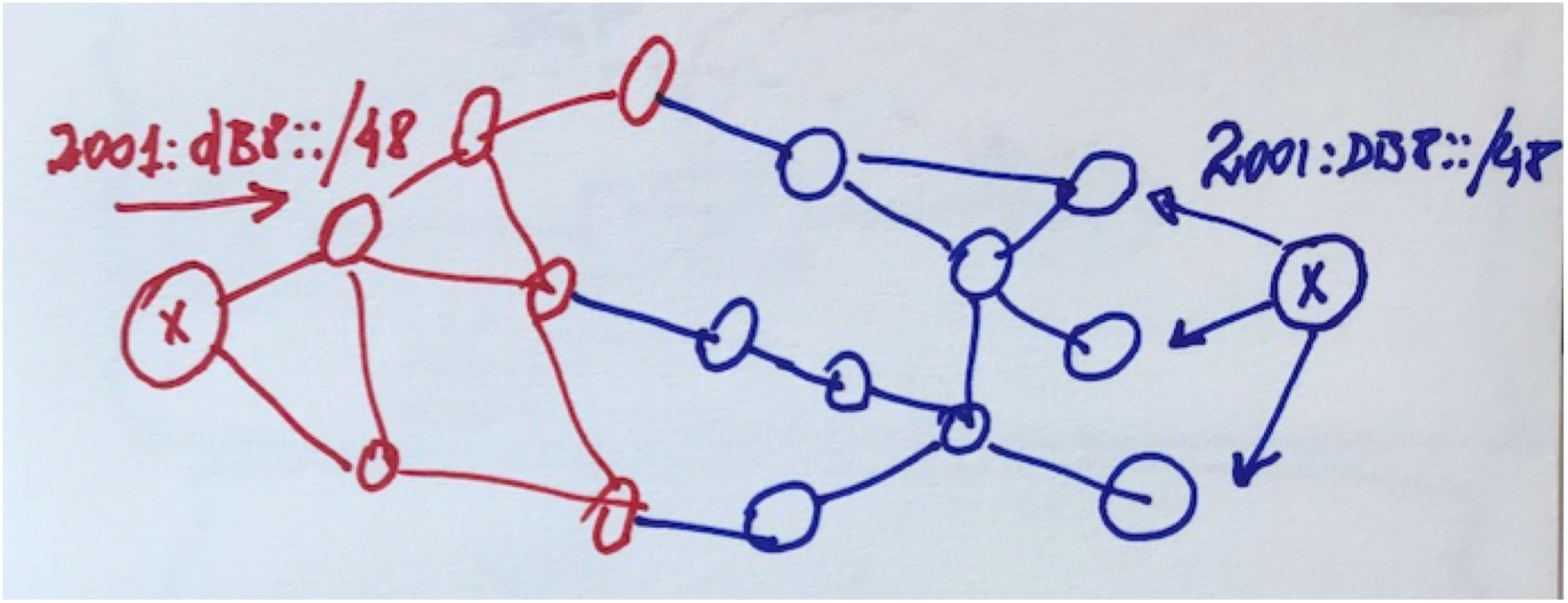
Ataques mais práticos contra a infraestrutura BGP

Man-in-the-middle
Negação de serviço
Sequestro de prefixos

Ataques conhecidos (praticos)

- **Negação de serviço ao protocolo**

  Anuncios BGP falsos podem causar um DoS contra um ASN



Ataques conhecidos (praticos)

- **Negação de serviço ao protocolo**
  - Ataques DoS / DDoS **contra algum IP** de roteadores BGP ou portas de serviço **BGP (179/tcp)** afetam todos o AS
  - Informações falsas no roteamento **IGP** podem representar uma negação de serviço no BGP
  - Excesso de **prefixos** estouram a tabela
    - IPv6: um provedor pode gerar 65k rotas com seu /32
      - O protocolo de roteamento BGP que anuncia um grande número de rotas mais específicas (isto é, prefixos mais longos) pode fazer com que o tráfego BGP e o **tamanho da tabela do roteador aumentem**, até estourar a memoria do equipamento

Ataques conhecidos (praticos)

- Negação de serviço a sessão BGP
  - **Pacotes** direcionados para **a porta TCP 179** são passados para o processo BGP, que geralmente é alocado em **um único processador**, tornando mais lento no roteador
  - Inundar um roteador com pacotes de porta TCP 179 é uma maneira de fazer um DoS para o roteador.
- **Nenhum mecanismo de BGP pode derrotar esses ataques**;
  - Outros mecanismos devem ser empregados
    - **(retirar acesso ao IP/Porta do BGP)**

Ataques conhecidos (práticos)

- **Sequestro de prefixo**
  - Um AS anuncia que **origina um prefixo que na verdade não é dele**.

Ataques conhecidos (práticos)

- **Sequestro de prefixo**
  - Um AS anuncia **um prefixo mais específico** do que aquele que pode ser anunciado pelo verdadeiro AS de origem.

Ataques conhecidos (práticos)

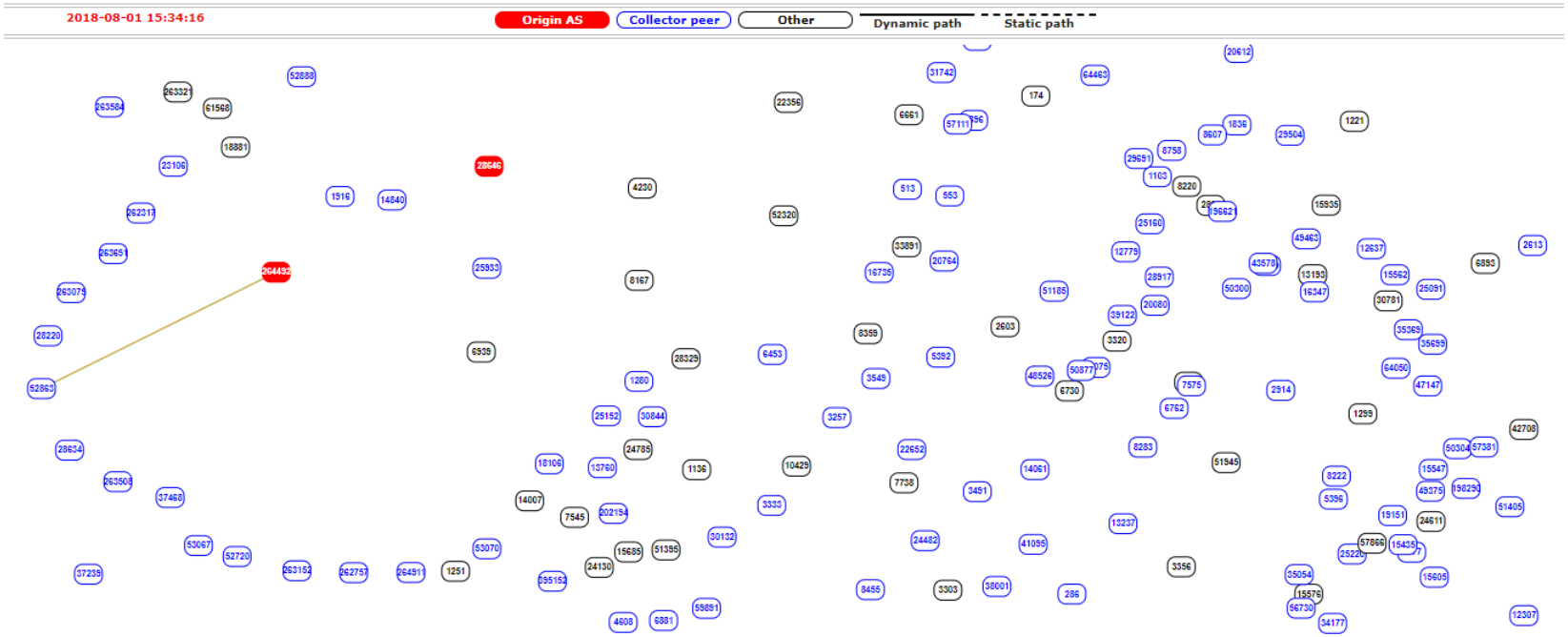
- **Sequestro de prefixo**
  - Um **AS mente que é caminho para o AS alvo** com um **rota mais curta** do que a que já está disponível.

Ataques de Sequestro de Prefixos

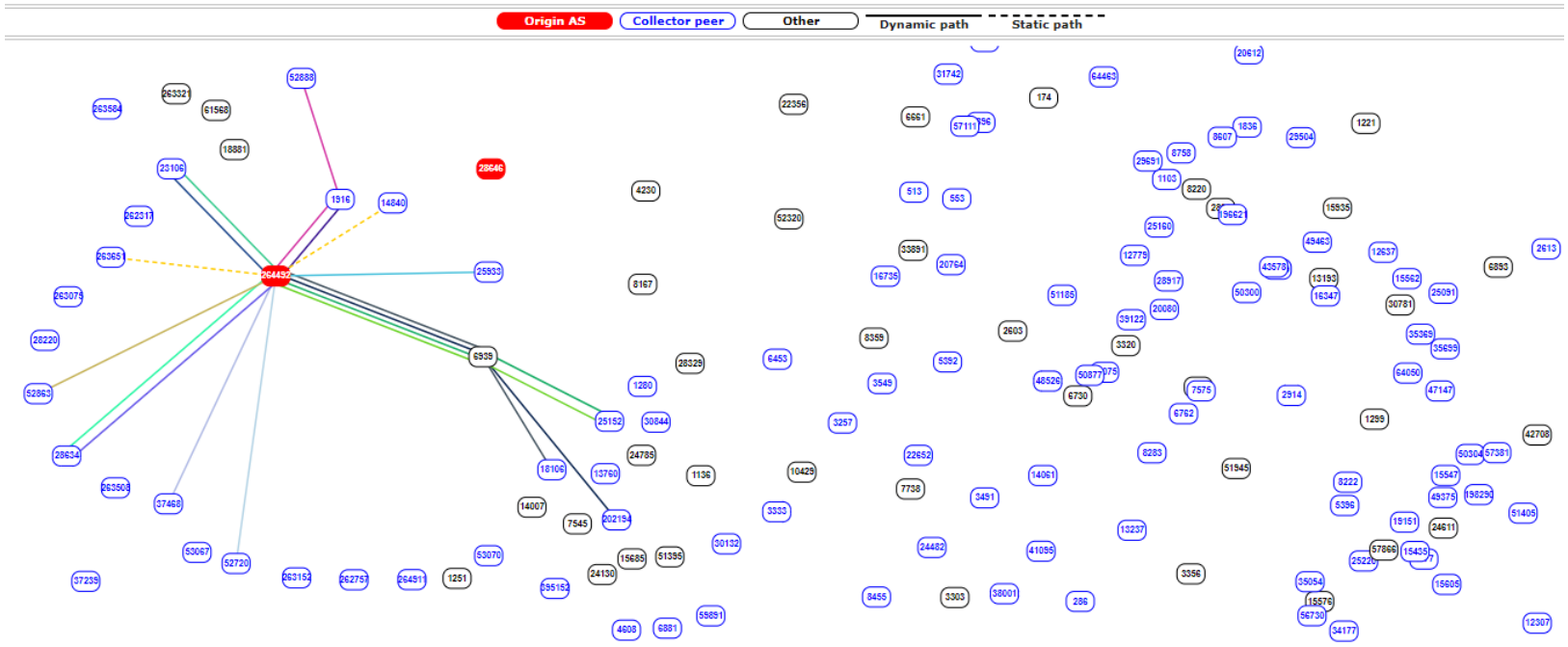
Olhando mais a fundo o problema:

- Exemplo de um dos casos ocorrido no Brasil em 2018

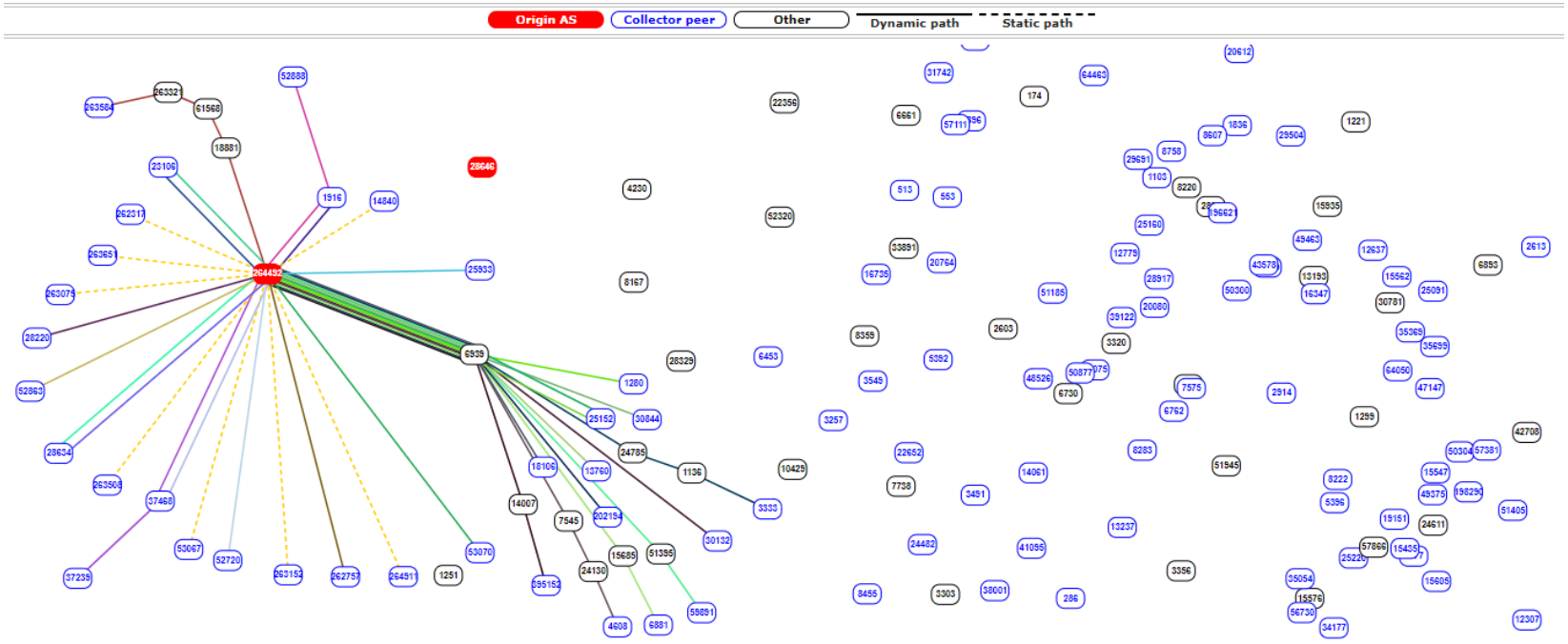
01/08/2018 12:34 – AS-EVIL divulga o bloco no PTT-SP



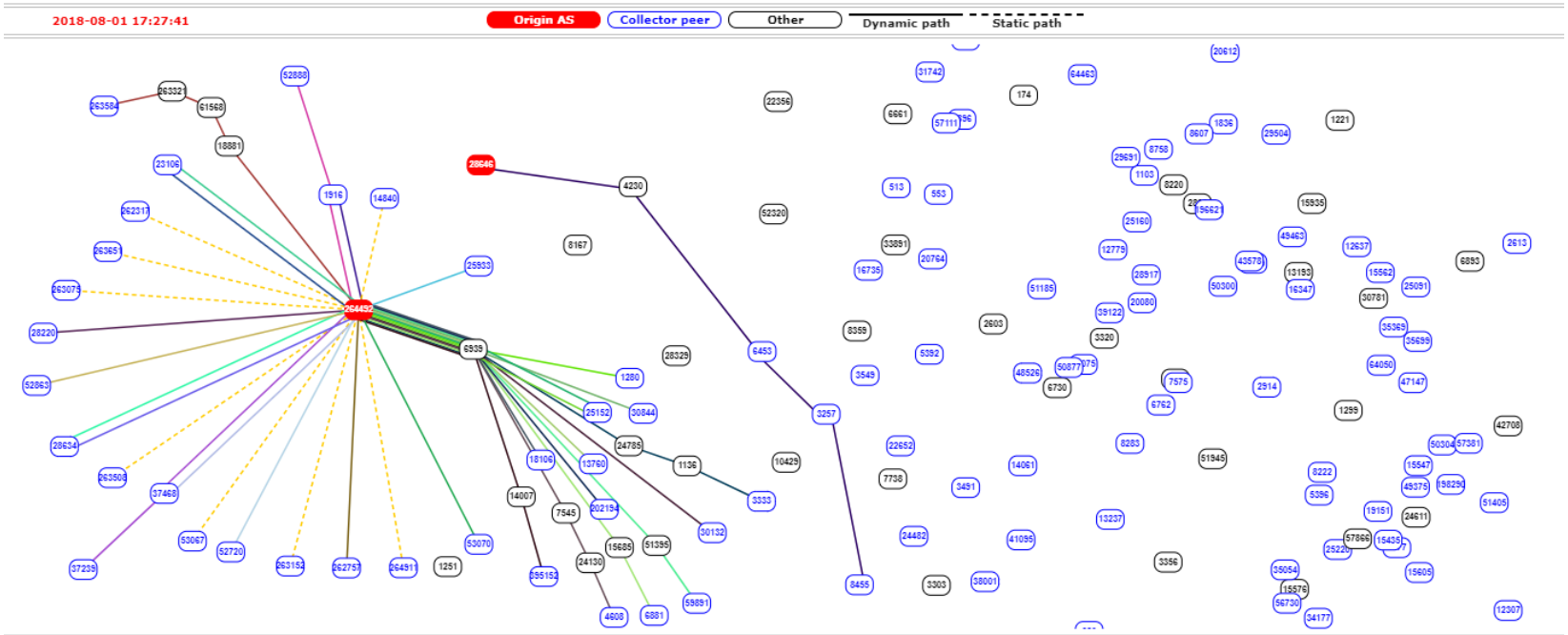
01/08/2018 12:34 – ASN-EVIL divulga o bloco no PTT-SP



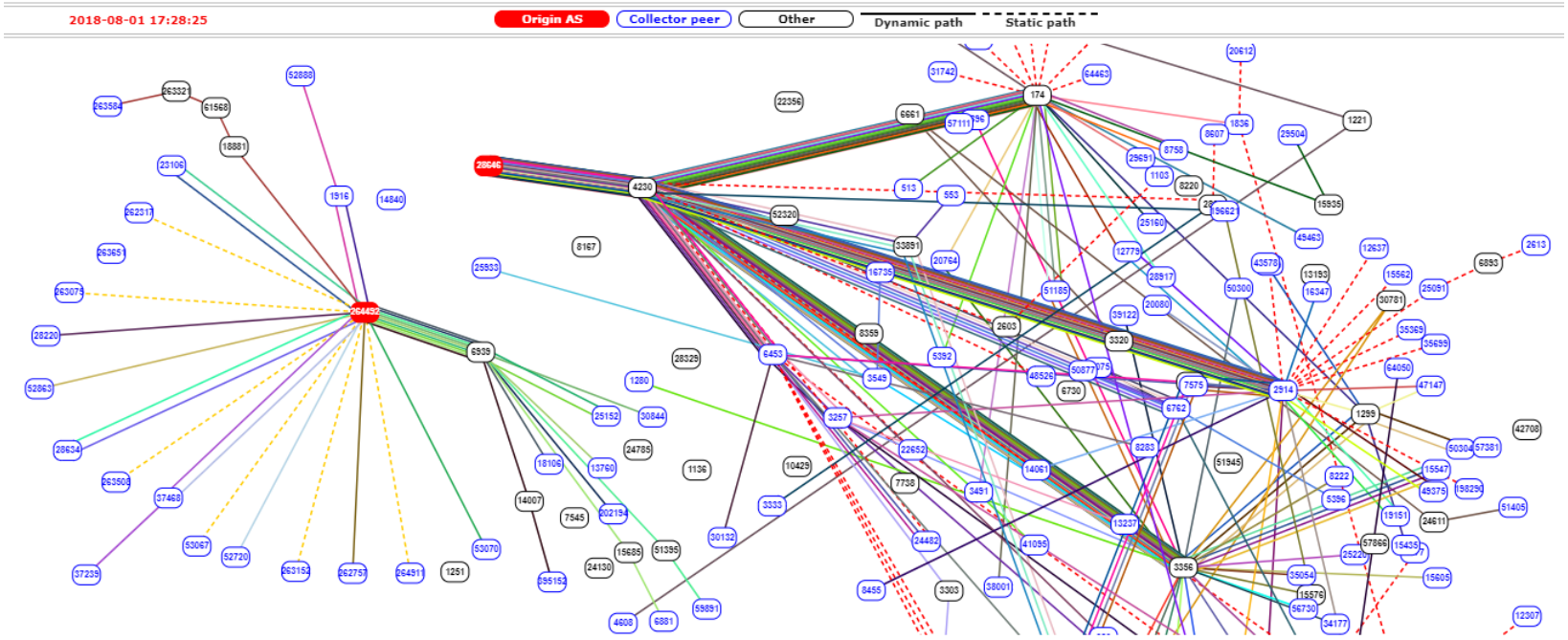
01/08/2018 14:24 – Propagação Hurricane



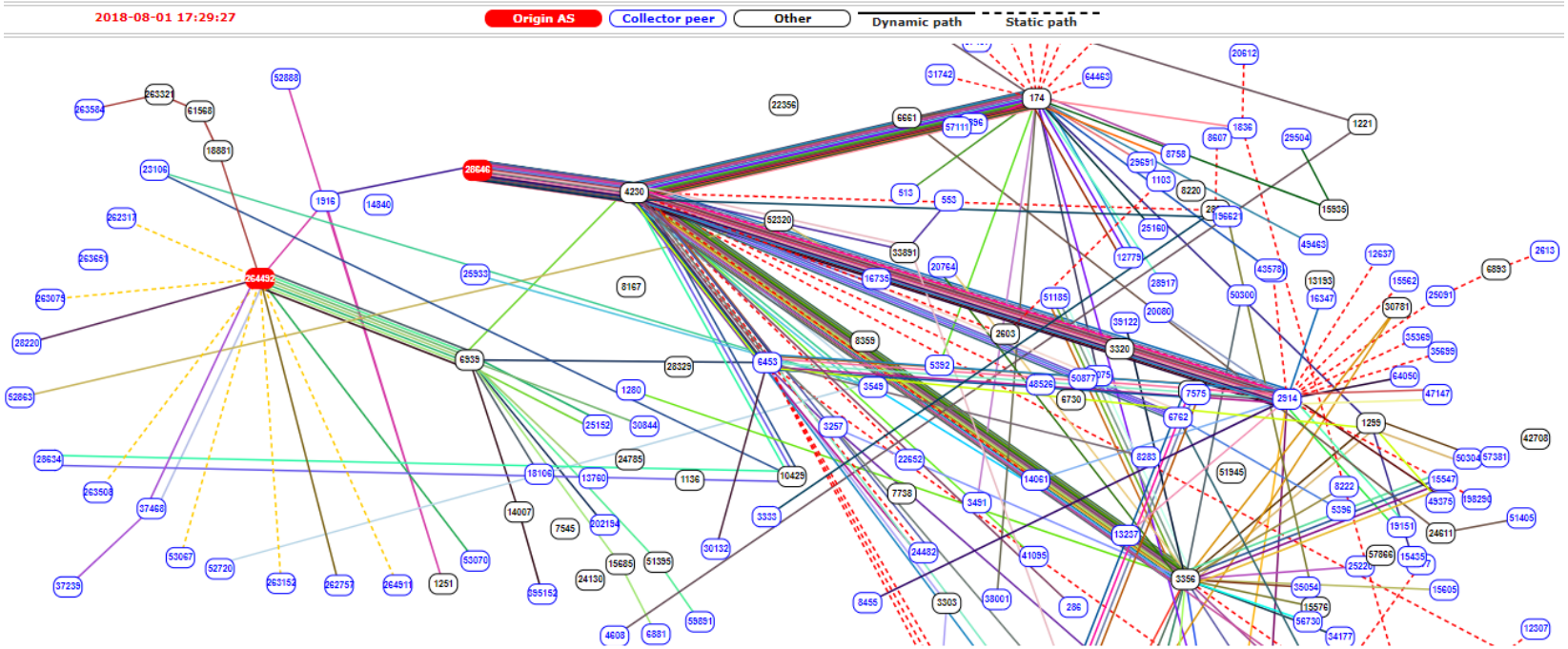
01/08/2018 14:27 – AS-True começa a divulgar bloco mais específico – Embratel Propaga



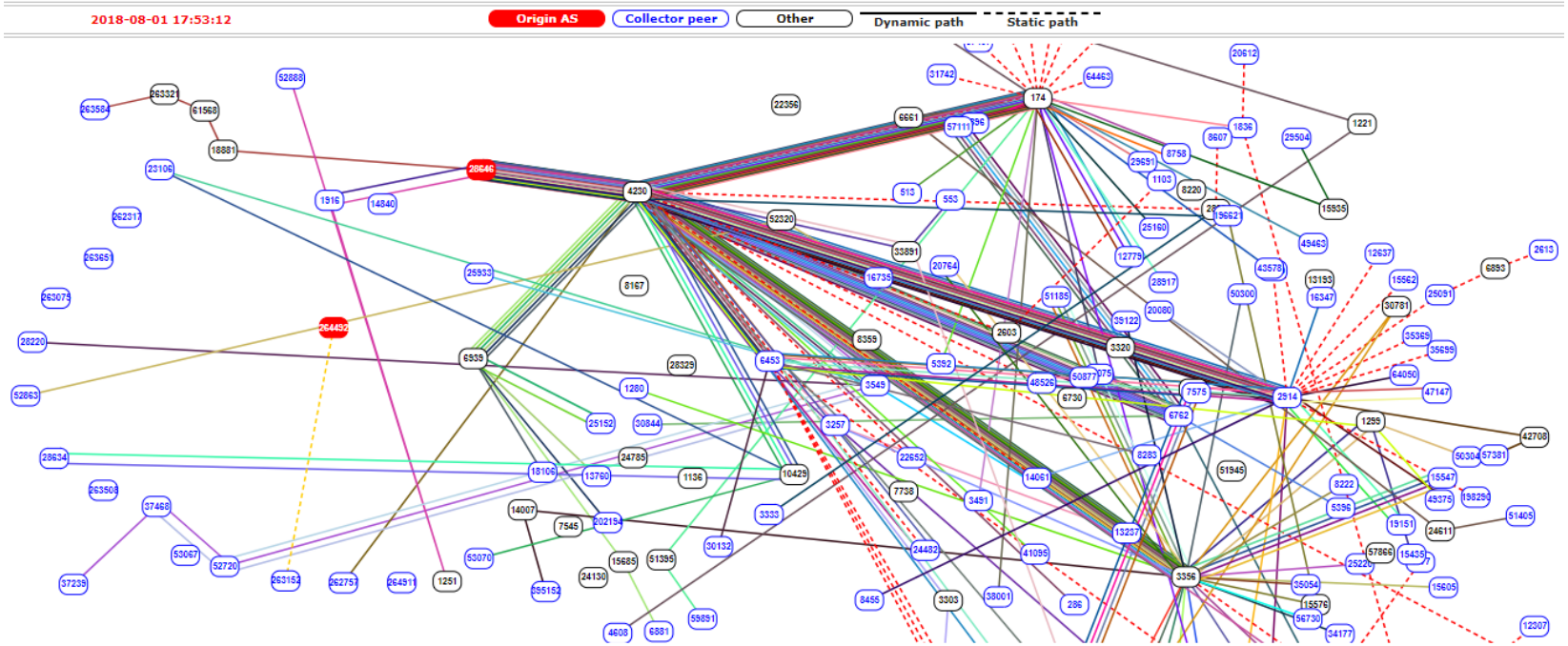
01/08/2018 14:28 – Propagação Embratel



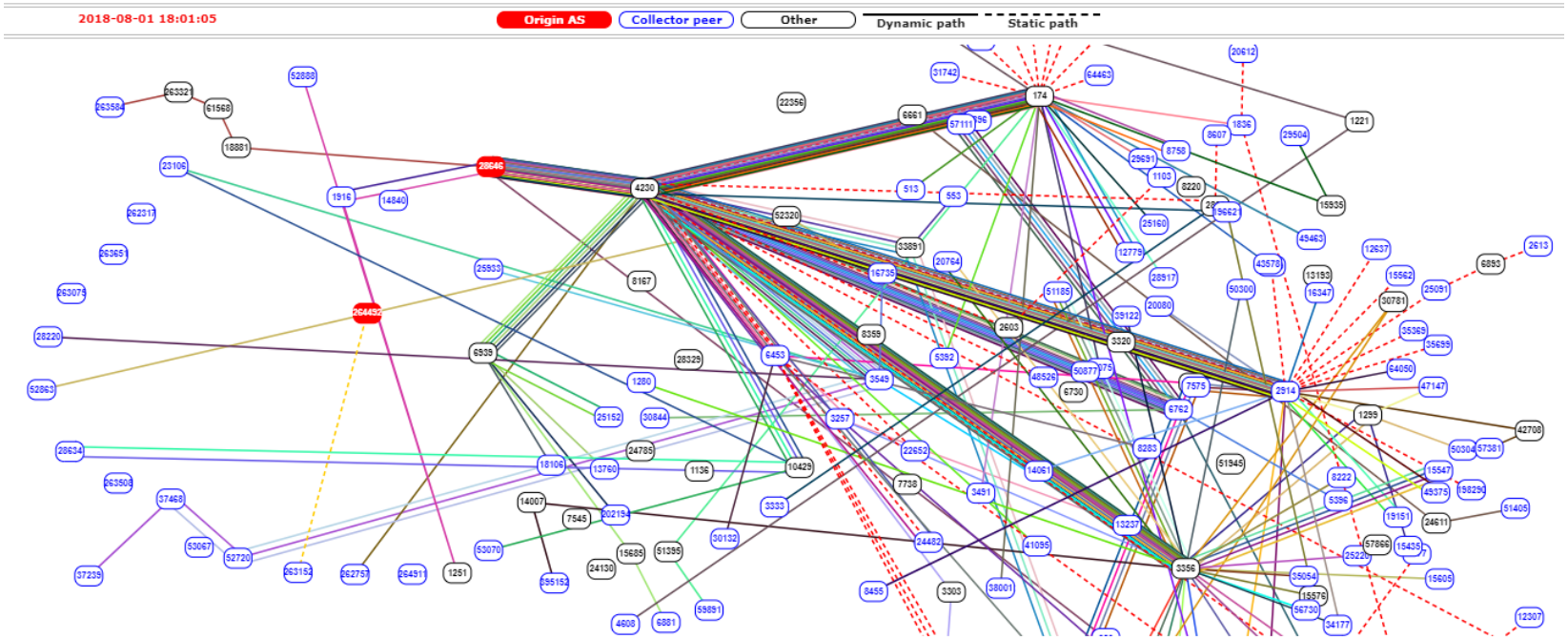
01/08/2018 14:29 – Hurricane converge para Embratel



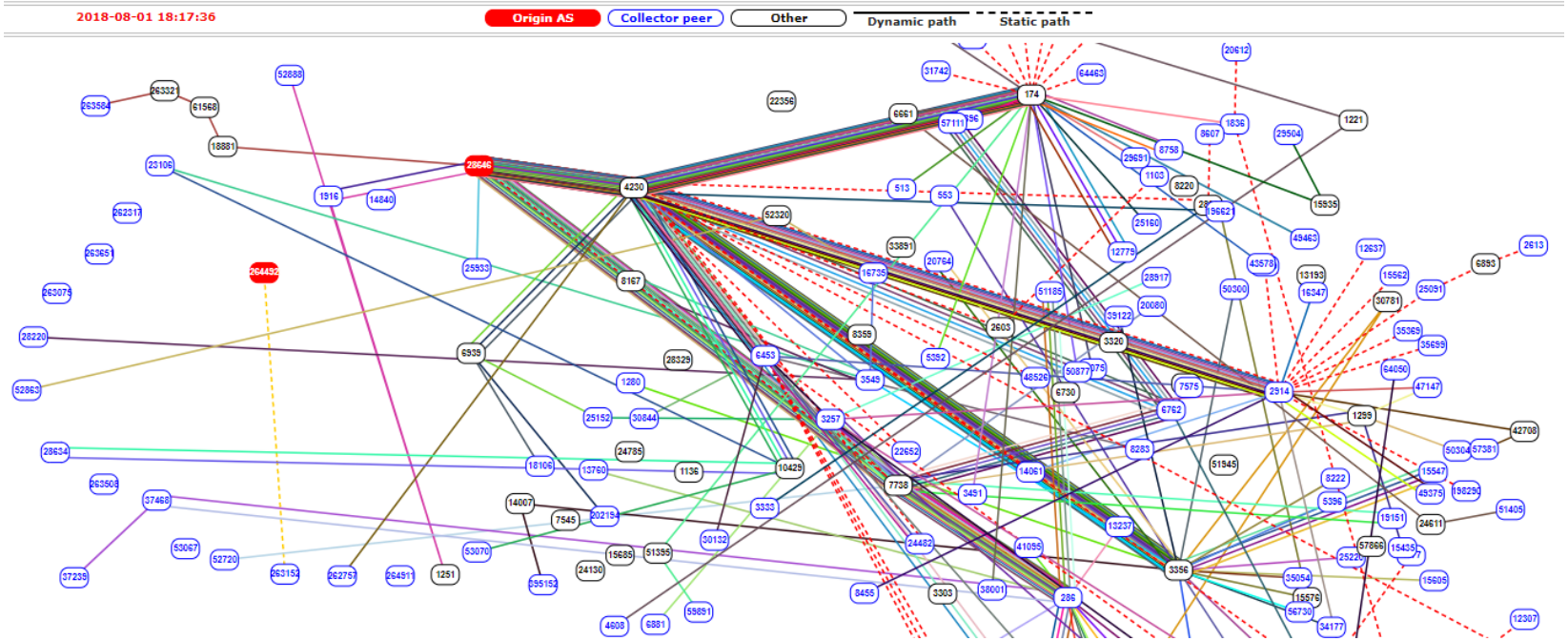
01/08/2018 14:53 – Hurricane converge para Embratel



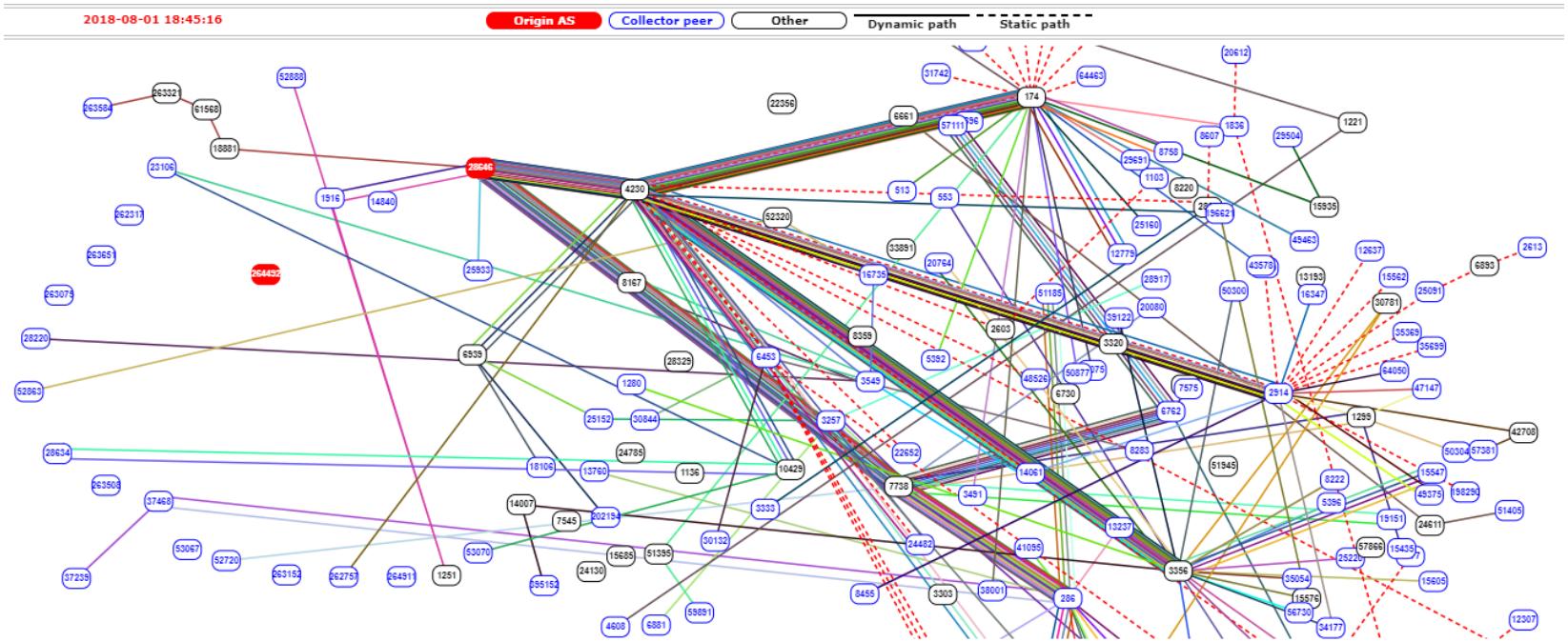
01/08/2018 15:01 – Propagação OI



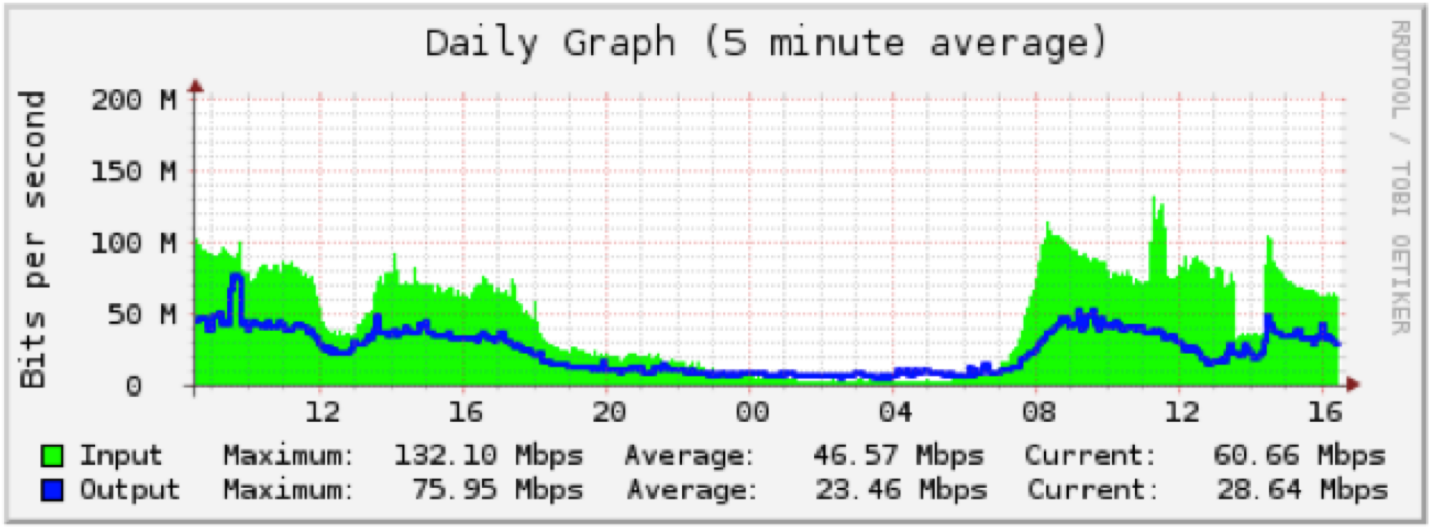
01/08/2018 15:17 – Propagação OI



01/08/2018 15:45 – Convergência total para AS-True



Consequência no Tráfego do AS-True



Mitigação Básica Utilizada

- Anunciar bloco mais especifico possível (/24) para igualar atacante
- Contatar operadora que originou o ataque
- Contatar provedores de trânsito envolvidos no anúncio

Preparação para evitar ataques

- Melhorar a conectividade aos PTTs
  - Diminuir efeitos de convergência
- Anunciar blocos “picados”
  - E como faz para um ipv6?
  - Vai anunciar todos os blocos /48 do /32 ?
    - 65536 anúncios?

Solução a Médio Prazo (BR-2019)

- Validação de prefixos
  - Rpki
  - Whois
  - RaDB
- Outras alternativas
  - Bgpsec

O que é RPKI

- RPKI: Resource Public Key Infrastructure
- RFC 6480 - An Infrastructure to Support Secure Internet Routing
- RPKI É uma solução baseada em assinaturas criptográficas para validar que os prefixos enviados por um AS pertencem a ele ou que está autorizado a fazê-lo.

Como funciona RPKI

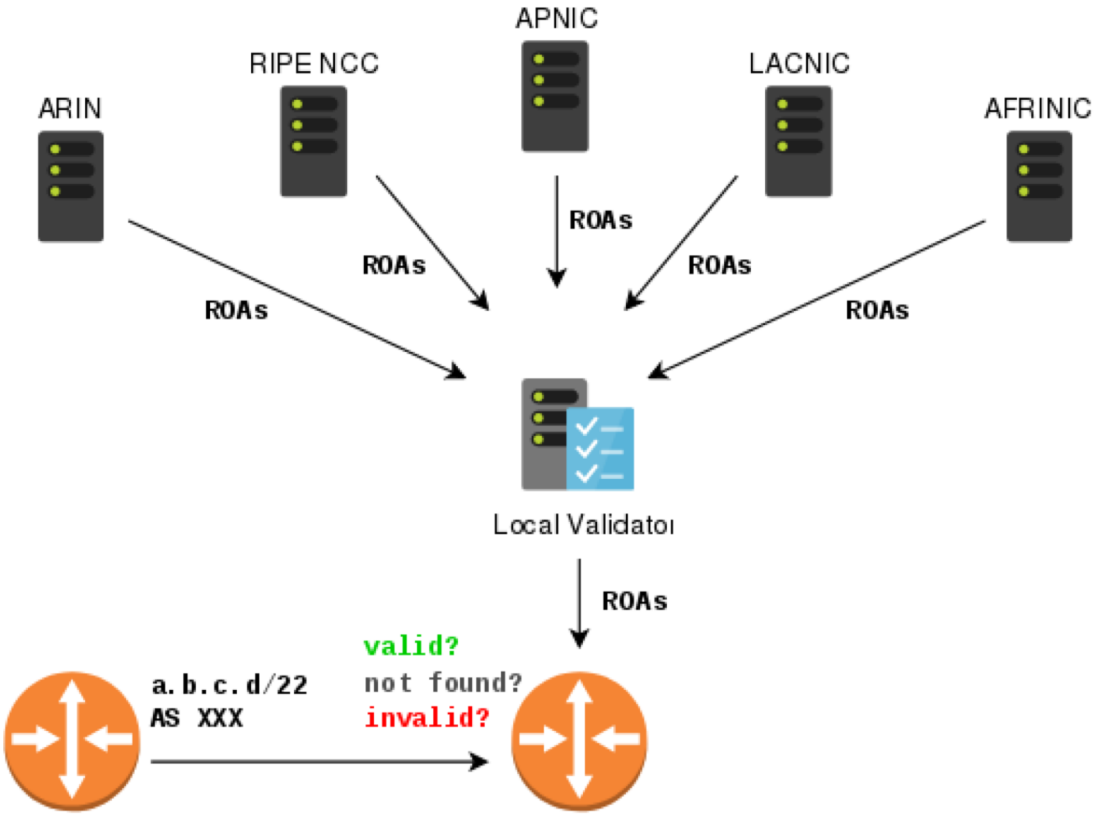
Certificados/Signaturas

- Gerado e assinado pelo RIR
- Emitidos quando os blocos são assinados

ROA - Route Origination Authorizations

- Gerado pelo AS que possui os blocos IP
- Assina que um AS pode ser a origen de um prefixo – inclui a maior e menor mascaras possiveis.

Estrutura RPKI (RFC 6480)



Como Configurar RPKI nos router

```
bgp rpki server tcp a.b.c.d port xxxx refresh 600
!
route-map RPKI permit 10
  match rpki valid
  set local-preference 500
!
route-map RPKI permit 20
  match rpki not-found
  set local-preference 400
!
route-map RPKI permit 30
  match rpki invalid
  set local-preference 300
!
route-map RPKI permit 40
  set local-preference 400
!
```

Obs.: Cisco não envía prefixos inválidos, FRR sim.

Software para RPKI

Softwares de validação:

- https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
- https://github.com/dragonresearch/rpki.net/
- https://github.com/bgpsecurity/rpstir

Estatísticas: https://rpki-monitor.antd.nist.gov/

Validador online: http://localcert.ripe.net:8088/

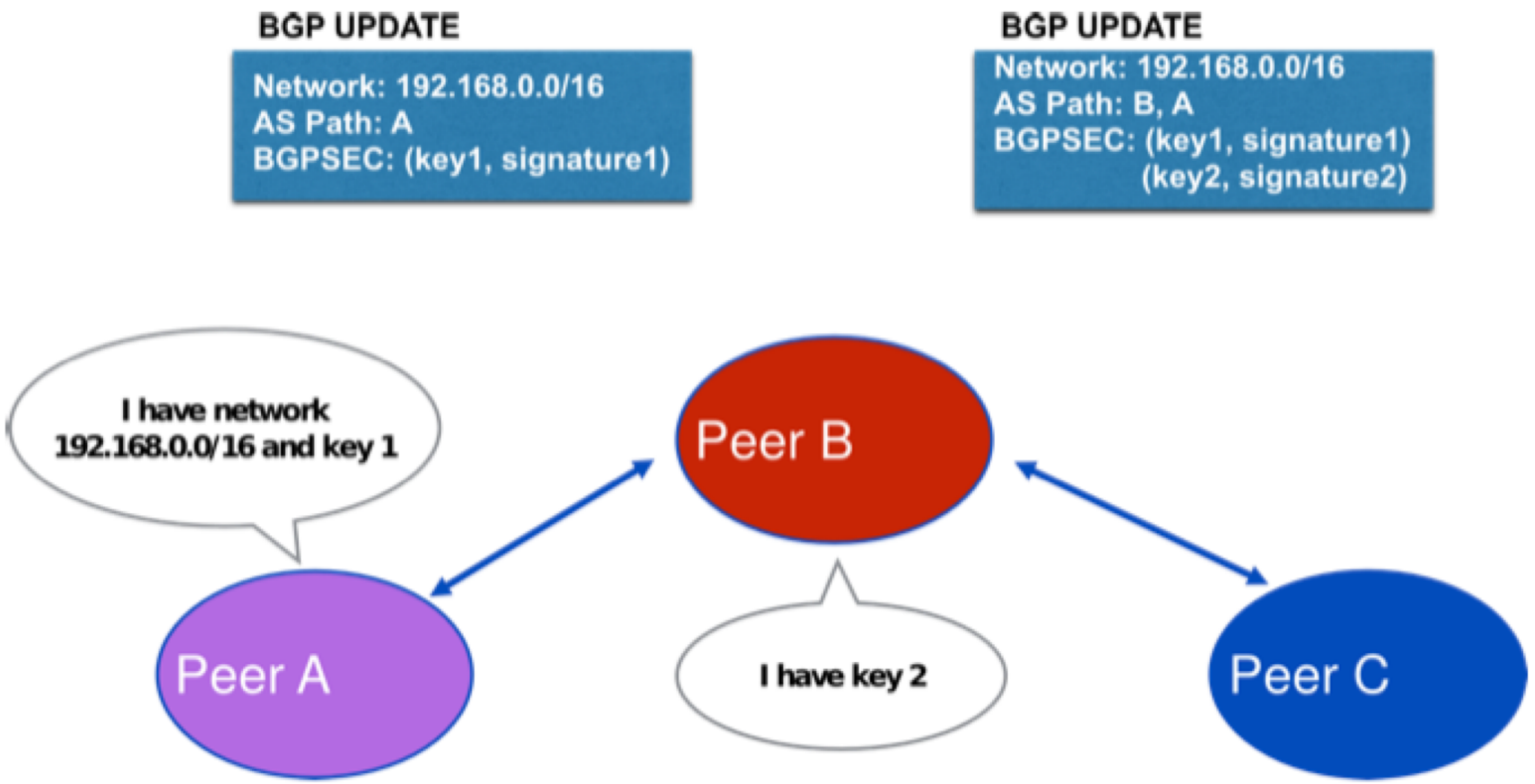
RPKI

- RPKI é útil para validação da origem ou autorização de anuncio
- Porém não protege contra **spoofing do AS_PATH** de origem ou modificações não autorizadas no caminho!
  - Ataques de Next-AS
    - roteamento incorreto terminando em origens válidas

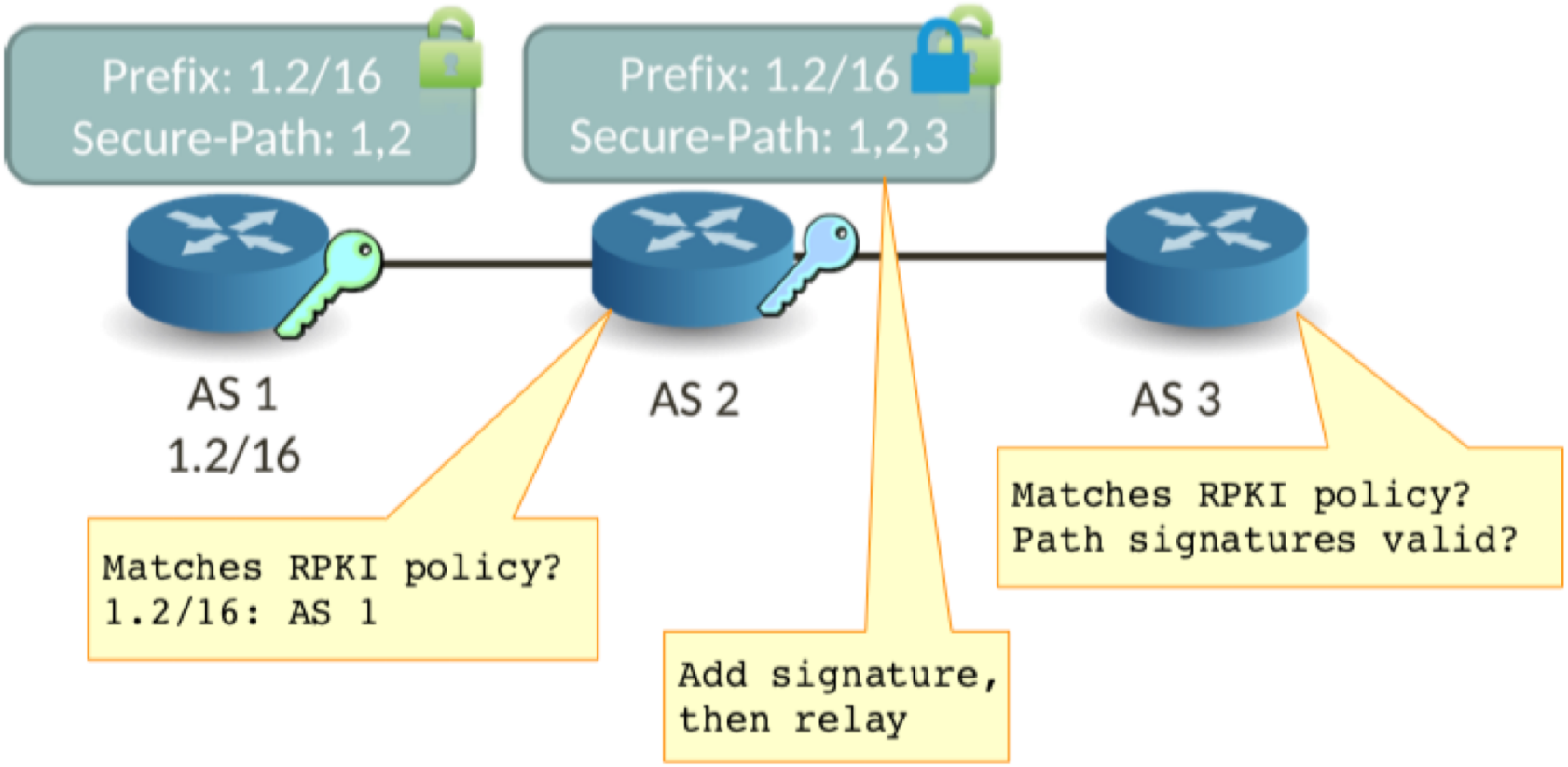
BGPSec

- Novo atributo, opcional, não transitivo, que leva a assinatura digital de cada AS
- Atributos negociados entre roteadores
- Possibilidade de implementação incremental
- Desafio de implementação e operação
- Assinatura e validação de prefixos em tempo real

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



BGPSEC + RPKI (Fonte: Jumpstarting, Avichai, SIGCOMM)



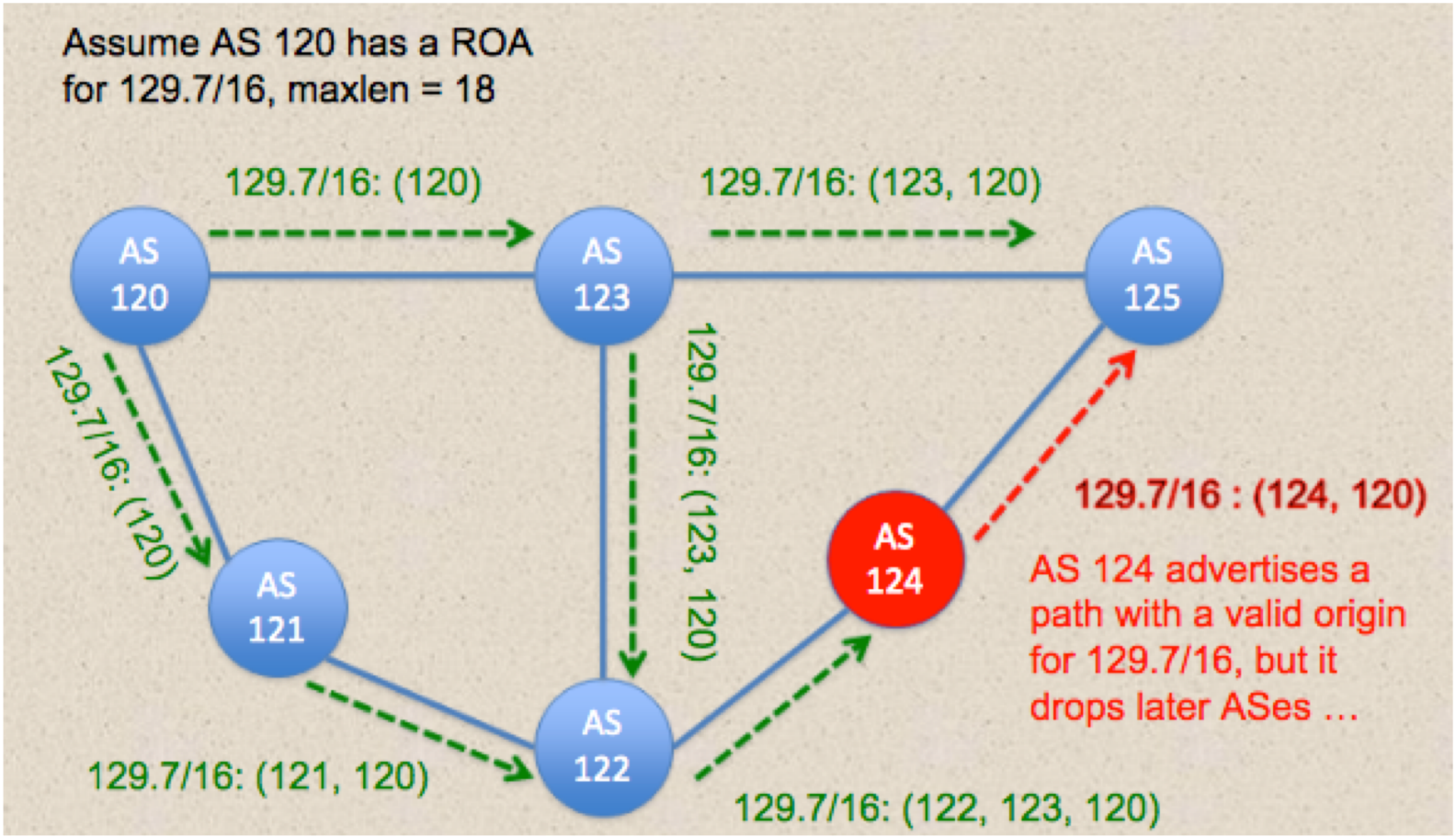
Ameaças ao BGP Path

- Alvo dos ataques
  - Escutas entre pares BGP (man-in-the-middle)
  - Ataque em um roteador BGP
  - Ataque a infra de validação
    - Nos computadores que administram o PSI
    - Ataque nos repositorios de Chaves
    - Ataques no RPKI CA

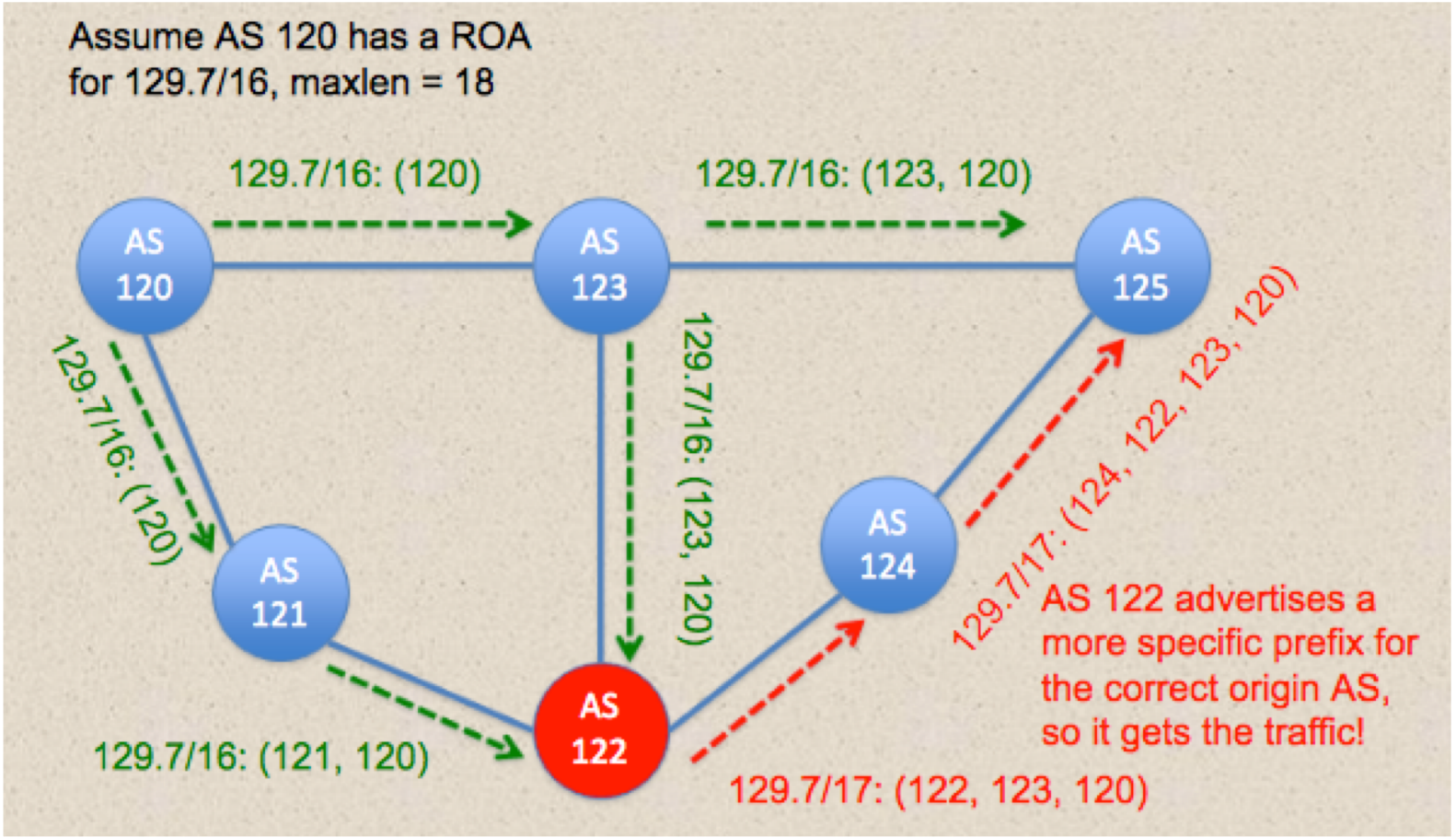
Ameaças ao BGP Path

- Origem valida, caminho falsificado
  - ROA detecta e rejeita uma rota não autorizada pelo ASN, mas no previne um path falsificado carregando uma origem válida
- Prefixos mais específicos falsificando o PATH
  - Um ASN da rota ainda pode forjar um prefixo mais específico. O ROA não resolve, a menos que o tamanho máximo seja exatamente o mesmo que o tamanho do prefixo.

Origem valida PATH falsificado



Prefixos mais específicos falsificando o AS_PATH



Exemplos de ataque ao AS_PATH

- Remoção de ASN
  - Remover um ou vários ASNs do AS_PATH torna o caminho mais curto e preferivel.
- Replay de uma mensagem de UPDATE
  - Uma autenticação de um AS_PATH válida no passado pode ser (re)utilizada no futuro
- Ataque de Man-In-The-Middle (MITM)
  - Uma rota falsificada atrai o tráfego de determinados ASNs e depois encaminha corretamente ao destino (permitindo a inspeção do tráfego)

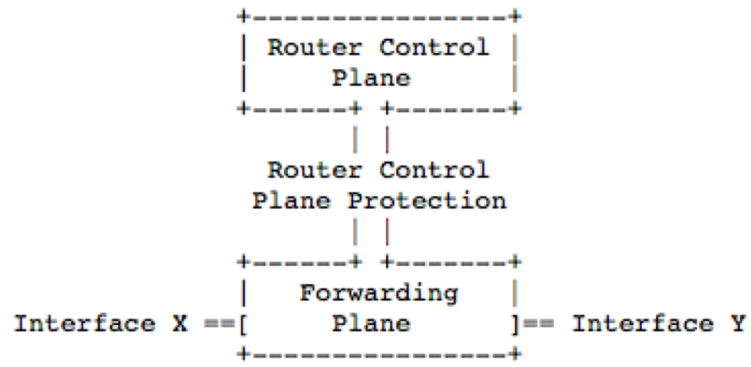
Comentários do BGPSec

- Muito difícil de operacionalizar
- Dificil de escalar com os equipamentos atuais
- Não é uma solução definitiva – não resolve todos os problemas

Defesas contra exploits BGP

Proteção do processo BGP

- Lista de controle de acesso para descartar todos os pacotes endereçados à porta TCP 179 no roteador
- ACL específica para o plano de controle do roteador
  - Se o hardware não pode fazer isso, as ACLs de interface podem ser usadas para bloquear pacotes direcionados ao roteador local.
  - Limitação de taxa de transmissao
- **RFC6192-Protect Control Plane**

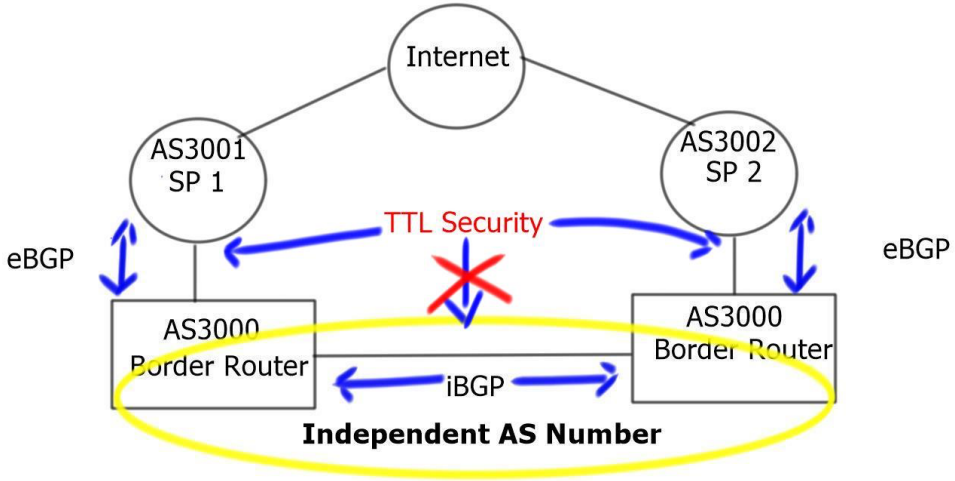


Proteção das sessões TCP do BGP

- Ataque com pacotes TCP RST falsificados
- Ataque falsificado ARP
- MD5 pode ser uma opção (obsoleta)
  - Prefiro a opção de autenticação **TCP (TCP-AO) - RFC 5925. Use-o!**
  - Prefiro IPSec para sessões IPv6
- Bloquear pacotes forjados em todas as arestas da sua rede (**RFC 2827 e RFC 3704) - ataque contra o iBGP**

Proteção das sessões TCP do BGP

- Sessões de BGP podem ser mais difíceis de falsificar com a **Segurança TTL** (**RFC 5082**)



- Como a proteção MD5, a segurança TTL deve ser configurada em ambos os peers BGP

Use Filtros!

- O principal aspecto de garantir o BGP é controlar os prefixos que são recebidos e anunciados em peerings do BGP
- **BOGUS** List (prefixos falsos) :
  - O registro de endereços de propósito especial IANA IPv4 / 6
  - Filtros de prefixo não atribuídos pela IANA (ipv6)
  - Filtros de prefixo atribuídos pelo RIR para o AS (meus IPs)
- Prefixos LAN **IXP**
  - Segurança da LAN (correspondência exata)
  - PMTUD e o problema uRPF ”loose"
- Filtros com **peers** da Internet
  - Filtragem recebida (solta ou estrita)
  - Filtragem de saída
- Filtros com **clientes**
- Filtros com **provedores** de upstream

Opção de filtro de ENTRADA
Prefixos que não são roteados globalmente
Prefixos não atribuidos pelo IANA (só IPv6)
Prefixos com máscara muito específica
Prefixos do AS local
Prefixos da LAN do IXP
Rota default não é esperada no full-routing

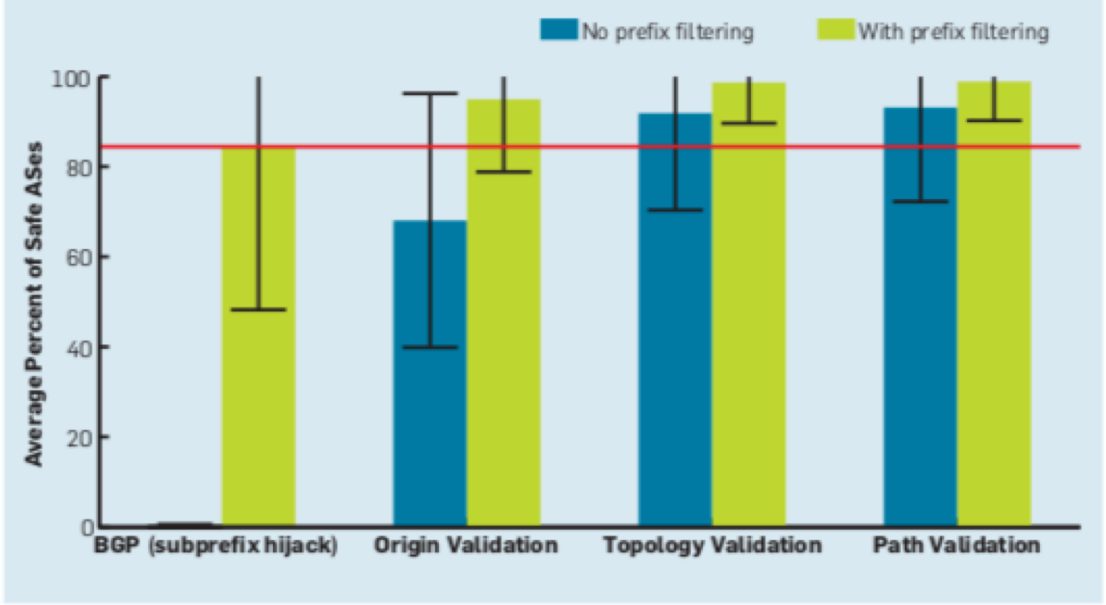
Opção de filtro de SAIDA
Prefixos roteados globalmente
Prefixos mais específicos
Prefixos da LAN do IXP
Nunca anunciar rota default

Valide a origem !!!

- Validação de origem com AS-SET (por exemplo, **RADb**)
- **SIDR: roteamento seguro entre domínios**
  - Validação de origem (RFC6811) com RPKI
  - Validação de rota fornecida pelo BGPsec (RFC7132)
- Prefixos que são muito específicos
- Prefixos de filtragem que pertencem ao AS local e aos Downstreams

Mecanismos de defesa e seus resultados

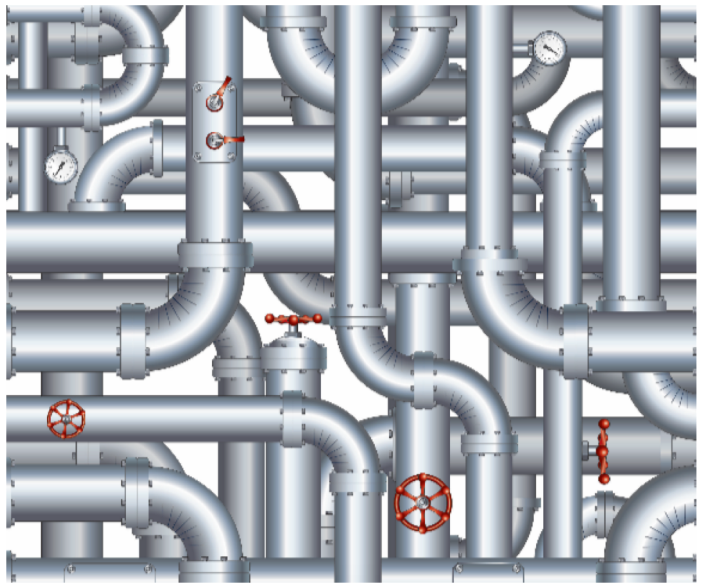
Figure 2. Comparing defenses. The average percentage of safe ASes during naive attack with a randomly chosen (attacker, victim) pair; error bars represent one standard deviation; and the horizontal line represents the effect of prefix filtering.



Rethinking Security for Internet Routing BY ROBERT LYCHEV, MICHAEL SCHAPIRA, AND SHARON GOLDBERG
COMMUNICATIONS OF THE ACM | OCTOBER 2016

Conclusões

- Não há uma solução definitiva
  - RPKI ajuda mas não resolve
  - BGPSec ajuda mas não resolve
- O que fazer?
  - Faça sua parte
    - filtros para validação de AS e caminos
    - Whois correto
    - RADB e políticas definidas
    - RPKI



- Sim, você precisa fazer a sua parte