Mitigação de Ataques ao BGP utilizando RPKI

Yuri de Abreu de Melo[1], **Ronaldo Moreira Salles**[1], **Frederico Sauer G. Oliveira**[2]

[1]Seção de Engenharia de Computação - Instituto Militar de Engenharia (IME)
Praça General Tibúrcio, 80 – Brasil - RJ – CEP: 22290-270

[2]Fundação Centro Universitário Estadual da Zona Oeste (UEZO)
Av. Manuel Caldeira de Alvarenga, 1203 - Campo Grande - RJ – CEP: 23070-200

{abreumelo,salles}@ime.eb.br, fredsauer@uezo.edu.br

Abstract. *BGP plays a key role in the WAN routing environment. However, it has vulnerabilities that were not addressed in its creation. Modifications to the BGP have been proposed over the years but have not been adopted. This article describes a research where a typical BGP routing environment is attacked and, after implementing mitigation strategies (RPKI), it is successfully secured. Other modalities of more intensive attacks will continue this research work.*

Resumo. *O BGP tem um papel fundamental no ambiente de roteamento WAN. Possui, entretanto, vulnerabilidades que não foram tratadas na sua criação. Modificações ao BGP foram propostas ao longo dos anos, mas não foram adotadas. Este artigo descreve uma pesquisa onde um ambiente de roteamento BGP típico é atacado e, após a implementação de estratégias mitigatórias (RPKI), é protegido com sucesso. Outras modalidades de ataques mais intensivos darão continuidade a este trabalho de pesquisa.*

1. Introdução

A internet é composta pela interconexão de milhares de *Autonomous Systems* (ASes), que usam o *Border Gateway Protocol* (BGP) para a troca de informações de roteamento e transmissão de tráfego [Mitseva et al. 2018].

O BGP está presente desde o início da internet, sendo a sua versão atual o BGP-4 [Rekhter et al. 2006]. Sua simplicidade e resiliência garantiram um papel duradouro. Os ASes o utilizam para anunciar blocos de prefixos IP e assim estabelecer rotas entre diferentes domínios. Os seus principais problemas são [Murphy 2006]:

- Devido a seu sistema de confiança mútuo, sem a apresentação de credenciais, há oportunidades de ataques, tornando-o vulnerável à inserção de informações maliciosas;
- Não há um mecanismo para validar a legitimidade de um AS em anúncios de *Network Layer Reachability Information* (NLRI). No BGP-4 [Rekhter et al. 2006] não é requisito que um roteador vizinho verifique a autenticidade das mensagens de atualização anunciadas pelo seu par; e
- Não há um mecanismo para assegurar a autenticidade dos atributos de caminho anunciados por um AS. Assim, um roteador BGP malicioso pode anunciar rotas com um *as-path* diferente da informação NLRI a ele associado, induzindo-o à escolha e instalação de rotas falsas.

2. Contextualização e Motivação

Falhas do BGP podem causar grandes danos, e até interromper todo o tráfego global. Ataques como *hijacking* (sequestro) de prefixos BGP possibilitam que agentes maliciosos interceptem ou redirecionem o tráfego da internet. Para isso, estes agentes atribuem para si a propriedade de um grupo de endereços e se utilizam do anúncio falso de prefixos IP para redirecionar o tráfego para onde desejem [Cho et al. 2019]. Há informações confiáveis [Moll 2020] de que o sequestro de prefixos BGP ameaça empresas em todo o mundo. Somente no ano de 2020 teriam sido identificados mais de 1430 incidentes, fora os não reportados ou ataques malsucedidos.

3. Análise do Estado da Arte

Ainda que vários trabalhos tenham proposto formas de tornar o BGP mais seguro, nenhum foi adotado de fato. As propostas mais promissoras são baseadas em criptografia assimétrica, devido à inviabilidade das trocas de chaves secretas entre pares de roteadores em um sistema global. Neste contexto, pode-se elencar soluções como o *secure-bgp*, *secure origin bgp* e o *pretty secure bgp*, como ilustrado na figura 1. Estas propostas introduzem o uso de *Public Key Infrastructure* (PKI) para atribuição e distribuição de chaves públicas [Mitseva et al. 2018].

Properties	Approach															
	Route filtering	IRR	Use of DNS	IRV	RPKI	RPKI enhanced	S-BGP	soBGP	psBGP	BGPsec	S-BGP enhanced	SPV	SMPC-based routing	Blockchain-based routing	Listen & Whisper	Use of traceroute
Security																
Control-/ Data-plane	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / □	■ / ■	□ / ■
Attacks Covered:																
Prefix / Subprefix hijack	▨ / ▨	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	■ / ■	□ / □
AS path forgery	▨	■	□	■	□	▨	■	■	▨	■	■	▨	■	■	□	□
Interception attack	▨	■	□	■	□	▨	■	■	▨	■	■	▨	■	■	▨	□
Replay/Suppression attack	□	□	□	□	□	□	□	□	□	▨	□	□	■	■	□	□
Collusion attack	□	□	□	□	□	□	□	□	□	▨	□	□	□	□	□	□
MED modification	□	□	□	■	□	□	■	■	□	□	□	□	■	□	□	□
Exploit RFD/MRAI timer	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Denial of service	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Route leak	▨	■	□	■	□	□	□	□	□	▨	□	□	■	■	□	□
Performance																
Convergence delay	□	□	□	■	□	□	■	■	■	■	■	▨	■	■	▨	■
Stability	■	■	■	▨	■	■	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Scalability	▨	▨	▨	□	▨	▨	□	□	□	□	□	▨	□	□	□	□
Computational overhead	□	□	□	▨	□	□	■	■	■	■	▨	▨	■	■	■	■
Bandwidth overhead	□	□	□	■	□	□	■	■	■	■	▨	▨	■	■	■	■
Storage overhead	■	■	■	■	■	■	■	■	■	■	■	▨	□	■	■	■
Privacy																
Routing privacy	▨	□	□	▨	▨	▨	▨	□	▨	▨	▨	▨	■	■	▨	□
Deployability																
Deployability	■	■	■	□	■	■	■	■	■	■	■	■	□	□	■	■
Adoptability	▨	▨	□	□	▨	▨	□	□	□	□	□	□	□	□	□	□
Status																
Adopted / Standardized	▨ / □	▨ / □	□ / □	□ / □	▨ / ■	□ / □	□ / □	□ / ▨	□ / □	□ / ▨	□ / □	□ / □	□ / □	□ / □	□ / □	▨ / □
Academic paper only	□	□	■	■	□	■	■	■	■	□	■	■	■	■	■	▨

Notion: ■ has feature, ▨ partially has feature, □ does not have feature.

Figura 1. Propriedades desejadas e abordagens existentes [Mitseva et al. 2018].

Observa-se que a maioria das soluções propostas permaneceram no campo acadêmico. Já a infraestrutura RPKI (Resource PKI) tem *status* de padronizada pelo IETF para adoção, e por isso foi adotada nessa pesquisa em andamento.

4. A infraestrutura RPKI

A infraestrutura RPKI (*Resource Public Key Infrastructure*) é uma especificação proposta pelo IETF (*Internet Engineering Task Force*) na RFC 6480 [Lepinski and Kent 2012], que permite a vinculação de blocos de endereços IP às chaves públicas de seus proprietários

[Registro.br 2019], sendo responsável por validar e vincular ASNs (*Autonomous System Numbers*) e prefixos IPs às chaves públicas por meio de certificados segundo o padrão X.509 [Chung et al. 2019]. Assim, o detentor legítimo de um bloco de endereços IP pode obter um certificado de propriedade onde estarão listados os recursos a ele alocados [Labs 2020][Registro.br 2019].

Na infraestrutura há a definição dos ROA (*Route Origin Authorization*), que são objetos assinados com chaves privadas e que contêm uma lista de blocos IPs que um ASN está autorizado a originar. O RPKI permite que os roteadores de borda executem a validação das rotas recebidas verificando, através de *softwares* validadores, os ROAs publicados em repositórios RPKI, evitando assim ataques como o sequestro de prefixo BGP [Registro.br 2019]. A figura 2 ilustra o uso do RPKI impedindo um anúncio falso ou incorreto.

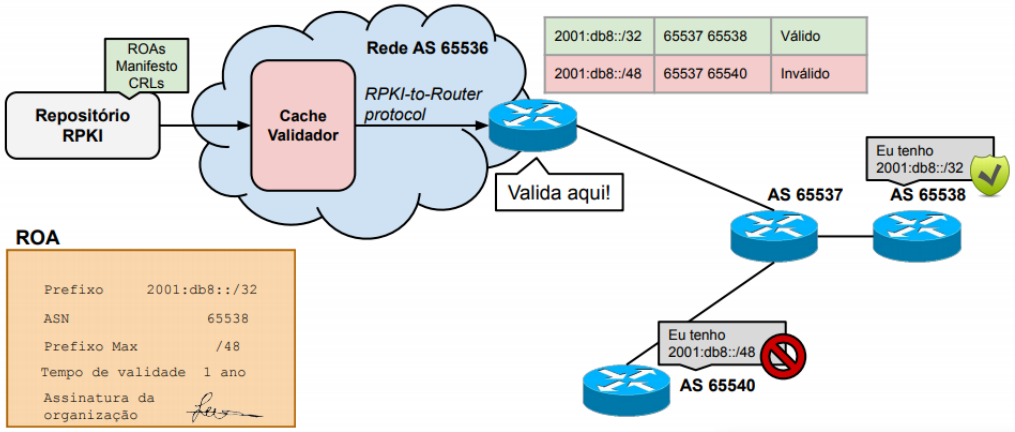

Figura 2. RPKI - Validação da Origem [Nic.br 2019].

Ao receber um anúncio mais específico para rede destino, ocorre a consulta e verificação de autenticidade da rota recebida com o *software* validador RPKI. Periodicamente o mesmo recupera e armazena em cache todos os certificados e ROAs publicados nos repositórios RPKI. O roteador de borda do AS65536 pode, portanto, confrontar as informações de roteamento recebidas com a sua respectiva autorização de origem da rota. O anúncio será classificado como válido, caso haja correspondência entre anunciante e ROA, inválido ou *Not Found*, caso um ROA para aquele anúncio não esteja cadastrado. Em seguida ocorre a validação da origem do anúncio e a rota via AS65538 é instalada como preferencial na tabela de roteamento.

Para garantir a origem da rede e sua autenticidade, o RPKI é respaldado pelos Registros Regionais da Internet (RIRs) [Testart et al. 2020] que atuam como âncoras de confiança, validando os anúncios para os seus recursos [Labs 2020]. Segundo [Künneke-Trenaman 2019], a infraestrutura RPKI representa uma camada adicional de proteção, que em termos dos benefícios atingidos em segurança, representa uma possível solução. O propósito dessa pesquisa é verificar a eficácia desta solução, mesmo sob severas condições de ataques.

5. Ambiente de Simulação

A infraestrutura utilizada para desenvolvimento desta pesquisa é composta por emuladores de rede EVE-NG e servidores virtualizados. As máquinas virtuais (VMs) estão hospedadas no VMware Workstation versão 16.1.2 build-17966106. O *software* validador RPKI emulado possui conexão real com a internet para obtenção dos recursos ROA para a VM. Foi escolhido para validador o Routinator versão 0.9.0, instalado em uma VM Ubuntu 16.04.7. Seis roteadores virtuais Cisco CSR 1000V com IOS 16.9.1 são utilizados por suportarem a tecnologia RPKI. Três *Switches* virtuais L2 IOS 15.2 e três servidores Ubuntu 18.04.4 completam a topologia. As imagens foram importadas para o EVE-NG 2.0.3-112. O roteador ATENAS foi configurado para se conectar a porta TCP 3323 do Routinator, de modo que as informações de ROA por ele coletadas possam ser utilizadas durante o processo de validação de origem da rota.

6. Metodologia

Foi implementado um cenário entre seis ASes. Aos roteadores AMAZONAS e CHILE foram atribuídos os números de ASes reais pertencentes à RNP e à TELEFÓNICA CHILE. AMAZONAS recebeu o prefixo 132.255.96.0/22 de seu RIR e, portanto, tem legitimidade em anunciá-lo. Adicionalmente, um ROA válido para esse prefixo encontra-se publicado e presente em *cache* no validador RPKI, como ilustrado na figura 3.

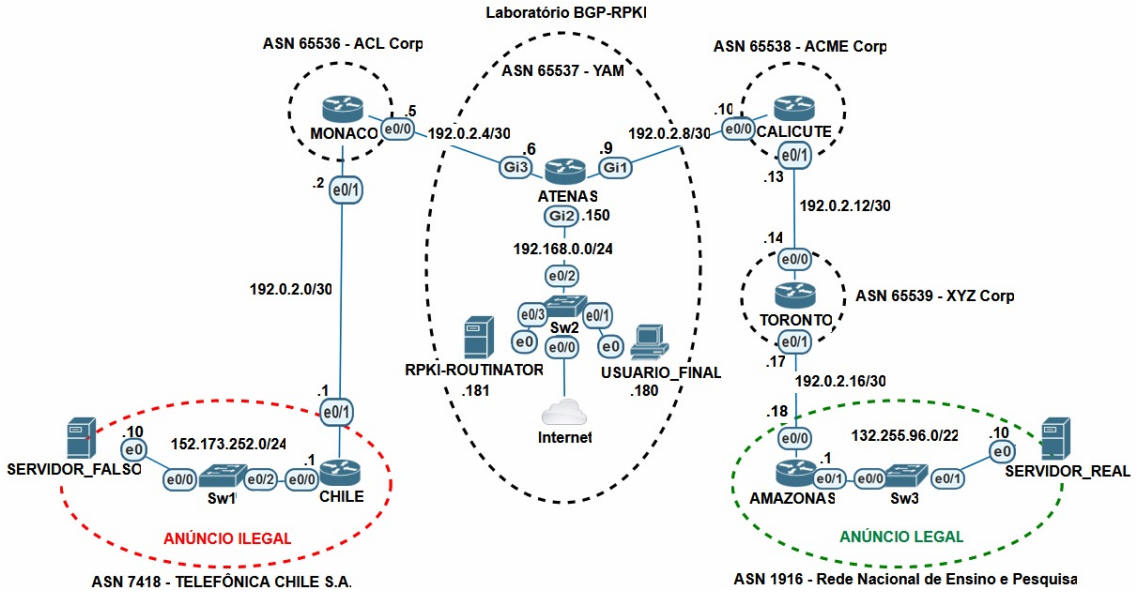

Figura 3. Ambiente de simulação.

Assim, o usuário final em ATENAS, para chegar ao servidor em 132.255.96.0, terá o fluxo de seus pacotes direcionados para o roteador AMAZONAS, conforme ilustrado pela figura 4.

Supondo que CHILE anuncie o mesmo prefixo em seus anúncios BGP, ATENAS receberá dois anúncios para a rede 132.255.96.0/22. Por ser uma rota mais rápida, ATENAS seria diretamente afetada pelo anúncio incorreto, e instalaria esta rota como preferencial. Se a ação for bem-sucedida, o tráfego direcionado a esse prefixo poderia ser sequestrado, conforme ilustrado pela figura 5.

```
AS-65537-ATENAS#show ip bgp 132.255.96.0
BGP routing table entry for 132.255.96.0/22, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 2
  65538 65539 1916
    192.0.2.10 from 192.0.2.10 (6.5.3.8)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
AS-65537-ATENAS#
```

Figura 4. Rota legítima de comunicação para com o servidor real.

```
AS-65537-ATENAS#show ip bgp
BGP table version is 12, local router ID is 6.5.3.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  132.255.96.0/22  192.0.2.5                             0 65536 7418 i
 *                    192.0.2.10                            0 65538 65539 1916 i
 *>  192.0.2.0/30     192.0.2.5                0            0 65536 ?
 *   192.0.2.4/30     192.0.2.5                0            0 65536 ?
 *>                   0.0.0.0                  0        32768 ?
 *   192.0.2.8/30     192.0.2.10               0            0 65538 ?
 *>                   0.0.0.0                  0        32768 ?
 *>  192.0.2.12/30    192.0.2.10               0            0 65538 ?
 *>  192.0.2.16/30    192.0.2.10                            0 65538 65539 ?
 *>  192.168.0.0      0.0.0.0                  0        32768 i
AS-65537-ATENAS#show ip bgp
```

Figura 5. Consequências do sequestro de prefixo realizado.

Os resultados da simulação evidenciam que ATENAS foi capaz de identificar o anúncio ilegal apenas após a utilização da infraestrutura RPKI, classificando a rota via AMAZONAS como válida e preferencial, como se observa pelos RPKI *Validation Codes* na figura 6.

```
AS-65537-ATENAS#show ip bgp
BGP table version is 11, local router ID is 6.5.3.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
I*   132.255.96.0/22  192.0.2.5                             0 65536 7418 i
V*>                   192.0.2.10                            0 65538 65539 1916 i
N*>  192.0.2.0/30     192.0.2.5                0            0 65536 ?
N*   192.0.2.4/30     192.0.2.5                0            0 65536 ?
V*>                   0.0.0.0                  0        32768 ?
N*   192.0.2.8/30     192.0.2.10               0            0 65538 ?
V*>                   0.0.0.0                  0        32768 ?
N*>  192.0.2.12/30    192.0.2.10               0            0 65538 ?
N*>  192.0.2.16/30    192.0.2.10                            0 65538 65539 ?
V*>  192.168.0.0      0.0.0.0                  0        32768 i
AS-65537-ATENAS#
```

Figura 6. Validação da origem através da RPKI.

6.1. Conclusões e Trabalhos Futuros

Esta pesquisa já materializou resultados promissores, e indicam o RPKI como uma proposta com grande potencial de adoção global devido à sua simplicidade e baixo *overhead*. Os atuais esforços buscam consolidar essa percepção, através de outras modalidades de ataque para atestar a sua eficácia. Uma das experiências em andamento é a de um ataque

de negação de serviço distribuído ao validador RPKI. Espera-se, com estas contribuições, agregar experiências consolidadoras documentadas aos esforços envidados pelo NIC-BR na implantação do RPKI no Brasil.

Referências

Cho, S., Fontugne, R., Cho, K., Dainotti, A., and Gill, P. (2019). *BGP hijacking classification*. IEEE, New York City, 1 edition.

Chung, T., Aben, E., Bruijnzeels, T., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., Rijswijk-Deij, R. v., Rula, J., and Sullivan, N. (2019). *RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins*. Association for Computing Machinery, New York, NY, USA, 1 edition.

Künneke-Trenaman, N. (2019). RPKI and the future of routing security. *Network Security*, 2019(11):18–19.

Labs, N. (2020). Introduction - RPKI documentation. `https://rpki.readthedocs.io/en/latest/rpki/introduction.html`. Acessado: 01/22/2021.

Lepinski, M. and Kent, S. (2012). An Infrastructure to Support Secure Internet Routing. RFC 6480.

Mitseva, A., Panchenko, A., and Engel, T. (2018). The state of affairs in BGP security: A survey of attacks and defenses. *Computer Communications*, 124:45 – 60.

Moll, O. (2020). Border Gateway Protocol Hijacking - Examples and Solutions. `https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions`. Acessado: 16/01/2021.

Murphy, S. L. (2006). BGP Security Vulnerabilities Analysis. RFC 4272.

Nic.br (2019). RPKI: Uma proteção para roubo de prefixos no BGP. `https://tutoriais.semanainfrabr.nic.br/files/apresentacao/arquivo/803/RPKI.pdf`. Acessado: 06/12/2021.

Registro.br (2019). RPKI - Numeração. `https://registro.br/tecnologia/numeracao/rpki/`. Acessado: 01/22/2021.

Rekhter, Y., Hares, S., and Li, T. (2006). A Border Gateway Protocol 4 (BGP-4). RFC 4271.

Testart, C., Richter, P., King, A., Dainotti, A., and Clark, D. (2020). *To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today*. Springer, New York City, lncs, volume 12048 edition.