Validação da solução RPKI para segurança do BGP

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 – Urca - RJ – CEP: 22290-270

[2]Universidade do Estado do RJ (UERJ-ZO)
Av. Manuel Caldeira de Alvarenga, 1203 - Campo Grande - RJ – CEP: 23070-200

{abreumelo,salles}@ime.eb.br, frederico.oliveira@uerj.br

Abstract. *BGP is vital for the interconnection of Internet Autonomous Systems, and the number of prefix hijacking attacks is increasing. Among the solutions discussed in the literature, RPKI has been the preferred option. The objective of this work is to validate the RPKI, through robustness tests against Prefix Hijacking attacks. The results were satisfactory, since the solution allowed the identification of unauthenticated routes. However, during the research, an RPKI resource that could be used in attacks, the SLURM FILE, was identified and tested. No works were found addressing this possibility, which is the main contribution of the dissertation.*

Resumo. *O BGP é vital para a interligação dos Sistemas Autônomos da Internet, e o número de ataques de sequestro de prefixos vem aumentando. Entre as soluções discutidas na literatura, o RPKI vem sendo a opção preferencial. O objetivo deste trabalho é o de validar o RPKI, através de testes de robustez a ataques de Prefix Hijacking. Os resultados foram satisfatórios, uma vez que a solução permitiu identificar as rotas não autenticadas. Porém, durante a pesquisa, foi identificado e testado um recurso do RPKI passível de ser usado em ataques, o SLURM FILE. Não foram encontrados trabalhos abordando essa possibilidade, sendo esta a principal contribuição da dissertação.*

1. Introdução

O BGP é responsável por desempenhar um papel crítico na infraestrutura de roteamento global, como o principal protocolo para transmissão de informações de roteamento entre diferentes Sistemas Autônomos [Mitseva et al. 2018].

Em virtude do aumento do número de incidentes de segurança com o BGP em todo o mundo, a comunidade acadêmica passou a discutir soluções viáveis [Mitseva et al. 2018], e o RPKI vem sendo apontado como uma delas. Neste trabalho, com o uso de uma topologia virtualizada com imagens reais de equipamentos largamente utilizados na WAN, o RPKI é implementado e suas competências para solucionar os problemas de segurança são testadas.

2. Objetivos e Contribuição

Com o objetivo de validar a solução, ataques são realizados e a eficácia do RPKI é avaliada. Como contribuição mais relevante, este trabalho identifica uma "brecha" de

segurança. O RPKI possui um conjunto de definições para filtros e exceções chamado de SLURM *file*. Este recurso foi identificado e utilizado em um ataque bem-sucedido durante a validação, indicando que a segurança do RPKI demanda maior aprofundamento, testes e um esforço de validação mais abrangente.

3. Trabalhos Relacionados

Observa-se na literatura que a maioria das soluções propostas consiste apenas em trabalhos acadêmicos, sendo que a infraestrutura RPKI (*Resource* PKI) tem *status* de padronizada pelo IETF para adoção. A RPKI é uma infraestrutura de PKI especializada em atender às demandas do BGP. Não foram observadas propostas de avaliação da resiliência da solução RPKI frente a ataques à sua infraestrutura. Por se tratar de um tema com alta relevância, o trabalho realizado por [de Melo et al. 2021] se destaca na literatura ao propor modalidades de ataques ao *software* validador RPKI, possível ponto único de falha na infraestrutura.

Adicionalmente, soluções reativas são discutidas [Al-Musawi et al. 2017]. O trabalho realizado por [Shapira and Shavitt 2020] engloba uma dessas vertentes ao tratar o sequestro de prefixos BGP sobre a perspectiva de um problema de aprendizagem supervisionada. Ao utilizar técnicas de *deep learning*, eventos passados são mapeados e uma acurácia de 99,99% é relatada em suas validações. A pesquisa de [Karimi et al. 2019] propõe a utilização de Redes Neurais, e [Arai et al. 2019] se utiliza de técnicas de aprendizagem de máquina para identificar comportamentos atípicos em mensagens de atualização BGP. Contudo, como sistemas reativos demandam complexos relacionamentos de dados nem sempre disponíveis para o reconhecimento de padrões de ataques, seus esforços de adoção são, ao que tudo indica, desencorajados a favor de soluções proativas como RPKI.

Pesquisas como a de [Lu et al. 2021] e [He et al. 2021] também revelam a introdução do conceito de *Blockchain* como forma de prover resiliência para a infraestrutura RPKI contra ataques de sequestro BGP. Usando-se dessa temática, [Angieri et al. 2020] explorou a estrutura descentralizada da *Blockchain* para idealizar um modelo alternativo à validação hierárquica do RPKI. Ao criar um conceito de veracidade tácita através de métricas estatísticas de consenso entre os participantes, seu modelo é, supostamente, capaz de coexistir ou até mesmo substituir a infraestrutura RPKI.

4. O RPKI

O RPKI permite que os roteadores BGP de borda verifiquem a autenticidade das rotas recebidas, através de *softwares* validadores que usam os ROAs publicados em repositórios RPKI globais. Isso permite que se evite ataques como o sequestro de prefixo BGP [Registro.br 2019]. Um anúncio malicioso não seria autenticado, logo, seria ignorado pelos roteadores. Os *softwares* validadores constituem ponto central na solução proposta, uma vez que são responsáveis pelas verificações criptológicas das informações obtidas nos repositórios.

Os validadores periodicamente sincronizam e validam os ROAs obtidos e geram um formato simplificado chamado VRP (*Validated ROA Payload*). Os VRP contêm apenas prefixo/máscara e ASN, já autenticados, para disponibilização aos roteadores através do protocolo RTR (RPKI *to Router Protocol*) [Bush and Austein 2013]

[Gilad et al. 2017]. A figura 1 exemplifica uma troca típica de informações entre validador e roteador.

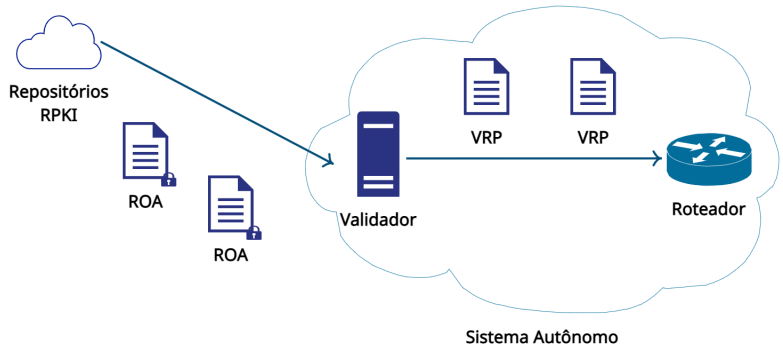

Figura 1. Como os roteadores obtêm informações RPKI

Assim, os roteadores armazenam uma base de dados, utilizando as informações confiáveis que recebem, e aplicando um conjunto de regras, designam um estado de validade a cada *update* BGP recebido.

A figura 2 descreve o uso do RPKI impedindo um anúncio falso ou incorreto. No cenário ilustrado, o AS 1916 envia seu prefixo através de um anúncio BGP para seus vizinhos, contendo: [132.255.96.0/22, AS 1916]. Concomitantemente, um anúncio ilegítimo do bloco de endereços é feito pelo AS 65536.

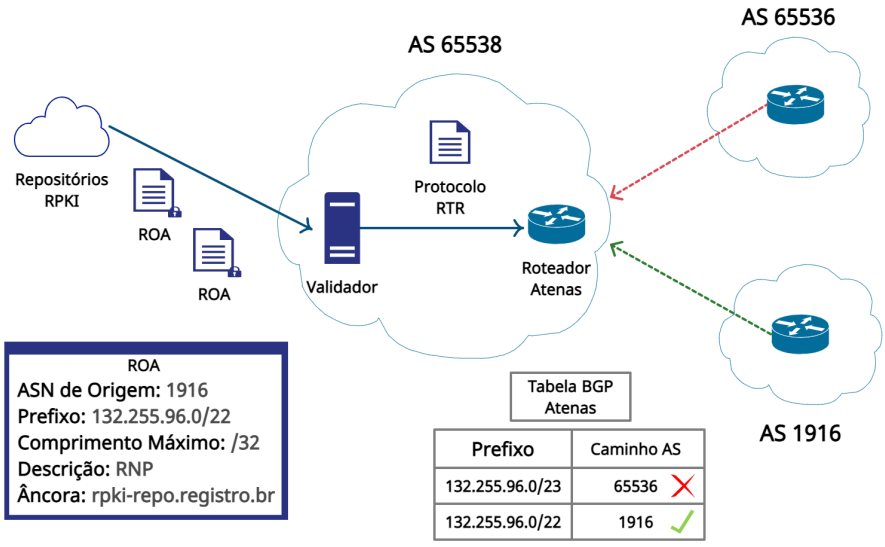

Figura 2. Validação de Origem RPKI

Ao receber um anúncio mais específico para rede destino de AS 65536, ocorre a consulta e verificação de autenticidade das rotas recebidas com o *software* validador RPKI. O roteador de borda do AS 65538 pode, portanto, confrontar as duas informações de roteamento recebidas com a sua respectiva autorização de origem da rota [132.255.96.0/22, AS 1916]. Como a outra rota, proveniente de AS 65536, apesar de ser mais específica, não está autenticada, ela é então descartada.

4.1. Validação do RPKI

Qualquer tentativa de teste no ambiente real, além de poder comprometer o funcionamento da internet global, também poderia ser enquadrada como uma atividade criminosa. Optou-se então por definir uma topologia rigorosamente comparável a uma região de trocas de anúncios BGP real, implementada através de máquinas virtuais de roteadores típicos de mercado, e uma implementação atualizada do Routinator em Linux. Os ROA utilizados, no entanto, foram obtidos e permanentemente atualizados a partir dos repositórios do NIC.br.

Como metodologia, foram realizados testes de sequestro de prefixos através de anúncios BGP maliciosos, com e sem o uso do RPKI. Após uma série de testes, foram buscadas e testadas formas alternativas de se burlar a segurança oferecida pelo RPKI.

A topologia virtualizada foi desenvolvida no *software* simulador de redes EVE-NG[1], imaginando-se um ataque no seguinte cenário: uma rede (AS 65536) empreende ataques de sequestro através da introdução de um agente malicioso, em um contexto onde os roteadores apresentam configurações típicas de roteamento e vizinhança. Após isso, a infraestrutura RPKI é usada, e o mesmo ataque é refeito, com o objetivo de observar a validação da origem.

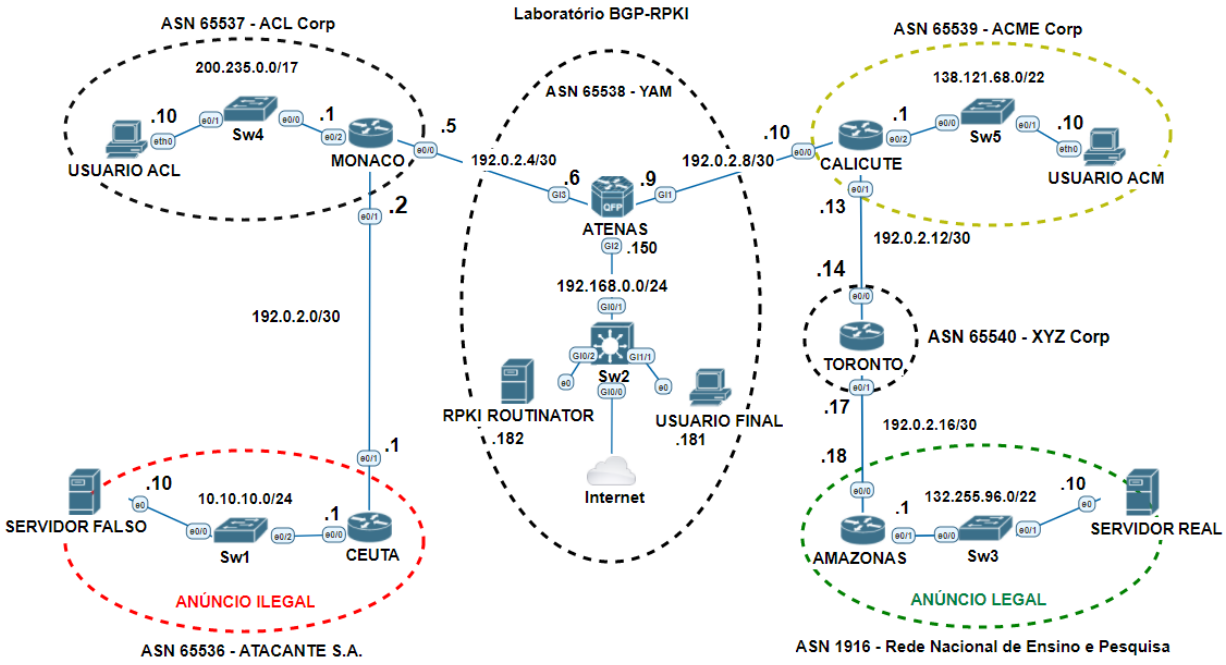

Figura 3. Ambiente de simulação proposto

Foram implementados seis ASes, conforme a figura 3. Os roteadores anunciam suas redes de forma típica.

4.2. Sequestro de Prefixo BGP

O ataque se inicia com a rede conectada ao roteador Amazonas sendo publicada pelo roteador Ceuta, ao anunciar o mesmo prefixo 132.255.96.0/22 em seus anúncios BGP.

[1] https://www.eve-ng.net/

Após a convergência, Atenas receberá dois anúncios para a rede destino 132.255.96.0/22, de origens distintas, sendo que a rota maliciosa fica com prioridade (*best*) por ser a de menor custo, configurando assim o sequestro do prefixo 132.255.96.0/22 bem-sucedido.

4.3. Uso do RPKI

Após a sincronização do Routinator com os repositórios RPKI, uma lista de *Validated ROA Payload* é emitida e armazenada em *cache*, contendo os respectivos ASes e prefixos IPs que foram validados criptograficamente, e o *software* validador estará operacionalmente pronto para suprir os roteadores BGP de borda com o *cache* validado via protocolo RTR.

Os resultados da simulação evidenciam que Atenas foi capaz de identificar o anúncio ilegal apenas após a comunicação com o *software* validador. Assim, Atenas é capaz de identificar o anúncio ilegal e classificar a rota via RNP como válida e preferencial, como evidencia os RPKI *validation codes* na figura 4. O anúncio da RNP é marcado como válido, uma vez que existe um ROA para esse prefixo, e o outro anúncio para o mesmo destino marcado como inválido, pois não existe um ROA correspondente.

```
AS-65538-ATENAS#show ip bgp
BGP table version is 24, local router ID is 6.5.3.8
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 65537 65536 i
V*>                   192.0.2.10                            0 65539 65540 1916 i
I*   138.121.68.0/22  192.0.2.10              0             0 65539 i
N*>  192.0.2.0/30     192.0.2.5               0             0 65537 ?
N*   192.0.2.4/30     192.0.2.5               0             0 65537 ?
V*>                   0.0.0.0                 0         32768 ?
N*   192.0.2.8/30     192.0.2.10              0             0 65539 ?
V*>                   0.0.0.0                 0         32768 ?
N*>  192.0.2.12/30    192.0.2.10              0             0 65539 ?
N*>  192.0.2.16/30    192.0.2.10                            0 65539 65540 ?
V*>  192.168.0.0      0.0.0.0                 0         32768 i
N*>  200.235.0.0/17   192.0.2.5               0             0 65537 i
AS-65538-ATENAS#
```

Figura 4. Validação da origem através da RPKI

5. Ataque ao RPKI através do *SLURM FILE*

A RFC 8416 [Ma et al. 2018] provisiona um mecanismo para possibilitar que os administradores de ASes estabeleçam uma visão personalizada, através da configuração de exceções locais sobre os dados RPKI globais.

O mecanismo adotado para fornecer essa funcionalidade foi definido como SLURM FILE (*Simplified Local Internet Number Resource Management*), um arquivo escrito em formato JSON[2] que contém parâmetros RPKI, como as entradas definidas na seção *prefixFilters* e *prefixAssertions*.

[2]O *JavaScript Object Notation* é um formato simples para troca de informações/dados entre sistemas, estruturado sobre um formato texto de fácil entendimento.

A seção *prefixFilter* define quais VRPs serão filtrados, ou seja, impedidos de serem entregues para o roteador. Caso existam entradas correspondentes aos parâmetros filtrados, serão ignoradas na geração das VRPs e, consequentemente, as informações de validação não serão entregues ao roteador.

A seção *prefixAssertions* é responsável por fazer declarações positivas adicionais acerca dos recursos numéricos enviados a um roteador, da mesma forma que na seção *prefixFilters*.

Em um cenário onde a atacante deseje bloquear a introdução no roteador de informações que sejam legitimamente recebidas da infraestrutura RPKI, a seção *prefixFilters* pode ser utilizada para filtrar a saída do Routinator para o Roteador. Na figura 5, a manipulação visa alterar o *status* RPKI válido de uma rota legítima para *Not Found*.

```
root@ubuntu:~# nano .exceptions.slurm

{
  "slurmVersion": 1,
  "validationOutputFilters": {
    "prefixFilters": [
      {
        "prefix": "132.255.96.0/22",
        "asn": 1916
      }
    ],
    "bgpsecFilters": [
    ]
  },
  "locallyAddedAssertions": {
    "prefixAssertions": [
    ],
    "bgpsecAssertions": [
    ]
  }
}
```

Figura 5. Ataque SLURM - Adulteração dos parâmetros RPKI de uma rota legítima

A figura 6 evidencia que a rota legítima (via *next hop* 192.0.2.10) é preterida em relação a rota com menor *As_path*. Como as duas rotas apresentam estado *Not found*, para o BGP é como se não houvessem ROAs descrevendo os dois anúncios.

Os ataques bem-sucedidos feitos durante o esforço de validação evidenciaram que a solução RPKI ainda não é uma solução completa e definitiva. Para que se possa efetivamente considerá-la uma solução de segurança para o BGP, ela prescinde de um *hardening* de todo o conjunto, ou até mesmo a proposição de novas versões do RPKI com maior controle da utilização do arquivo SLURM.

Em uma primeira e superficial abordagem do problema, a introdução de filtros para a utilização do arquivo SLURM pode ser uma solução viável. É intenção, como proposta de trabalhos futuros, desenvolver um *draft* específico para a introdução de mecanismos de controle no uso do RPKI, e submeter ao *working group* do IETF responsável por ele.

```
AS-65538-ATENAS#show ip bgp
BGP table version is 25, local router ID is 6.5.3.8
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
N*    132.255.96.0/22  192.0.2.10                           0 65539 65540 1916 i
N*>                    192.0.2.5                            0 65537 65536 i
I*    138.121.68.0/22  192.0.2.10               0            0 65539 i
N*>   192.0.2.0/30     192.0.2.5                0            0 65537 ?
N*    192.0.2.4/30     192.0.2.5                0            0 65537 ?
V*>                    0.0.0.0                  0        32768 ?
N*    192.0.2.8/30     192.0.2.10               0            0 65539 ?
V*>                    0.0.0.0                  0        32768 ?
N*>   192.0.2.12/30    192.0.2.10               0            0 65539 ?
N*>   192.0.2.16/30    192.0.2.10                            0 65539 65540 ?
V*>   192.168.0.0      0.0.0.0                  0        32768 i
N*>   200.235.0.0/17   192.0.2.5                0            0 65537 i
AS-65538-ATENAS#
```

Figura 6. Resultados do ataque de supressão SLURM

6. Conclusão e Trabalhos Futuros

Esse trabalho foi conduzido com a motivação de contribuir para a avaliação das possíveis soluções para a proteção do BGP, em especial os ataques de sequestro de prefixo. O RPKI, principal mecanismo em discussão, foi escolhido para validação. Uma infraestrutura baseada em imagens virtualizadas de roteadores e do próprio Routinator foi planejada, instalada e configurada, de forma a representar ao máximo as condições reais da internet.

No esforço de validação, bem sucedido, ataques de sequestro foram realizados trivialmente. Após a introdução da camada adicional de segurança oferecida pelo RPKI, a inserção de rotas falsas foi neutralizada, consolidando as expectativas de competência da solução. No entanto, um recurso existente para contornar problemas de configuração foi identificado e testado com intenções maliciosas, e os resultados dos testes mostraram que não basta adotar o RPKI apenas. O uso do SLURM FILE precisa ser feito mediante recursos que garantam que a intenção é legítima e feita por agentes autorizados e de acordo com as regras de negócio.

Um trabalho futuro já em andamento trata da revisão da RFC 8416 [Ma et al. 2018], propondo um tratamento baseado em AAA *(Authentication - Autorization - Accounting)* simplificado e leve, porém suficiente para eliminar a grande facilidade para ataques atual existente.

Referências

Al-Musawi, B., Branch, P., and Armitage, G. (2017). BGP Anomaly Detection Techniques: A Survey. *IEEE Communications Surveys Tutorials*, 19(1):377–396.

Angieri, S., Bagnulo, M., García-Martínez, A., Liu, B., and Wei, X. (2020). InBlock4: Blockchain-based Route Origin Validation. In *IEEE INFOCOM 2020 - IEEE Confe-*

rence on Computer Communications Workshops (INFOCOM WKSHPS), pages 291–296.

Arai, T., Nakano, K., and Chakraborty, B. (2019). Selection of Effective Features for BGP Anomaly Detection. In *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)*, pages 1–6.

Bush, R. and Austein, R. (2013). The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6810.

de Melo, Y., Salles, R., and Oliveira, F. (2021). Mitigação de Ataques ao BGP utilizando RPKI. In *Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 385–390, Porto Alegre, RS, Brasil. SBC.

Gilad, Y., Sagga, O., and Goldberg, S. (2017). Maxlength Considered Harmful to the RPKI. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '17, page 101–107, New York, NY, USA. Association for Computing Machinery.

He, G., Su, W., Gao, S., Yue, J., and Das, S. K. (2021). ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing. *IEEE Transactions on Network and Service Management*, 18(2):1690–1705.

Karimi, M., Jahanshahi, A., Mazloumi, A., and Sabzi, H. Z. (2019). Border Gateway Protocol Anomaly Detection Using Neural Network. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 6092–6094.

Lu, H., Tang, Y., and Sun, Y. (2021). Drrs-bc: Decentralized Routing Registration System Based on Blockchain. *IEEE/CAA Journal of Automatica Sinica*, 8(12):1868–1876.

Ma, D., Mandelberg, D., and Bruijnzeels, T. (2018). Simplified Local Internet Number Resource Management with the RPKI (SLURM). RFC 8416.

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.

Registro.br (2019). RPKI - Numeração. `https://registro.br/tecnologia/numeracao/rpki/`. (Acessado: 06/02/2022).

Shapira, T. and Shavitt, Y. (2020). A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding. In *Proceedings of the Workshop on Network Meets AI & amp; ML*, NetAI '20, page 35–41, New York, NY, USA. Association for Computing Machinery.