Um Estudo para Identificação e Mitigação de *IP Spoofing* em Redes IPv6 utilizando SDN

Manoel F. Ramos[1], **Rafael B. Ávila**[1]

[1]Escola Politécnica – Universidade Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950 – Bairro Cristo Rei – 93.022-000 – São Leopoldo – RS – Brasil

manoel@dropreal.com, rafael.avila@gmail.com

Resumo. *A técnica de IP Spoofing é empregada em diversos tipos de ataques cibernéticos para forjar o real endereço de rede do atacante. Com a expansão do uso do IPv6, projeta-se que a utilização dessa técnica será intensificada, principalmente porque o protocolo NDP — parte do IPv6 responsável pela descoberta de vizinhança — não possui mecanismos de validação dos endereços de rede e de enlace inseridos em seu cabeçalho. Este artigo apresenta uma análise sobre as possibilidades de aplicação de spoofing em IPv6 e os principais mecanismos e protocolos utilizados em sua exploração. Além disso, apresenta uma proposta para identificar e mitigar o uso da técnica de IP Spoofing na rede local de origem através do uso de SDN em redes IPv6.*

Abstract. *IP Spoofing is used in various types of cyber attacks in order to forge the real network address of an attacker. Its use is expected to be intensified with the expansion of IPv6, mainly because the NDP protocol—part of IPv6 responsible for neighborhood discovery—does not present validation mechanisms for network and link layer addresses employed in its header. This paper presents an analysis on the possibilities of applying IPv6 spoofing and the main mechanisms and protocols used in exploiting it. Furthermore, it proposes a method for identification and prevention of IP spoofing at the source local network by using SDN in IPv6 networks.*

1. Introdução

A maioria dos ataques cibernéticos utilizam técnicas de falsificação (*Spoofing*) do endereçamento de rede de origem do atacante, tanto para amplificar ou redirecionar respostas de comunicação a um determinado alvo, quanto para forjar o real endereço de origem do computador do atacante. Esta técnica é conhecida como IP *Spoofing*. [Tanase 2003].

O IP *Spoofing* foi inicialmente discutido através de meios acadêmicos na década de 1980 onde foi descoberta uma falha de segurança no protocolo TCP (*Transmission Control Protocol*), conforme especificado por [Morris 1985] e aprofundado por [Bellovin 1989]. Essas falhas já foram solucionadas, porém a técnica de IP *Spoofing* ainda é muito utilizada nos dias de hoje. O protocolo IP é uma fraqueza presente nos sistemas utilizados na internet atualmente pois permite que o endereço IP de origem seja alterado ou seja, um atacante pode, além de utilizar o IP *Spoofing* para garantir o seu anonimato, enviar pacotes IPs com o endereço de origem falsificado para lançar ataques direcionados como *Non-Blind Spoofing*, *Blind Spoofing*, *Man in The Middle* (MiTM), DoS, *Decoy Scan*, entre outros. [Mukaddam et al. 2014].

O objetivo deste estudo é compreender o funcionamento da técnica de IP *Spoofing* em redes IPv6, destacando a preocupação da comunidade acadêmica sobre o tema, assim como apresentar um novo método delineado para mitigar e combater a sua usabilidade utilizando Redes Definidas por Softwares (SDN) na origem do tráfego.

2. Fundamentação Teórica

Nesta seção é apresentada uma breve descrição sobre o protocolo IPv6, o protocolo NDP e SDN.

2.1. IPv6

O IPv6 possui diversas melhorias perante o seu antecessor, entre estas destaca-se o cabeçalho no tamanho de 40 *bytes* sendo mais simples e versátil, aumento do tamanho do endereço de 32 *bits* (IPv4) para 128 *bits*, possibilidade de redução de fluxo e propriedade (rotulação de pacotes) e a substituição do protocolo ARP, utilizado pelo IPv4 para a resolução de endereços MAC, pelo protocolo NDP (*Neighbor Discovery Protocol*). [Kurose and Ross 2006].

Conforme [Narten et al. 2007], cada nó (dispositivos de rede que utilizam IPv6) utiliza o NDP para encontrar, identificar e registrar em *cache* os endereços MAC de nós vizinhos e se tornarem conhecidos, permitindo efetuar uma conectividade de forma rápida entre eles. Um nó utiliza o NDP para manter informações sobre os vizinhos que são ou não acessíveis. Quando o caminho para acessar um determinado nó já identificado anteriormente esteja indisponível para efetuar a conectividade, o NDP procura de forma ativa e rápida os vizinhos mais próximos para estabelecer a comunicação.

2.2. *Neighbor Discovery Protocol*

O protocolo NDP corresponde com a combinação do protocolo ARP [Plummer 1982], ICMP *Router Discovery Mensagens* [Deering 1991] e do ICMP *Redirect* [Postel 1981], possuindo diversas melhorias e novas funcionalidades. Além de efetuar a resolução de endereços da camada de rede com a camada de enlace, o NDP permite a descoberta de roteadores e nós, efetua a autoconfiguração de endereçamentos, permite que roteadores anunciem o MTU de seus vizinhos, detecta falhas de *links*, permite a utilização do *link* local para identificar exclusivamente roteadores, permite definir o limite até 255 saltos sem interromper a comunicação, além de utilizar o ICMPv6 para permitir a autenticação da camada de rede conforme o mecanismo de segurança definido pelas políticas de segurança.

Para a troca de mensagens, o NDP define cinco tipos de mensagens ICMPv6 para efetuar trocas de mensagens necessárias para a execução de determinadas funções, sendo elas as mensagens RS (*Router Solicitation*), que são originadas por um determinado *host* para solicitar que um roteador envie uma mensagem RA (*Router Advertisement*). As mensagens RA são enviadas por roteadores para anunciar seus parâmetros de presença e de um determinado *link*. As mensagens NS (*Neighbor Solicitation*) que são enviadas por um host a outro para solicitar o seu endereço MAC. Já as mensagens NA (*Neighbor Advertisement*) informam o endereço MAC a um determinado *host* ou responde a uma solicitação NS. Por fim, a mensagem *Redirect* informa os parâmetros necessários para redirecionar um determinado tráfego de um roteador a outros. [Narten et al. 2007].

Conforme [Barbhuiya et al. 2013], os seguintes ataques utilizam o uso da técnica de IP *Spoofing* através do envio de mensagens NDP em redes IPv6:

- *Neighbor solicitation/advertisement Spoofing*;
- *Man-in-the-Middle attack*;
- *Duplicate Address Detection attack* (Ataque DAD);
- *Neighbor Unreachability Detection attack* (Ataque NUD);
- *Spoofed Router Redirect Message attack*;
- *Replay attack.*

2.3. Redes Definidas por *Software*

SDN (*Software-Defined Networking*) está mudando a maneira de como as redes são concebidas. O conceito das Redes Definidas por *Software* vem atraindo a atenção de diversos pesquisadores e empresas. SDN possui duas características definidas, a primeira é a separação do plano de controle do plano de dados. O plano de controle decide como lidar com o tráfego da rede, já o plano de dados encaminha o tráfego conforme decisão do plano de controle. A segunda característica é que SDN consolida o plano de controle de modo que o *software* exerça o controle direto sobre o estado dos elementos contidos no plano de dados como, por exemplo, *switches* e roteadores. Este *software* de controle, também denominado "controlador SDN" é uma interface de programação de aplicativos (*Application Programming Interface* - API) definida como, por exemplo, o protocolo OpenFlow. [Feamster et al. 2014].

Conforme ilustrado na Figura 1, a arquitetura SDN consiste em três camadas, sendo elas a camada superior, a camada inferior e a camada do meio (controlador). A camada superior é a camada de aplicação, que inclui os aplicativos que oferecem serviços como virtualização de rede, *firewall*, balanceadores, gerenciamento de fluxo, etc. A camada de aplicação é captada a partir da camada inferior no qual é a base da camada de rede física, também denominada como camada de infraestrutura. A camada do meio é o controlador SDN, também denominada de camada de controle, esta camada é o elemento crítico e primordial para o funcionamento de SDN pois o controlador remove o plano de controle da rede de *hardware* e passa a tratá-lo como *software*. É importante ressaltar que em SDN, todos os elementos físicos e virtuais são integrados. Desta forma o controlador facilita a gestão da rede automatizada e torna mais fácil de integrar e administrar a infraestrutura com o negócio das organizações. [Kreutz et al. 2015].

3. Trabalhos Relacionados

Existem diversos estudos relacionados ao entendimento e mitigação do uso da técnica de IP *Spoofing* em redes IPv4. Por outro lado, poucos mecanismos de segurança são propostos para a prevenção do uso da técnica em redes IPv6 e muito menos tratam o problema diretamente em sua origem.

[Barbhuiya et al. 2013] apresentam um IDS ativo para detecção e prevenção de ataques baseados nas fragilidades do protocolo NDP em redes IPv6, objetivando que uma determinada rede seja protegida caso sofra ataques que utilizam IP *Spoofing* através das mensagens do NDP. Os autores afirmam que a solução é eficaz para a validação de endereços MAC em redes IPv6. Os algoritmos desenvolvidos, chamados de NS_HANDLER() e NA_HANDLER() e os seus submódulos VERIFY_IP-MAC() e RESPONSE_ANALYSER() se destacam pela simplicidade do processo para a identificação e a validação de endereçamentos MAC e IPv6.

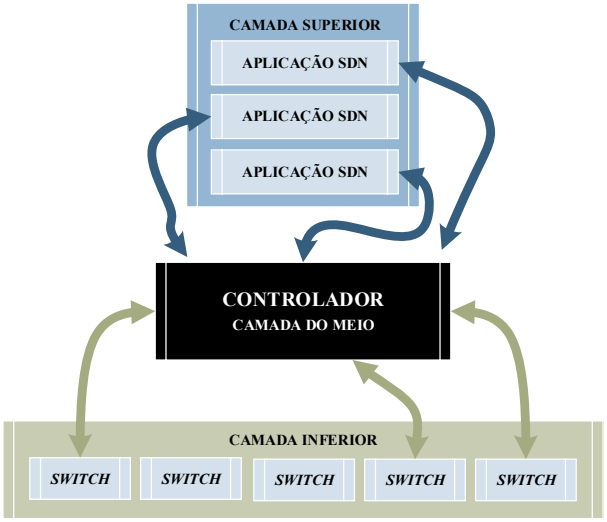

Figura 1. Arquitetura básica de SDN.

[Yao et al. 2011] contribuem com a implementação do mecanismo denominado VAVE (*Virtual source Address Validation Edge*), desenvolvido através do *framework* SAVI (*Source Address Validation Improvement*), o qual emprega o uso do protocolo OpenFlow [McKeown et al. 2008] para validar os endereços de origem do tráfego de entrada em uma rede local. SAVI é discutido através do grupo de trabalho da IETF descrito em [Wu et al. 2013].

[Mowla et al. 2015] propõem um mecanismo de defesa para combater os ataques relacionados ao uso da técnica de IP *Spoofing* no tráfego de dados recebidos, validando o tráfego legítimo e bloqueando o tráfego de *Spoofing*. A solução é composta por SDN com base na tecnologia CDNi (*Content Distribution Network Interconnection*), juntamente com a tecnologia ALTO (*Application Layer Traffic Optimization*). O objetivo da solução é utilizar SDN para detectar IP *Spoofing*, seguindo de um mecanismo para alimentar regras em *switches* com suporte à SDN através do controlador utilizando os mapas de marcação (*mark*) fornecidos pelo servidor ALTO. Um fator negativo desta solução é a complexidade de implementação pois, além da infraestrutura SDN baseada em CDNi, no qual poucos fabricantes de equipamentos de rede possuem suporte, a solução necessita de servidores e clientes ALTO em cada uma das redes gerenciadas, sendo um item indispensável para o processo de detecção de IP *Spoofing*.

[Yan et al. 2011], observando as fragilidades do protocolo IP, o qual não possui mecanismos de validação dos endereços de origem e a real expansão do uso do IPv6, desenvolveram um experimento de implementação do SAVI em uma rede local. É importante salientar que o SAVI utiliza funções de acompanhamento para filtrar pacotes não confiáveis, explorando as mensagens do NDP. Nesta contribuição, os autores consultam servidores DHCPv6 para efetuar o processo de validação através de mensagens NDP emitidas através do SAVI.

A partir de uma análise dos trabalhos apresentados, foi possível elaborar uma proposta alternativa para combater o IP *Spoofing* em redes IPv6. A proposta é fundamentada principalmente nas características dos algoritmos NS_HANDLER() e NA_HANDLER() e seus submódulos propostos por [Barbhuiya et al. 2013], da integração de servidores DHCP para auxiliar o processo de validação de endereços de rede em uma rede local proposto por [Yan et al. 2011] e do algoritmo de manipulação de IP *Spoofing* proposto por [Mowla et al. 2015] que, assim como o trabalho anterior, utiliza SDN para auxiliar no processo de manipulação de pacotes.

4. Mitigação do uso da técnica de IP *Spoofing* na origem

Segundo [Moura et al. 2014], os ISPs (*Internet Service Provider*) deveriam investir na mitigação de tráfegos maliciosos originados internamente em seu *Autonomous System* (AS), garantindo que seus clientes não originem ataques externos. Porém, os ISPs se abstém de investir na mitigação do tráfego originado por seus clientes. Com a expansão crescente do IPv6, a não necessidade de utilização da técnica de NAT e as fragilidades do próprio protocolo NDP, pode-se supor que o uso de IP *Spoofing* continuará em constante ascensão.

Através deste estudo, foi possível compreender os principais componentes que permitem que a técnica de IP *Spoofing* seja aplicada em uma rede de computadores. Analisando os trabalhos relacionados, foi possível identificar métodos eficientes para identificar e mitigar o uso da técnica de IP *Spoofing*, assim como compreender como a comunidade acadêmica está discutindo o tema. O estudo sobre SDN foi realizado para compreender e verificar como as redes definidas por *software* podem colaborar com o combate de IP *Spoofing*.

4.1. Método identificado para o combate de IP *Spoofing*

Através dos trabalhos relacionados analisados, foi possível identificar que a maioria das soluções de combate ao uso da técnica de IP *Spoofing* trata a sua prevenção diretamente no destino, ou seja, no local onde um possível ataque possa ser realizado. Como já citado, é notável que se cada rede de computadores e/ou os IPSs mitigassem o tráfego de saída de seus perímetros, validando os endereços de origem de suas redes, o problema do uso da técnica de IP *Spoofing* possivelmente poderia ser solucionado.

4.2. Componentes da solução identificada

A solução identificada é composta pelo uso de SDN que, além permitir que se tenha uma visão global de todo o tráfego da rede através de uma análise de fluxos, permite que seja desenvolvida uma aplicação com base na API do controlador. Esta aplicação é a responsável por validar os endereços MAC e endereços IP de cada pacote que está saindo de uma rede local. O método de validação do endereçamento MAC e IP é desenvolvido com base na solução proposta por [Barbhuiya et al. 2013], destacando os algoritmos VERIFY_IP-MAC() e RESPONSE_ANALYSER(). Sua arquitetura global é baseada nas soluções propostas por [Yao et al. 2011] e por [Mowla et al. 2015], descartando a utilização do protocolo SAVI. Por fim, a implementação desta solução é baseada na solução proposta por [Yan et al. 2011], mas mitigará o tráfego de saída em vez do tráfego de entrada.

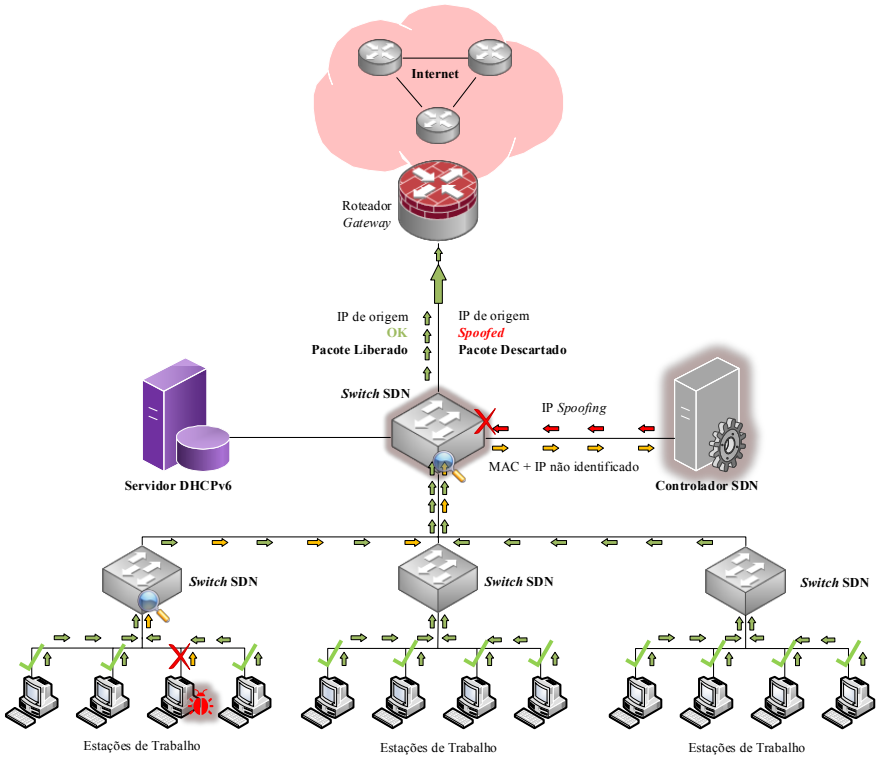

Figura 2. Infraestrutura e implementação da solução identificada.

A Figura 2 ilustra a implementação da solução em uma rede local. O *switch* com suporte à tecnologia SDN fica localizado entre o roteador (*gateway*) de borda e dos demais ativos da rede local. O controlador SDN encontra-se conectado neste *switch* para poder gerenciar o tráfego da rede. Todo o tráfego de saída será analisado pelo *switch* que analisará o endereço MAC e endereço IPv6 de origem de cada pacote que sair da rede. O *switch* compara o endereço MAC e o endereço IP através de sua tabela de fluxos. Caso estes endereços não estejam inseridos nesta tabela, o *switch* encaminha o pacote para o controlador SDN que, consequentemente, decide qual a ação a ser tomada sobre o respectivo pacote. O controlador, através do processo de validação de endereços, autoriza ou descarta o pacote através do *switch*, assim como atualiza a tabela de fluxos do equipamento.

4.3. Combatendo o IP *Spoofing*

A identificação do IP *Spoofing* é realizada através da comparação do endereço MAC e do endereço IP contido no campo "Endereço de Origem" (*Source Address*) do cabeçalho do protocolo IPv6 do respectivo pacote analisado. Ao receber o pacote, o controlador valida o endereço MAC, consultando a lista de endereços atribuídos na base de dados do servidor DHCPv6 e sua lista endereços IP atribuídos manualmente (*whitelist*). É importante

ressaltar que esta *whitelist* é uma forma alternativa que permite ao administrador inserir manualmente os endereços de rede e de MAC para liberar endereços e seus respectivos pacotes da rede.

Primeiramente a aplicação faz uma busca do endereço MAC em sua *whitelist*; caso seja encontrado e esteja atribuído o mesmo endereço IP do pacote analisado, o controlador atualiza a tabela de fluxos do *switch* e o autoriza a liberar o pacote.

Caso o endereço MAC não esteja inserido na *whitelist* ou a comparação com o endereço IP do pacote esteja errada, a aplicação consulta a base de dados do servidor DHCPv6 na tentativa de identificar a presença do endereço MAC. Caso o endereço seja localizado, ele é validado comparando o endereço IP do pacote com o endereço IP atribuído pelo servidor DHCPv6. Caso os dois endereços estejam em conformidade, o controlador atualiza a tabela de fluxos do *switch* e autoriza o repasse do pacote.

Caso o endereço MAC não esteja em conformidade com o endereço IP inserido na base do servidor DHCPv6 ou simplesmente os endereços MAC ou IP não sejam encontrados na base de dados do servidor DHCPv6, o uso da técnica de IP *Spoofing* é identificado. Com isto, o controlador descarta esse pacote, assim como registra um evento (*log*) contendo o endereço de origem e o endereço de destino do pacote, emitindo um alerta ao administrador da rede.

5. Conclusão e Trabalhos Futuros

Através do estudo realizado, foi possível compreender o funcionamento da técnica de IP *Spoofing*, entender os principais protocolos envolvidos, assim como identificar a preocupação e como a comunidade acadêmica está tratando o tema. Por fim, um novo e possível método para mitigar e combater o IP *Spoofing* foi delineado. Como trabalho futuro, este método deverá ser experimentado em uma rede real, validando sua teoria.

Referências

Barbhuiya, F., Bansal, G., Kumar, N., Biswas, S., and Nandi, S. (2013). Detection of neighbor discovery protocol based attacks in IPv6 network. *Networking Science*, 2(4):91–113.

Bellovin, S. M. (1989). Security Problems in the TCP/IP Protocol Suite. *SIGCOMM Comput. Commun. Rev.*, 19(2):32–48.

Deering, S. (1991). ICMP Router Discovery Messages. RFC 1256, Internet Engineering Task Force.

Feamster, N., Rexford, J., and Zegura, E. (2014). The road to SDN: An intellectual history of programmable networks. *SIGCOMM Comput. Commun. Rev.*, 44(2):87–98.

Kreutz, D., Ramos, F., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., and Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76.

Kurose, J. F. and Ross, K. W. (2006). *Redes de Computadores e a Internet: uma abordagem top-down*. Addison Wesley, São Paulo, third edition.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). Openflow: Enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74.

Morris, R. T. (1985). *A Weakness in the 4.2BSD Unix TCP/IP Software*.

Moura, G., Sadre, R., and Pras, A. (2014). Bad Neighborhoods on The Internet. *Communications Magazine, IEEE*, 52(7):132–139.

Mowla, N., Doh, I., and Chae, K. (2015). An efficient defense mechanism for spoofed IP attack in SDN based CDNi. In *Proc. of the International Conference on Information Networking (ICOIN)*, pages 92–97.

Mukaddam, A., Elhajj, I., Kayssi, A., and Chehab, A. (2014). IP Spoofing Detection Using Modified Hop Count. In *Proc. of 28th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, pages 512–516.

Narten, T., Nordmark, E., Simpson, W., and Soliman, H. (2007). Neighbor Discovery for IP version 6 (IPv6). RFC 4861, Internet Engineering Task Force.

Plummer, D. (1982). Ethernet Address Resolution Protocol Or Converting Network Protocol Addresses. RFC 826, Internet Engineering Task Force.

Postel, J. (1981). Internet Protocol. RFC 0791, Internet Engineering Task Force.

Tanase, M. (2003). IP Spoofing: An Introduction. Disponível em: <http://www.symantec.com/connect/articles/ip-spoofing-introduction/>. Acesso em: abr. 2015.

Wu, J. Bi, J., Bagnulo, M., Berker, F., and Vogt, C. (2013). Source Address Validation Improvement (SAVI) Framework. RFC 7039, Internet Engineering Task Force.

Yan, Z., Deng, G., and Wu, J. (2011). Savi-based IPv6 source address validation implementation of the access network. In *Proc. of Computer Science and Service System (CSSS), 2011 International Conference on*, pages 2530–2533.

Yao, G., Bi, J., and Xiao, P. (2011). Source address validation solution with openflow/nox architecture. In *Proc. of Network Protocols (ICNP), 2011 19th IEEE International Conference on*, pages 7–12.