Ferramentas para Prevenção e Monitoramento de Ataques DoS em Redes IPv6

Christopher Breno Coelho Xavier, José Fernando Almeida Teobaldo Júnior, David Teixeira de Masin

Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE
Graduando em Tecnologia em Telemática
Avenida 13 de Maio, 2081, Benfica
Fortaleza/CE, Brasil, 60040-531
{christopherbreno}@gmail.com, {jfernandoalmeidatj}@gmail.com, {divield}@gmail.com

Fernando Ramiro Lavor Chacon e Silva

Centro Universitário Estácio do Ceará
Graduando em Telemática
Rua Vicente Linhares, 308, Aldeota
Fortaleza/CE, Brasil, 60135-270
{fernando.ramiro.lavor}@gmail.com

Resumo - O rápido aumento no número de usuários das redes de computadores logo fez transparecer que o protocolo IPv4 teria que ser substituído. A expansão das redes logo demandaria um maior espaço de endereçamento e novas funcionalidades também teriam que ser implantadas para atender melhor essa nova realidade. O IPv6 foi desenvolvido visando resolver os problemas presentes no antigo protocolo, e sua implantação mostrou que algumas deficiências foram sanadas, mas que outras surgiram. Inicialmente, iremos abordar as principais características do novo protocolo e algumas de suas novas funcionalidades, para, após essa fundamentação, focarmos nas falhas de segurança do IPv6 e destacarmos, especificamente, as que possibilitam ataques de negação de serviço. Para finalizar mostraremos algumas ferramentas que trabalham em cima desse tipo de ataque e como estas atuam para prevenir e solucionar o problema.

Abstract – The quick increasing in the number of network users shows that the IPv4 should be replaced. The networks expansion demands a bigger address space and also new functions should be implanted to provide a better way to this new reality. The IPv6 was developed to resolve the current problems on the old protocol, and its implementation shows that some deficiencies were solved, but others problems appeared. Firstly, we will show the main characteristics of the new protocol and some of its new functions to, after this grounding, focusing on the security failures of IPv6 and detach the failures that enable a denial of service attacks. Finally, we will show some tools that work on this kind of attack and how this tools operate to prevent and solve the problem.

I. INTRODUÇÃO

No início da popularização das redes de computadores já era possível perceber que, em um curto prazo de tempo, os endereços IPv4 não seriam capazes de suprir a demanda. Desde então, várias técnicas começaram a ser criadas para prolongar a existência do protocolo, dentre as quais podemos destacar o DHCP e os endereços de IP privados declarados na RFC 1918. Entretanto a utilização destas técnicas se caracterizou apenas como medida paliativa, isto é, apenas para protelar a utilização do antigo protocolo, pois não solucionavam os problemas apresentados por este. Consequentemente a definição de um novo protocolo tornou-se algo inevitável [1].

Através do uso de técnicas de transição como o tunelamento ou a pilha dupla, a implantação do protocolo IPv6 está acontecendo gradativamente e funcionando concomitantemente com o IPv4.

Apesar da implantação do novo protocolo de internet solucionar vários dos problemas presentes na antiga versão, sua utilização gerou algumas falhas de segurança. Estas surgiram por causa das novas funcionalidades, pela má

implementação do protocolo, pela utilização do MAC na definição do IP ou pelas próprias técnicas de transição.

Visando a resolução dessas fragilidades na segurança do IPv6, além de algumas recomendações propostas, foram desenvolvidas aplicações que auxiliam na manutenção da integridade dos sistemas computacionais. Na sequência do artigo abordaremos algumas destas soluções, destacando, para este fim, as principais ferramentas presentes no mercado.

II. O NOVO PROTOCOLO DE INTERNET

Surgindo para resolver o problema de esgotamento de endereços IP, o IPv6 tem como principal finalidade aumentar o espaço de endereçamento. O IPv4 tem um espaço de endereçamento de 32 bits, que possibilita 4.294.967.296 endereços diferentes. Já o IPv6 possui um espaço de endereçamento de 128 bits, que possibilita um total de 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços diferentes, representando aproximadamente 79 octilhões de vezes o quantitativo de endereços IPv4 [2].

O modo como é apresentado o endereçamento do novo protocolo é bastante diferente em relação ao modo usado em sua versão anterior. Os 128 bits de endereçamento do IPv6 são representados em hexadecimal (0-F), organizados em grupos de 16 bits e separados por dois pontos (:). Por ser muito extenso, existem regras de abreviação para facilitar a escrita desses endereços. Utilizando o endereço 2001:0DB8:0000:0000:ABCD como exemplo, pode-se: omitir os zeros a esquerda de cada bloco de 16 bits (2001:DB8:0:0:ABCD:0:0:21) e substituir grupos sequentes de zeros por "::" (2001:DB8::ABCD:0:0:21 ou 2001:DB8:0:0:ABCD::21), possível apenas uma única vez na representação do endereço [3].

Além do aumento do espaço de endereçamento para 128 bits, foram agregadas ao IPv6 novas funcionalidades e algumas funcionalidades já existentes foram aprimoradas.

A. Endereço Unicast

É um endereço que identifica uma única interface. No novo protocolo de internet existem alguns tipos importantes de endereços *unicast*, como o *Global Unicast* e o *Link Local*. O *Global Unicast* é semelhante aos endereços públicos do IPv4 e é roteável na internet. O *Link Local* é um endereço utilizado apenas no enlace onde a interface está conectada, atribuída automaticamente e utilizando o prefixo FE80::, com 64 bits reservados para identificação da rede [1].

B. Endereço Anycast

É um endereço que identifica um conjunto de interfaces, onde o pacote enviado é recebido pela interface do conjunto mais próxima da origem. São atribuídos na mesma faixa dos endereços *unicast*, onde um endereço *unicast* configurado em mais de uma interface torna-se um endereço *anycast* [1].

C. Endereço Multicast

É um endereço que identifica grupos de interfaces, e pacotes enviados por esse endereço são recebidos por todas as interfaces que pertencem ao grupo. No IPv6, são identificados através do bloco FF00::/8, onde FF é o prefixo que identifica o endereço *multicast* [1].

Quando é atribuído um endereço *unicast* ou *anycast* a uma interface, ela passa a fazer parte de um grupo *multicast* identificado por um endereço *multicast solicited-node*, utilizado no protocolo de descoberta de vizinhança para resolver o endereço MAC de uma interface do enlace, agregando os 24 bits menos significativos do endereço da interface ao prefixo FF02::1:FF00:0000/104 [1].

Tabela I - Endereços *Multicast* em um Enlace.

Descrição	Endereço
All-nodes (Todos os nós)	FF02::1
All-routers (Todos os roteadores)	FF02::2
Solicited-node	FF02::1:FFXX:XXXX

III. DESCOBERTA DE VIZINHANÇA

O protocolo de descoberta de vizinhança (NDP) foi adicionado ao IPv6 para tornar mais dinâmico alguns métodos de configuração de rede, como encontrar roteadores vizinhos e detectar endereços duplicados na rede. Atua na autoconfiguração de nós e na transmissão de pacotes [4].

Ele foi incluído no protocolo ICMPv6, que é a versão nova do protocolo ICMP que funciona no IPv4. Esse protocolo foi

desenvolvido para atuar em conjunto com o IPv6 e é de extrema importância para sua arquitetura. Sua implementação deve ser feita em todos os nós da rede que utilizam o IPv6. No ICMPv6 também foram inclusas funções de protocolos integrantes do IPv4, como o ARP, RARP e IGMP, e funciona inteiramente na camada de rede. Portanto, deve-se tomar cuidado para não bloquear esse protocolo, pois integra funções extremamente básicas do IPv6 [1].

O NDP foi construído com base em cinco mensagens para realizar as suas funções: *Router Solicitation*, *Router Advertisement*, *Neighbor Solicitation*, *Neighbor Advertisement* e *Redirect*.

A. Router Solicitation

Uma mensagem *Router Solicitation* é enviada por um dispositivo para que os roteadores da rede se apresentem, recebendo como resposta uma mensagem *Router Advertisement*. Essa mensagem solicita apenas que um roteador envie uma resposta rapidamente. O endereço de destino da mensagem deve ser *All-router multicast Group (FF02::2*), já que não se sabe as informações dos roteadores, e o endereço de origem dever ser o *unicast link local* ou um endereço não especificado (::) [4].

B. Router Advertisement

A mensagem *Router Advertisement* é difundida pelo roteador periodicamente ou enviada em resposta à mensagem *Router Solicitation*, enviando dados para a autoconfiguração dos nós. Tem como endereço de destino da mensagem o *All-nodes multicast Group* (FF02::1), quando a mensagem é difundida para todos os nós do enlace, ou o endereço *unicast link local* da interface que fez a solicitação. O endereço de origem é sempre o *unicast link local* do roteador [4].

C. Neighbor Solicitation

Esse tipo de mensagem é utilizado em três casos e recebe como resposta uma mensagem *Neighbor Advertisement*. No primeiro caso, realiza uma função semelhante a do ARP no IPv4, ou seja, a descoberta do endereço físico de uma interface utilizando um endereço lógico. No segundo caso, realiza testes de acessibilidade dos nós do enlace. E o terceiro caso seria identificar endereços IPv6 duplicados no enlace, utilizado com a finalidade de descobrir se o endereço que a interface solicitante deseja configurar não está configurado em qualquer outra interface do enlace [4].

O endereço de destino desse tipo de mensagem seria o *Solicited-node* (FF02::1:FFXX:XXXX), em casos de descoberta de endereço físico e detecção de endereços duplicados, ou seria um endereço *unicast link local* em verificações de acessibilidade.

O endereço de origem dessa mesma mensagem poderia ser o endereço *unicast link local* da interface, para descoberta de um endereço físico ou verificação de acessibilidade, ou não especificado (::) para verificação de endereços duplicados.

D. Neighbor Advertisement

Pode ser enviada espontaneamente por determinada interface em virtude de alguma mudança nas características de rede do dispositivo ou em resposta a uma mensagem *Neighbor Solicitation*. É utilizada também nos mesmos três casos da mensagem citada anteriormente [4].

Para anunciar alguma mudança ou para responder mensagens com endereço de origem não especificado, o endereço de destino será o *All-nodes* (FF02::1). No caso de respostas a mensagens que possuem um endereço de origem, o endereço de destino será o endereço *unicast link local* especificado na mensagem de *Neighbor Solicitation* que está sendo respondida.

O endereço de origem será o endereço *unicast* da interface que está enviando a mensagem.

E. Redirect

Tem como função informar aos nós do enlace que há rotas melhores para o encaminhamento de pacotes.

IV. ATAQUES SOB O PROTOCOLO

O protocolo de descoberta de vizinhança tornou mais simples o uso do IPv6, mas também deixaram falhas que podem gerar ataques de negação de serviço (DoS) no protocolo. Esses ataques podem ser feitos através da falsificação das mensagens utilizadas no NPD, ditas anteriormente.

Na Fig. 1, supomos que a interface "A" deseja configurar o endereço 2001:DB8::1 e a interface "B" será a que realizará o

ataque de DoS. A interface "A" envia uma mensagem *Neighbor Solicitation* a todas as interfaces do enlace tendo como origem um endereço não especificado e como destino o endereço *Solicited-node*. A interface "B" receberá a mensagem da interface "A" e responderá com uma falsa mensagem *Neighbor Advertisement* para todas as interfaces do enlace, contendo como endereço de origem o mesmo endereço que a interface "A" desejava configurar, ou seja, a interface "B" informa que está configurada com esse endereço mesmo que não esteja. Isso fará com que a interface "A", ou qualquer outra interface do enlace que deseja conectar-se a rede, nunca consiga um IP válido.

Fig. 1 - Exemplo de Detecção de Endereços Duplicados

Na Fig. 2, mostramos as mensagens *Router Solicitation* e *Router Advertisement*, onde a primeira é enviada pelas interfaces do enlace solicitando a presença de um roteador e a segunda é enviada pelo roteador para todas as interfaces do enlace.

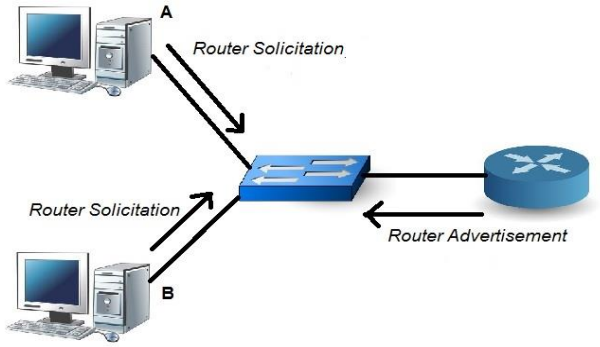

Fig. 2 - Mensagens *Router Solicitation* e *Router Advertisement*

Outro problema se dá quando um dispositivo que não é um roteador falsifica uma mensagem *Router Advertisement* para que se torne o roteador principal do enlace ou anunciar um roteador falso. Isso pode gerar negação de serviço para os demais dispositivos do enlace, pois os pacotes encaminhados para o falso roteador seriam descartados. Com isso, nenhum dispositivo do enlace conseguiria se conectar.

V. FERRAMENTAS DE SEGURANÇA

Para solucionar os problemas mencionados no tópico anterior e para proporcionar mais segurança para os usuários, surgiram algumas ferramentas para monitorar e prevenir ataques de DoS sob o protocolo de descoberta de vizinhança.

A. NDPMon

O NDPMon é um software, usado em redes IPv6, que monitora pacotes ICMPv6. Ele é utilizado em uma rede local para buscar irregularidades nas mensagens utilizadas no protocolo de descoberta de vizinhança, principalmente na autoconfiguração de endereços dos nós do enlace. Caso o software encontre alguma anomalia, serão gerados logs do sistema ou o usuário receberá um alerta pelo e-mail [5].

No caso mostrado na Fig. 1, o NDPMon seria uma boa solução do problema, pois sempre que esse problema acontecesse o usuário seria alertado sobre um possível ataque DoS.

O NDPMon age apenas no monitoramento da rede e não é capaz de evitar os ataques, apenas emitindo alertas para que o administrador da rede tome providências.

B. Router Advertisement Guard

O RA Guard (*Router Advertisement Guard)* é uma solução prevista na RFC 6105, onde um switch é configurado para impedir a passagem de mensagens *Router Advertisement* vindas de portas em que não há um roteador conectado. Para que isso seja possível essa função deve ser implementada no switch [6].

Na Fig. 3, mostramos o funcionamento do RA Guard, onde mensagens de *Router Advertisement* vindas de qualquer outra porta que não seja a porta "A" são descartadas.

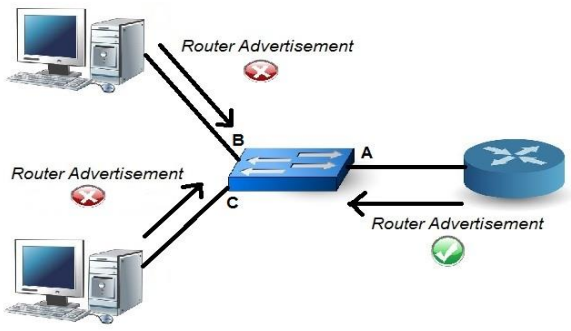

Fig. 3 - Utilização do RA Guard

Essa solução previne que dispositivos que não são roteadores falsifiquem mensagens de *Router Advertisement* e consequentemente causem negação de serviço aos demais dispositivos do enlace.

IV. CONCLUSÃO

Apesar do pouco tempo de uso, o IPv6 já mostrou alguns problemas com relação a segurança do protocolo. As ferramentas tratadas neste artigo ajudam a proteger os usuários contra ataques de negação de serviço, através do monitoramento de irregularidades em mensagens recebidas pela interface de rede e da utilização de um switch para descarte de mensagens de dispositivos tentando se passar por roteadores. A utilização dessas ferramentas será bastante necessária em redes locais, principalmente em redes com muitos dispositivos conectados, para que os usuários obtenham conexão com a Internet dentro destas redes.

REFERÊNCIAS

[1] NIC.br. "Curso IPv6 Básico". Publicação Ceptro.br, 2012.

[2] http://ipv6.br/. Em 15/09/2013, 11:25h.

[3] http://tools.ietf.org/html/rfc3513. Em 17/09/2013, 23:20h.

[4] http://tools.ietf.org/html/rfc4861. Em 18/09/2013, 22:34h.

[5] http://ndpmon.sourceforge.net/. Em 18/09/2013, 01:40h.

[6] http://tools.ietf.org/html/rfc6105. Em 21/09/2013, 21:57h.