

RAT: Implementação de um Serviço de Rastreamento de Pacotes*

Marcelo D. D. Moreira¹, Gustavo L. Coutinho¹,
Igor M. Moraes¹, Rafael P. Laufer² e Otto Carlos M. B. Duarte¹

¹Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro (UFRJ)

²Computer Science Department
University of California, Los Angeles (UCLA)

{marcelo,gustavo,igor,otto}@gta.ufrj.br, rlaufer@cs.ucla.edu

Abstract. *This paper presents the deployment of an effective IP traceback system against denial-of-service (DoS) attacks. The RAT system uses a new technique based on a data structure called Generalized Bloom Filter in order to trace IP packets back to its true source. The system was deployed in the Linux kernel and installed in personal computers working as routers. Experimental results show that the RAT system can trace in less than one second the real source of a single IP packet without any storage in the network infrastructure.*

Resumo. *Este artigo apresenta a implementação de um sistema de rastreamento eficaz contra ataques de negação de serviço. O sistema RAT (Rastreamento de ATAques) utiliza uma nova técnica para rastrear pacotes IP baseada em uma estrutura de dados denominada Filtro de Bloom Generalizado. O sistema foi implementado no núcleo (kernel) do sistema operacional Linux e instalado em computadores pessoais usados como roteadores. Os resultados experimentais mostram que com o sistema RAT é possível determinar em menos de um segundo a origem e a rota de um único pacote sem armazenar informações na infra-estrutura de rede.*

1. Introdução

Ainda hoje, sítios da Internet estão expostos a ataques de negação de serviço. Este tipo de ataque visa tornar indisponíveis serviços providos pela vítima de forma a impedi-la de atender a usuários legítimos. Ataques de negação de serviço têm se mostrado eficientes e aparecido com frequência na mídia. Sítios conhecidos como Amazon, CNN, eBay, Microsoft e Yahoo já foram prejudicados e um relatório anual do CSI/FBI (*Computer Security Institute/Federal Bureau of Investigation*) [Gordon et al. 2005] informa que ataques de negação de serviço estão entre os incidentes de segurança que mais causam prejuízos às instituições americanas. Segundo um estudo recente [Moore et al. 2001], estima-se em mais de 4.000 o número de ataques de negação de serviço por semana, sendo que o domínio `.br` é o quarto mais atacado. O domínio brasileiro concentra cerca de 5 a 7% dos ataques de negação de serviço de toda a Internet.

*Este trabalho foi financiado com recursos do CNPq, CAPES, RNP/FUNTEL, FAPERJ e UOL.

Um dos fatores que contribuem para a ocorrência de ataques de negação de serviço é a falta de autenticação do protocolo IP (*Internet Protocol*). Como não há nenhuma verificação da fonte dos pacotes durante o encaminhamento, pacotes com endereço de origem forjado podem ser utilizados durante os ataques para manter o anonimato do atacante. Além disso, como os protocolos de roteamento se baseiam estritamente no endereço de destino, nenhuma informação acerca da origem dos pacotes é armazenada nos roteadores. Dessa maneira, torna-se impossível determinar a rota percorrida por um pacote recebido se não existir um sistema de rastreamento ativo e operacional durante o ataque.

No caso de ataques baseados em inundação da vítima, é até possível descobrir a origem dos pacotes, porém a solução atualmente empregada para o rastreamento desse tipo de ataque é bastante precária, pois se serve de procedimentos que requerem a intervenção humana. Assim, quando ocorre um ataque, a vítima entra em contato com o administrador da rede do seu provedor de serviço (*Internet Service Provider - ISP*) e solicita a determinação da rota de ataque. A vítima ou o administrador do ISP procura uma característica dos pacotes usados no ataque ou faz-se uma análise do tráfego no roteador associado à vítima. É feito um teste no roteador mais próximo da vítima para determinar por qual enlace o tráfego do ataque chega a esse último roteador. Uma vez determinado o enlace correto, o procedimento é repetido no roteador localizado na outra extremidade do enlace. Depois, salto-a-salto, este processo é repetido até que seja determinado o roteador de onde parte o ataque. Em alguns casos, é necessária a interação entre provedores de serviço, o que torna o processo lento. Além disso, esse procedimento não é automatizado, depende da cooperação de outros operadores de rede e o ataque precisa ser suficientemente longo para permitir o rastreamento completo, não sendo possível realizá-lo após o término do ataque.

Devido a essa dificuldade dos administradores de rede em descobrir a origem de pacotes IP, sistemas de rastreamento foram propostos e alguns deles são apresentados na Seção 2. O rastreamento de pacotes IP [Savage et al. 2001] surgiu com o objetivo de identificar a verdadeira origem e a rota percorrida pelo tráfego de ataque. A partir de pacotes recebidos pela vítima, deseja-se encontrar quem realmente os enviou, de forma a interromper o ataque e a aplicar punições para inibir futuros ataques. Dessa maneira, redes que possuem esse tipo de serviço observam um incremento significativo de segurança.

Os autores em um trabalho anterior [Laufer et al. 2005c] apresentam um sistema de rastreamento de pacotes IP denominado RAT (Rastreamento de Ataques). Este sistema é capaz de determinar a origem e a rota percorrida por todo pacote recebido pela vítima sem armazenar estado na infra-estrutura de rede. O sistema de rastreamento é baseado na marcação de pacotes. A idéia é que cada roteador insira uma informação que o identifique no pacote de forma que a vítima consiga reconstruir a rota de ataque posteriormente. O objetivo final é que a vítima seja capaz de rastrear o atacante a partir de um único pacote de ataque. Tal vantagem é necessária para o rastreamento de ataques de negação de serviço constituídos por um único pacote. É introduzida também uma nova estrutura de dados denominada Filtro de Bloom Generalizado (FBG). Essa estrutura é adicionada a cada pacote IP e é a responsável por armazenar os endereços IP dos roteadores atravessados de forma compacta. Outras vantagens principais surgem da adoção desta nova estrutura para armazenar os endereços dos roteadores, como a rapidez com que cada roteador atravessado realiza a atualização e a segurança contra a burla do atacante. O presente

artigo apresenta a implementação deste sistema de rastreamento, detalhando a marcação dos pacotes, a reconstrução de rota, a ferramenta de geração de pacotes e os resultados experimentais obtidos. A partir de um único pacote, o sistema implementado é capaz de identificar a verdadeira origem de um atacante e reconstruir rotas de até 7 saltos em menos de um segundo.

O artigo está organizado da seguinte forma. Na Seção 2 são apresentados os principais sistemas de rastreamento encontrados na literatura. A Seção 3 descreve os procedimentos que compõem o sistema de rastreamento proposto. A implementação do sistema RAT é apresentada na Seção 4. Ainda na mesma seção, é descrita a implementação de uma ferramenta para geração de pacotes IP com endereço de origem forjado. A Seção 5 discute os resultados experimentais obtidos a partir da implementação do sistema. Por fim, a Seção 6 conclui este trabalho e apresenta as suas futuras direções.

2. Sistemas de Rastreamento de Pacotes

Os sistemas de rastreamento de pacotes IP podem ser divididos em duas categorias: sistemas de rastreamento sem estado e sistemas de rastreamento baseados em auditoria [Laufer et al. 2005b]. Os sistemas de rastreamento sem estados não armazenam nenhum tipo de informação sobre a origem dos pacotes nem na infra-estrutura da rede, nem nas estações finais. Neste caso, toda a atividade de rastreamento se baseia no estado da rede no momento em que o rastreamento é feito. Por outro lado, os sistemas baseados em auditoria armazenam de alguma forma, durante o processo de envio dos dados, informações que podem ser úteis para reconstruir o caminho real percorrido pelos pacotes.

Um sistema pioneiro de rastreamento sem estado [Burch e Cheswick 2000] foi proposto por Burch e Cheswick. O sistema tem como objetivo detectar a origem de fluxos de ataque através de uma técnica de teste de enlaces. A técnica se baseia na inundação sistemática dos enlaces a fim de identificar aquele pelo qual chega o tráfego de ataque, que será o enlace cuja inundação causar uma queda no recebimento do tráfego de ataque. Esse processo é repetido recursivamente, a partir do roteador mais próximo à vítima, até a fonte do ataque. Esta técnica presume um conhecimento do mapa topológico da rede e que os nós estejam dispostos a sofrer curtas inundações. Além disso, o ataque deve ser suficientemente longo a fim de que se possa chegar até a sua verdadeira origem. Outra desvantagem é que o sistema pode não ser capaz de rastrear ataques distribuídos ou de pequenos fluxos, uma vez que a variação de fluxo observada nesses casos pode não ser detectada.

Savage *et al.* introduzem um sistema baseado em auditoria, onde a informação necessária para o rastreamento é armazenada na vítima [Savage et al. 2001]. É suposto que ataques são constituídos por um grande número de pacotes. Assim, os dados de auditoria podem ser distribuídos dentre os diversos pacotes de ataque. A proposta se baseia na marcação probabilística de pacotes, na qual os roteadores inserem de forma compacta, em campos raramente usados do cabeçalho IP, informações que posteriormente a vítima poderá usar para reconstruir a rota de ataque. Embora inovadora, a proposta necessita de um alto poder computacional durante a reconstrução da rota de ataque pela vítima e gera diversos falsos positivos mesmo em ataques distribuídos de pequeno porte [Song e Perrig 2001]. Análises realizadas por Park e Lee mostram ainda a vulnerabilidade do sistema para o caso do atacante forjar as marcações do cabeçalho IP do

pacote [Park e Lee 2001].

Outro método baseado em auditoria [Bellovin et al. 2003] foi proposto por Bellovin *et al.*. Nessa proposta, cada roteador envia probabilisticamente dados de auditoria através de pacotes ICMP (*Internet Control Message Protocol*) para a vítima. Após recebido um número suficiente de pacotes, a origem do tráfego de ataque pode ser identificada. Além disso, é proposta a utilização de uma infra-estrutura de chaves públicas a fim de garantir a autenticação das mensagens de rastreamento e, assim, evitar que o atacante burle o sistema enviando pacotes ICMP forjados. Em uma extensão desse trabalho [Mankin et al. 2001], novos conceitos como utilidade e valor das mensagens de rastreamento são introduzidos, assim como uma proposta para melhorá-los.

Os sistemas de rastreamento baseados em auditoria também podem armazenar informações na própria infra-estrutura de rede. Uma solução simples usando essa abordagem seria coletar dados de auditoria registrando os pacotes que atravessam os roteadores da rede e, então, utilizar técnicas de mineração para determinar, a partir dos dados coletados, a rota de cada pacote [Stone 2000]. Esse método é capaz de rastrear pacotes mesmo após o término do ataque e, além disso, é eficiente inclusive quando o tráfego de ataque é pequeno. Porém, recursos excessivos são exigidos tanto para armazenagem quanto para a mineração dos dados. Além disso, a invasão de um roteador acarretaria ainda em problemas de privacidade, uma vez que ele contém informações sobre todos os pacotes roteados.

Uma alternativa para reduzir a armazenagem de um grande volume de informações é utilizar um filtro de Bloom [Bloom 1970]. Snoeren et al. propõem um mecanismo que possui a vantagem de rastrear um único pacote IP que tenha passado na rede sem a necessidade de se armazenar todo o tráfego roteado [Snoeren et al. 2002]. Para isso, são usados filtros de Bloom em dispositivos acoplados aos roteadores que armazenam os pacotes roteados de forma compacta. Periodicamente, os filtros saturados são armazenados para futuras requisições e trocados por novos filtros vazios. Para mais tarde determinar se um pacote passou pelo roteador, o seu filtro simplesmente é verificado. Cada roteador pode realizar um processo repetitivo para reconstruir o caminho do pacote até a sua verdadeira origem. Porém, mesmo com o uso de filtros de Bloom, tal sistema exige uma alta capacidade de armazenamento. Melhorias propostas por Li *et al.* diminuem o espaço necessário para o armazenamento embora a capacidade de se rastrear um único pacote seja comprometida [Li et al. 2004].

3. O Sistema de Rastreamento RAT

O RAT (Rastreamento de ATaques) é um sistema de rastreamento baseado na marcação de pacotes. Um sistema deste tipo é composto por dois procedimentos distintos: a marcação de pacotes e a reconstrução de rota. A marcação de pacotes é o procedimento no qual cada roteador insere uma informação no pacote para identificar a sua presença na rota de ataque. Esta tarefa é realizada por todo roteador que o pacote atravessa. Dessa forma, ao receber um pacote, a vítima dispõe de informações suficientes para reconstruir a rota de ataque. Este procedimento é denominado reconstrução de rota e é realizado pela vítima em conjunto com os roteadores da rede. A seguir, os procedimentos de marcação de pacotes e reconstrução de rota do sistema RAT são brevemente explicados.

3.1. O Procedimento de Marcação de Pacotes

A maneira mais simples de se rastrear a origem de um pacote é fazer com que cada roteador insira o seu próprio endereço IP no pacote roteado. Entretanto, a adição de dados ao pacote durante o roteamento implica um acréscimo significativo de processamento e um aumento do tamanho do pacote a cada salto. Tal fato pode acarretar em fragmentações desnecessárias dos pacotes, o que pode sobrecarregar os roteadores.

No sistema RAT, cada pacote IP possui um campo para armazenar a rota tomada. Este campo tem tamanho fixo de forma a evitar a fragmentação do pacote. O procedimento de marcação é ilustrado na Figura 1, onde A representa o atacante, V representa a vítima e R_i representa os roteadores. Pouco antes de reencaminhar um pacote, cada roteador insere no pacote alguma informação que possa identificá-lo posteriormente. Desta forma, ao receber um pacote, a vítima dispõe de informações de todos os roteadores atravessados por aquele pacote. A partir desse ponto, a vítima inicia o procedimento de reconstrução da rota, explicado na Seção 3.2. O sistema proposto não armazena o endereço IP de cada roteador nos pacotes. De forma a economizar espaço e reduzir o processamento nos roteadores, um Filtro de Bloom Generalizado (FBG) [Laufer et al. 2005c] é usado em cada pacote para armazenar a rota tomada.

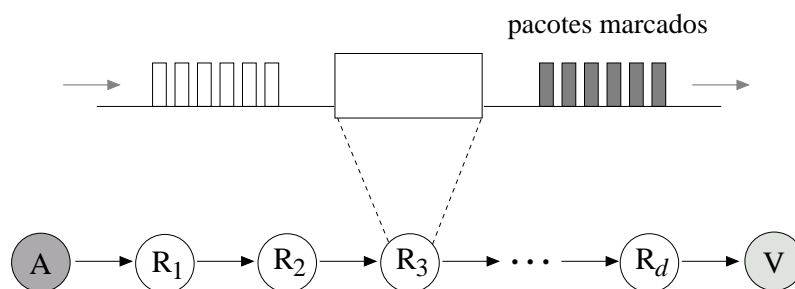


Figura 1. O procedimento de marcação de pacotes.

3.2. O Procedimento de Reconstrução de Rota

Conforme mencionado na seção anterior, a vítima recebe um Filtro de Bloom Generalizado (FBG) em cada pacote que representa a rota tomada por aquele pacote. Entretanto, os endereços dos roteadores não podem ser determinados diretamente pela vítima. Para verificar se um determinado roteador está presente na rota, é preciso testar se o seu endereço IP está contido no FBG. O procedimento de reconstrução é então iniciado. A Figura 2 ilustra a reconstrução de rota iniciada pela vítima V em direção ao atacante A . Inicialmente, o atacante envia um pacote para a vítima que passa por (R_5, R_4, R_2, R_1) . Ao receber o pacote de ataque, a vítima inicia o procedimento de reconstrução, testando a presença de R_1 no filtro do pacote recebido (1). Como R_1 é reconhecido, ele recebe o filtro de V e continua o procedimento. Assim, R_1 verifica a presença dos seus vizinhos R_2 e R_3 no filtro (2). Como somente R_2 é reconhecido, o filtro é então repassado somente para R_2 , que faz o mesmo procedimento com seu vizinho R_4 (3). O roteador R_4 verifica qual dos seus dois vizinhos R_3 e R_5 é reconhecido pelo filtro (4); somente R_5 é reconhecido. Finalmente, R_5 testa a presença de R_7 no filtro (5). Uma resposta negativa é retornada e o procedimento de reconstrução termina.

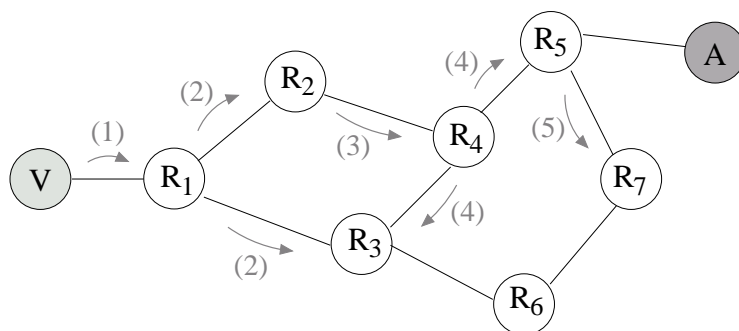


Figura 2. O procedimento de reconstrução de rota.

3.3. Aplicações

As potencialidades do sistema RAT podem ser exploradas em diversas aplicações. Essa subseção descreve, a partir das características do sistema RAT, algumas aplicações nas quais ele pode ser utilizado.

Em primeiro lugar, o sistema RAT mostra-se bastante eficaz contra ataques de negação de serviço, inclusive ataques distribuídos. Como o RAT é capaz de determinar a origem de todos os pacotes de ataque, todos os atacantes são facilmente detectados e contra-medidas podem ser adotadas de forma a interromper o ataque e impedir futuras investidas daquelas fontes.

A identificação da origem de ataques de negação de serviço é a grande motivação para o uso do sistema RAT, devido aos enormes prejuízos causados por este tipo de ataque. Porém, o sistema proposto não se restringe a essa aplicação. Uma vez que o sistema é capaz de determinar a rota completa percorrida, o RAT pode ser usado para outras aplicações. Por exemplo, o sistema RAT pode ser usado para determinar a topologia de uma rede e até mesmo da Internet, caso seja implementado em escala global.

O sistema proposto detecta fontes de tráfego com endereço forjado. Desse modo, nós maliciosos presentes na rede podem ser identificados ao realizarem qualquer tentativa de ataque, pois, ainda que falsifiquem o endereço de origem dos pacotes, são descobertos pelo sistema de rastreamento. Além disso, o administrador da rede poderia detectar máquinas invadidas ou infectadas por pragas virtuais ao realizarem atividades suspeitas. Dessa maneira, o serviço RAT não só impediria que a rede sofresse ataques de negação de serviço, mas também evitaria que nós da própria rede fossem utilizados como “zumbis” por pessoas mal-intencionadas.

Há ainda o caso em que não se trata de um nó malicioso, mas de fontes de tráfego que utilizam endereços de origem forjados para burlar o seu perfil de tráfego, firmado em um acordo de nível de serviço (*Service Level Agreement* - SLA) com um provedor. Por exemplo, um usuário poderia realizar transmissões de vídeo e voz com tráfego maior do que o acordado sem que lhe seja cobrada sobretaxa. Basta, para isso, enviar os pacotes de forma anônima. Numa rede na qual funcionasse o serviço RAT de rastreamento de pacotes esse tipo de ação seria detectado.

4. A Implementação do Sistema de Rastreamento

Tanto o procedimento de marcação de pacotes quanto o de reconstrução de rota devem ser implementados em todos os roteadores da rede. Por isso, a implementação

destes procedimentos se torna dependente do sistema operacional de cada roteador. Neste trabalho, considera-se o uso de roteadores executando o sistema Linux, distribuição Debian Sarge 3.1, com núcleo (*kernel*) 2.6.10. A seguir, é descrito como a rota percorrida é armazenada em um pacote, e apresentada a ferramenta usada para simular ataques de negação de serviço e as ferramentas que compõem o sistema RAT.

4.1. Armazenamento da Rota Percorrida

Para armazenar a rota percorrida, é preciso determinar um campo do cabeçalho IP para esta finalidade. Duas escolhas são geralmente adotadas. A primeira escolha é sobrecarregar os campos já existentes do cabeçalho IP para armazenar as informações da rota [Savage et al. 2001]. A desvantagem desta opção é que as funcionalidades providas pelo campo em questão são diretamente afetadas. Uma segunda opção é adicionar um campo ao cabeçalho IP. A desvantagem neste caso é o *overhead* adicional por pacote. Neste trabalho, foi escolhida a segunda opção de forma a não afetar outras funcionalidades do protocolo IP.

O campo adicional usado para o armazenamento da rota foi então definido como uma nova opção do protocolo IP. A Figura 3 ilustra a nova opção criada. O primeiro campo é formado por um octeto e é responsável por identificar os diversos tipos de opções existentes do protocolo IP. Para a nova opção criada, foi definido o número 0x99 como tipo. O segundo octeto define o tamanho da opção, incluindo o octeto do tipo, o próprio octeto do tamanho e os octetos dos dados. O terceiro campo contém os dados da opção. No caso do rastreamento, este campo é composto pelo Filtro de Bloom Generalizado, responsável por armazenar os roteadores atravessados.

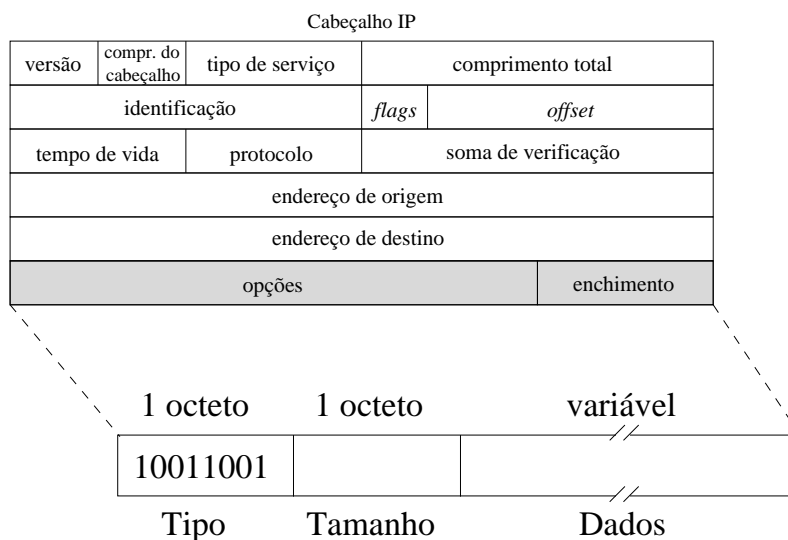


Figura 3. A nova opção criada para o protocolo IP (versão 4).

Apesar de definido como uma opção do protocolo IP nesta implementação, o campo usado para armazenar a rota percorrida deve ser obrigatório em qualquer pacote em um sistema real. Desta forma, qualquer pacote injetado na rede pode ser rastreado, se necessário.

4.2. A Ferramenta de Simulação de Ataques

Foi desenvolvida uma ferramenta usando-se a linguagem C para simular ataques de negação de serviço. A ferramenta gera pacotes ICMP *Echo Request* com a opção descrita na seção anterior incluída no cabeçalho do protocolo IP. Além disso, pacotes com endereço de origem forjado podem ser enviados de forma a simular um ataque de negação de serviço anônimo. Na implementação da ferramenta, utiliza-se a técnica de soquetes brutos (*sockets raw*) disponível no núcleo do Linux. Com essa técnica, é possível construir um pacote preenchendo manualmente todos os campos do cabeçalho IP, o que permite a criação de pacotes com qualquer endereço IP de origem. Usando esta ferramenta, é possível enviar pacotes forjados para a vítima de forma a testar o procedimento de marcação de pacotes e o procedimento de reconstrução.

4.3. O Procedimento de Marcação de Pacotes

A marcação de pacotes pode ser implementada no núcleo do sistema operacional ou como um aplicativo para o usuário. Neste trabalho, a implementação é feita no núcleo para garantir a eficiência do procedimento e torná-lo transparente para o usuário.

O procedimento de marcação de pacotes é realizado logo após a decisão de roteamento do pacote. Uma vez decidida a interface de saída do pacote, a marcação é então realizada de acordo com o endereço IP daquela interface. Neste trabalho, o procedimento de marcação de pacotes foi implementado no núcleo do sistema operacional Linux. Em linhas gerais, determinadas funções de roteamento foram alteradas de forma a lidar com a nova opção do protocolo IP criada. Os detalhes da implementação se encontram a seguir.

As modificações no núcleo se concentram basicamente nos arquivos `include/linux/ip.h` e `net/ipv4/ip_options.c`. No primeiro arquivo, foram apenas definidos alguns parâmetros novos, como o identificador da nova opção. No segundo arquivo, mais modificações foram realizadas. A primeira alteração é na função `ip_options_compile()`, responsável por identificar se um pacote IP recebido pelo roteador possui opções. Em caso positivo, cada opção é tratada de forma sequencial. Nesta função, adicionou-se uma condição para verificar se o pacote recebido contém a opção criada para o rastreamento. Uma vez detectada que a opção está presente, o pacote é tratado de acordo com o seu destino final. Caso o roteador não seja o destino final do pacote, então o pacote é reencaminhado e, antes de reencaminhar o pacote, o roteador deixa a sua marca na opção do rastreamento. Para isso, a função `ip_forward_options()` foi alterada. Esta função é a responsável por preencher as opções do pacote a ser encaminhado. À esta função foi adicionada a funcionalidade de atualizar o campo de dados da nova opção, onde se encontra o FBG. Caso o receptor do pacote seja o destinatário final, deve ser enviada uma resposta ao remetente com um pacote ICMP *Echo Reply* contendo o FBG recebido. Para tanto, a função `ip_options_echo()` foi alterada. A versão modificada do núcleo do sistema operacional foi denominada `rat-2.6.10`.

4.4. O Procedimento de Reconstrução de Rota

Para a realização do procedimento de reconstrução de rota, foi implementado um *daemon*, processo que roda no nível de usuário sem exigir interação com o mesmo. O programa, chamado de RATd, é capaz de reconhecer os pacotes ICMP *Echo Request* enviados pela ferramenta de simulação de ataques e realizar o procedimento de reconstrução

de rota. Ao final do processo, são informadas ao usuário a origem e a rota de ataque. A ferramenta RATd suporta dois modos de operação. O primeiro modo de operação é usado para iniciar o procedimento de reconstrução e o segundo modo para atender a pedidos de reconstrução de rota vindos de roteadores vizinhos.

O primeiro modo de operação permite que uma estação inicie o processo de reconstrução de rota. Para isso, ela deve receber um pacote originado pela ferramenta de simulação de ataques contendo a opção de rastreamento no seu cabeçalho. O programa, então, extrai o FBG do pacote e inicia os testes de acordo com o algoritmo explicado na Seção 3.2. Primeiro, a estação verifica se o endereço IP dos roteadores vizinhos está inserido no filtro recebido. Um pacote de reconstrução de rota é então enviado àqueles roteadores que forem reconhecidos como pertencentes ao FBG. Um pacote de reconstrução de rota consiste de um pacote ICMP contendo a opção do rastreamento e uma lista de endereços IP encapsulada no campo de dados do pacote. A lista de endereços IP contém os endereços dos roteadores por onde a reconstrução já passou e serve para evitar a formação de *loops* durante esse procedimento. Inicialmente, esta lista só contém o endereço da vítima, que é inserido quando o pacote é gerado. Após enviar os pacotes de reconstrução de rota, a ferramenta espera por um pacote de resposta contendo a rota de ataque no seu campo de dados.

O segundo modo de operação é comum a todos os roteadores da rede. Os roteadores que executam o RATd nesse modo de operação são capazes de atender pedidos de reconstrução de rota vindos de outros roteadores. Esses pedidos são feitos através de pacotes de reconstrução de rota. Ao receber um pacote desse tipo, o programa verifica a presença dos roteadores vizinhos no FBG extraído do cabeçalho do pacote recebido. Com exceção do roteador de origem, um novo pacote de reconstrução de rota é enviado a todos os roteadores vizinhos reconhecidos no FBG. Este pacote contém o FBG no cabeçalho e uma lista de endereços que é copiada do pacote recém-chegado. Os endereços contidos nessa lista são os dos roteadores da rota de ataque que está sendo reconstruída. Antes de enviar o pacote aos roteadores vizinhos, o roteador insere o seu endereço ao final da lista. Caso nenhum vizinho seja reconhecido como elemento do FBG, considera-se que o roteador em questão é a fonte do ataque. Sendo assim, um pacote de resposta contendo a lista completa dos integrantes da rota de ataque é enviado ao iniciador do processo de reconstrução.

É importante ressaltar que o atacante, de fato, não é encontrado. Esse é um problema inerente aos sistemas de rastreamento, decorrente da natureza do roteamento da Internet. Dessa maneira, o problema do rastreamento de pacotes [Savage et al. 2001] é determinar o primeiro roteador de ataque, considerado como o atacante em si. A partir deste ponto novos esforços são necessários para se determinar a verdadeira origem do ataque. Apesar disso, uma vez que o primeiro roteador de ataque foi identificado, pode-se filtrar o tráfego de ataque em um ponto próximo à vítima, evitando o consumo de recursos da rede e impedindo que os pacotes de ataque cheguem à vítima.

4.5. Roteadores Comerciais

É possível implementar o sistema RAT em roteadores comerciais, uma vez que o sistema não requer recursos excessivos de *hardware* e o processamento adicional exigido é reduzido. Isso é relevante devido às limitações de processamento dos roteadores na

Internet.

A implementação do procedimento de marcação em roteadores comerciais pode ser realizada com duas simples operações booleanas. Para atualizar o FBG é necessária uma operação OU bit-a-bit seguida de uma operação E bit-a-bit do FBG com registradores previamente configurados. Por outro lado, a implementação do procedimento de reconstrução de rota vai depender do sistema operacional utilizado pelo roteador. Como esta operação é pouco freqüente, a oferta do serviço de rastreamento não irá afetar o desempenho do roteador. Ademais, os resultados experimentais apresentados na próxima seção ratificam essa afirmação, uma vez que evidenciam a rapidez com que a reconstrução de rota é realizada.

4.6. A Instalação do Sistema

O primeiro passo para a instalação do sistema RAT numa rede é instalar o sistema operacional Linux com o núcleo `rat-2.6.10` em todos os roteadores da rede. O passo seguinte é a instalação da ferramenta RATd. Essa ferramenta deve ser instalada, configurada e iniciada em cada roteador. É importante ressaltar que este procedimento inicial só precisa ser realizado uma única vez. Após isso, os pacotes que trafegam na rede serão marcados automaticamente e a reconstrução de rota será iniciada sempre que houver solicitação de um usuário.

Após a etapa de instalação do sistema, é possível simular um ataque usando a ferramenta de simulação de ataques descrita na Seção 4.2. Para utilizar esta ferramenta, basta fornecer o endereço IP da vítima e o endereço IP de origem a ser usado no pacote de ataque. O pacote gerado então atravessa a rede e cada roteador da rota de ataque insere o seu endereço IP no FBG embutido no cabeçalho do pacote. Ao receber o pacote contendo um FBG como opção, o *daemon* RATd em execução na vítima inicia a reconstrução de rota e em seguida exibe o resultado do procedimento na tela.

5. Resultados Experimentais

Os experimentos realizados a partir da implementação do sistema têm como objetivo avaliar o desempenho do sistema em um ambiente controlado de testes. A rede de testes desenvolvida é composta por computadores pessoais configurados como roteadores e que rodam o sistema operacional Linux com o núcleo `rat-2.6.10` e a ferramenta RATd. Além disso, para aumentar o número de roteadores da rede de testes, utilizou-se máquinas virtuais.

Em um computador Pentium IV equipado com dois processadores Xeon de relógio igual 1,8 GHz e 1,0 GB de memória RAM foram instaladas as máquinas virtuais. Para cada máquina foram reservados 100 MB de memória RAM. Para criar as máquinas virtuais utilizou-se uma versão *shareware* da ferramenta VMware.

O roteamento na rede de testes é configurado manualmente. São criadas rotas estáticas para garantir que os pacotes de ataque atravessem corretamente os nós intermediários da rede até chegar à vítima. Para verificar o correto funcionamento do sistema, são gerados pacotes de ataque com endereços de origem reais. Comparou-se, então, o resultado produzido pelo sistema com o resultado apresentado pela ferramenta *ping* executada com a opção *-R* (*Record Route*). Ambos foram idênticos, o que comprova o funcionamento correto do RATd.

Um dos experimentos realizados tem como objetivo determinar o tempo gasto para a vítima identificar um atacante. O tempo de rastreamento é definido como o intervalo de tempo entre a chegada do pacote de ataque à vítima e o recebimento do pacote contendo a rota completa pela vítima. A Figura 4 mostra o tempo de rastreamento em função do tamanho da rota de ataque. Os resultados são obtidos levando-se em consideração um intervalo de confiança de 95% em relação à média das amostras, representado no gráfico por barras de erro verticais.

É possível observar que para encontrar um atacante distante 7 saltos da vítima, o sistema gasta menos de um segundo no cenário da rede de testes. Além disso, nota-se que à medida que o tamanho da rota de ataque cresce, o tempo de rastreamento cresce linearmente. Isto se deve ao fato de que a cada salto é acrescentado somente o tempo para que um roteador localize um vizinho presente no FBG e envie este filtro ao vizinho identificado.

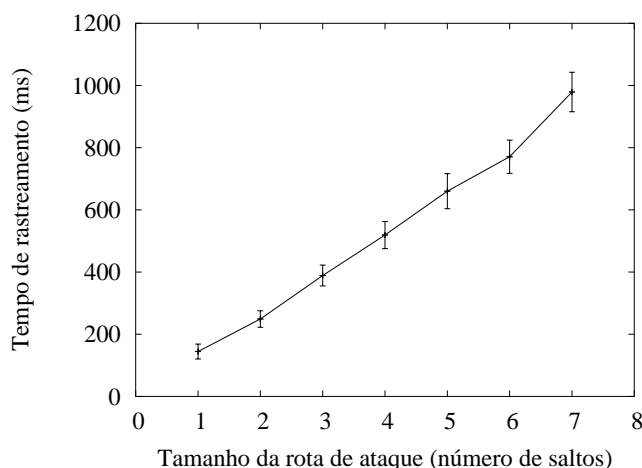


Figura 4. Tempo de rastreamento x tamanho da rota de ataque.

6. Conclusões

Este artigo apresentou a implementação de um novo sistema de rastreamento de ataques de negação de serviço. O sistema RAT é composto por dois procedimentos: a marcação de pacotes e a reconstrução de rotas. A marcação de pacotes foi implementada no núcleo do sistema operacional Linux, uma vez que exige a modificação de funções de encaminhamento dos pacotes IP. Já o procedimento de reconstrução de rota é feito por um *daemon* capaz de identificar pacotes contendo o Filtro de Bloom Generalizado como opção e determinar as suas verdadeiras origens.

Para avaliar o desempenho do sistema implementado, foi desenvolvida uma rede de testes. A realização de experimentos em um ambiente controlado possibilitou a verificação da eficácia do mecanismo proposto. Os resultados mostram que o tempo necessário para que o sistema proposto identifique um atacante distante até 7 saltos é menor do que um segundo. Vale ressaltar que este resultado é obtido considerando apenas um pacote e sem armazenar informações na infra-estrutura de rede, além de ser realizado através de máquinas virtuais que consomem mais recursos do que uma máquina real.

Futuramente, pretende-se implementar um procedimento de reconstrução aprimorado [Laufer et al. 2005a]. Tal procedimento sempre localiza a verdadeira rota de ata-

que. Pretende-se também modificar o RATd para que pacotes TCP sejam utilizados na reconstrução de rota, ao invés de pacotes ICMP.

Referências

- Bellovin, S. M., Leech, M. D. e Taylor, T. (2003). ICMP Traceback Messages. *Internet Draft: draft-ietf-itrace-04.txt*.
- Bloom, B. H. (1970). Space/Time Trade-offs in Hash Coding with Allowable Errors. *Communications of the ACM*, 7(13):442–426.
- Burch, H. e Cheswick, B. (2000). Tracing Anonymous Packets to their Approximate Source. Em *USENIX LISA'00*, páginas 319–327, Nova Orleans, LA, EUA.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W. e Richardson, R. (2005). *CSI/FBI Computer Crime and Security Survey*.
- Laufer, R. P., Velloso, P. B., de O. Cunha, D. e Duarte, O. C. M. B. (2005a). Um Procedimento Alternativo de Reconstrução de Rota para o Rastreamento de Pacotes IP. Em *XXII Simpósio Brasileiro de Telecomunicações - SBrT'05*, páginas 1013–1018.
- Laufer, R. P., Velloso, P. B. e Duarte, O. C. M. B. (2005b). Defeating DoS Attacks with IP Traceback. Em *IFIP Open Conference on Metropolitan Area Networks - MAN'2005*, páginas 131–148, Ho Chi Minh, Vietnã.
- Laufer, R. P., Velloso, P. B. e Duarte, O. C. M. B. (2005c). Um Novo Sistema de Rastreamento de Pacotes IP contra Ataques de Negação de Serviço. Em *XXIII Simpósio Brasileiro de Redes de Computadores - SBRC'2005*.
- Li, J., Sung, M., Xu, J. e Li, L. (2004). Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Theoretical Foundation. Em *Proceedings of the 25th IEEE Symposium on Security and Privacy*, Oakland, CA, EUA.
- Mankin, A., Massey, D., Wu, C.-L., Wu, S. F. e Zhang, L. (2001). On Design and Evaluation of “Intention-Driven” ICMP Traceback. Em *Proceedings of the IEEE ICCCN 2001 Conference*, Scottsdale, AZ, EUA.
- Moore, D., Voelker, G. e Savage, S. (2001). Inferring Internet Denial of Service Activity. Em *Proceedings of the 2001 USENIX Security Symposium*, páginas 9–22.
- Park, K. e Lee, H. (2001). On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack. Em *Proceedings of the IEEE INFOCOM 2001 Conference*, Anchorage, AK, EUA.
- Savage, S., Wetherall, D., Karlin, A. e Anderson, T. (2001). Network Support for IP Traceback. *IEEE/ACM Transactions on Networking*, 9(3):226–237.
- Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Schwartz, B., Kent, S. T. e Strayer, W. T. (2002). Single-Packet IP Traceback. *IEEE/ACM Transactions on Networking*, 10(6):721–734.
- Song, D. X. e Perrig, A. (2001). Advanced and Authenticated Marking Schemes for IP Traceback. Em *Proceedings of the IEEE INFOCOM 2001 Conference*, Anchorage, AK, EUA.
- Stone, R. (2000). CenterTrack: An IP Overlay Network for Tracking DoS Floods. Em *9th USENIX Security Symposium*, páginas 199–212, Denver, CO, EUA.