ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa **Inovadora em Engenharia de Computação e Comunicação**

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

Defesa contra ataques DDoS usando IP Falsificação de endereço

Archana .S. Pimpalkar1 ,AR Bhagat Patil2

Estudante de pós-graduação, Departamento de Tecnologia da Computação, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, Índia1

Professor, Departamento de Tecnologia da Computação, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, Índia2

RESUMO: Ataques de Negação de Serviço Distribuída (DDoS) são lançados por um grande número de hosts comprometidos para interromper os serviços de usuários legítimos. A defesa contra esses ataques é muito desafiadora porque a maioria dos invasores usa falsificação de endereço IP de origem para ocultar sua identidade, e esses pacotes de ataque aparecem para o servidor de destino como se tivessem vindo de um cliente legítimo. Neste artigo, é apresentado um mecanismo de defesa que classifica os pacotes como legítimos ou de ataque usando técnicas criptográficas e filtra os pacotes de ataque. Uma vez classificados, os pacotes de ataque são descartados no roteador de borda da rede de destino antes de chegar à vítima. O mecanismo é fácil de implementar, sem exigir restrições ou alterações adicionais nos protocolos de roteamento da Internet. A eficiência do algoritmo na identificação de pacotes de ataque falsificados é avaliada por experimentos de simulação no NS3.

PALAVRAS-CHAVE: Ataques DDoS, spoofing, detecção, defesa, criptografia, filtragem.

I. INTRODUÇÃO

Negação de Serviço Distribuída (DDoS) é um ataque lançado por um grande número de atacantes distribuídos de forma coordenada para interromper os serviços de clientes legítimos e consumir excessivamente os recursos do alvo, impedindo o servidor de responder a clientes legítimos. As ferramentas de ataque estão em constante evolução, mas não existem mecanismos de defesa eficazes o suficiente contra esses ataques. Os mecanismos de defesa devem ser capazes de classificar cada pacote que trafega pelo roteador como legítimo ou um ataque, e os pacotes identificados como pacotes de ataque não devem ser encaminhados ao alvo.
Isso pode evitar o ataque DDoS e economizar recursos valiosos do alvo.

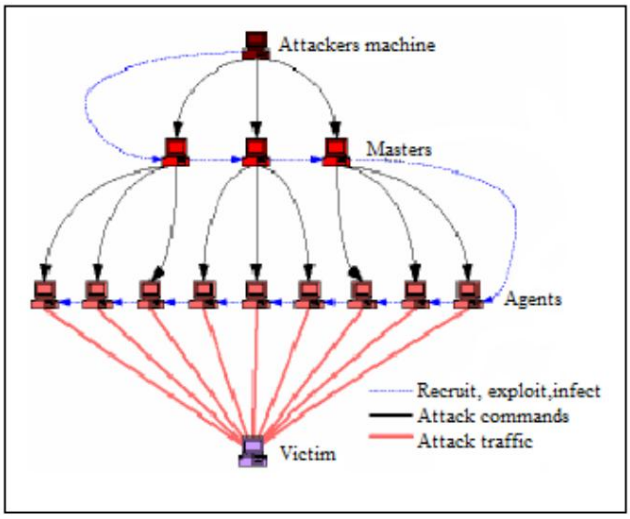

Fig. 1: Modelo de ataque DDoS.

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

Os ataques DDoS com falsificação de endereço IP de origem são de dois tipos. O primeiro é o ataque direto, no qual os invasores enviam pacotes malformados com endereço IP de origem falso, e o segundo é o ataque refletor, no qual o invasor envia um grande número de pacotes de ataque por meio de um grande número de hosts comprometidos na rede. Dessa forma, recursos da rede são desperdiçados no processamento desses pacotes de ataque, causando negação de serviço a clientes legítimos.

Ao encaminhar pacotes para o destino, frequentemente é usado apenas o endereço de destino, e o endereço de origem nunca é verificado. Os invasores aproveitam esse fato para lançar ataques usando falsificação do endereço IP de origem para se esconder.
sua identidade e evitando a possibilidade de serem pegos. Muitos mecanismos de defesa foram propostos contra a falsificação de endereços IP de origem, como filtragem de entrada, filtragem de pacotes baseada em contagem de saltos, aplicação da validade do endereço de origem, etc., que são úteis no controle de pacotes de ataque falsificados, mas a prevenção completa de ataques de endereços IP falsificados ainda é um problema desafiador.

Neste artigo, o mecanismo de defesa utiliza técnicas criptográficas para identificar pacotes de ataque com endereço IP de origem falso e descartá-los no roteador de borda do servidor de destino. O restante deste artigo está organizado da seguinte forma. Na Seção II, são apresentados resumidamente trabalhos recentes propostos para defesa contra ataques DDoS. Na Seção III, são apresentados mecanismos de defesa que utilizam técnicas criptográficas. Na Seção IV, é mencionado o pseudocódigo para o algoritmo, e a Seção V contém resultados de simulação, seguidos de uma conclusão na Seção VI.

II. TRABALHOS RELACIONADOS

Nesta seção, é apresentada uma revisão da literatura existente sobre mecanismos de defesa contra ataques de Negação de Serviço Distribuída.

S. Yu, et al. [1], propôs uma técnica de alocação dinâmica de recursos para proteger clientes individuais de nuvem durante ataques DDoS garantindo a qualidade do serviço durante o ataque. O ambiente de nuvem é capaz de controlar a alocação de recursos porque tem um grande número de recursos para alocar a usuário individual. A estratégia de alocação de recursos usada em nuvens desempenha um papel vital na mitigação do impacto do ataque, dando acesso aos recursos. No ambiente de nuvem o sucesso do ataque ou defesa depende de quem está detendo mais recursos, invasor ou usuário da nuvem. A alocação dinâmica de recursos extras previne a fome, defendendo assim contra ataques DDoS. Eles também apresentaram um modelo baseado em fila de alocação de recursos em vários cenários de ataque. Eles usaram conjuntos de dados do mundo real disponíveis em ataques DDoS para análise de alocação de recursos. Em cenário normal, o servidor virtual na nuvem tem sistema de prevenção de intrusão (IPS) para fins de segurança e fila que mantém a lista de pacotes recebidos. Durante a situação de ataque, um grande número de pacotes passa pela fila como botnets são usados para lançar ataques DDoS, surge a necessidade de duplicar os recursos para aumentar os sistemas de prevenção de intrusão. Isso é possível graças à alocação dinâmica de recursos. Eles avaliaram o desempenho do modelo desenvolvido por meio de simulações em situações normais e de ataque, utilizando a nuvem Amazon EC2 para obter os resultados.

B. Liu et al. [2] propuseram a filtragem de saída mútua para fornecer proteção contra ataques de inundação baseados em falsificação de IP, utilizando conjuntos de dados reais da internet para obter resultados de simulação. A lista de controle de acesso de sistemas autônomos (AS) é utilizada, contendo uma lista de regras para aplicação da filtragem de entrada/saída. Este método protege os sistemas que implantam o mecanismo, ao mesmo tempo em que impede que não implantadores o utilizem livremente. A filtragem sob demanda é fornecida e o registro global é mantido, contendo relacionamentos de peering e políticas dos deploradores. A taxa de falsos positivos é reduzida com o uso da filtragem de saída mútua.

Em [3], R. Maheshwari et al. implementaram a filtragem probabilística distribuída por contagem de saltos com base no tempo de ida e volta. O mecanismo foi implantado em um sistema de rede intermediário para maximizar a taxa de detecção de tráfego de ataque e minimizar o tempo computacional para filtragem de pacotes de ataque. Os resultados da simulação usando Matlab 7 mostraram até 99% de detecção de pacotes maliciosos. Isso é vantajoso para resolver problemas de esgotamento de recursos do host e congestionamento da largura de banda da rede.

Em [4], A. Compagno et al. apresentaram defesas contra ataques de negação de serviço distribuídos por inundação de inertes em redes de dados nomeados. A inundação de interesse requer recursos limitados para iniciar o ataque. A tabela de interesse pendente é mantida nos roteadores para evitar interesses duplicados. O framework Poseidon é introduzido para detecção e mitigação de inertes.

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

ataques de inundação. A avaliação da estrutura em um ambiente de simulação de rede usando NS3 mostrou que é possível utilizar até 80% da largura de banda disponível durante um ataque usando esta estrutura.

J. Francois et al. [5] propôs uma arquitetura colaborativa, FireCol, composta por sistemas de prevenção de intrusão no nível de provedores de serviços de Internet. Ela utiliza os anéis de sistemas de prevenção de intrusão ao redor de um host, visto que um único sistema de prevenção não é suficiente para defender-se de ataques DDoS baseados em inundação. Os ataques são detectados pela observação da Janela de detecção para descobrir o desvio do tráfego em relação ao padrão normal. Com base na porcentagem de desvio, os ataques são classificados como de baixo ou alto potencial. O sistema FireCol possui algumas regras definidas para assinantes que correspondem a um padrão de endereços IP. O processador de pacotes do sistema examina o tráfego de entrada e atualiza o contador e as frequências sempre que uma regra é correspondida. O gerenciador de métricas calcula entropias e entropias relativas.
O gerenciador de seleção verifica se a distribuição de tráfego está dentro do perfil. Uma pontuação é atribuída a cada regra selecionada com base em entropias e frequências. Por fim, o gerenciador de colaboração confirma o ataque de inundação se o tráfego gerado for superior à capacidade do cliente. A taxa de falsos positivos é baixa para este mecanismo, além de ser robusto, e a sobrecarga computacional e de comunicação é menor. Os resultados foram verificados usando conjuntos de dados reais de padrões de tráfego normais e de ataque.

F. Soldo, et al. [6], propuseram um método para bloquear o tráfego de ataque usando filtragem baseada na fonte. A lista de controle de acesso mantida no roteador usa algumas regras predefinidas para bloquear os endereços IP ou prefixos de tipo predefinido, mas o acesso a essa lista de controle de acesso é caro, pois é armazenado na memória endereçável de conteúdo ternário e consome mais espaço e energia. Portanto, eles sugeriram o método de agregação que usa filtragem de prefixos de origem em vez de endereços IP. Esse método tem algumas desvantagens, pois às vezes filtra o tráfego legítimo. Para superar esse problema, eles formularam a filtragem como um problema de otimização para bloquear os invasores com dano mínimo e filtros limitados.
Eles desenvolveram um algoritmo econômico e avaliaram os resultados da simulação usando logs do Dshield.org. Os resultados foram benéficos em comparação com a seleção de filtros não otimizados.

K. Verma et al. [7] propuseram um método para detectar e defender ataques de inundação UDP sob diferentes técnicas de falsificação de IP em VANET. O método de detecção IPCHOCKREFERENCE utilizou estrutura de dados com eficiência de armazenamento e filtro Bloom para detectar alterações anormais no tráfego. Envolve testes aleatórios e não paramétricos para classificar eventos detectados em falsificação aleatória, falsificação de sub-rede ou falsificação fixa, analisando uma tabela hash para as características do IP de origem com menos requisitos computacionais. A avaliação no simulador de rede NS2.34 demonstrou uma detecção precisa com baixo custo.

S. Khanna, et al. [8], apresentaram um método de verificação seletiva adaptável para prevenir ataques DDoS. Ele envolve amostragem aleatória seletiva iniciada pelo servidor para pacotes de entrada e classificação de pacotes como ataque ou legítimos. Neste método, a largura de banda é usada como moeda e cada cliente que deseja acessar recursos do servidor tem que gastar largura de banda para obter o estado do servidor. O nível de proteção empregado pelos clientes se ajusta dinamicamente ao nível de ataque. Neste método, o cliente C envia uma solicitação ao servidor para a qual ele obtém reconhecimento do servidor. A janela de tempo limite de duração T é usada pelos clientes com base no pior tempo de ida e volta entre o cliente e o servidor. Durante o ataque, o cliente não recebe reconhecimento para sua solicitação. O protocolo de replicação é usado pelos clientes nesta situação. A taxa de replicação é proporcional à taxa de ataque atual. No lado do servidor, a amostragem aleatória é usada para selecionar uma amostra aleatória de pacotes que chegam sequencialmente. Isso evita ataques de temporização. A simulação realizada no simulador de rede NS2 ilustra a eficácia do mecanismo desenvolvido em taxas de ataque variáveis.

L. Kavisankar et al. [9] propuseram uma técnica para prevenir ataques de spoofing. A sondagem TCP para pacotes com argumentos de resposta é usada para anexar mensagens de confirmação TCP de forma inteligente. O receptor do TCP SYN envia uma confirmação que altera o tamanho da janela ou causa a retransmissão do pacote. Se a suposta fonte não se comportar conforme o esperado, isso é considerado um ataque. Custos indiretos e computacionais estão envolvidos no recebimento e na análise da resposta do cliente.

Em [10], J. Mirkovic et al. apresentaram uma comparação entre mecanismos de defesa que filtram tráfego de ataques falsificados com base em algumas métricas de desempenho. As defesas disponíveis são implantadas na rede final ou requerem a colaboração do roteador central para filtragem ou marcação de pacotes. Cada defesa é avaliada em seu ambiente controlado; portanto, eles realizaram uma Análise comparativa para determinar o desempenho de cada mecanismo em um ambiente de rede geral, sem alterações na topologia.
O trabalho deles se concentrou em responder a algumas perguntas que avaliam o desempenho dessas defesas, por exemplo, se a implantação da rede final pode ser eficiente com o suporte de roteadores principais, a otimização necessária

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

local de implantação para roteadores principais, etc. Eles avaliaram as defesas individualmente e comparativamente em configurações de rede comuns e seus resultados indicam que três defesas, ou seja, filtragem de contagem de saltos, filtragem de pacotes baseada em rota e PiIp podem trazer redução significativa em ataques de spoofing em usuários da Internet.

Y. Ma [11] propôs um método de defesa baseado na cooperação de nós adjacentes confiáveis. Este método contém três módulos. O primeiro módulo é a autenticação IP que verifica o endereço IP. Se o endereço IP for verificado, o nó é chamado de nó confiável e é considerado como host alcançável no segundo módulo, ou seja, módulo de rastreamento de rota. O terceiro módulo é a filtragem na qual os hosts identificados como não alcançáveis são considerados invasores e seus pacotes são bloqueados enquanto o acesso ao nó de destino é concedido para nós confiáveis. O mecanismo desenvolvido foi avaliado no ambiente de simulação Visual C++ que usou a tabela de informações do nó para armazenar informações de nós confiáveis e a tabela de informações de rota que mantém as informações de roteamento dos hosts.

P. Du, et al. [12], propôs um mecanismo de sondagem chamado Bypass Check para autenticação de clientes de serviços TCP ou UDP.
O método de detecção empregado para detectar mudanças abruptas na simetria sequencial de pacotes (razão entre tráfego transmitido e recebido) utilizou a técnica de soma cumulativa (CUSUM). Fluxos suspeitos são testados usando testes de descarte preferencial para bloquear fluxos sem resposta. O mecanismo foi desenvolvido em Linux utilizando o roteador modular Click e avaliado no PlanetLab.

B. KrishnaKumar et al. [13] propuseram uma abordagem de processamento de pacotes baseada na contagem de saltos para identificar invasores usando endereços IP de origem falsificados. Neste método, os pacotes provenientes de sistemas com a mesma contagem de saltos passam pelo mesmo Os roteadores são marcados com o mesmo número de identificação, que é a combinação do endereço IP de 32 bits do caminho do roteador e o valor criptografado da contagem de saltos. Este valor é comparado com o valor já armazenado no roteador receptor. Assim, os pacotes de ataque são identificados precocemente e as ameaças de spoofing são reduzidas.

G. Jin et al. [14] propuseram um esquema de marcação de pacotes chamado identificação de caminho baseada em hash para defesa contra ataques DDoS com falsificação de endereços IP. O campo de identificação IP de 16 bits em cada pacote é usado para gerar um identificador único correspondente ao caminho pelo qual o pacote passa. O hash dos últimos 16 bits é realizado por roteadores ao longo do caminho, permitindo que a vítima diferencie entre pacotes legítimos e de ataque. O filtro HPi2HC é apresentado, fornecendo recursos de filtragem para que a vítima descarte pacotes maliciosos.

Em [15], M. Nagaratna et al. apresentaram um mecanismo de defesa contra falsificação de endereço IP de origem que utiliza técnicas criptográficas para classificar o pacote de ataque e o pacote legítimo, descartando o pacote de ataque. Os resultados ilustraram a filtragem de alta velocidade de pacotes falsificados e a melhoria na transmissão de pacotes.

Y. Xiang, et al. [16], propôs um novo método de rastreamento de IP chamado marcação determinística flexível de pacotes para defesa contra fontes de ataque. Eles usaram duas características, a saber, estratégia de comprimento de marca flexível e esquema de marcação baseado em fluxo flexível para tornar o método compatível com diferentes ambientes de rede e para marcar pacotes de acordo com a carga do roteador participante. Quando um pacote entra em uma rede protegida, ele é marcado pelos roteadores de borda de entrada. A marcação de pacotes consome memória e tempo de CPU do roteador envolvido. Portanto, para superar esse problema de sobrecarga, eles sugeriram um esquema de marcação baseado em fluxo. A marcação baseada em fluxo mantém um estado separado para cada fluxo com o objetivo de reduzir a complexidade e aumentar a eficiência. Este método isola os fluxos que consomem mais largura de banda e provavelmente contêm pacotes de ataque DDoS. Esses pacotes são marcados com certa probabilidade de ataque.
As estruturas de dados utilizadas são uma tabela de fluxo dinâmico e uma fila FIFO. O mecanismo foi avaliado tanto em ambiente real quanto em simulação. Foi utilizado o simulador SSFNet, que é uma coleção de componentes Java para simulação de redes.

BR Swain et al. [17] apresentaram um método de mitigação de DDoS baseado no valor da contagem de saltos implementado no lado do servidor em um ambiente sem fio. Uma abordagem probabilística foi desenvolvida para contar o número de pacotes maliciosos. Com base nessa contagem, os pacotes maliciosos são filtrados, permitindo a passagem de pacotes legítimos. Para calcular a contagem de saltos, é utilizado o campo "time to live" no pacote, que não pode ser alterado pelo invasor. Esse método descartou de 80 a 85% dos pacotes de ataque, reduzindo o tempo computacional e a memória durante o processamento dos pacotes.

IB Mopari et al. [18] apresentaram um mecanismo de defesa contra ataques DDoS envolvendo spoofing, no qual os pacotes de ataque de spoofing são identificados com base na contagem de saltos que o pacote percorre antes de chegar ao destino. O método

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

Contém dois estados: estado de aprendizagem e estado de filtragem. No estado de aprendizagem, os invasores são identificados, enquanto no estado de filtragem, os pacotes de ataque são descartados. Isso reduz o atraso no caminho crítico do processamento de pacotes. Após detectar o invasor no estado de aprendizagem, o mecanismo alterna para o estado de filtragem, descartando os pacotes de ataque. Este método é eficiente em termos de tempo e reduz o uso de memória da CPU.

Em [19], Y. Shen et al. apresentaram um método de prevenção de falsificação de IP baseado em assinatura e verificação para níveis inter-AS e intra-AS. No nível intra-AS, o host final marca uma chave de uso único em cada pacote de saída e o gateway na borda do AS verifica a chave. No nível inter-AS, o gateway na borda do AS marca uma chave alterada periodicamente no pacote de saída e o gateway na borda do AS de destino verifica e remove a chave.

Z. Duan et al [20] apresentaram um esquema de filtragem de pacotes baseado em rotas, denominado filtro de pacotes interdomínio, implantado em roteadores de borda de rede que identificam o invasor com base nas atualizações do Protocolo de Gateway de Borda antes de entrar no sistema de rede. Esse método garante que os pacotes com endereço de origem válido não sejam descartados e, quando não for possível interromper completamente o ataque, os pacotes sejam encaminhados para um número relativamente menor de sistemas autônomos. Os filtros de pacotes interdomínio podem ser implantados independentemente nos sistemas autônomos.

S. Malliga et al. [21] apresentaram um esquema de marcação determinística de pacotes, denominado técnica de módulo, para marcação de interfaces, que permite o rastreamento de pacotes individuais. O campo ID do pacote IP é usado para marcação de pacotes. O roteador marca o pacote usando seu número de interface em vez do endereço IP associado a ele, reduzindo assim o tempo e o conteúdo necessários para a marcação.
O desempenho é avaliado usando parâmetros como tempo de convergência, armazenamento e sobrecarga de comunicação.

C. Chae et al. [22] propuseram um método de rastreamento de IP que contém um sistema de agentes que relata qualquer fenômeno anormal de tráfego, cria uma mensagem iTrace e a envia ao sistema servidor. O sistema de destino detecta o ataque analisando a mensagem iTrace e coleta informações relevantes, que são usadas para o rastreamento de IP. O método é escalável e não requer alterações estruturais na rede existente.

A. Yaar et al [23] apresentaram defesa contra ataques DDoS de spoofing usando marcação e filtragem de pacotes. Dois esquemas de marcação são utilizados, a saber, marcação baseada em pilha e marcação com escrita antecipada para melhorar o desempenho do esquema de marcação Pi. A estratégia de limite ótimo é utilizada para ataques de endereço IP de origem de spoofing baseados em inundação. A marcação de pilha é baseada no campo TTL para identificar o caminho da origem ao destino e, na marcação com escrita antecipada, os roteadores marcam para o seu próximo roteador de salto. Os resultados mostraram que o método é eficiente mesmo quando apenas 20% dos roteadores estão envolvidos no processo de marcação.

TKT Law et al. [24] propôs um algoritmo de marcação probabilística de pacotes para rastreamento da origem do ataque. Este algoritmo cria um gráfico de ataque no local da vítima, a partir do qual a intensidade do tráfego normal pode ser obtida. Os domínios de rede com a maior parte do tráfego de ataque podem ser previstos a partir deste gráfico. O algoritmo deles funciona para encontrar o tempo mínimo necessário para encontrar a localização do ataque com precisão, com base nos rastreamentos de tráfego disponíveis. A avaliação experimental do algoritmo desenvolvido, aplicado à topologia geral de rede em várias taxas de chegada de pacotes e sob diferentes padrões de ataque, fornece o tempo mínimo necessário para encontrar a origem do ataque de forma eficiente, de modo que possa ser bloqueado o mais cedo possível.
possível para minimizar os danos.

Y. Xiang, et al. [25] propôs uma técnica de defesa de rastreamento de IP em larga escala chamada marcação determinística flexível de pacotes. O fluxo de pacotes é marcado na interface do roteador perto da fonte que passa inalterado por todos os roteadores. A marcação escalável é fornecida com base nos protocolos de rede implantados dentro da rede protegida. A tabela de fluxo dinâmico é usada para armazenar registros de fluxo que é o hash dos endereços IP de origem e destino. Os fluxos que consomem uma parte injusta da largura de banda são identificados e os pacotes nesses fluxos são descartados. As simulações foram realizadas usando o simulador de rede SSFNet incorporando três novos pacotes Java nele, a saber, subsistema de codificação, subsistema de reconstrução e subsistema de marcação baseada em fluxo.

III. ALGORITMO DE DEFESA

Ambas as extremidades da comunicação devem ser autenticadas e verificadas por sua identidade para uma comunicação segura, a fim de evitar ataques com falsificação de endereço IP de origem, que causam negação de serviço a usuários legítimos. A técnica criptográfica baseada em hash é usada para fornecer autenticação aos pacotes transmitidos dos clientes para o servidor. Certos campos no

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

O cabeçalho IP do pacote é extraído e criptografado usando o mecanismo de hash. A chave secreta necessária para o processo de criptografia é obtida de certos valores de campo do pacote. No campo Tipo de Serviço de 8 bits do cabeçalho IP, os primeiros 6 bits são para o Campo de Serviço Diferenciado (DSF) e os dois últimos bits representam a Notificação Explícita de Congestionamento (ECN). Esses dois últimos bits, ou seja, bits ECN, são usados no processo de geração da chave secreta. A combinação diferente desses dois bits resulta na geração de chaves diferentes. A chave secreta é gerada a partir do OU exclusivo do endereço de origem e do campo de sinalizador no cabeçalho IP do pacote se os dois bits forem 11. E a chave secreta é gerada a partir do OU exclusivo do endereço de origem e do campo de identificação do cabeçalho IP do pacote se os dois bits forem 10. O processo de geração da chave secreta é mostrado na figura 2. O HMAC é usado para criptografar o endereço de origem com a chave secreta gerada. O resultado gerado é armazenado nos primeiros 32 bits do campo de opção do cabeçalho IP do pacote que está sendo transmitido.

Fig. 2: Geração de chave secreta.

O roteador de borda do cliente anexa essas informações seguras a todos os pacotes encaminhados para o servidor, o que é verificado pelo roteador de borda da rede receptora. Com base nessa verificação, os pacotes são classificados como pacotes de ataque ou pacotes normais.
O roteador próximo à rede do cliente gera a chave secreta e criptografa o endereço de origem usando essa chave secreta. As informações criptografadas são armazenadas nos primeiros 32 bits do campo de opção do cabeçalho IP. O roteador próximo à rede do servidor recebe os pacotes, extrai o cabeçalho IP do pacote recebido e obtém os primeiros 32 bits do campo de opção desse cabeçalho IP.
A chave secreta é gerada com base na combinação de bits no campo ECN. O endereço de origem do pacote recebido é criptografado usando essa chave. O valor de hash obtido é comparado com o valor obtido dos primeiros 32 bits no campo de opção do pacote recebido. Se ambos os valores corresponderem, o pacote é considerado legítimo e encaminhado ao servidor; caso contrário, o pacote é considerado um pacote de ataque com endereço IP de origem falso e descartado no roteador.

IV.PSEUDO CÓDIGO

Se o novo nó N então
Gerar hash ÿ} =ÿsrc_ip|| id do nó|| chave de sessão} **ÿÿ**
Encaminhar para N
N anexa **ÿÿ** com pacote e encaminha
Extrair ÿÿno roteador de borda
ÿÿ Calculado= **ÿ** Se
    ÿÿ Remover do pacote
    Marcação de pacotes de processo
Outro
    Descartar pacote

V. RESULTADOS DA SIMULAÇÃO

O ambiente de simulação é criado utilizando o simulador de rede NS3 para testar o mecanismo de defesa desenvolvido. O ataque DDoS é iniciado usando spoofing de endereço IP. Cada pacote normal contém informações secretas anexadas que fornecem autenticação. Essas informações secretas são verificadas no roteador de borda da rede alvo. Os pacotes do invasor são separados dos pacotes normais e descartados no roteador antes de chegarem ao servidor alvo. Os resultados obtidos na simulação mostraram que os pacotes de ataque são identificados de forma eficiente, com 0% de falsos positivos.

O gráfico da Figura 3 mostra que, à medida que os pacotes de ataque aumentam com o tempo, todos os pacotes de ataque são verificados e descartados no roteador. Durante o experimento de simulação, 1.130 pacotes TCP normais foram enviados ao servidor e a rede do invasor enviou 2.289 pacotes TCP de ataque contendo falsificação do endereço IP de origem em 20 ms. O algoritmo

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

classificou eficientemente todos os pacotes normais e de ataque e o ataque DDoS foi evitado ao descartar os pacotes no roteador de borda antes de atingir o alvo.

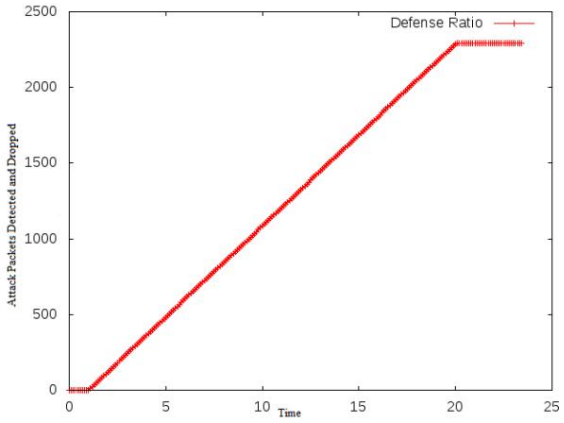

Fig. 3: Total de pacotes de ataque detectados e descartados

O gráfico na figura 4 mostra que os pacotes de ataque que chegam ao servidor de destino antes da aplicação da defesa são grandes em número e os pacotes de ataque que chegam ao servidor de destino após a aplicação do mecanismo de defesa são quase zero, enquanto os pacotes normais que chegam ao servidor de destino antes e depois da aplicação da defesa são os mesmos (indicados pela sobreposição de linhas vermelhas e verdes, respectivamente), indicando que o tráfego normal é encaminhado sem ser afetado pelo mecanismo de defesa.

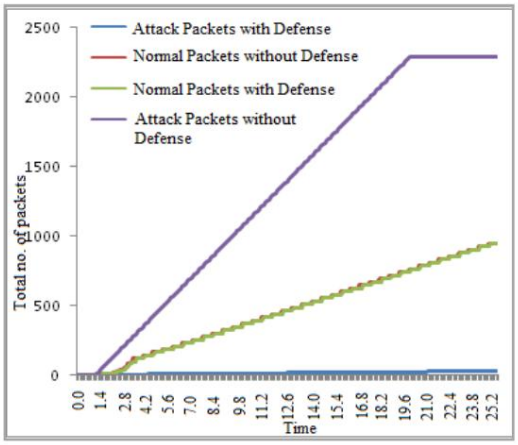

Fig. 4: Total de pacotes transmitidos com e sem defesa

VI.CONCLUSÃO

Neste artigo, apresentamos uma técnica criptográfica leve para defesa contra ataques de spoofing que não requer sobrecarga adicional nos roteadores nem alterações nos protocolos de roteamento da internet. Ao fornecer autenticação para cada pacote no lado do cliente e verificar a identidade do pacote nos roteadores próximos ao servidor de destino, é possível identificar com eficiência os pacotes de ataque com endereço IP de origem falso. Os pacotes de ataque são separados dos pacotes normais e descartados antes de chegarem ao servidor de destino, enquanto os pacotes normais são encaminhados sem serem afetados, permitindo que clientes legítimos acessem os recursos do servidor. Os resultados da simulação ilustraram a eficiência do mecanismo de defesa contra ataques DDoS com 99,9% de precisão, 0% de falsos positivos e tempo de resposta rápido.

ISSN (Online): 2320-9801
ISSN (Impresso): 2320-9798

Revista Internacional de Pesquisa Inovadora em Engenharia de Computação e Comunicação

(Uma organização certificada ISO 3297:2007)

Vol. 3 , Edição 3, março de 2015

REFERÊNCIAS

[1] Português S. Yu, Y. Tian, S. Guo, D. Wu, “Podemos vencer ataques DDoS em nuvens?”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, n.º 9, pp. 2245-2254, 2014.
[2] B. Liu, J. Bi, AV Vasilakos, “Para incentivar a implantação anti-spoofing”, IEEE Transactions on Information Forensics and Security, vol. 9, n.º 3, pp. 436-450, 2014.
[3] R. Maheshwari, CR Krishna, MS Brahma, “Defendendo o sistema de rede contra ataques DoS distribuídos baseados em falsificação de IP usando a técnica de filtragem de pacotes DPHCF-RTT”, Conferência Internacional IEEE sobre questões e desafios em técnicas de computação inteligente (ICICT), pp. 206-209, 2014.
[4] A. Compagno, M. Conti, P. Gasti, G. Tsudik, “Poseidon: mitigando ataques DDoS de inundação de interesse em redes de dados nomeados”, 38ª Conferência IEEE sobre Redes Locais de Computadores, pp. 630-638, 2013.
[5] Português J. Francois, I. Aib, R. Boutaba, “FireCol: Uma rede de proteção colaborativa para a detecção de ataques DDoS de inundação”, IEEE/ACM Transactions on Networking, vol. 20, n.º 6, pp. 1828-1841, 2012.
[6] Português F. Soldo, K. Argyraki, A. Markopoulou, “Filtragem otimizada baseada na fonte de tráfego malicioso”, IEEE/ACM Transactions on Networking, vol. 20, n.º 2, pp. 381-395, 2012.
[7] K. Verma, H. Hasbullah, A. Kumar, “Um método de defesa eficiente contra tráfego de inundação falsificado por UDP de ataques de negação de serviço (DoS) em VANET”, IEEE 3ª Conferência Internacional de Computação Avançada (IACC), pp. 550-555, 2012.
[8] Português S. Khanna, SS Venkatesh, O. Fatemieh, F. Khan, CA Gunter, “Verificação seletiva adaptativa: uma contramedida adaptativa eficiente para impedir ataques DoS”, IEEE/ACM Transactions on Networking, vol. 20, n.º 3, pp. 715-728, 2011.
[9] Português L. Kavisankar, C. Chellappan, “Um modelo de mitigação para inundação de TCP SYN com falsificação de IP”, Conferência Internacional IEEE sobre Tendências Recentes em Tecnologia da Informação (ICRTIT), pp. 251-256, 2011.
[10] J. Mirkovic, E. Kissel, “Avaliação comparativa de defesas contra falsificação”, IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 2, págs. 218-232, 2011.
[11] Y. Ma, “Um método eficaz para defesa contra ataques de falsificação de IP”, Conferência Internacional IEEE sobre redes de comunicações sem fio e computação móvel (WiCOM), pp. 1-4, 2010.
[12] P. Du, A. Nakao, “Trilogia Mantlet: Defesa DDoS implantável com anti-spoofing inovador, detecção e mitigação de ataques”, 19º Conferência Internacional sobre Comunicações e Redes de Computadores (ICCCN), pp. 1-7, 2010.
[13] B. KrishnaKumar, PK Kumar, R. Sukanesh, “Abordagem de processamento de pacotes baseada em contagem de saltos para combater ataques DDoS”, IEEE International Conferência sobre Tendências Recentes em Informação, Telecomunicações e Computação, pp. 271-273, 2010.
[14] G. Jin, F. Zhang, Y. Li, H. Zhang, J. Qian, “Um esquema de identificação de caminho baseado em hash para defesa de ataques DDoS”, IEEE 9th International Conferência sobre Computação e Tecnologia da Informação, pp. 219-224, 2009.
[15] M. Nagaratna, VK Prasad, ST Kumar, “Detecção e prevenção de ataques DDoS falsificados por IP por detecção e filtragem baseadas em marcação criptografada (EMDAF)”, Conferência Internacional IEEE sobre avanços em tecnologias recentes em comunicação e computação, pp. 753-755, 2009.
[16] Y. Xiang, W. Zhou, M. Guo, “Marcação de pacotes determinística flexível: um sistema de rastreamento de IP para encontrar a verdadeira fonte de ataques”, IEEE Transações em sistemas paralelos e distribuídos, vol. 20, n.º 4, pp. 567-580, 2009.
[17] BR Swain, B. Sahoo, “Mitigação de ataques DDoS e economia de tempo computacional usando uma abordagem probabilística e método HCF”, IEEE Conferência Internacional de Computação Avançada (IACC), março, pp. 1170-1172, 2009.
[18] IB Mopari, SG Pukale, ML Dhore, “Detecção e Defesa Contra Ataques DDoS com Spoofing de IP”, Conferência Internacional sobre Computação, Comunicação e Redes (ICCCN), pp. 1-5, 2008.
[19] Y. Shen, J. Bi, J. Wu, Q. Liu, “Uma prevenção de falsificação de endereço de origem de dois níveis baseada em mecanismo automático de assinatura e verificação”, Simpósio IEEE sobre Computadores e Comunicações, pp. 392-397, 2008.
[20] Z. Duan, X. Yuan, J. Chandrashekar, “Controlando a falsificação de IP por meio de filtros de pacotes entre domínios”, Transações IEEE em redes confiáveis e Computação Segura, vol. 5, n.º 1, pp. 22-36, 2008.
[21] S. Malliga, A. Tamilarasi, “Um mecanismo defensivo para defesa contra ataques DoS/DDoS por rastreamento de IP com DPM”, IEEE International Conference on Computational Intelligence and Multimedia Applications, pp. 115-119, 2007.
[22] C. Chae, SH. Lee, JS. Lee, JK. Lee, “Um estudo de ataques DDoS de defesa usando IP Traceback”, Conferência Internacional IEEE sobre Computação Inteligente Pervasiva, pp. 402-408, 2007.
[23] A. Yaar, A. Perrig, “StackPi: Novos mecanismos de marcação e filtragem de pacotes para defesa contra DDoS e falsificação de IP”, IEEE Journal em Selected Áreas em Comunicações, vol. 24, n.º 10, pp. 1853-1863, 2006.
[24] TKT Law, JCS Lui, DKY Yau, “Você pode correr, mas não pode se esconder: uma metodologia estatística eficaz para rastrear DDoS Atacantes”, IEEE Transactions on Parallel and Distributed Systems, vol. 16, n.º 9, pp. 799-813, 2005.
[25] Y. Xiang, W. Zhou, “Um sistema de defesa contra ataques DDoS por rastreamento de IP em larga escala”, IEEE 3ª Conferência Internacional sobre Tecnologia da Informação e Aplicações (ICITA), pp. 431-436, 2005.