UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
ESCOLA POLITÉCNICA
DEPARTAMENTO DE ELETRÔNICA E DE COMPUTAÇÃO

Análise e Teste de Mobilidade com HIP

Autor:

Lyno Henrique Gonçalves Ferraz

Orientador:

Prof. Otto Carlos Muniz Bandeira Duarte, Dr.Ing.

Examinadores:

X

XX

XXX

XXXX

DEL
Março de 2010

À minha família.

Agradecimentos

Agradecimentos.

Resumo do Projeto Final apresentado ao DEL/UFRJ como parte dos requisitos necessários para a obtenção do grau de Engenheiro Eletrônico e de Computação.

Análise e Teste de Mobilidade com HIP

Lyno Henrique Gonçalves Ferraz

Março de 2010

Orientador: Otto Carlos Muniz Bandeira Duarte

Departamento: Engenharia Eletrônica e de Computação

A internet funciona hoje com dois domínios importantes: os endereços IP (*Internet Protocol*) e os nomes do serviço de domínio de nomes (DNS - *Domain Name Service*). A presença de somente dois domínios simplifica bastante o funcionamento da Internet, entretanto isso traz problemas para novas tendências tais como mobilidade e múltiplas conexões com a internet. Grande parte desses problemas é devido à sobrecarga semântica do endereço IP.

O HIP (*Host Identity Protocol*)surge como solução para esses problemas, pois separa os dois papéis do IP. Para realizar tal separação, HIP cria uma nova camada na pilha de protocolos TCP/IP, a camada de identificação. O IP, o identificador da camada de rede, cumpre somente o papel de localizar as estações. A nova camada cumpre o papel de identificador da estação, de forma a garantir a segurança dos usuários. Para mostrar as capacidades e o funcionamento do HIP foi construído um cenário de teste.

Palavras Chave

Redes de Computadores

Mobilidade

HIP

Lista de Acrônimos

API : *Application Programming Interface*;

BEX : *Base Exchange*;

DHCP : *Dynamic Host Configuration Protocol*;

DHT : *Distribuited Hash Table*;

DNS : *Domain Name System*;

DSA : *Digital Signature Algorithm*;

DoS : *Denial of Service*;

ESP : *Escapsulated Security Protocol*;

FDQN : ;

FTP : *File Transfer Protocol*;

HASH : ;

HI : ;

HIT : ;

HMAC : ;

IANA : ;

IKEv2 : ;

Internet : ;

IP : *Internet Protocol*;

IPSec : *IP Security*;

LDAP : ;

LSI : *Local Scope Identifier*;

MitM : *Man in the Middle*;

MODP : ;

NAT : *Network Address Translation*;

ORCHID : *Overlay Routable Cryptografic Hash Identifier*;

PPP : ;

QoS : *Quality of Service*;

RSA : *Rivest-Shamir-Aldeman*;

RVS : *Rendezvous Server*;

SA : *Security Association*;

SHIM6 : ;

SPI : *Security Parameter Index*;

SSH : ;

TCP : *Transmission Control Protocol*;

TCP/IP : *TCP IP Protocol Suite*;

TLV : *Type, Length and Value*;

Sumário

Capítulo I

Introdução

I.1 Motivação

I.1.1 Problemática

Quando o conjunto de protocolos TCP/IP foi criado no final da década de 1970 e início da década 1980, não se pensava na dimensão que a rede iria tomar. Algumas questões também, como mobilidade e múltiplas conexões com a internet (multihoming), não foram previamente pensadas. O conjunto TCP/IP foi pensado para estações estáticas, não móveis e sem nenhuma redundância de conexões. Naquela época o papel do IP de localizar as estações para o roteamento de pacotes e o papel de identificá-las, era suficiente e cumpria muito bem as necessidades. As estações raramente moviam-se então o IP era um bom identificador.

Quando a alocação dinâmica de IP foi criada com o PPP e DHCP, a identificação única de estações por IPs foi quebrada. A situação piorou ainda mais com a criação do NAT.

Além da natureza dos hospedeiros, mudou também o tipo dos usuários. No início era uma pequena comunidade de usuários que confiavam uns nos outros, posteriormente o número aumentou significativamente e a confiança entre eles ficou afetada. Para prover segurança entre as conexões hoje são necessários mecanismos criptográficos.

Em suma, o ambiente da internet, a natureza dos usuários e os dispositivos, mudaram desde sua criação. Com isso requisitos de mobilidade, múltiplas conexões com a Internet e segurança surgiram. As soluções existentes mantêm a arquitetura são difíceis, então se faz necessária uma mudança radical na arquitetura de protocolos TCP/IP.

I.1.2 HIP

Para resolver os problemas apresentados HIP ataca a ambiguidade do IP. HIP faz a separação dos papéis do IP, a função de localizador e de identificardor. Para realizar a separação de localizadores e identificadores uma nova camada na pilha de protocolos TCP/IP é criada, a camada de identificação. O IP continua a ser responsável pela localização, e perde a função de identificar estações.

A camada de identificação é inserida entre a camada de transporte e a camada de rede. A camada de transporte se conecta com a camada de identificação, não mais com a camada de rede diretamente. A camada de identificação, por sua vez, liga-se com a camada de rede. Portanto quaisquer alterações nas camadas inferiores à camada de identificação não serão percebidas pelas camadas superiores (transporte e aplicação).

Ao se tirar a função de identificação do IP, será necessário criar um novo método para se fazer a validação dos endereços IP. Na arquitetura atual, não existe a necessidade de validar o IP com alguma identidade, pois o IP exerce também esse papel. Entretanto, ao separar a identificação da localização do IP, deve-se garantir a validade do endereço associado ao identificador.

A identificação das estações será feita por meio de um identificador. Esses identificadores serão de natureza criptográfica, uma chave pública de um par de chaves pública/privada. O motivo do identificador ser uma chave pública é a possibilidade de ser usada para autenticação do usuário. Ela pode ser usada também para a geração de uma chave de sessão e para encriptação de mensagens.

O identificador utilizado poderia ser utilizado em vários mecanismos de autenticação já existentes como o IKEv2. Apesar disso, a arquitetura apresentada introduz um novo protocolo (HIP) e uma troca criptográfica HIP Base exchange (BEX) fim-a-fim. Os protocolos definidos pelo HIP provêem formas de confiança, mobilidade, multihoming, renumeração dinâmica de IP, ajudam na tradução e transição de endereços IP e evitam certos tipos de ataque de negação de serviços.

Cada estação terá ao menos um identificador. Cada um será único, duas estações jamais possuirão o mesmo identificador. A estação pode possuir mais de um identificador. Eles podem ser publicados em sistema do tipo DNS ou não. A não publicação de um identificador caracteriza uma forma de prover anonimato.

I.1.3 Mobilidade

Nesse trabalho, mobilidade será considerado como o fenômeno de uma entidade mover-se e manter o contexto de comunicação ativo [ref article 3] como mostrado na figura I.1. Uma estação pode modificar o ponto de conexão com a rede livremente, e todos os contextos de conexão permanecerão ativos. Os processos não irão perceber a mobilidade, entretanto podem sentir uma diferença na qualidade de serviço.

Para compor um cenário real, existe um número de nós móveis, conectados a uma rede relativamente fixa. Além disso, os prefixos dos endereços da camada de rede são determinados pela estrutura da rede. Ou seja, a topologia da rede determina a porção dos endereços IP relativa ao roteamento. Isso reflete o fato que em redes grandes, é importante manter os prefixos do endereço IP consistentes com sua topologia. Isso é feito com o intuito de preservar as tabelas de roteamento com um tamanho gerenciável e sem redundâncias.

Como consequência, todas as vezes que um nó se move, seu endereço de rede irá também mudar. Então, para continuar a comunicação a estação deve ser capaz de sinalizar essa modificação de endereços para os pares ativos.

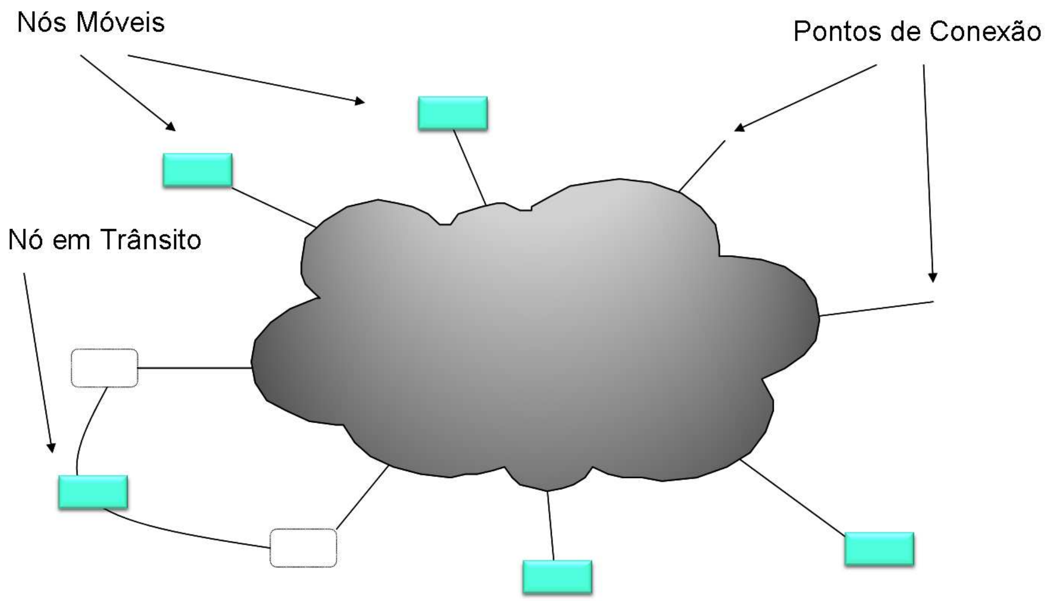

Figura I.1: Mobilidade de estações.

I.1.4 Multihoming

Multihoming se refere uma situação que uma estação possui múltiplos caminhos paralelos de comunicação que ela pode usar. Normalmente isso é consequência de uma estação possuir diversas interfaces de rede (host multihoming) ou da rede onde ela está ter caminhos de comunicação redundantes com o resto da rede (site multihoming) como mostrado na figura I.2.

Do ponto de vista teórico, multihoming é o fato de uma estação ter dois ou mais pontos de conexão com a rede. Esta situação pode ser caracterizada pelo fato da estação ser alcançável por mais de um caminho. Como consequência, a estação possuirá diveros endereços de rede, cada um reflete a localização topológica referente a ele.

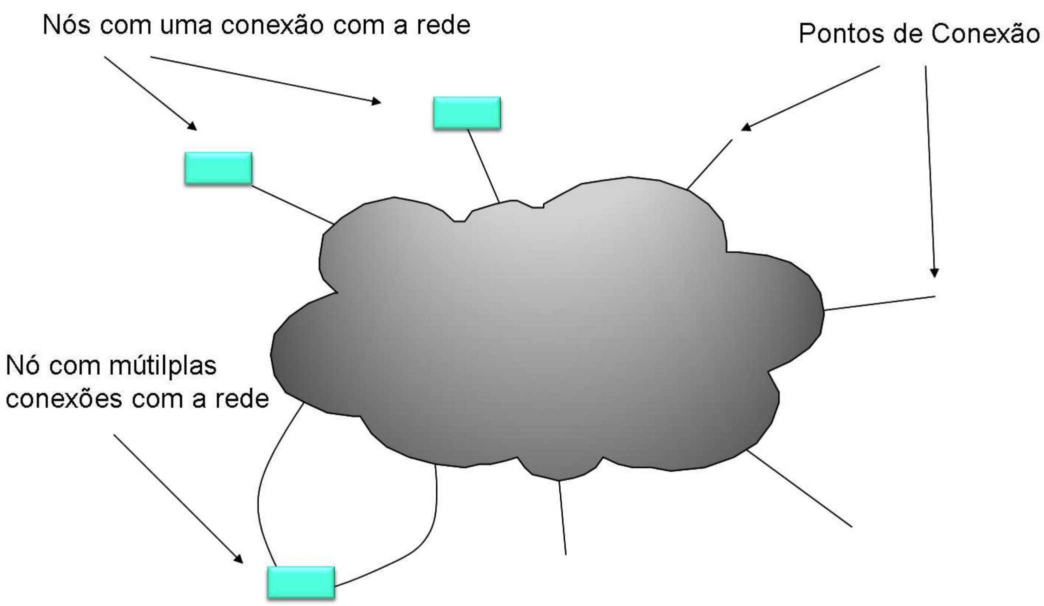

Figura I.2: Estações com *multihoming*.

I.1.5 Segurança

Mobilidade e Multihoming implicam em vários problemas de segurança. Esses problemas decorrem do fato de que vários endereços IPs podem ser designados para uma estação e podem ser intercambiados. Em uma solução ideal os pares podem utilizar qualquer um dos endereços dos outros, sem a preocupação da validade deles.

Existem dois problemas básicos: furto de endereço (I.3 e inundação de endereço (I.4). No furto de endereço, o atacante anuncia a posse de um endereço que está sendo utilizado por outro nó. Ele então, pode forçar uma atualização de endereço e realizar um ataque de mascaramento (Masquerade), homem no meio (MitM) ou negação de serviço (DOS) contra o dono do endereço com o novo endereço. Na inundação de endereço, o nó malicioso (ou um grupo) anunciam sua disponibilidade para nós inocentes em certo endereço alvo. Isso pode ser feito com uma mensagem de atualização de nedereço. Os nós inocentes acreditam que o nó foi modificado para um endereço alvo e o inundam de pacotes não desejados.

Esses ataques são possíveis se mensagens de atualização de endereço forem utilizadas

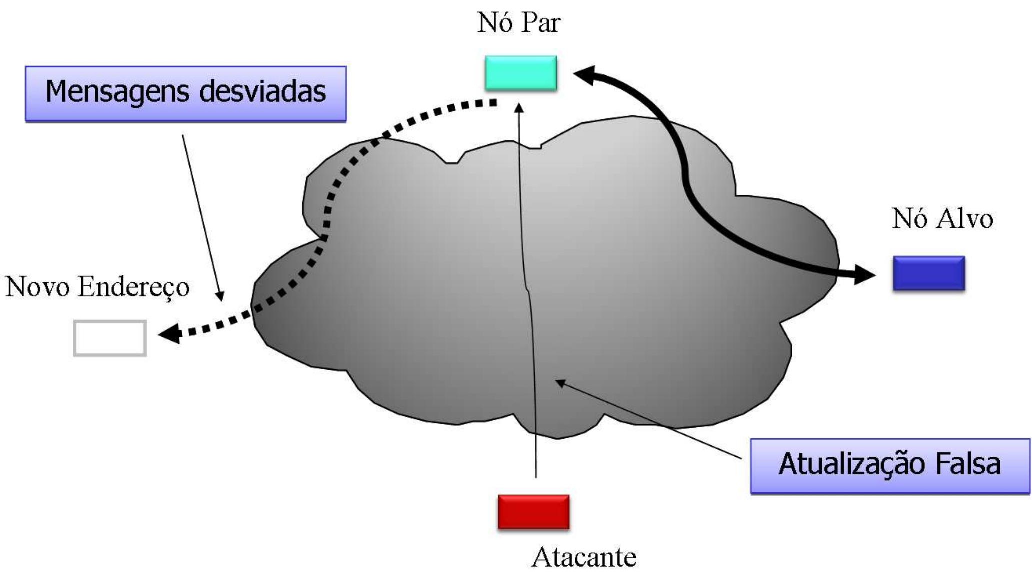

Figura I.3: Furto de endereços.

sem algum mecanismo de segurança. No furto de endereço, o par deve verificar se a mensagem de atualização foi realmente enviada pelo dono do endereço antigo. Isso pode ser feito por assinatura das mensagens.

Na inundação de endereço, se a vítima receber alguns pacotes errados não será muito problema, entretanto se o número de nós enganados for muito alto, os pacotes poderão encher o link da vítima. Os nós ao receber uma atualização de endereço, devem fazer alguma verificação da mudança de endereço, para confirmar a validade da atualização e evitar esse problema.

Esses problemas são difíceis de resolver com a arquitetura atual, na qual a identificação é o endereço topológico como mostrado na figura I.5. Não existe um mecanismo de conferir que um nó que se diz dono de tal endereço está e fato naquela localização. Ou seja, se um nó acredita que se comunica com algum outro que diz possuir um endereço X, ele não pode verificar se o outro está de fato no endereço X ou outro no meio do caminho. Esse outro nó poderá então escutar todas do nó as mensagem para o endereço X.

A dualidade do IP da arquitetura atual pode causar os problemas citados anterior-

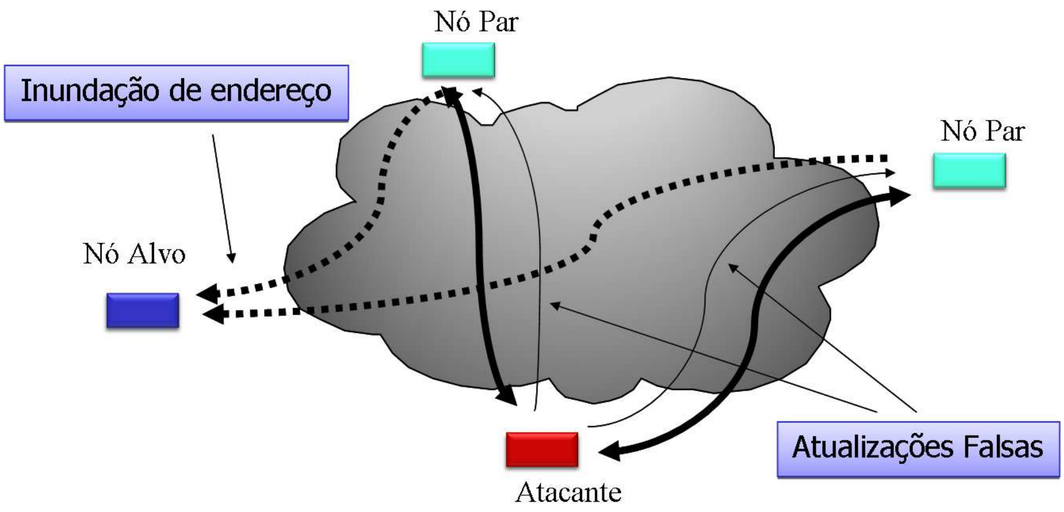

Figura I.4: Inundação de endereço.

mente mesmo se houver verificação. Não há como um nó dizer que quer se comunicar com outro específico diretamente. Ele pode somente se comunicar com o endereço que acredita o par possui. Então se um nó intermediário interceptar as mensagens e fingir ser o par, poderá fazer uma atualização de endereço que resultará em um furto de endereço ou inundação de endereço.

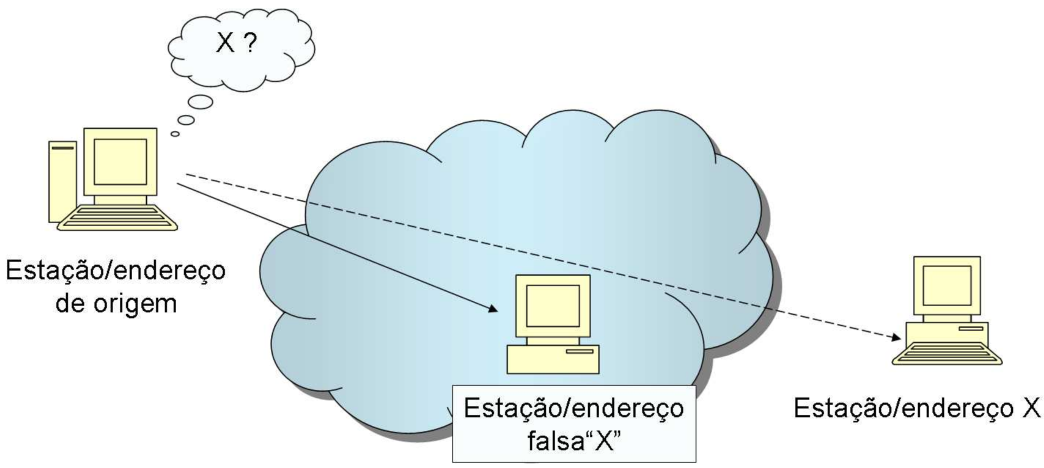

Figura I.5: Verificação atual.

Como solução para a arquitetura atual, poderiam ser relacionadas chaves públicas com endereços IP. Para isso uma infraestrutura de credenciamento deve ser criada, com o propósito de ligar os nós aos endereços de maneira segura. Entretanto, prover tal infraestrutura seria difícil de ser implementada devido a questões práticas.

I.2 Objetivos

O trabalho desenvolvido tem como objetivo testar a viabilidade de utilizar o HIP. Para mostrar as funcionalidades do foi construído um cenário de testes, no qual foram feitos testes objetivos (medições) e subjetivos (percepção de usuários).

O cenário de testes inclui diversas ferramentas já existentes assim como algumas desenvolvidas para fim específico. Todas elas serão descritas no III.

I.3 Organização do Texto

Este trabalho está organizado da seguinte forma. No Capítulo II é apresentado o Host Identity Protocol. São descritas suas principais características e protocolos envolvidos. No Capítulo III são apresentados, em detalhes, o cenário de testes, e a plataforma de testes desenvolvida. Ainda nesse capítulo são descritas as ferramentas usadas e criadas no desenvolvimento deste trabalho. Detalhes referentes aos testes e à análise dos resultados são abordados no Capítulo IV. Por fim, no Capítulo V serão apresentadas as conclusões sobre este trabalho e as considerações sobre trabalho futuros.

Capítulo II

Descrição detalhada do *Host Identity Protocol*

II.1 Identificadores

HIP apresenta um novo domínio, o domínio de identificação de hospedeiros. Existem alguns identificadores desse domínio. O principal é identificador de hospedeiro (HI - Host Identifier), que é uma chave pública de um par assimétrico de chaves. O outro muito importante é o tag de identidade de hospedeiro (HIT - Host Identity Tag). Um outro identificador LSI (Local Scope Identifier), utilizado localmente.

II.1.1 Identidade e Identificadores de Hospedeiros

A identidade de hospedeiros adiciona duas características essenciais nos protocolos da Internet. A primeira é o desacoplamento da camada de transporte e de rede. Isso possibilita a evolução independentes das duas camadas. Ademais, possibilita serviços fim-a-fim em ambientes de rede. A segeunda característica a autenticação dos hospedeiros. Devido o identificador ser uma chave pública, poderá ela ser usada para autenticação em protocolos de segurança como o IPsec.

HI

A única definição imposta pelos protocolos do HIP é que a identidade de hospedeiros seja um par de chaves pública/privada. Nesse caso o identidade é referenciada pela parte pública do par. Então o nome representando a identidade no domínio de identificação, ou seja, o identificador de hospedeiro (HI), é uma chave pública. A própria posse da chave privada indica a identidade. O hospedeiro é então definido como o proprietário da chave privada correspondente do par de chaves. Se mais de um nó possuir a chave privada, a identidade pode ser considerada distribuída.

Arquiteturalmente qualquer outra convenção de nomes na internet pode ser uma base utilizável para os identificadores de hospedeiros. Entretanto, nomes não criptográficos devem ser usados em situações de alta confiança ou baixo risco. Em situações nas quais autenticação não é necessário.

As identidades reais nunca não são utilizados diretamente em protolos da internet. Os HI correspondentes podem ser armazenados em registros especializados DNS [1] ou em diretórios LDAP (Lightweigth Directory Access) e são transmitidos nas trocas definidas pelo HIP. Outros identificadores como HIT e LSI são utilizados para representar a identidade em protocolos e APIs.

HIT

O outro identificador principal é um resumo (HASH) dessa identidade, o tag de identidade de hospedeiro (HIT - *Host Identity Tag*). A motivação por trás do HIT é padronizar um tamanho para ser usado nos protocolos envolvidos no HIP. Existem diversos algoritmos diferentes de chaves públicas que podem ser utilizados com comprimentos diferentes. Portanto, a chave pública HI não é indicada para ser usada como um identificador de pacotes ou índice para as diversas tabelas operacionais necessárias para o funcionamento dos protocolos. O HIT é um HASH de 128 bits. Ele é utilizado nos payloads do HIP e para indexar os estados correspondentes na estação.

Nos pacotes do HIP, o HIT é usado para identificar o remetente e destinatário. Ele deve portanto ser único no universo IP enquanto estiver em uso. Na eventualidade dO HIT mapear mais de uma identidade, o HI fará a diferenciação final. Se houverem mais de uma chave pública para um dado nó, o HIT será uma dica para a chave correta a ser usada.

As propriedades do HIT são:

1. tem o mesmo comprimento que o endereço Ipv6, para poder ser utilizado no campo de endereços em API e protocolos existentes;
2. é auto certificante (dado um HIT, é computacionalmente difícil achar o HI correspondente);
3. a probabilidade de colisão entre dois HIT é bem baixa.

Colocar o HIs e HITs no cabeçalho de cada pacote aumentaria muito a sobrecarga deles. Então para se evitar este problema é proposto um mapeamento entre os pacotes de dados e os HIs. Em alguns casos, é possível utilizar HIP sem qualquer cabeçalho extra nos pacotes de dados. Um exemplo disso é se o ESP for utilizado para proteger o tráfego. Neste caso o SPI (presente no cabeçalho ESP) pode ser usado para mapear o pacote de dados encriptado com a associação HIP correta.

A geração do HIT é um tipo de ORCHID (*Overlay Routable Cryptografic Hash Identifier* [2]), baseado no algoritmo HASH SHA-1 do identificador de hospedeiro. ORCHID possui um prefixo alocado do bloco Ipv6 e é definido no documento RFC 4843 [2].

LSI

O identificador de escopo local (LSI - *Local Scope Identifier*) é uma representação local da identidade. Ele pode ter 32 ou 128 bits (normalmente 32 bits). Ele é utilizado para facilitar a utilização de identidades de hospedeiros em protocolos e API existentes. O seu problema é ser somente de escopo local.

Exemplos de seu uso podem ser: o endereço em um comando FTP, e endereço de uma chamada de Socket. Ele atua como uma conexão da arquitetura HIP com protocolos e APIs (IPv4 principalmente).

II.2 Protocolo

O cabeçalho HIP poderia ser carregado por todos os pacotes IP. Entretanto, por possuir um tamanho relativamente grande (40 bytes), é desejável comprimir o cabeçalho. O cabeçalho deve estar presente somente em pacotes de controle para estabelecer ou modificar conexões. O método para fazer essa compressão definido é o Encapsulated Security Protocol (ESP). Mais tarde outros métodos poderão ser definidos. O número de protocolo definido pela IANA para o HIP foi o 139.

Capítulo III

Cenário de testes de mobilidade com HIP

Capítulo IV

Testes e Resultados

Capítulo V

Conclusão

Referências Bibliográficas

[1] NIKANDER, P., LAGANIER, J., *Host Identity Protocol (HIP) Domain Name System (DNS) Extension*. RFC 5205, IETF, Apr. 2008.

[2] P. NIKANDER, J. L., DUPONT, F., *An IPv6 Prefix for Overlay Routable Cryptografic Hash Identifier (ORCHID)*. RFC 4843, IETF, Apr. 2007.

[3] TANENBAUM, A. S., *Computer Networks*. Terceira ed. Prentice Hall Inc, 1996.

[4] MARCELO D. D. MOREIRA, NATALIA C. FERNANDES, L. H. M. K. C. E. O. C. M. B. D., "Internet do Futuro: Um Novo Horizonte", *Mini-Curso do ?? Simpósio Brasileiro de Redes de Computadores - SBRC'200?*, pp. 1–59.

[5] PEKKA NIKANDER, J. Y., WALL, J., "Integrating Security, Mobility, and Multi-Homing in a HIP Way". In: *Network and Distributed Systems Security Symposium (NDSS'03)*, pp. 87–99, Feb. 2003.

[6] AL-SHRAIDEH, F., "Host Identity Protocol". In: *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, pp. 87–99, Feb. 2003.

[7] MOSKOWITZ, R., NIKANDER, P., *Host Identity Protocol Architecture*. RFC 4423, IETF, May 2006.

[8] R. MOSKOWITZ, P. NIKANDER, P. J., HANDERSON, T., *Host Identity Protocol*. RFC 5201, IETF, Apr. 2008.

[9] P. JOKELA, R. M., NIKANDER, P., *Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)*. RFC 5202, IETF, Apr. 2008.

[10] J. LAGANIER, T. K., EGGER, L., *Host Identity Protocol (HIP) Registration Extension*. RFC 5203, IETF, Apr. 2008.

[11] J.LAGANIER, EGGER, L., *Host Identity Protocol (HIP) Rendezvous Extension*. RFC 5204, IETF, Apr. 2008.

[12] P. NIKANDER, T. HANDERSON, C. V., ARKKO, J., *End-Host Mobility and Multihoming with the Host Identity Protocol*. RFC 5206, IETF, Apr. 2008.

[13] KENT, S., *IP Encapsulating Security Payload (ESP)*. RFC 4303, IETF, Dec. 2005.

[14] ADAMS, A., NICHOLAS, J., SIADAK, W., *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)*. Work in progress, <draft-ietf-pim-dm-new-v2-04.txt>, IETF, Sep. 2003.

[15] HOLBROOK, H. W., CHERITON, D. R., "IP Multicast Channels: EXPRESS Support for Large-scale Single-source Applications". In: *ACM SIGCOMM'99*, Sep. 1999.

[16] "Darwin Streaming Server", Jan. 2004, `http://developer.apple.com/darwin/projects/streaming/`.

[17] MACKIE, D., "Video Streaming and MPEG4IP". In: *Cisco Technology Center*, 2001.