UMA FERRAMENTA PARA PROTEÇÃO DO TRÁFEGO DE SERVIÇOS UTILIZANDO O IPSEC

Jansen Carlo Sena
Instituto de Computação
Universidade Estadual de Campinas
13083-970 Campinas - SP
jansen.sena@ic.unicamp.br

Paulo Lício de Geus
Instituto de Computação
Universidade Estadual de Campinas
13083-970 Campinas - SP
paulo@ic.unicamp.br

RESUMO

*O nível de granularidade e a miscelânea de parâmetros a serem definidos no IPSec podem fazer com que o tráfego sob sua proteção não contemple os requisitos desejados, limitando seu uso a ambientes pré-definidos. Com base neste cenário, este artigo apresenta o SLM (*Security Level Model*), um modelo que visa racionalizar a utilização do IPSec através de níveis de segurança que agrupam parâmetros de acordo com seus graus de proteção.*

1 Introdução

Desenvolvido para dar suporte a uma estrutura de rede capaz de continuar em operação mesmo diante de mudanças inesperadas em sua topologia, o protocolo IP não tinha a segurança como um aspecto fundamental em seu projeto.

A Internet, inicialmente limitada aos meios acadêmico e militar, mantinha uma cooperação harmoniosa entre os seus usuários. Porém, com a sua popularização, a rede mundial e, conseqüentemente, toda a sua tecnologia envolvida, mostraram-se extremamente frágeis e despreparadas diante de vulnerabilidades não exploradas anteriormente. Neste contexto, na tentativa de adicionar segurança ao protocolo IP, o IETF (*Internet Engineering Task Force*) resolveu especificar o IPSec, um conjunto de extensões ao IP capaz de evitar ataques como o *spoofing* de endereços e a modificação e análise do conteúdo de pacotes. A proteção é aplicada com base em regras que filtram os diversos conjuntos de pacotes para que sejam utilizados os parâmetros pré-estabelecidos. Algoritmos criptográficos, tempo de vida e tamanho das suas chaves, modos de operação e sentido da conexão devem ser relacionados a cada serviço que se pretende proteger. Além disso, a política de segurança[1] utilizada deve ser compartilhada por todas as entidades que necessitam trocar informações. Tais fatores podem elevar o custo de implantação do IPSec. Sendo assim, o SLM (*Security Level Model*) foi definido no intuito de diminuir a complexidade do processo de formulação de regras e centralizar a política de segurança visando facilitar o uso do IPSec.

Na Seção 2 são elucidadas as características gerais do IPSec, fundamentais para o contextualização deste artigo. Na Seção 3 é apresentado o SLM, seus componentes e estruturas gerais. A seguir, na Seção 4, os aspectos básicos da sua implementação são descritos. As Seções 5 e **??** apresentam considerações finais e extensões do modelo proposto.

[1]No decorrer do texto, política de segurança refere-se ao conjunto de regras utilizado pelo IPSec para filtrar o tráfego IP.

2 IPSec

O IPSec (*IP Security*) [7, 2] baseia-se, fundamentalmente, em dois protocolos: o AH (*Authentication Header*) [5], que provê autenticação e integridade, e o ESP (*Encapsulating Security Payload*) [6], que, além dos serviços anteriores, provê confidencialidade. Implementados como dois cabeçalhos inseridos após o cabeçalho de um pacote IP, o AH e o ESP podem ser utilizados separadamente ou em conjunto.

A autenticação e integridade providas pelo AH e pelo ESP diferenciam-se pela abrangência da proteção. Quando oferecidos pelo AH, estes serviços protegem todos os campos de um pacote excetuando-se aqueles cujos valores são alterados em trânsito por roteadores. Por outro lado, a autenticação e integridade do cabeçalho ESP limita-se a parte do próprio cabeçalho ESP e a porção de dados do pacote.

2.1 Associações de Segurança

Antes que dois *hosts* possam trocar pacotes seguramente através do IPSec, um conjunto de parâmetros deve ser estabelecido: protocolo de segurança, modo de operação, algoritmo criptográfico, chave, seu tempo de vida e tamanho, dados para a proteção contra reenvio de pacotes, entre outros. Tal conjunto é denominado associação de segurança (AS) [7, 2].

Um *host* pode estabelecer diversas associações de segurança com outros. O nível de granularidade deve ser definido pelo administrador: uma política genérica, baseada em *hosts*, poderia proteger todo e qualquer tráfego entre duas entidades através de uma única AS. Em contrapartida, uma outra política, mais específica, poderia gerar uma AS para cada sessão aberta entre o *host* local e outro qualquer. Para finalizar, uma política mediana exigiria uma AS para cada tipo de tráfego (FTP, DNS, etc). Outro fator importante é que ASs são unidirecionais e comportam somente um protocolo de segurança (AH ou ESP). Desta forma, é possível que um tráfego entre dois *hosts* tenha proteções distintas nos dois sentidos.

O estabelecimento de uma AS pode ser estático ou dinâmico. No primeiro caso, todos os parâmetros devem ser manualmente inseridos pelo administrador. Este método, além de limitar a abrangência da proteção do IPSec, pode resultar em erros capazes de impedir a comunicação dada a grande quantidade de intervenção humana. No segundo caso, a AS é estabelecida através do protocolo IKE (*Internet Key Exchange*) [3], sem qualquer intervenção por parte do administrador, o que representa uma solução adequada para tornar a aplicação do IPSec automática. Neste processo, o *initiator*, entidade que inicia o processo de estabelecimento de uma AS, envia uma proposta pré-definida de parâmetros, incluindo uma relação de algoritmos criptográficos em ordem de preferência, ao outro extremo da comunicação, denominado *responder*.

Ao receber a proposta, de acordo com sua política e configuração, o *responder* deve selecionar os parâmetros desejados e enviar suas escolhas ao *initiator*. Caso os parâmetros recebidos pelo *responder* não contemplem suas especificações de proteção (e.g. nenhum dos algoritmos propostos está relacionado como aceitável na política local para proteger aquele tipo de tráfego), o estabelecimento da AS pode ser rejeitado, fazendo com que as duas entidades não consigam trocar dados referentes ao serviço específico que a AS pretendia proteger.

2.2 SPD e SAD

Para que determinados pacotes sejam submetidos a proteção do IPSec, é necessário segregá-los através de regras presentes em um repositório denominado SPD (*Security Policy Database*) [7]. As regras são compostas por seletores que identificam endereços IP, portas de origem e destino, protocolo transportado (TCP, UDP, etc), entre outros e sua modelagem é de responsabilidade do administrador.

Uma vez classificado em alguma regra no SPD, um pacote deverá ser protegido de acordo com os parâmetros consultados no SAD (*Security Association Database*), uma estrutura que armazena todas as ASs ativas de um *host*. Caso o método de estabelecimento de ASs seja manual, o administrador deverá inserir entradas diretamente no SAD. Caso contrário, o protocolo IKE irá manipulá-las.

3 *Security Level Model*

Apesar do IPSec ser capaz de resolver muitos dos problemas de segurança detectados no IP ao longo dos anos, suas elevadas complexidade e flexibilidade certamente são fatores limitantes no que diz respeito ao seu uso para a proteção do tráfego de serviços entre dois *hosts* quaisquer em uma rede [1]. Utilizá-lo sem o conhecimento de suas numerosas opções pode significar um risco à segurança de um sistema [2].

No estado atual da especificação, o IPSec representa uma solução viável e de baixo custo para a criação de ambientes estáticos e pré-definidos como as VPNs (*Virtual Private Networks*) tradicionais. Porém, apesar de suportar tal possibilidade, sua utilização em cenários onde o tráfego entre duas entidades quaisquer deve ser protegido adequadamente não parece tão simples, principalmente tratando-se de grandes estruturas. Além das limitações citadas, para prover tal característica é necessário que as políticas de segurança sejam bem-definidas e mantenham um nível mínimo de compatibilidade entre si. Todos estes requisitos podem tornar-se uma tarefa demasiadamente complexa para o administrador de sistema.

Na tentativa de facilitar a utilização do IPSec e, conseqüentemente, a criação destes cenários, propõe-se o SLM (*Security Level Model*) que, baseado em especificações de alto nível, gera as políticas e parâmetros correspondentes ao SPD e ao IKE. Os primeiros elementos para a definição do SLM foram apresentados em [8]. Nesta oportunidade definiu-se um mecanismo capaz de proteger o tráfego de serviços através de associações de segurança estabelecidas a partir de parâmetros agrupados em níveis.

3.1 Níveis de segurança

Os níveis de segurança [8] são componentes do SLM que encapsulam parâmetros necessários para o estabelecimento de ASs, incluindo: protocolos de segurança, algoritmos criptográficos, tamanho das chaves e tempo de vida das ASs. Os parâmetros de cada nível fazem com que a proteção provida por cada um seja distinta.

Foram definidos quatro níveis para o SLM com base na oferta dos serviços de autenticação, integridade e confidencialidade, através de diferentes algoritmos criptográficos e demais parâmetros do IPSec. São eles: *Unclassified*, *Confidential*, *Secret* e *Top Secret* [8]. No SLM, os parâmetros que compõem cada nível são armazenados em uma base de dados denominada *Security Level Definition*.

Nível de Segurança	Serviços
Top Secret	Telnet, SSH, FTP, POP3, HTTPS, SMTP, SNMP
Secret	DNS(*zone transfer*), NNTP, Syslog, LDAP
Confidential	FTP-DATA, HTTP, BOOTPC, BOOTPS, TFTP
Unclassified	DNS(*query*), Time, Daytime, Echo, Finger

Tabela 1: Exemplo de distribuição de serviços comuns nos níveis de segurança do SLM.

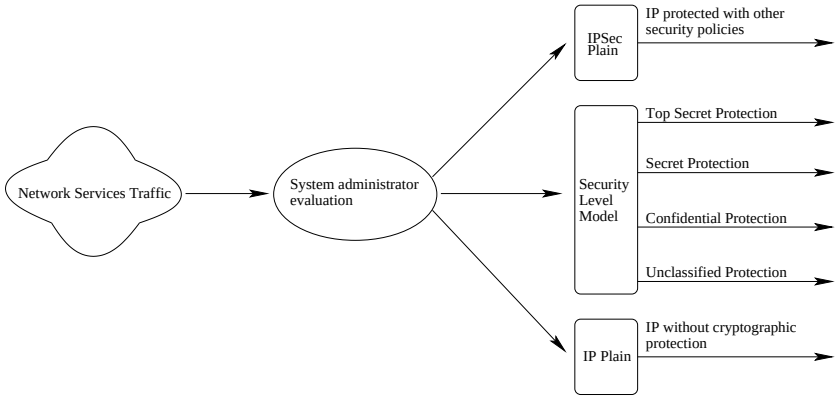

Figura 1: Proteção do tráfego de uma entidade utilizando o SLM.

Com base nas descrições dos níveis é necessário associar cada serviço a ser protegido a um nível compatível com seus requisitos de segurança[2]. Tais associações são armazenadas na base de dados *Protected Services*. Como exemplo, a Tabela 1 mostra uma possível classificação de serviços. Vale ressaltar que o objetivo principal dos níveis de segurança é a possibilidade de abstrair os seus parâmetros específicos e criar políticas baseadas somente nas suas especificações.

A Figura 1 exibe um esquema que resume a classificação dos serviços que deve ser feita para a utilização do SLM. Vale ressaltar que a proteção do tráfego das aplicações restringe-se a distribuição dos serviços nos níveis de segurança ao invés da definição de regras específicas com parâmetros próprios para cada tipo de tráfego. Além disso, serviços que não devem possuir qualquer proteção ou algum tipo de proteção específica através do IPSec podem, perfeitamente, conviver conjuntamente com aqueles sob a proteção do SLM. Por exemplo, para evitar que qualquer tipo de serviço produza tráfego desprotegido, pode-se criar uma política no IPSec, externa ao SLM, capaz de proteger todos os serviços que não possuem regras específicas contempladas no modelo. Desta forma, se algum usuário passa a utilizar alguma aplicação ainda não classificada em um nível de segurança, seu tráfego será automaticamente submetido à proteção desta regra *default*.

3.1.1 Distribuição de algoritmos de criptográficos nos níveis de segurança

Os principais componentes dos níveis de segurança são os algoritmos criptográficos e os respectivos tamanhos de suas chaves. Apesar do SLM, da mesma forma que o IPSec, não restringir-se a um conjunto fixo e limitado de algoritmos, uma atribuição inicial é necessária para o funcionamento do modelo.

[2]Neste contexto, requisitos de segurança representam a necessidade ou não de autenticação, integridade e/ou cifragem de pacotes e em que grau de proteção.

Nível de Segurança	Autenticação		Cifragem	
	Algoritmo	Chave	Algoritmo	Chave
Top Secret	HMAC-SHA2-512-96	512	AES	256
			Twofish	256
			Serpent	256
			Cast	256
			Blowfish	256
Secret	HMAC-SHA2-384-96	384	AES	128/192
			Twofish	128/192
			Serpent	128/192
			Idea	128
	HMAC-SHA2-256-96	256	Blowfish	192
			Cast	128
			3DES	168
Confidential	HMAC-SHA-1-96	160	AES	128
			Twofish	128
			Serpent	128
			Idea	128
	HMAC-RIPEMD-96	160	Blowfish	128
			Cast	128
			DES	56
Unclassified	HMAC-MD5-96	128	Não aplicável	

Tabela 2: Proposta de distribuição de algoritmos criptográficos nos níveis de segurança.

A Tabela 2[3] apresenta uma proposta utilizando protocolos publicamente conhecidos e amplamente analisados em ordem decrescente de preferência. A descoberta de vulnerabilidades em um dado algoritmo pode resultar na sua realocação para um nível inferior ou até mesmo na sua exclusão do modelo, dependendo da gravidade do problema detectado.

Na proposta apresentada existem algoritmos de cifragem com o mesmo tamanho de chave distribuídos em níveis distintos. Observe que chaves de 128 *bits* provêem garantia de proteção superior a descrição de *Confidential* e o agrupamento de algoritmos com este parâmetro no mesmo nível que o DES, com 56 *bits*, certamente mais vulnerável a ataques de força-bruta, pode representar uma inconsistência. Contudo, o custo computacional de cifrar mensagens com o DES é, na maioria das implementações, mais alto que a utilização de outros algoritmos com tamanhos de chaves superiores a 56 *bits*. Por outro lado, sua permanência se explica pelo fato de sua proteção estar de acordo com os pré-requisitos de *Confidential*. Além disso, implementações que não contenham qualquer um dos algoritmos anteriores ao DES, podem utilizá-lo para serviços classificados neste nível.

3.2 *Security Level Converter*

As três bases de dados do SLM, *Security Level Definition*, *Protected Services* e *Host Services*, apresentadas anteriormente, contêm informações de alto-nível que não são capazes de transmitir diretamente qualquer instrução ao IPSec e às suas estruturas. Em outras palavras, é necessário converter tais informações para o formato específico de uma implementação contida em uma determinada plataforma. Esta é, dentro do SLM, a função do SLC (*Security Level Converter*).

De maneira geral, o SLC processa as informações das três bases de dados e, como resultado, produz as regras da política de segurança para o SPD e os parâmetros necessários à elaboração das propostas para o IKE. Na Figura 2 é mostrado um diagrama que ilustra o funcionamento geral do SLC, que, através de parâmetros independentes de plataforma, gera, sem qualquer intervenção por parte do administrador de sistemas, as configurações de uma implementação específica do IPSec, dependentes de plataforma, portanto, necessárias à efetiva proteção dos pacotes IP dos serviços vinculados ao SLM.

[3]Os algoritmos HMAC-MD5-96, HMAC-SHA-1-96 e MD5 são de implementação obrigatória no IPSec.

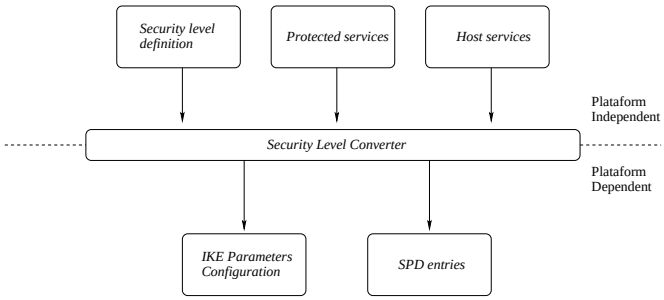

Figura 2: Esquema de abstração provido pelo SLM.

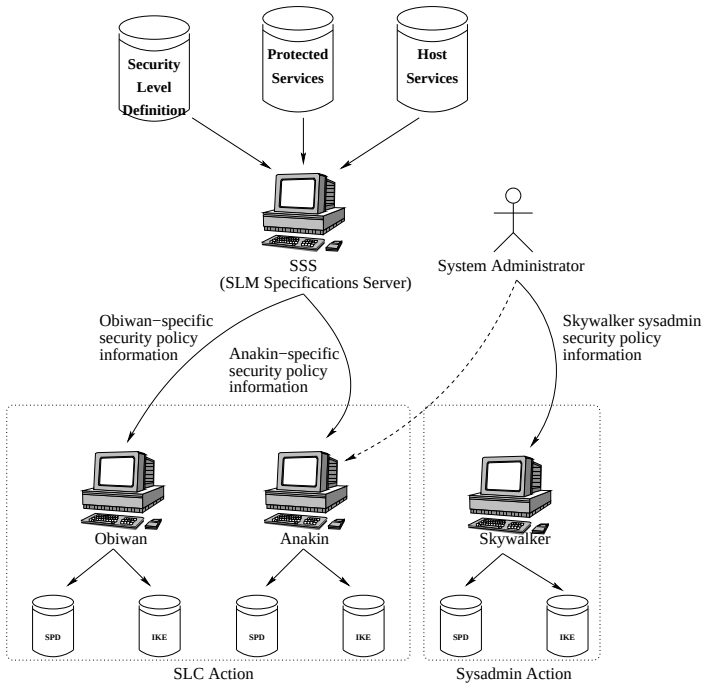

Figura 3: Cenário de um ambiente onde dois *hosts* estão protegidos pelo SLM.

3.3 Aspectos gerais de funcionamento

Com o intuito de facilitar suas manutenções, as bases de dados são centralizadas em um servidor da rede denominado SSS (*SLM Specifications Server*), responsável por prover a todos os *hosts* incluídos na proteção do SLM as informações necessárias à geração de seus parâmetros de configuração.

No momento da inicialização de um sistema, o SLC é executado e sua primeira providência é fazer uma consulta ao SSS solicitando a entrada relativa ao *host* em *Host Services*, para obter conhecimento a respeito dos serviços e os respectivos modos de interação. Em seguida, são consultados os níveis de segurança associados a cada serviço listado para o *host*, de acordo com a distribuição realizada pelo administrador, armazenada em *Protected Services*. Posteriormente, o SLC solicita ao SSS o recebimento das especificações do nível de segurança de cada um dos serviços associados ao *host*, contidas em *Security Level Definition*.

De posse das informações de alto-nível, armazenadas nas bases de dados mantidas

no SSS, o SLC, que deve compreender o formato de funcionamento da implementação do IPSec contida na plataforma utilizada, processa os dados recebidos e os traduz para a linguagem de especificação da plataforma em uso. A partir desse momento, o *host* contendo as configurações necessárias terá o tráfego dos seus serviços contemplados pelo SLM protegido através do IPSec, conforme os parâmetros de segurança produzidos. É importante notar que o SLM não interfere mais na segurança da comunicação dos serviços, a não ser que o sistema seja reiniciado ou o administrador altere alguma especificação nas bases de dados e execute manualmente o SLC. A Figura 3 exibe um ambiente onde dois *hosts*, *Obiwan* e *Anakin*, utilizam o SLM para a geração automática das configurações do IPSec e outro, *Skywalker*, cuja configuração é realizada através da intervenção manual do administrador de sistemas, que pode, inclusive, acrescentar outros parâmetros às máquinas protegidas pelo SLM, conforme o indicado através da linha pontilhada.

As regras geradas para cada serviço (como cliente, servidor ou ambos) exigem sempre que sejam estabelecidas duas associações de segurança para cada protocolo de segurança, uma para cada sentido da comunicação. Desta forma, a combinação dos dois protocolos requer a definição de quatro associações de segurança onde cada par é definido com base na mesma proposta de algoritmos e parâmetros. Caso um *host* cujas regras do SPD e parâmetros do IKE não tenham sidos gerados pelo SLM tente se comunicar com um dos serviços em um *host* com regras criadas a partir do SLM, dois requisitos básicos fazem-se necessários. Primeiro, a concordância, segundo as regras do SPD, quanto à aplicação do IPSec, os protocolos de segurança e a criação de um par de associação de associação de segurança para cada protocolo (exigido pelo SPD do *host* incluso no SLM). Segundo, a definição de pelo menos uma combinação de algoritmos e outros parâmetros comuns entre os dois extremos, de acordo com a proposta elaborada pelo IKE.

Caso as configurações do IKE (algoritmos criptográficos, por exemplo) sejam propositalmente manipuladas para que seja gerada uma proposta composta por parâmetros com garantia de proteção inferior àquela que deveria ser provida segundo o nível de segurança associado ao serviço, o outro extremo da comunicação, contemplado pelo SLM, irá rejeitá-la, devido a sua incompatibilidade com a relação de parâmetros aceitáveis inseridos pelo SLC na configuração do IKE para proteção da aplicação em questão.

4 Implementação

O SLM foi desenvolvido com base na implementação do IPSec e IKE mantidas pelo projeto KAME[4], iniciativa de empresas japonesas para a união de esforços destinados a um suporte unificado dos dois protocolos anteriores para sistemas BSD. Como plataforma, o FreeBSD foi utilizado dada a sua popularidade e quantidade de documentação disponível em relação as outras variantes do sistema BSD, o OpenBSD e o NetBSD, por exemplo.

As três bases de dados são implementadas como classes definidas para o modelo no LDAP (*Lightweight Directory Access Protocol*) [4], um protocolo capaz de centralizar informações e distribuí-las a um conjunto de entidades de acordo com estruturas pré-estabelecidas. Os objetos das classes, dispostos de maneira hierárquica, facilitam o gerenciamento e a organização das informações. *Security Level Definition*, *Protected Services* e *Host Services* correspondem as classes `secLevel`, `secServ` e `slmHost`, respectivamente.

No desenvolvimento do SLC foi utilizado o Perl dada a sua facilidade para lidar com

[4]http://www.kame.net

strings e arquivos, sua popularidade para a implementação de ferramentas de administração e segurança de sistemas e, ainda, pelo suporte estável para a conexão com servidores LDAP. As funções contidas no módulo `Net::LDAP` serviram como apoio para a manipulação das informações contidas nas bases de dados do SLM.

As regras da política de segurança contidas no arquivo gerado pelo SLC são inseridas no SPD através do `setkey`, utilitário da plataforma IPSec do projeto KAME. O arquivo contendo os parâmetros do IKE, também criado pelo SLC, é passado como argumento para o *daemon* `racoon`, implementação desse protocolo na mesma plataforma. Estas operações são feitas através da chamada do SLC e dos aplicativos correspondentes a partir do *script* `/etc/rc`, executado no momento da inicialização do sistema.

5 Conclusões

A criação de políticas de segurança no IPSec voltadas para a proteção do tráfego de cada serviço é um processo complexo e custoso para o administrador de sistemas. Além disso, dado que cada *host* deve conter sua política armazenada localmente, a manutenção do sincronismo entre as informações presentes em todos os *hosts* é outro fator que contribui com a dificuldade de utilizar o IPSec para a finalidade em questão. Contudo, se por um lado, o uso de políticas especializadas requer alto custo de implantação e manutenção, por outro, o uso de políticas genéricas pode colocar em risco a segurança do ambiente computacional uma vez que o tráfego de aplicações com requisitos distintos de segurança é protegido com base nos mesmos parâmetros.

Desenvolvido com o intuito de reduzir o custo de implantação do IPSec, o SLM provê mecanismos para a definição de políticas de segurança baseadas em cada aplicação através do encapsulamento de parâmetros em níveis e da representação de suas informações, centralizadas em um servidor, através de uma linguagem independente de plataforma utilizada para a criação dos parâmetros do IPSec e do IKE específicos da plataforma utilizada, sem qualquer intervenção por parte do administrador de sistemas.

Referências

[1] Niels Ferguson e Bruce Schneier. A Cryptographic Evaluation of IPsec. Relatório técnico, Counterpane Internet Security, Inc., San Jose, CA, USA, 2000.

[2] Sheila Frankel. *Demystifying the IPsec Puzzle*. Artech House, Norwood, Massachusetts, 2001.

[3] D. Harkins e D. Carrel. *The Internet Key Exchange (IKE)*. Internet Engineering Task Force, RFC 2409, 1998.

[4] Tim Howes, Mark Smith, e Gordon Good. *Understanding and Deploying LDAP Directory Services*. NewRiders Publishing, 1998.

[5] S. Kent e R. Atkinson. *IP Authentication Header (AH)*. Internet Engineering Task Force, RFC 2402, 1998.

[6] S. Kent e R. Atkinson. *IP Encapsulating Security Payload (ESP)*. Internet Engineering Task Force, RFC 2406, 1998.

[7] S. Kent e R. Atkinson. *Security Architecture for the Internet Protocol*. Internet Engineering Task Force, RFC 2401, 1998.

[8] Jansen Carlo Sena e Paulo Lício de Geus. Um Mecanismo para Estabelecimento de Associações de Segurança Baseado em Categorias de Serviço. Em *III Simpósio Segurança em Informática*, pp. 193–202, São José dos Campos, São Paulo, Brasil, 2001.