UM MECANISMO PARA ESTABELECIMENTO DE ASSOCIAÇÕES DE SEGURANÇA BASEADO EM CATEGORIAS DE SERVIÇOS

RESUMO

Este artigo apresenta um modelo capaz de prover, através do IPSec, diferentes níveis de proteção ao tráfego IP de serviços comuns a diversos ambientes computacionais, de acordo com seus requisitos de segurança. Este modelo tem como objetivo especificar um uso racional e escalável do IPSec, viabilizando seu uso transparente por aplicações voltadas para o ambiente heterogêneo e descentralizado da Internet.

ABSTRACT

This paper presents a model that provides, through IPSec, different protection levels to the IPSec traffic generated by services common to must computing environments, according to their security requirements. The goal of this model is to specify a rational and scalable use of IPSec, allowing for its transparent use by applications hosted in the heterogenous and decentralized environment of the Internet.

1 Introdução

A especificação do IPSec na tentativa de prover segurança ao nível de rede e a definição do IPv6 com o objetivo de adaptar o protocolo IP aos novos requisitos necessários para a manutenção da Internet, trouxeram consigo a possibilidade de definir novas arquiteturas de segurança, através da utilização de algoritmos de autenticação, integridade e cifragem para proteger os dados carregados nos datagramas IP.

Neste artigo, é proposto um modelo onde serviços de rede são dispostos em níveis de segurança pré-estabelecidos de acordo com os requisitos de proteção identificados para cada conjunto.

Cada nível de segurança relaciona uma lista de algoritmos criptográficos compatíveis com suas especificações e necessidades. Tal lista deve ser utilizada como base na formulação de parâmetros para o estabelecimento de associações de segurança entre entidades que pretendem fazer uso de um dos serviços contidos num determinado nível. Este mecanismo pode ser utilizado como um elemento adicional para protocolos de estabelecimento de associações dinâmicas de segurança, como o ISAKMP, e, conseqüentemente, para a especificação de *firewalls*, utilizando os protocolos AH e ESP, definidos pelo IPSec.

Na Seção 2 são apresentados conceitos básicos relacionados ao IPSec, incluindo suas principais estruturas e seu funcionamento geral. Na Seção 3, o protocolo ISAKMP é brevemente explanado.

O modelo proposto neste artigo é estabelecido em duas etapas distintas. Na primeira (Seção 4), é descrito o modelo de níveis de segurança definido, incluindo as especificações propostas para cada nível. Na segunda (Seção 5), é especificado o modelo para utilização da categorização de serviços em níveis de segurança, estebelecidos na etapa anterior, seus componentes e sua interação com o IPSec e ISAKMP.

Na Seção 6 são apresentadas considerações finais e, em seguida, na Seção 7, são identificadas possíveis extensões ao modelo.

2 IP Security (IPSec)

O protocolo IPv4 [20, 21], versão atual do IP utilizada na Internet, não foi projetado para um ambiente seguro. Isto se deve ao fato de que a rede mundial era utilizada fundamentalmente por universidades e centros de pesquisa, sendo seu uso baseado em uma cooperação harmoniosa entre os usuários. Contudo, o aumento exponencial do uso da Internet fez surgir a necessidade de definição de mecanismos de segurança como os *firewalls* e os protocolos de aplicação baseados em algoritmos criptográficos, como o HTTPS e SSH [22].

Após muitas discussões sobre qual seria a camada correta para prover proteção, quais os algoritmos ideais a serem utilizados e até mesmo se tais serviços seriam realmente necessários [12], o IETF resolveu especificar o IPSec [4], uma família de protocolos cujo objetivo é prover serviços de segurança ao IPv4 e ao IPv6 [7] [1].

Entre os serviços oferecidos pelo IPSec tem-se: controle de acesso, integridade sem conexão[2], autenticação da origem dos dados, proteção contra pacotes retransmitidos (ataques de *replay*), confidencialidade dos dados e confidencialidade do fluxo de tráfego limitado. Tais serviços são implementados através de dois protocolos: o AH (*Authentication Header*) [5] e o ESP (*Encrypted Security Payload*) [6]. A Tabela 1, mostra o conjunto de serviços

[1] No IPv6, a implementação do IPSec é obrigatória e, portanto, deverá fazer parte dos *firewalls* a serem desenvolvidos para este protocolo.

[2] *connectionless integrity*

	AH	ESP[a]	ESP[b]
Controle de acesso	✓	✓	✓
Integridade sem conexão	✓		✓
Autenticação	✓		✓
Proteção contra *replay*	✓	✓	✓
Confidencialidade		✓	✓
Confidencialidade do fluxo de tráfego limitado		✓	✓

[a] ESP provendo somente cifragem.
[b] ESP provendo autenticação e cifragem.

Tabela 1: Serviços oferecidos pelos protocolos de segurança AH e ESP.

disponibilizados por cada protocolo. É importante notar que o ESP oferece, opcionalmente, além de confidencialidade, serviços de autenticação e integridade aos dados cifrados. Isto se dá pela possibilidade de ataques ao serviço de cifragem quando utilizado sem qualquer mecanismo de autenticação [10]. A comunicação entre entidades pode fazer uso de um dos cabeçalhos ou de ambos, de acordo com as necessidades de cada serviço.

Diversos algoritmos podem ser utilizados para implementar os serviços do IPSec, porém sua especificação relaciona algoritmos cuja implementação é obrigatória estabelecendo-se, assim, um conjunto mínimo de algoritmos comuns a todas as implementações [4]. São eles:

- **HMAC/MD5** e **HMAC/SHA-1**: utilizados pelo ESP e AH para serviços de autenticação e integridade;
- **DES/CBC**: utilizado pelo ESP para a privacidade dos dados;
- Dois algoritmos nulos, um para autenticação/integridade e outro para cifragem, utilizados para depuração e testes.

Muito se discute sobre a segurança dos algoritmos utilizados como padrão. Por exemplo, peculiaridades do MD5 permitem que um computador, com determinada capacidade de processamento, encontre mensagens associadas a um determinado *checksum* em poucos dias [17]. Já o DES/CBC utiliza chaves de 56 bits que não são seguras para garantir a privacidade de dados por muito tempo, não sendo, por exemplo, adequado para a segurança de transações comerciais [16, 14]. Porém, o uso deste algoritmo pode ser adequado para determinados fins que necessitam de privacidade por períodos curtos de tempo, como simples consultas em servidores DNS.

Apesar da complexidade do IPSec apontada em [11], Ferguson e Schneier afirmam que o IPSec "é provavelmente o melhor protocolo de segurança para o IP disponível no momento". Aliado a isto, o

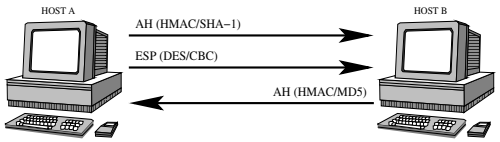

Figura 1: Exemplo de associações de segurança estabelecidas entre dois *hosts*.

fato deste protocolo ser nativo no IPv6, seu uso parece ser extremamente importante para a definição de novos mecanismos de segurança.

2.1 Associações de Segurança

Para que duas ou mais entidades se comuniquem de forma segura, utilizando algoritmos criptográficos de autenticação, integridade e/ou cifragem, um conjunto de parâmetros deve ser pré-estabelecido. Entre eles, os algoritmos a serem utilizados, seus modos de operação, as chaves criptográficas e o tempo de vida destas chaves. Tal conjunto é denominado associação de segurança (AS) [4, 12].

Uma entidade pode estabelecer diversas associações de segurança com diversas outras entidades. Para que seja possível diferenciar os vários contextos de segurança, uma entidade precisa definir um SPI (*Security Parameter Index*) para cada AS estabelecida. Cada extremo de uma AS precisa conhecer o SPI fornecido pelo outro extremo[3]. Toda AS deve ser identificada de maneira única através da tripla: SPI, endereço de destino e identificador do protocolo de segurança (AH ou ESP, no caso do IPSec). É importante notar que uma associação de segurança é unidirecional, podendo listar somente um protocolo de segurança. Por exemplo, se o AH e o ESP são utilizados para proteger o tráfego IP entre duas máquinas em ambas as direções, quatro ASs devem ser estabelecidas, duas para cada sentido. A Figura 1 mostra uma configuração entre dois *hosts*, A e B, onde todo o tráfego de A para B é autenticado com o HMAC-SHA1 (AH) e cifrado com o DES-CBC (ESP), e o tráfego de B para A utiliza HMAC-MD5 (AH) para autenticar e garantir a integridade dos pacotes enviados.

O estabelecimento de uma associação de segurança pode ser estático ou dinâmico. No modo estático, os parâmetros da AS devem ser configurados manualmente pelo administrador do sistema, inviabilizando seu uso em ambientes onde associações de segurança podem ser estabelecidas entre quaisquer entidades. O modo dinâmico utiliza protocolos para a troca de chaves, como o SKIP [18] e o OAKLEY [3], e protocolos para o estabelecimento e manutenção das ASs, como o ISAKMP [1], e é de especial interesse para o desenvolvimento de mecanismos de segurança capazes de interagir de maneira segura com qualquer entidade em uma rede.

[3] SPIs gerados para endereços *multicast* possuem características especiais que fogem do contexto deste artigo.

2.2 SPD e SAD

Duas bases de dados, o SPD (*Security Policy Database*) e o SAD (*Security Association Database*), são definidas para auxiliar a implementação do IPSec [4]. O SPD contém uma lista ordenada de políticas de segurança que especificam a proteção (serviços de segurança, algoritmos, etc.) que deve ser aplicada ao tráfego IP, filtrado através de parâmetros denominados seletores. Cada pacote filtrado deve ser submetido a um dos três seguintes modos de processamento:

- **Discard**: pacote não deve continuar sendo processado e, portanto, deve ser descartado;
- **Bypass IPSec**: pacote não deve ser submetido a qualquer manipulação por parte do IPSec e deve continuar sendo processado;
- **Apply IPSec**: pacote deve ser processado pelo IPSec com a política de segurança relacionada;

Os seletores são informações que podem ser extraídas dos cabeçalhos dos protocolos IP, UDP, TCP, entre outros. Utilizados nas políticas de segurança presentes no SPD, eles definem o nível de granularidade de aplicação do IPSec. Por exemplo, assim como toda a comunicação entre duas entidades pode ocorrer através da mesma AS, o uso de seletores mais específicos pode fazer com que cada tipo de serviço (NFS, DNS, etc) utilize ASs diferentes. Seis conjuntos de seletores estão relacionados na especificação do IPSec [4]: endereço IP[4] de destino[5], endereço IP de origem, nome (de usuário ou de sistema), nível de sensibilidade[6], protocolo da camada de transporte (TCP ou UDP) e portas origem e destino do protocolo de transporte.

Todos os pacotes (chegando ou saindo) de uma entidade devem ser analisados de acordo com os seletores das políticas de segurança relacionadas no SPD. A Figura 2, mostra um diagrama elaborado para ilustrar o processamento inicial de pacotes quando da utilização do IPSec. Após comparar os valores contidos em um pacote com os dos seletores, é possível determinar o próximo passo para o processamento do pacote. Caso o pacote seja descartado, tal ação pode ser registrada para auditorias futuras [4]. Se forem detectadas políticas de segurança correspondentes, o IPSec dá continuidade ao processamento do pacote.

O SAD (*Security Association Database*) permite que uma entidade armazene os parâmetros de cada AS ativa. Desta forma, toda AS estabelecida em uma entidade deve conter uma entrada no SAD. Quando um pacote é recebido por uma entidade, é feita uma busca no SAD com a chave (SPI, endereço de destino, identificador do protocolo de segurança) para verificar a existência de uma AS a ser utilizada no processamento do pacote.

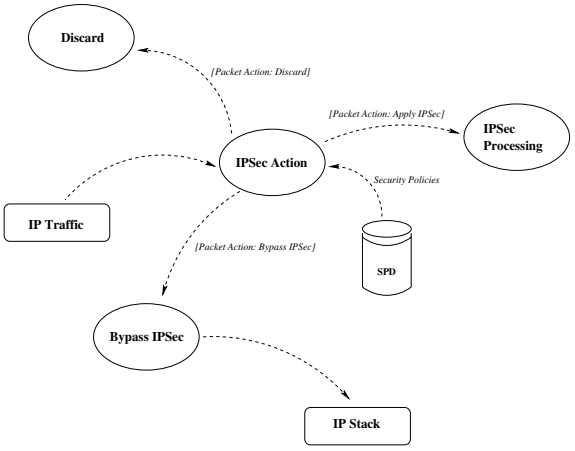

Figura 2: Modelo de processamento de pacotes no IPSec de acordo com os valores de seletores do SPD.

2.2.1 Interação

Para que seja possível gerenciar a criação e manutenção de ASs, é necessário que os dados do SPD e do SAD estejam relacionados e consistentes entre si.

Quando um pacote está sendo enviado por uma entidade, as políticas de segurança relacionadas devem ser consultadas no SPD. De posse de tais informações, uma busca no SAD deve verificar a existência de ASs correspondentes às políticas selecionadas. Caso tais ASs não existam, novas ASs devem ser estabelecidas. Por outro lado, se as ASs necessárias já constam no SAD, o IPSec insere os cabeçalhos necessários (AH, ESP ou ambos), utilizando os requisitos estabelecidos em cada AS, e envia o pacote.

Ao receber um pacote, uma entidade primeiramente verifica a existência das ASs indicadas pelo pacote no SAD. Se estas não existem, o pacote deve ser descartado e, de acordo com a implementação, tal evento deve ser registrado [4]. Caso contrário, os dados das ASs devem ser utilizados para processar o pacote, validando a autenticação e integridade, no caso do AH, e decifrando os dados, no caso do ESP. Opcionalmente, como já foi descrito anteriormente, a origem e a integridade dos dados cifrados podem ser conferidas (Seção 2). Antes do pacote ser repassado à pilha IP, os seus campos são comparados aos seletores do SPD, com o objetivo de verificar se as ASs utilizadas no processamento do pacote estão de acordo com as políticas de proteção pré-estabelecidas.

A Figura 3 mostra um exemplo onde dois *hosts*, A e B, comunicam-se utilizando o AH e ESP em

[4] Os endereços IPs citados referem-se a IPv4 e IPv6.

[5] Quando o modo de tunelamento está sendo utilizado, existem diferenças entre este endereço e o endereço destino utilizado para identificar uma AS [4]. Este último pode ser o endereço do *gateway* na extremidade de um túnel e o primeiro, o endereço destino contido no pacote tunelado

[6] Utilizado em sistemas que classificam informações em rótulos pré-definidos. Este seletor não é obrigatório em toda implementação.

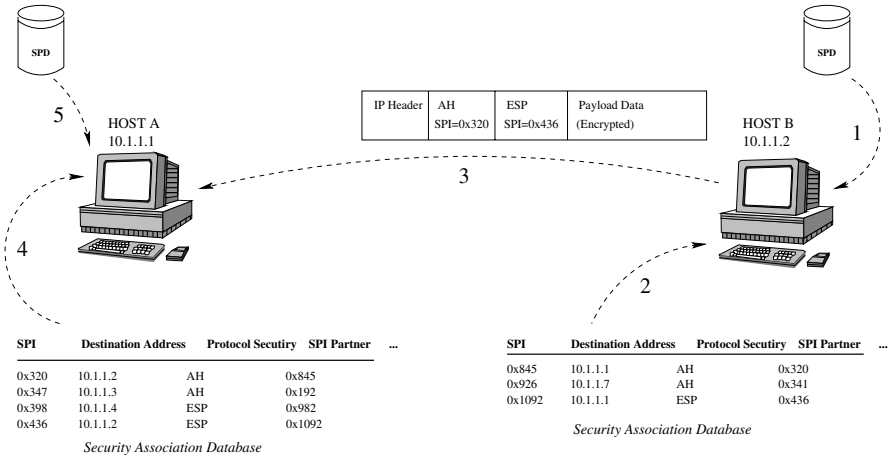

Figura 3: Exemplo simplificado de *hosts* comunicando-se através de uma associação de segurança existente. Antes de enviar um pacote para A, B consulta o seu SPD para determinar qual ação deverá ser aplicada ao pacote, e detecta a necessidade de utilização do AH e ESP (1). Em seguida, o SAD é consultado para verificar a existência ou não de ASs relacionadas. Neste exemplo, duas ASs (uma para o AH e outra para o ESP) são encontradas (2). Os cabeçalhos correspondentes são acrescentados e o pacote é enviado para A (3). Ao receber este pacote, A consulta o seu SAD e recupera os dados das ASs para processar o pacote (4). Após o processamento, o SPD é consultado para verificar se as ASs utilizadas realmente contém a proteção contida na política de segurança estabelecida (5).

ambos os sentidos através de ASs já estabelecidas.

Há ainda algumas considerações a serem feitas a respeito da forma como o SAD deve utilizar os dados das políticas fornecidas pelo SPD. Considere, por exemplo, que uma determinada política, contida no SPD de um *gateway*, especifica que todos os endereços de origem, dentro da faixa 10.1.1.1 até 10.1.1.100, devem utilizar o mesmo conjunto de parâmetros para o estabelecimento das ASs. Se uma entidade de endereço 10.1.1.43 envia um pacote, certamente o *gateway* irá utilizar os parâmetros definidos pela política anterior para criar uma AS e, conseqüentemente, uma nova entrada no SAD. Se, em seguida, uma outra entidade, 10.1.1.65, envia um pacote, o *gateway* utilizará a mesma política de segurança de 10.1.1.43. Sendo assim, existem duas formas de continuar o processamento:

- 10.1.1.65 utiliza a mesma AS estabelecida para 10.1.1.43;
- 10.1.1.65 estabelece uma nova AS.

A questão está em determinar se uma política de segurança estabelecida pelo uso de faixas de endereços deve gerar uma entrada no SAD com a mesma faixa de endereço ou uma entrada com o valor do endereço contido no pacote. No primeiro caso, é possível que todos os pacotes representados por uma política de segurança compartilhem uma mesma AS. No segundo, somente os pacotes que possuem os mesmos valores nos cabeçalhos podem fazer uso da mesma AS. Ambos os casos possuem utilidade e, portanto, o SPD deve indicar como o SAD deve derivar os valores dos seletores para gerar uma entrada [4].

3 ISAKMP

O estabelecimento manual de ASs é simples e pode proporcionar o uso do IPSec entre ambientes pré-estabelecidos. Porém, tal procedimento é demasiadamente dispendioso, altamente passível de erros no que diz respeito aos parâmetros de configuração e, portanto, não-escalável, tornando-o inadequado para ambientes que, como a Internet, necessitam do estabelecimento de ASs sob demanda. Desta forma, um conjunto de mecanismos foi definido pelo IETF para prover o estabelecimento dinâmico de ASs.

O ISAKMP (*Internet Security Association and Key Management Protocol*) é um *framework* que define diretrizes e estruturas para o estabelecimento, negociação, modificação e remoção de ASs [1] para diversos protocolos, por exemplo: OSPF, TLS e em especial, o IPSec. A geração de ASs para um protocolo se dá em duas etapas: primeiro é estabelecida uma AS do próprio ISAKMP para proteger o tráfego para a segunda fase, onde é definida a AS do protocolo de segurança utilizado.

Na terminologia do ISAKMP, um conjunto de serviços de segurança a ser utilizado compõe uma suíte de proteção[7]. Por exemplo, uma suíte de proteção pode especificar a utilização do 3DES/CBC para cifragem com o ESP e HMAC/MD5 para autenticação/integridade no AH. Para sinalizar quais serviços devem ser utilizados no estabelecimento das ASs é necessário repassar ao ISAKMP uma proposta, composta por uma lista de suítes de proteção em ordem decrescente de preferência [1]. Este mecanismo é de fundamental importância para o modelo que será apresentado, pois através dele é possível estabelecer ASs dinâmicas utilizando parâmetros diferentes entre duas entidades, de acordo com os re-

[7] *protection suite*

quisitos de segurança do tráfego.

O ISAKMP, porém, não define mecanismos específicos para a troca de chaves e manutenção de ASs. Para tanto, foi definido o IKE (*Internet Key Exchange*), um protocolo baseado nos mecanismos de troca de chaves OAKLEY [3] e SKEME [9] utilizando as definições do ISAKMP.

4 Níveis de segurança

Uma grande variedade de serviços é disponibilizada em uma rede. Serviços podem possuir requisitos de segurança distintos. Neste caso, entende-se por requisitos de segurança a necessidade de autenticação/integridade e/ou cifragem e em que grau de proteção. Por exemplo, o serviço *time* não requer o uso de algoritmos de cifragem extremamente seguros que podem prejudicar o seu desempenho. Por outro lado, para serviços como transferência de zonas de DNS, é suficiente pensar que o uso de algoritmos mais seguros é de extrema conveniência para a proteção dos dados transmitidos, dada a possibilidade de, por exemplo, um atacante capturar a relação de todas as máquinas cadastradas pelo servidor de nomes ou mesmo, falsificar uma transferência de zona trocando os endereços de todos os *hosts*.

A primeira etapa de especificação do modelo a ser proposto neste artigo, compreende o agrupamento de serviços que possuem requisitos de segurança semelhantes em diversos níveis. Desta forma, é possível especificar, para cada nível, algoritmos criptográficos comuns a serem utilizados no estabelecimento de ASs. Por exemplo, serviços que necessitam somente de autenticação por períodos curtos de tempo devem estabelecer ASs baseando-se nos algoritmos relacionados em seu nível. Com isto, pretende-se utilizar um conjunto pré-definido de algoritmos, adequados para cada nível de segurança, na tentativa de: prover a proteção necessária para seus serviços e padronizar os algoritmos a serem utilizados no estabelecimento de ASs. Evita-se, assim, o emprego de algoritmos caros em situações desnecessárias, minimizando o impacto sobre o desempenho do sistema, e a utilização de algoritmos fracos para serviços que requerem maior proteção. Além disso, garante-se a compatibilidade dos algoritmos utilizados na negociação de parâmetros para a geração de novas ASs em ambientes heterogêneos.

É importante salientar que, a categorização de serviços em níveis proposta, impede que ASs deixem de ser estabelecidas por falta de algoritmos comuns entre dois ambientes distintos. Além disso, os algoritmos utilizados garantem a proteção especificada por cada nivel, evitando que, dois sistemas concordem sobre o uso de um algoritmo inadequado para proteger um serviço específico.

Pos.	Nível	Categorias
1	*Top Secret*	*marketing*, financeiro, estatísticas, estratégias
2	*Secret*	*marketing*, financeiro, estatísticas
3	*Confidential*	estatísticas, produtos
4	*Unclassified*	produtos

Tabela 2: Instância do modelo de LaPadula utilizando quatro níveis, aplicado a uma empresa hipotética.

4.1 Especificação dos níveis

Diversos modelos foram especificados para rotular informações em níveis com o intuito de segregá-las em graus de importância e confidencialidade. Um dos principais modelos descritos é o de LaPadula [19], também conhecido como MLS (*Multi-Level Security*), desenvolvido para prover suporte à informações militares e governamentais.

No modelo de LaPadula, cada objeto é associado a um nível de segurança, que descreve a forma de tratamento e manipulação de suas informações, representado na forma (Classificação do Nível, Conjunto de Categorias).

Categorias são segmentações internas de um nível. Por exemplo, dentro de um nível que contém informações restritas aos gerentes de uma empresa pode-se ter categorias como *marketing*, dados financeiros e estatísticas. Entre os níveis existe o conceito de dominância: um nível domina outro se for hierarquicamente superior e contiver o conjunto de categorias do nível inferior. A Tabela 2 exibe uma instânciação do modelo de LaPadula, contendo quatro níveis, voltado para a segregação das informações de uma empresa. Neste exemplo, o nível *Top Secret* domina *Secret*, pois: *Top Secret* > *Secret* e (*marketing*, financeiro, estatísticas, estratégias) $\supseteq$ (*marketing*, financeiro, estatísticas). Por outro lado, *Secret* não domina *Confidential*, pois apesar de *Secret* > *Confidential*, (*marketing*, financeiro, estatística) $\not\supseteq$ (estatísticas, produtos).

Baseado na estrutura de LaPadula, propõe-se um novo modelo contendo quatro níveis de segurança (*Unclassified*, *Confidential*, *Secret* e *Top Secret*), voltados para a segregação do tráfego de aplicações. Diferentemente de LaPadula, onde a proteção é aplicada a informações estáticas, a organização proposta tem o objetivo de prover proteção a conteúdos dinâmicos: pacotes sendo transmitidos entre dois ambientes. Desta forma, é necessário caracterizar cada um dos níveis, definido seus requisitos com base nos tipos de aplicação e suas necessidades e implicações de segurança.

A seguir são apresentadas as especificações propostas para cada nível:

- **Unclassified**: serviços que necessitam somente de autenticidade e integridade de seu tráfego por períodos curtos de tempo. Neste nível a

cifragem não é fundamental e, portanto, não deve ser utilizada;

- **Confidential**: serviços que necessitam de autenticação, integridade e cifragem do seu tráfego por períodos curtos de tempo. Este nível pode ser adequado para a inclusão de algoritmos de cifragem experimentais;

- **Secret**: serviços que necessitam de autenticação, integridade e cifragem do seu tráfego por períodos razoáveis de tempo. Os algoritmos de autenticação e cifragem deste nível podem estar entre os utilizados pelo nível anterior, contanto que possuam modos de operação e tamanho de chaves mais seguros;

- **Top Secret**: serviços que necessitam de autenticação, integridade e cifragem do seu tráfego por períodos indeterminados de tempo. Neste nível devem ser utilizados algoritmos criptográficos que sejam garantidamente seguros, que tenham sido submetidos a análises e testes rigorosos de segurança, tendo chaves suficientemente grandes para evitar ataques de força bruta em tempos factíveis por parte de computadores com alta capacidade de processamento. As informações contidas no tráfego deste nível são potencialmente perigosas, se descobertas a qualquer momento.

Todos os níveis definidos requerem, no mínimo, a utilização de autenticação e integridade dos dados, na tentativa de evitar ataques de *spoofing*. Além disso, assume-se que os níveis que utilizam cifragem (*Confidential*, *Secret*, *Top Secret*) fazem uso dos serviços de autenticação e integridade dos dados cifrados, providos pelo ESP. Desta forma, elimina-se a possibilidade de ataques baseados na ausência destes serviços em dados cifrados [10].

Outra diferença do modelo proposto para segregar os serviços de rede em níveis para o modelo de LaPadula está na ausência de dominância entre os níveis. No modelo de LaPadula, por exemplo, o acesso ao nível *Secret* autoriza o acesso aos níveis inferiores, *Confidential* e *Unclassified*. Na estrutura proposta isto não se aplica: serviços classificados em um nível não podem ter acesso ao tráfego dos outros níveis, mesmo que sejam níveis com menos requisitos de proteção. Além disso, categorias para subdividir níveis não são requeridas.

4.2 Algoritmos criptográficos

Os níveis de segurança devem prover segurança através do uso de algoritmos criptográficos de autenticação/integridade e cifragem. Desta forma, cada nível deve conter uma lista de algoritmos criptográficos compatíveis com suas necessidades, possuindo, pelo menos, um algoritmo de cada serviço oferecido.

NS	Autenticação	
	Algoritmo	Chave
Unclassified	MD4	128
Confidential	HMAC/MD5	128
Secret	HMAC/SHA-1	160
Top Secret	HMAC/SHA-1	160
	HMAC/RIPEMD	160

Tabela 3: Algoritmos de autenticação/integridade a ser utilizados pelos níveis de segurança do modelo proposto.

NS	Cifragem	
	Algoritmo	Chave
Confidential	DES/CBC	56
Secret	3DES/CBC	192
	Cast128	40-128
	Rijndael	128/192
Top Secret	Twofish	128-256
	RC-5/CBC	40-2040
	Rijndael	256
	Idea	128

Tabela 4: Algoritmos de cifragem a serem utilizados pelos níveis de segurança do modelo proposto.

A distribuição dos algoritmos nos diversos níveis está baseada em descrições sobre as vantagens e desvantagens dos principais algoritmos criptográficos públicos [14, 15]. A Tabela 3 e a Tabela 4 mostram a relação proposta de algoritmos a ser utilizada para a implementação dos serviços de autenticação/integridade e cifragem, respectivamente, em cada um dos níveis de segurança especificado. As suítes de proteção, para o modelo apresentado, são definidas como todas as combinações possíveis de algoritmos de autenticação/integridade e cifragem (exceto para o nível *Unclassified*, que provê somente autenticação e integridade).

É importante notar que, para que se tenha garantia de interoperabilidade, os ambientes devem concordar sobre os algoritmos utilizados em todos os níveis. Ou seja, se um determinado ambiente define um conjunto próprio de algoritmos para um determinado nível, o estabelecimento de ASs com outros ambientes não contará com compatibilidade total em relação as suítes de proteção que podem ser utilizadas. Num âmbito mais geral, este é um problema associado com a utilização do IPSec em estruturas heterogêneas e descentralizadas como a Internet. Sendo assim, se não forem estabelecidos padrões para a utilização de diversas propostas comuns, todas as associações, independentemente do serviço utilizado, deverão ser estabelecidas com base em uma única proposta, contendo todos os algoritmos implementados em um sistema. Tal situação poderia ser obtida através da redução do modelo de níveis de segurança proposto a um único nível de

Nível	Serviços
Unclassified	Time, Daytime, Echo, Finger, DNS[a]
Confidential	FTP[b], SMTP, HTTP, TFTP, SSH, RPC
Secret	DNS[c], FTP[d]
Top Secret	Telnet, POP, SMTP

[a] Consultas (UDP)
[b] Conexão de dados
[c] Transferência de zona (TCP)
[d] Conexão de controle

Tabela 5: Disposição dos serviços nos níveis de segurança.

segurança, contendo todos os serviços.

4.3 Distribuição de serviços

Os serviços precisam ser dispostos nos níveis de segurança estabelecidos para que seja possível prover a proteção correspondente ao seu tráfego. Para a distribuição de cada serviço em um determinado nível, é necessário que se compreendam: os riscos envolvidos no que diz respeito à observação e falsificação do tráfego e o tempo para que as informações cifradas percam sua importância.

A Tabela 5 mostra a possível disposição proposta dos principais serviços utilizados na maioria dos ambientes computacionais nos níveis de segurança. Vale ressaltar que um serviço pode estar presente em mais de um nível. No DNS, por exemplo, consultas simples são classificadas como *Unclassified*, utilizando somente autenticação dos seus dados, evitanto o *spoofing* de respostas geradas por servidores. Já a transferência de zona, onde todo o mapa de um domínio é transferido, está classificada como *Secret* utilizando, além de autenticação, cifragem. Outro exemplo é o FTP, que utiliza duas conexões para prover o serviço. A conexão de controle, estabelecida na porta 21, usada para a passagem de comandos, faz parte do nível *Secret*, enquanto que a conexão de dados, na porta 20, está inclusa no nível *Confidential*. A distinção entre os diversos níveis de que um serviço pode fazer parte deve ser feita através do uso de seletores que identificam o protocolo de tranporte, as portas de origem e destino, entre outros.

Os serviços podem mudar de nível, de acordo com necessidades futuras, porém é necessário que se mantenha, da mesma forma que os algoritmos criptográficos, uma uniformidade da disposição, para que o modelo possa manter-se escalável, garantindo assim a interoperabilidade entre ambientes distintos.

5 Security Level Trader (SLT)

Definida a estrutura para segregar o tráfego em diversos níveis de segurança (Seção 4), a segunda etapa para a definição do modelo proposto neste artigo, visa especificar um elemento capaz de extrair o nível de proteção a ser utilizado e repassar os parâmetros para o estabelecimento de ASs para cada serviço entre duas entidades. Tal elemento deve ser ainda, capaz de conferir se o tráfego dos serviços está utilizando os algoritmos correspondentes.

Para viabilizar a implementação do modelo propõe-se a inclusão de um novo campo no SPD, denominado *Security Level*, cujo objetivo é direcionar o tráfego de um serviço segregado por um conjunto de seletores no SPD, para os níveis de segurança correspondentes, dispostos em uma base de dados cujo nome proposto é SLD (*Security Level Database*), contendo as suítes de proteção de cada nível.

Para gerenciar a aplicação dos requisitos de proteção do modelo, propõe-se a especificação de um processo, denominado SLT (*Security Level Trader*), cujos objetivos principais são:

- Extrair as informações das bases de dados (SPD e SLD) e repassar os parâmetros de segurança ao mecanismo de estabelecimento dinâmico de ASs, o ISAKMP, no caso;
- Conferir a aplicação dos requisitos de proteção, gerenciando todo o tráfego processado por uma entidade.

A Figura 4 mostra um diagrama que representa a incorporação do modelo proposto ao processamento convencional de pacotes do IPSec (Figura 2). Quando é detectada a necessidade de utilização do IPSec, o pacote é repassado primeiramente ao SLT, que consulta no SPD o valor do campo *Security Level*, para recuperar do SLD as suítes de proteção que podem ser utilizadas. De posse de tais informações, uma proposta é repassada ao ISAKMP, caso seja necessário o estabelecimento de nova(s) AS(s). Se o serviço não estiver categorizado em um dos níveis do modelo, o SLT repassa o processamento do tráfego ao IPSec convencional.

Fazendo um comparativo com o processamento do IPSec em relação à ASs já existentes (Figura 3), a utilização do modelo proposto acarreta as modificações ilustradas na Figura 5.

É importante salientar que, o uso do SPD não está restrito ao SLT. Ou seja, outras interfaces podem utilizar o SPD para fazer uso dos serviços do IPSec. Caso um pacote não possua valor no campo *Security Level*, seu processamento pode ser repassado para outro processo, permitindo o uso de diferentes políticas para o tráfego que não está comtemplado nos níveis de segurança. Porém, é fundamental que o SLT seja o primeiro processo a manipular os pacotes, evitando que políticas locais se sobreponham às políticas de segurança estabelecidas no modelo. Outra observação importante refere-se aos registros do SPD utilizados pelo modelo. Tais registros devem ser "marcados" somente para leitura, impedindo que outras interfaces alterem os registros utilizados para identificação do tráfego dos serviços

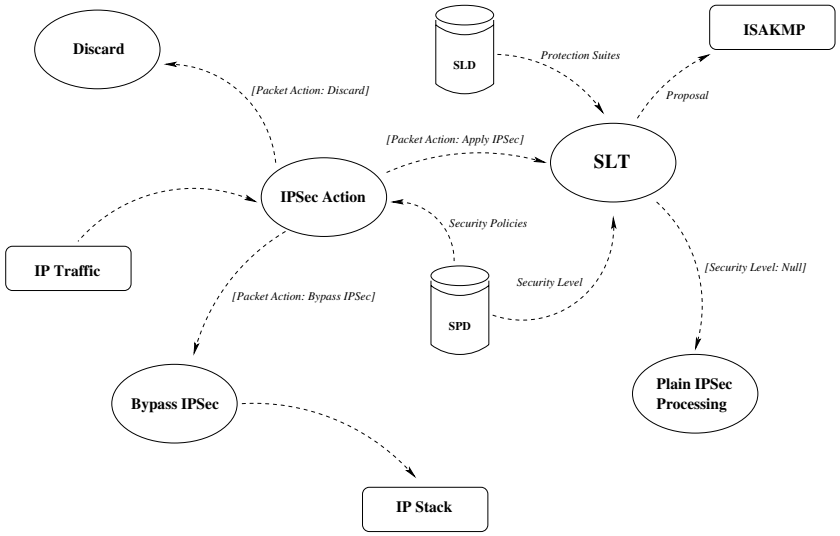

Figura 4: Modelo proposto para a aplicação dos níveis de segurança através do IPSec.

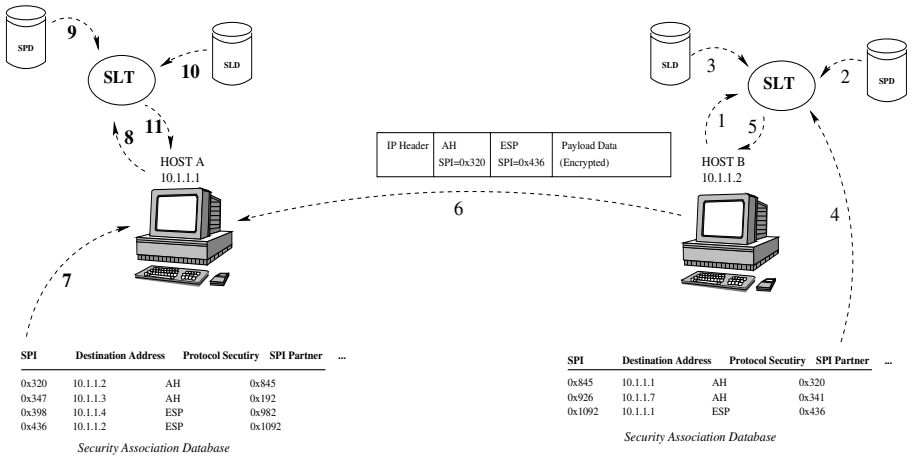

Figura 5: Exemplo de *hosts* comunicando-se através de uma associação de segurança existente utilizando o SLT. Antes de enviar um pacote para A, B requisita o SLT (1), que por sua vez, verifica o SPD (2) e o SLD (3), para determinar o nível de segurança e os algoritmos a serem utilizados. Em seguida, o SLT recupera as ASs relacionadas ao pacote (4), e repassa tais parâmetros para o processamento IPSec (5) para que o pacote seja enviado (6). Ao receber o pacote, A processa o mesmo com base nas ASs recuperadas do seu SAD, de acordo com as informações contidas no pacote (7) e repassa o pacote ao SLT (8), que verifica os dados do pacote com as políticas de segurança do SPD (9) e SLD (10) e, finalmente, retorna a validade ou não da proteção aplicada (11).

e prejudiquem o funcionamento do modelo. Certamente, para implementar tal mecanismo outra modificação na estrutrura do SPD é requerida, hava vista a ausência de estruturas capazes de impedir a modificação de registros.

A derivação dos valores dos dados de cada política no SPD deve ser feita com base nos valores do pacote (Seção 2.2.1), evitando o uso de máscaras nas ASs do SAD. Desta forma, pretende-se impedir o compartilhamento de ASs por muitos serviços ou *hosts*.

Garantindo-se a uniformidade e padronização dos algoritmos criptográficos e da disposição dos serviços nos níveis de segurança, as associações de segurança serão sempre estabelecidas de modo bidirecional, evitando que o tráfego tenha níveis de proteção distintos em cada sentido. Além disso, é possível prover proteção adequada e transparente ao tráfego IP e, conseqüentemente, às aplicações e aos usuários finais, permitindo que programadores e desenvolvedores dêem maior atenção na depuração e correção de problemas específicos das aplicações.

6 Conclusões

O IPSec é um protocolo capaz de prover segurança, através de algoritmos criptográficos de autenticação/integridade e/ou cifragem, à camada de rede. Porém, políticas locais que utilizam um conjunto próprio de algoritmos criptográficos, por exemplo, podem impedir o estabelecimento de associações de segurança entre este sistema e outro utilizando um conjunto de algoritmos distintos. Tal inconsistência limita o uso do IPSec em ambientes heterogêneos e descentralizados como a Internet. Além disso, utilizar um conjunto de algoritmos fixo para a proteção de todo o tipo de tráfego é computacionalmente custoso e inseguro.

O modelo apresentado, composto da: especificação de quatro níveis de segurança sem dominância entre si; um processo (SLT) para consulta de suítes de proteção de cada nível, repasse de propostas ao protocolo de estabelecimento de associação de segurança e verificação do uso das políticas de proteção estabelecidas; uma base de dados (SLD) com os parâmetros associados a cada nível; e pequenas alterações no SPD definido pelo IPSec, tem o objetivo de prover níveis distintos de proteção transparente ao tráfego IP.

Através do modelo proposto pretende-se estabelecer o uso racional dos recursos disponibilizados pelo IPSec, permitindo que o mesmo torne-se escalável o suficiente para prover proteção transparente ao tráfego IP de serviços comuns na Internet. Contudo, o modelo não impede o uso de políticas de segurança locais através de outros processos e interfaces para o tráfego que não estiver associado a um dos níveis de segurança.

Falhas na implementação das estruturas especificadas podem comprometer o tráfego de aplicações porém, os esforços dispendidos na implementação segura deste modelo visam beneficiar todos os serviços categorizados em um dos níveis propostos. Portanto, a centralização de esforços pode contribuir, em muito, para a definição de um mecanismo padrão para a proteção do tráfego IP.

7 Trabalhos Futuros

O uso do IPSec é capaz de prover serviços de autenticação, integridade e cifragem dos dados de pacotes IP, evitando um conjunto de ataques baseados neste protocolo, como por exemplo o *IP spoofing* e o uso de *sniffers* para observação de dados não cifrados. Porém, este protocolo não é suficiente para proteger serviços de ataques baseados no nível de aplicação. Neste contexto, o IPSec e, conseqüentemente, o modelo apresentado neste artigo devem ser incorporados aos *firewalls* e não substituí-los. Desta forma, o desenvolvimento de *firewalls* capazes de absorver os serviços oferecidos pelo IPSec é de fundamental importância para a manutenção de ambientes seguros.

Uma outra expansão do modelo seria o refinamento da disposição dos algoritmos utilizados para a especificação das suítes de proteção dos níveis de segurança. Além disso, outros algoritmos, não citados neste artigo, podem ser utilizados para compor novas suítes de proteção.

É possível, ainda, ampliar o modelo proposto através da incorporação, no SLD, de valores para o tempo de vida máximo das chaves criptográficas dos algoritmos utilizados em cada suíte de proteção, de acordo com os requisitos de cada nível de segurança.

Referências

[1] Maughan, D., Schertler, M., et al. (1998). *Internet Security Association and Key Management Protocol (ISAKMP)*. RFC 2408. Internet Engineering Task Force.

[2] Piper, D. (1998). *The Internet IP Security Domain of Interpretation for ISAKMP*. RFC 2407. Internet Engineering Task Force.

[3] Orman, H. (1998). *The OAKLEY Key Determination Protocol*. RFC 2412. Internet Engineering Task Force.

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

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

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

[7] Deering, S., Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460. Internet Engineering Task Force.

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

[9] Krawczyk, H. (1996). *SKEME: A Versatile Secure Key Exchange Mechanism for Internet*. Proceedings of the 1996 Symposium on Network and Distributed Systems Security, pp.114-127, San Diego, California.

[10] Bellovin, S. (1996). *Problem Areas For The IP Security Protocols*. Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California.

[11] Ferguson, N., Schneier, B. (1999). *A Cryptographic Evaluation of IPsec*. Counterpane Internet Security.

[12] Huitema, C. (1997). *IPv6 The New Internet Protocol*. 2nd Edition. Prentice Hall.

[13] Schneier, B. (2000). *Secrets And Lies*. John Wiley & Sons.

[14] Schneier, B. (1996). *Applied Cryptography*. 2nd Edition. John Wiley & Sons.

[15] Menezes, A. (1996). *Handbook of Applied Cryptography*. CRC Press Inc.

[16] Blaze, M., Diffie, W., Rivest, R., Shimomura, T., Thompson, E., Weiner, M. (1996). *Minimal Key Lengths of Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientist*. In URL: http://www.crypto.com/papers/keylenght.ps.

[17] Oorschot, P. C., Wiener, M. J. (1994). *Parallel Collision Search with Application to Hash Functions and Discrete Logarithms*. Proceedings of the 2nd ACM Conference on Computer and Communication Security, pp.210-218, Fairfax, Virginia.

[18] Aziz, A., Patterson, M. (1995). *Design and Implementation of SKIP*. Proceedings of the INET'95 Conference, Honolulu, Hawaií. In URL: http://skip.incog.com/inet-95.ps.

[19] Bell, D. E., LaPadula, L. J. (1973). *Technical Report M74-244*. The MITRE Corporation, Bedford, MA.

[20] Stevens, R. W. (1994). *TCP/IP Illustrated, Volume I: The Protocols*. Addison-Wesley.

[21] Comer, D. E. (2000). *Internetworking With TCP/IP Volume I: Principles, Protocols and Architecture*. 4th Edition. Prentice Hall.

[22] Zwicky, E. D., Cooper, S., Chapman, D. B. (2000). *Building Internet Firewalls*. 2nd Edition. O'Reilly and Associates.