Suporte para Segurança e Mobilidade no IPv6*

Frederico Sauer Guimarães Oliveira (1) E-Mail: fsauer@gta.ufrj.br
Aloysio de Castro P. Pedrosa (1,2) E-Mail: aloysio@gta.ufrj.br
Otto Carlos M.B. Duarte (1,2) E-Mail: otto@gta.ufrj.br

(1) Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro (UFRJ)
COPPE/PEE – Programa de Engenharia Elétrica
C.P. 68504 – CEP 21945-970 – Rio de Janeiro – RJ – Brasil
(2)Departamento de Eletrônica/EE-UFRJ

Resumo

A mobilidade e a segurança em redes de computadores são temas que vem despertando crescente interesse no momento atual. Este trabalho enfoca a utilização do IPv6 e seus cabeçalhos de autenticação e privacidade para garantir relacionamentos seguros com mobilidade de nós. Propõe, ainda, um protocolo para gerenciamento de chaves com um mecanismo assimétrico, que tem a vantagem de não exigir o compartilhamento prévio de "segredos" entre usuários.

Abstract

Mobility and security in computer networks are subjects of great interest nowadays. This work focuses on the use of IPv6 and its authentication and privacy headers to assure safe relationships concerning node mobility. Moreover, it proposes the development of a key management protocol with an asymmetric mechanism, since it does not need share "secrets" among users in advance.

1 Introdução

A mobilidade de nós e a segurança em redes de computadores têm sido assuntos de intensa discussão. As premissas estabelecidas pelo IETF (*Internet Engineering Task Force*) [1] para o desenvolvimento de uma nova versão do IP (*Internet Protocol*) incluem aspectos visando garantir transparência para os usuários, além da manutenção do endereço de rede original, características que

* Este trabalho foi realizado com recursos da UFRJ, FUJB, PROTEM-CC, CNPq, CAPES e COFECUB.

possibilitam a mobilidade. Tal transparência requer mecanismos que estabeleçam relacionamentos autenticados e otimizações no roteamento entre os nós móveis e seus correspondentes.

Vários pesquisadores vêm conduzindo trabalhos em mobilidade e suas implicações, como os projetos das Universidades de Stanford [2] e Carnegie Mellon [3]. A Universidade de Portland [4] já apresenta como resultado a implementação de um protocolo IP seguro (IPSEC) portado para FreeBSD. No Brasil, pode ser citada a pesquisa sobre o desempenho do protocolo em mobilidade VIP feita na Universidade Federal de Pernambuco [5].

Este trabalho apresenta a proposta de um protocolo que procura viabilizar a plena utilização do IPv6 em um ambiente que suporte mobilidade. Para executar esta função com segurança, os nós (móveis ou não) necessitam do estabelecimento de chaves de sessão, que são *strings* secretas, compartilhadas apenas pelos nós que estão se correspondendo. O protocolo proposto estabelece estas chaves usando um mecanismo assimétrico, dispensando contatos pessoais e diretos entre os usuários que desejam efetuar uma comunicação segura.

A seção 2 apresenta os conceitos básicos de segurança e mobilidade, a seção 3 descreve o suporte para a mobilidade no IPv6, a seção 4 detalha o protocolo proposto e a seção 5 apresenta as considerações finais.

2 Segurança e Mobilidade

Desde a criação da Internet, várias fragilidades vêm sendo detectadas e protocolos mais seguros vem sendo desenvolvidos, como o S-HTTP *(Secure HyperText Transport Protocol*) [15], SSL (*Secure Sockets Layer*) [15], SNMPv2 (*Simple Network Management Protocol version 2*) [15], além de mecanismos populares como o PGP (*Pretty Good Privacy*) [17] e PEM (*Privacy Enhanced Mail*) [17]. Todos estes produtos tem em comum o fato de serem específicos a um determinado segmento de aplicações, cabendo ao usuário uma intensa relação com a segurança de seu ambiente operacional.

A utilização de *lap-tops* e de outros equipamentos passíveis de mobilidade vem sendo cada vez mais explorados, e, a exemplo dos telefones celulares, tornam-se ferramentas indispensáveis para a condução de negócios e a tomada de decisões por seus usuários; num ambiente em que a mobilidade seja intensamente explorada, as vulnerabilidades tornam-se maiores, como no caso dos "grampos" nos ambientes sem-fio, em que uma troca de mensagens é passivamente capturada por alguém não-autorizado.

Verifica-se, portanto, a importância de um rigoroso suporte para segurança em ambientes que implementem mobilidade. As sub-seções seguintes apresentarão conceitos básicos de segurança e mobilidade.

2.1 Segurança

Alguns conceitos são básicos para a implementação de segurança em redes de computadores, no contexto deste trabalho:

- Confidencialidade - requerer que a informação seja acessível apenas por usuários autorizados. Usualmente obtida por criptografia;
- Autenticação - requerer que a origem da mensagem seja corretamente identificada, com a garantia de que esta identidade não seja falsa;
- Integridade de dados - requerer que uma mensagem não tenha sido alterada durante seu trânsito entre a origem e o destino; e
- Não-repudiação - requerer que nenhum dos parceiros possa recusar a autoria de uma transação já efetuada.

A obtenção destas características é feita através de mecanismos de criptografia e funções de *hash*. Os mecanismos de criptografia são divididos em duas categorias principais: os simétricos, em que uma única chave é compartilhada entre os nós que estão se comunicando, e os assimétricos, em que é utilizado um par de chaves para cada usuário, sendo que uma delas é pública e a outra é privada. Uma vez que um texto seja cifrado com a chave pública de um usuário, somente o possuidor de sua respectiva chave secreta conseguirá decifrá-la, mantendo a confidencialidade das mensagens trocadas entre estes usuários. No caso inverso, em que um usuário use sua própria chave secreta para codificar um texto, ao decifrá-lo com a chave pública correspondente, pode-se comprovar a autenticidade do mesmo. As funções de *hash* são usadas para gerar uma *string* de tamanho fixo a partir de um texto qualquer. Estas funções são usualmente empregadas para garantir a autenticidade de uma mensagem, conforme mostra o exemplo da figura 1.

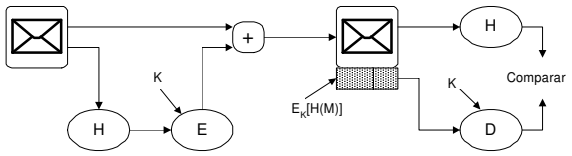

Figura 1 - Mecanismo de *hash*

Nesta figura, a mensagem original passa por um algoritmo (H) que a transforma numa *string* de tamanho fixo. Essa *string* é cifrada (E) com uma chave secreta K e concatenada à mensagem original (+), sendo então enviada ao destinatário. O resultado da decifragem (D) deste anexo ($E_K[H(M)]$), comparado com a mensagem em texto claro, provê a autenticação e a garantia da integridade da mensagem recebida.

2.2 Mobilidade

Sem um suporte específico definido para mobilidade na camada IP, um pacote destinado a um nó móvel poderia não ser recebido quando este não estivesse conectado em sua rede local (*home network*), uma vez que a única forma de roteamento utilizada é baseada no prefixo de rede no endereço de destino do pacote IP [9]. Para continuar utilizando os serviços da rede, o nó móvel deveria alterar o seu endereço IP toda vez que alterasse sua localização, de acordo com a sub-rede com a qual ele estivesse associado naquele momento. No entanto, o nó móvel não teria como manter conexões de transporte e de camadas mais altas quando ocorresse a mudança de localização.

Assim sendo, a cada nó móvel é atribuído um endereço IP permanente, e este endereço é denominado de endereço local do nó móvel (*Mobile Node Home Address*), que permanecerá inalterado independentemente de sua localização. A sub-rede IP indicada por seu endereço local é denominada sub-rede local (*home subnet*) e os mecanismos padrão de roteamento enviarão pacotes destinados ao endereço do nó móvel apenas para a sua sub-rede local. Qualquer nó com o qual o nó móvel esteja se comunicando é denominado de nó correspondente (*Correspondent Node*), que pode ser um nó móvel ou não.

A comunicação entre nós móveis e correspondentes ocorre da seguinte forma:

- quando um nó móvel está fora de sua rede local, ele adquire um endereço denominado "aos cuidados" (*care-of address*). Este endereço pode ser adquirido através de algum mecanismo de configuração automática de endereços na rede estrangeira, como o DHCPv6 (*Dinamic Host Configuration Protocol*) [10] ou pode ser o próprio endereço de um roteador (roteador *default*) que lhe prestará serviços na rede que o nó móvel está visitando, denominada de sub-rede estrangeira (*foreign subnet*);
- a associação entre o endereço local (permanente) do nó móvel e seu endereço aos cuidados é chamado de *binding*. O nó móvel envia então uma mensagem chamada *binding update* ao seu Agente Local;
- este Agente então, através de um mecanismo como o *Neighbor Discovery Protocol* [11], intercepta os pacotes na sub-rede local endereçados ao nó móvel e os encapsula para envio via túnel, de acordo com o encapsulamento para IPv6 [12], com o endereço de destino indicado pelo *binding* para o endereço do nó móvel; e
- os nós móveis e correspondentes possuem estruturas de dados denominadas *cache bindings*, destinadas a armazenar endereços IP de nós móveis e seus respectivos endereços aos cuidados. Uma vez que o nó correspondente "descubra" o endereço aos cuidados do nó móvel, um *binding*

correspondente a esta localização do nó móvel pode ser armazenada pelo nó correspondente em seu *binding cache*, possibilitando um roteamento direto para o nó móvel, evitando-se o caminho sub-ótimo representado pelo roteamento de todos os pacotes endereçados à um nó correspondente ao seu Agente Local. A figura 2 exemplifica as situações descritas acima.

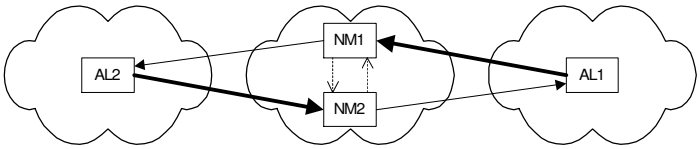

Figura 2 - Troca de pacotes entre nós móveis

Na figura 2, as setas cheias representam o roteamento normal dos pacotes, dos nós correspondentes para os Agentes Locais, e as tracejadas o roteamento direto, usando as entradas dos *cache bindings*.

3 Suporte para Segurança em Mobilidade - O Protocolo IPv6

A principal motivação para o desenvolvimento de uma nova versão para o protocolo de rede (*Internet Protocol* - IP) é o espaço de endereços, que na prática já encontrava limitações, conduzindo ao uso de 128 bites, no lugar dos 32 bites atuais. No entanto, outros problemas já apontados foram abordados, como aqueles relacionados com a segurança. Na versão atual do IP (IPv4), há apenas um campo opcional com a opção "security", que informaria apenas o quanto secreta é a informação contida no datagrama, evitando roteamentos através de sub-redes "inimigas". Outros mecanismos de segurança podem ser providos a nível de aplicação, cabendo ao usuário a responsabilidade pela sua utilização.

Na nova versão do IP [6], além do cabeçalho principal, de tamanho fixo, são criados cabeçalhos de extensão, sendo quatro de especial interesse para a segurança em mobilidade: opções de destino, roteamento, autenticação (*Authentication Header* - AH) e encapsulamento de segurança (*Encapsulating Security Payload* - ESP). O cabeçalho de opções de destino pode ser incluído para conduzir uma ou mais opções, que deverão ser processadas apenas ao chegar no endereço indicado. O pacote então não é inspecionado e/ou processado nos roteadores intermediários entre a origem e o destino. Isto é particularmente útil para o envio de mensagens de atualização de *binding* entre nós móveis e correspondentes. O cabeçalho de roteamento possui função semelhante à opção de roteamento pela fonte do IPv4, porém foi especificado para não ser inspecionado ou processado em nós intermediários entre a origem e o destino. Este cabeçalho é bastante útil para a implementação da mobilidade,

por possibilitar que otimizações de roteamento sejam feitas com menor sobrecarga, por não usar extensões (como no IPv4), e principalmente por evitar a necessidade de encapsulamento. Os cabeçalhos de Autenticação e de Encapsulamento são fortemente baseados no estabelecimento de Associações de Segurança. São detalhados a seguir os conceitos das Associações de Segurança, do AH, ESP, e a aplicação destes conceitos nos aspectos da mobilidade.

3.1 Associações de Segurança

Este é o conceito fundamental dos mecanismos de segurança concebidos para o IPv6. Uma Associação de Segurança é univocamente identificada por um endereço Internet de destino e um Índice de Parâmetros de Segurança (SPI), contido no cabeçalho de Autenticação ou de Encapsulamento de Segurança. O SPI é uma referência para uma dos possíveis contextos de Segurança a ser utilizado no pacote enviado.

Uma Associação de Segurança pode ser definida pelos seguintes parâmetros:

- informações sobre o algoritmo de autenticação/criptografia empregado com o AH e/ou ESP;
- chave(s) usada(s) com o algoritmo de autenticação/criptografia empregado com o AH e/ou ESP;
- indicação de presença/ausência e tamanho do sincronizador criptográfico ou campo de vetor de inicialização para o algoritmo de criptografia (para ESP);
- tempo de vida da chave e da Associação de Segurança; e
- endereço de origem da Associação de Segurança.

A especificação do IP [6] não restringe a utilização de mecanismos para distribuição de chaves, possibilitando um acompanhamento mais próximo do estado-da-arte. Os mecanismos de geração e distribuição de chaves devem ser desenvolvidos em protocolo à parte.

3.2 Autenticação - Cabeçalho AH

O cabeçalho de autenticação provê meios de incluir dados especiais em um pacote, baseado, por exemplo, numa função de *hash*, como a efetuada pelo algoritmo criptográfico MD5 [8], permitindo assim verificar a autenticidade do emissor do pacote e a integridade do conteúdo do pacote original, uma vez que um único bite alterado no mesmo gerará uma *string* diferente pelo MD5. Este cabeçalho pode também ser utilizado para proteção contra ataques por repetição (aqueles em que um pacote é copiado durante o seu trânsito para re-emissão do mesmo em uma ocasião futura), com a inclusão de informações como *nonces* (identificadores gerados randomicamente) ou *timestamps.* A computação dos dados de autenticação e o uso da proteção contra ataques por repetição são

controlados pela Associação de Segurança. O AH possui o formato apresentado na figura 3.

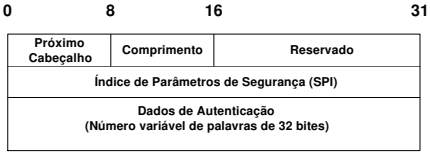

Figura 3 - Cabeçalho de Autenticação do IPv6

Nesta figura, o conteúdo do campo de dados de autenticação dependerá do algoritmo utilizado. Em qualquer caso, os dados de autenticação são calculados sobre todo pacote IP, excluindo qualquer campo que possa ser alterado em trânsito, ou seja, durante sua rota entre a origem e o destino.

A RFC1828 [7] especifica o uso do algoritmo MD5 em conjunto com a chave secreta para autenticação (*Keyed*-MD5). O MD5 é executado sobre o pacote IP e uma chave secreta pela fonte e o resultado é então inserido no campo de dados de autenticação. Ao chegar ao destino, o mesmo cálculo é executado sobre o pacote e a chave secreta, comparado-se o resultado ao valor recebido. Este algoritmo possui seu código otimizado para utilização em máquinas de 32 bites [8].

3.3 Privacidade - Cabeçalho ESP

O uso do cabeçalho ESP provê o suporte para privacidade e integridade dos dados em pacotes IP [6]. Dependendo dos requisitos do usuário, esse mecanismo pode ser usado para criptografar um segmento da camada de transporte, como TCP (*Transport Control Protocol*), UDP (*User Datagram Protocol*) ou ICMP (*Internet Control Message Protocol*), procedimento denominado ESP no modo de Transporte, ou ainda todo o pacote IP, no modo *tunel*. O cabeçalho ESP possui o formato da figura 4 (exemplo aplicando o método DES-CBC - *Data Encription Standard - Cipher Block Chaining*).

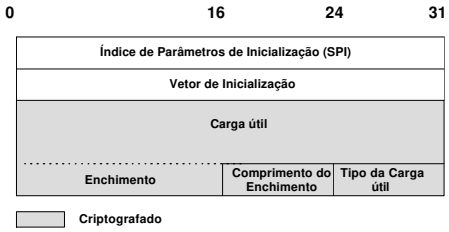

Figura 4 - Cabeçalho ESP no modo DES-CBC

O CBC é uma forma de utilizar o DES com um vetor de inicialização,

contornando a característica original do DES de possuir sempre a mesma correspondência entre o texto claro e o cifrado, facilitando a ação dos criptoanalistas.

Na especificação do IP[6], é definido o DES-CBC para criptografia, porém, as Associações de Segurança, indicadas pelo SPI, podem definir outros algoritmos, possibilitando o emprego de mecanismos mais atuais.

O serviço de segurança a nível de rede fornecido no IPv6 é importante para que qualquer aplicação possa utilizá-lo ser necessitar de implementações adicionais embutidas, possibilitando a criação de redes virtuais seguras dentro da Internet ou em uma rede corporativa (Intranet). Isso seria realizado através do estabelecimento de Associações de Segurança próprias aos nós autorizados a corresponderem-se, independentemente das aplicações utilizadas.

3.4 Segurança em Mobilidade

No caso da mobilidade de nós IPv6, além das preocupações relativas à transparência para o usuário, uma outra questão importante deve ser observada. Um nó qualquer poderia enviar atualizações de *binding* por um nó móvel, e passar a receber os pacotes direcionados ao verdadeiro nó, caso o mesmo não fosse autenticado. No protocolo básico de mobilidade [13] desenvolvido com base no IPv4, o conceito das Associações de Segurança, bem como das atualizações de *binding* já eram explorados. O *Binding Request* é utilizado por nós correspondentes que desejam atualizar seus *cache bindings*, por inexistência ou obsolescência. Neste *request* há um campo, o *identification*, que deve ser utilizado para proteção contra ataques por repetição e para identificação dos *updates* (atualizações de endereço) recebidos. As mensagens de *update* possuem a informação atualizada da associação (*binding*) entre o *home address* do nó móvel e o seu endereço aos cuidados, além do campo *identification*, entre outros. Para garantir a autenticidade destas mensagens, os *binding updates* são acompanhados de extensões especiais de autenticação, que permitem sua verificação em três instâncias:

- autenticação nó móvel x Agente Local - transação particularmente importante, pois o Agente Local deve sempre conhecer o *binding* corrente dos nós móveis para os quais ele presta serviços (*através dos binding updates*);
- autenticação nó correspondente x Agente Local - usada para assegurar a um nó correspondente solicitando uma atualização de seu *cache binding* (com um *binding request*) que a informação que ele está recebendo é confiável; e
- autenticação nó móvel x Agentes Estrangeiros - necessária no caso de mudanças (alterações) de sub-rede visitada, para redirecionamento de pacotes enviados para um endereço aos cuidados desatualizado para o atual.

Nos protocolos de mobilidade propostos em [3,13], estas autenticações já são caracterizadas pela utilização do MD5 com chave secreta entre nó móvel e Agente Local. São definidas mensagens para registro (*Registration Request e Registration Reply*), e as autenticações são tratadas como extensões a estas mensagens de registro (feitas via UDP porta 434) cujo formato possui os campos tipo, comprimento, SPI (*Security Parameter Index*) e um autenticador, que deve ser gerado à partir dos dados de registro. O autenticador *default* é um valor de 128 bites computado através do MD5 com chave secreta.

Com relação à privacidade, não são providos mecanismos específicos, implicando na necessidade do uso de criptografia pela aplicação. A inexistência deste mecanismo facilita eventuais análises de tráfego.

Com o IPv6, uma vez que todos os nós possuirão capacidade de autenticação, pode-se garantir que os *binding updates* emitidos por um nó móvel serão confiavelmente recebidos pelos nós correspondentes. Nesta versão, apenas os nós móveis podem fornecer *binding updates* a seus nós correspondentes, conferindo ao nó móvel a responsabilidade sobre a manutenção do sigilo de suas movimentações. Havendo necessidade de privacidade, como na transmissão de números de cartão de crédito, por exemplo, pode ser usado o cabeçalho de encapsulamento, evitando-se a "escuta" desta informação sensível, que é agravada no caso de enlaces sem fio.

4.0 Um Protocolo para o Estabelecimento de Chaves de Sessão

O acréscimo de características de otimizações de roteamento em mobilidade implica em habilitar qualquer nó correspondente a autenticar um *binding* recebido para um nó móvel, ou seja, que qualquer nó possua uma Associação de Segurança adequada para a sua autenticação, o que é pouco provável de ocorrer pela necessidade prévia da chave secreta compartilhada. A inexistência do potencial para aplicação de mecanismos de segurança padronizados não estimulava o investimento em infra-estruturas de distribuição de chaves.

Com a oportunidade da troca gradual de versão do IP, e a utilização do suporte à segurança da nova versão, viabilizam-se investimentos dos grupos preocupados com a segurança em infra-estruturas a nível mundial. O grande potencial da Internet para transações comerciais e bancárias já evidencia várias propostas promissoras [14,15]. O grupo VISA-MASTERCARD vem conduzindo o projeto SET (*Secure Eletronic Transactions*) [16]. Pode também ser citado o projeto ICE-TEL (*Internetworking Public Key Infraestructure for Europe*) cujo principal objetivo é o de estabelecer uma infra-estrutura escalável de certificação de chaves públicas na Europa [16], utilizando uma hierarquia de certificadores para prover a escalabilidade desejada, baseada no padrão ISO/ITU-T X.509.

Os orgãos que manipulam dados e projetos sensíveis possuem grandes preocupações com a segurança. Neste contexto, situam-se as Forças Armadas. Para um melhor planejamento e coordenação destes aspectos, a Marinha do Brasil (MB) lançou em 1993 o P2IRC (Segundo Plano de Implantação de Redes de Computadores), que deu início aos estudos para padronização de software e de hardware para uso administrativo nas instalações navais. Foram adquiridos equipamentos para suporte de uma INTRANET na MB, com sub-redes locais *Ethernet*, um *backbone* FDDI na área do Primeiro Distrito Naval (Região Sudeste) e enlaces com todas as localidades do Brasil onde se situam repartições da Marinha, inclusive em navios.

Como parte deste plano, está prevista a substituição dos métodos convencionais de autenticação e privacidade aplicados em documentação não-classificada (administrativa) por mecanismos informatizados, utilizando a infra-estrutura da INTRANET MB. Para este fim, foi padronizado o software ARGOS, um programa "inspirado" no PGP, combinando algoritmos de criptografia por chave pública Rivest-Shamir-Adleman (RSA), algoritmos de criptografia convencional e algoritmos de compactação.

Com o objetivo de atender as necessidades da MB, já visando a utilização do IPv6 e a mobilidade de nós, este trabalho apresenta um protocolo para o estabelecimento de chaves de sessão a partir de chaves públicas/privadas. Os certificados seguem a norma X-509, generalizando o protocolo e viabilizando sua aplicação não apenas na INTRANET MB, mas em qualquer ambiente integrado a uma estrutura de certificação.

A utilização de chaves de sessão se justifica pela performance dos mecanismos simétricos, que é muito superior aos assimétricos [17]. A Figura 5 ilustra o procedimento básico do protocolo proposto, que utiliza troca de mensagens via UDP para o estabelecimento das chaves de sessão.

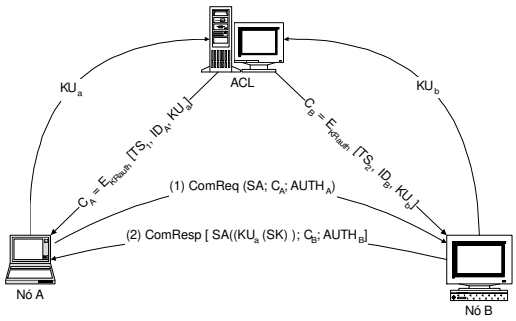

Figura 5 - Protocolo para o Estabelecimento de Chaves de Sessão

As mensagens da parte superior da figura (não-numeradas) referem-se ao protocolo de obtenção dos certificados com a Autoridade de Certificação Local

(ACL), que no caso em questão representam os Distritos Navais. No topo desta hierarquia está a Autoridade de Policiamento de Certificação (APC), que no caso da Intranet MB é a Diretoria de Informática da Marinha. Visando favorecer a manutenção do sigilo de chaves secretas, os certificados possuirão prazo de validade, e poderão ser também revogados. Para obtenção de um certificado, o nó solicitante gera o seu par de chaves pública/secreta (KU e KR, respectivamente) e envia KU para o ACL. Como esta transação será esporádica, admite-se a utilização dos meios atuais de comunicação interna disponíveis (Fax, Telex, ofícios, etc.) para confirmação da autenticidade da origem desta chave. Uma vez autenticada, é gerado pela ACL o certificado correspondente, de acordo com o padrão X.509, que conterá informações como: número de série, emissor do certificado, período de validade, possuidor do certificado, sua chave-pública e a assinatura do ACL, que é um *hash* dos campos do certificado, cifrado com a chave pública do ACL. Após a geração do certificado, o ACL o envia ao nó solicitante cifrado com a sua própria chave privada. É incluído um *Timestamp* para proteção contra os ataques por repetição.

Uma vez que seja feita a geração e o acesso aos respectivos certificados, a seguinte negociação ocorre:

- um nó desejando estabelecer uma troca segura de mensagens com outro nó envia uma mensagem ComReq, via UDP, cuja PDU (*Protocol Data Unit*) inclui a Associação de Segurança (SA) proposta, o Certificado do iniciador e um autenticador desta mensagem;
- Com base no certificado enviado, o nó respondedor pode verificar a autenticidade da mensagem, e após a avaliação da SA proposta, emitir uma mensagem ComResp via UDP, em cuja SA estará incluída a chave de sessão correspondente, cifrada com a chave pública do iniciador; é incluído também o certificado do respondedor e um autenticador desta mensagem.

5.0 – Considerações Finais

Este trabalho apresentou um estudo da segurança e da mobilidade da Internet, considerando em particular o suporte oferecido pelo IPv6, onde observa-se a grande utilidade dos cabeçalhos de Autenticação e de Encapsulamento de segurança para a implementação da mobilidade e transmissões seguras na camada IP. Como resultado deste estudo, foi proposto um protocolo que busca permitir a troca segura de chaves de sessão a partir de um mecanismo assimétrico, viabilizando o emprego do suporte à segurança provido pelo IPv6 e por propostas de suporte à mobilidade que estão sendo consideradas no âmbito da Internet. O protocolo proposto está sendo, no momento, especificado formalmente e será, em seguida, submetido a simulação, aplicando-se sequências de testes geradas com o emprego de técnicas

apropriadas. O protótipo resultante será implementado sobre ambiente UDP de forma semi-automatizada.

Referências

[1] S.Bradner e A.Mankin. "RFC-1752 - The Recommendation for the IP Next Generation Protocol". *Internet RFC*. janeiro de 1995.

[2] S.Cheshire e M.Baker. "Internet Mobility 4 x 4". *SIGCOMM'96*, agosto de 1996.

[3] D.B.Jonhson, A.Myles e C.Perkins. "A Mobile Host Protocol supporting Route Optimization and Autentication." *IEEE Journal of Selected Areas in Communications*, junho de 1995.

[4] J.R.Binkley e J.Mc.Hugh. "Secure Mobile Networking - Winter 1997". *Technical Report*, Portland State University, abril de 1997.

[5] R.W.S.Rodrigues, A.A.Souza e J.A.S.Monteiro. "Simulando um Protocolo da Camada de Rede que Suporta a Comunicação Móvel". *Anais do 14º Simpósio Brasileiro de Redes de Computadores*, 1996.

[6] W. Stallings. "IPv6: The New Internet Protocol". *IEEE Comunications Magazine*, setembro de 1996.

[7] Metzer e Simpson. "RFC-1828 - IP Authentication using *Keyed* MD5". *Internet RFC*, agosto de 1995.

[8] R.Rivest. "RFC-1321 - The MD5 Message-Digest Algoritm*". Internet RFC*, abril de 1992.

[9] C. Perkins. "Mobile IP". *IEEE Communications Magazine*, maio de 1997.

[10] J.Bound e C.Perkins. "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". *Internet Draft*, maio de 1997.

[11] T.Narten , E.Nordmark e W.Simpson. "RFC-1970 - Neighbor Discovery Protocol". *Internet RFC*, agosto de 1996.

[12] C.Perkins e D.B.Johnson. "Mobility Support in IPv6". *Proceedings of the Second Annual International Conference on Mobile Computing and Networking - MOBICOM 96*, novembro de 1996.

[13] C.Perkins. "RFC-2002 - IP Mobility Support". *Internet RFC*, setembro de 1996.

[14] M.Gehrke e T.Hetschold. "Management of a Public Key Certification Infraestructure - Experiences from the DeTeBerkom project BMSec". *Computer Networks and ISDN Systems* 28 (1996) 1901-1914.

[15] S.Kolletzki. "Secure Internet banking with Privacy Enhanced mail - A protocol for reliable exchange of secured order forms". *Computer Networks and ISDN Systems* 28 (1996) 1891-1899

[16] D.W.Chadwick, A.J.Young e N.K.Cicovic. "Merging and Extending the PGP and PEM Trust Models". *IEEE Network*, maio/junho de 1997.

[17] Stallings, W. "Network and Internetwork Security". *Prentice-Hall*, 1995.