Utilizando o IPSec para garantir segurança a transmissões multimídia em redes IPv4

Eduardo S. Machado da Silva
esms@acm.org

Joni da Silva Fraga
fraga@lcmi.ufsc.br

Jean-Marie Farines
farines@lcmi.ufsc.br

Departamento de Automação e Sistemas (DAS)
Núcleo de Redes de Alta Velocidade (NURCAD)
Universidade Federal de Santa Catarina (UFSC)
88040-900 Florianópolis, SC

Resumo

Este trabalho apresenta um estudo do desempenho da comunicação entre redes conectadas através de um canal seguro utilizando a proposta IP Security da IETF. Para tal, foi construída uma Rede Privada Virtual (VPN) entre duas sub-redes com enlace Ethernet em um *backbone* ATM sem alterar a estrutura preexistente baseada em IPv4. Os resultados exibem o impacto da segurança fornecida na camada de rede visando aplicá-la a audio e videoconferências.

Palavras-chave: IPSec, VPN, Unix BSD, multimídia

1 Introdução

Atualmente grande parte dos serviços de segurança são providos em níveis próximos das aplicações estabelecendo segurança dita fim-a-fim. Neste caso, a transparência não é total. É necessária alguma interação envolvendo o usuário, como a escolha do algoritmo criptográfico e a chave secreta utilizados na cifragem. Algumas aplicações, como a videoconferência, por apresentarem requisitos mais severos (número de quadros por segundo, taxa de erro e atraso máximo) possuem soluções específicas como a cifragem parcial de quadros ou a utilização de metade dos dados de fluxos MPEG para proteção da outra metade via *one-time pad* [QN98].

A segurança na comunicação também pode ficar a cargo da camada de rede. Dentre as vantagens desta abordagem destacam-se a possibilidade da utilização das aplicações sem nenhuma alteração, a otimização no tempo dedicado a gerência das chaves criptográficas e a possibilidade da criação de Redes Privadas Virtuais (VPN) seguras. A segurança em nível de rede, embora menos específica, é a que melhor trata problemas de análise de fluxo.

Para fornecer segurança na camada de rede, a IETF (*Internet Engineering Task Force*) propôs um padrão chamado IPSec (*IP Security Protocol*) cujo objetivo é fornecer os

serviços de autenticação, integridade, confidencialidade e contra mensagem antiga aos datagramas IP [KA98]. O IPSec surgiu como cabeçalho estendido do IPv6 [DH98], onde seu uso é obrigatório, mas também é possível utilizá-lo para garantir serviços de segurança em redes baseadas no IPv4. O objetivo deste trabalho é avaliar o impacto da utilização do IPSec em redes IPv4 para aplicá-lo à comunicação multimídia.

Na seção 2 deste trabalho é feita uma breve apresentação da arquitetura IPSec e sua aplicação em VPNs; na seção 3 são descritos os cenários dos testes e as medições realizadas e finalmente, na seção 4, estão as conclusões, encaminhamento da pesquisa e referências.

2 IPSec

Os serviços de autenticação da origem, integridade e confidencialidade de datagramas IP [KA98] são fornecidos por dois cabeçalhos estendidos: AH (*Authentication Header*) e ESP (*Encapsulating Security Payload*). Além disso, a arquitetura IPSec define um protocolo de gerência de chaves criptográficas, o IKE (*Internet Key Exchange*). Os dois cabeçalhos estendidos podem autenticar os datagramas, porém com distinto escopo de atuação. Apenas o ESP é capaz de garantir a confidencialidade do seu campo de dados. O AH e ESP possuem dois modos de funcionamento: no modo transporte os cabeçalhos IPSec são inseridos entre o protocolo de rede (IP) e o de transporte (UDP/TCP). Em modo túnel, o datagrama IP que será protegido é encapsulado de maneira inalterada no campo de dados do AH ou ESP.

O IPSec é adotado como *framework* de VPNs por ser um padrão proposto pela IETF e fornecer os serviços de confidencialidade e autenticidade frequentemente requeridos pelos usuários de VPNs [GLJH+00]. A nomenclatura do IPSec define *security gateways* como os roteadores que ficam nas pontas dos túneis criptográficos.

3 Arquitetura e Cenários

3.1 Arquitetura e Ferramentas

Os testes foram realizados entre duas sub-redes (NURCAD e DAS) com enlace IEEE802.3 (Ethernet) 10 Mbps conectadas ao *backbone* ATM 155 Mbps da UFSC. No processo de mensuração do desempenho de redes de computadores, os parâmetros taxa de transferência de dados, atraso e MTU (*Maximum Transmission Unit*) destacam-se por afetarem diretamente a velocidade da rede [PAM98]. Outros fatores que afetam a taxa efetiva de transferência são a CPU e a interface de rede. Como *security gateways* foram utilizados dois computadores de arquitetura i386: Pentium 166 MHz, 32 MB, HD IDE, NIC PCI 10 Mbps (fig. 1, N1) e 80486 DX2/66, 16 MB, HD IDE, NIC ISA 10 Mbps (D1). Para gerar tráfego na rede e caracterizar a taxa de transferência de dados, RTT (*Round-Trip Time*) e perdas de pacotes entre os *security gateways* foi utilizado o pchar [Mah], uma reimplementação do pathchar de Van Jacobson. O pchar faz uso de datagramas UDP de tamanho variável (entre 64 e 1500 bytes), aguarda o retorno através de mensagens ICMP e varia os valores do campo TTL do IP a fim de limitar o caminho onde estão sendo feitas as medidas. Em camadas superiores foram realizados testes de

trasferência de arquivos (50 transferências de um mesmo arquivo de 100 kbytes através do protocolo FTP) e transmissão de voz em audioconferência utilizado RAT [HP99] (*Robust Audio Tool*) na versão 3 com codificação GSM em modo *unicast*. O tradicional tcpdump [VLM] e o snort [Roe] serviram como ferramentas para análise de tráfego e checagem do conteúdo do cabeçalho e dados dos protocolos.

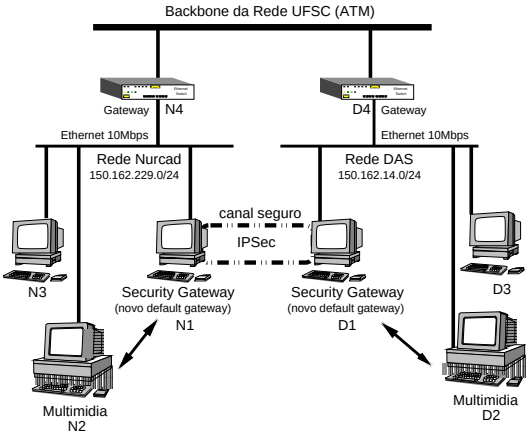

Figura 1: VPN Nurcad e DAS

3.2 Cenários

Os testes foram realizados em 3 cenários, sendo que dois deles dependiam da configuração da VPN. O cenário mais simples (IP) corresponde às sub-redes NURCAD e DAS em seu estado natural onde a rota padrão de todos os equipamentos é N4 e D4 (fig. 1, Nurcad e DAS respectivamente). Nos dois outros cenários que dependiam da VPN foi utilizado o sistema operacional OpenBSD 2.7 nos *security gateways* (N1 e D1) pelo seu suporte nativo ao IPSec, código fonte aberto, documentação e estabilidade [dRHG+99]. Apenas a rede do DAS estava protegida por um *firewall*, no qual foi criada uma regra para permitir a entrada de qualquer tráfego IP provenientes de N1 (fig. 1). Como os cenários envolveram apenas duas sub-redes, optou-se pela gerência manual das chaves criptográficas (sem a utilização o IKE).

O cenário IP-IP é a implementação do Tunelamento IP em IP sem serviços de segurança (RFC1853), ou seja uma VPN "insegura". Finalmente no cenário ESP foi utilizado apenas o protocolo ESP em modo túnel com os algoritmos Blowfish [Sch93] 160 bits (para garantir confidencialidade) e HMAC-SHA-1 também 160 bits (visando garantir autenticidade) configurados em duas associações de segurança nos *security gateways*, uma em cada sentido, além dos fluxos IPSec.

Nos dois cenários baseados em tunelamento (IP-IP e ESP) foi alterada a rota padrão de uma máquina da rede local envolvida nos testes. No caso da rede do Nurcad, a máquina N2 teve sua rota padrão alterada de N4 para N1. No DAS ocorreu configuração análoga: D2 teve sua rota padrão alterada de D4 para D1.

3.3 Resultados

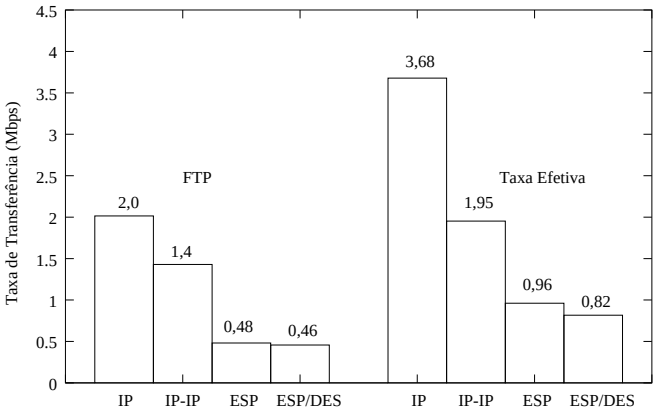

Figura 2: Taxa de transferência de bits nos 3 cenários

A figura 2 exibe em dois histogramas o resumo dos valores obtidos nos principais testes realizados entre os *security gateways*. O lado direito do histograma representa a taxa de transferência de bits efetiva disponível entre N1 e D1 nos três cenários. O cenário ESP também foi montado substituindo o algoritmo simétrico Blowfish (160 bits) pelo DES (56 bits) em modo CBC, que é de implementação obrigatória.

O gráfico ao lado esquerdo da fig. 2 representa a taxa de transferência de bits obtida através da transferência de um mesmo arquivo 100 vezes via FTP entre N1 (cliente) e D1 (servidor).

As medidas indicaram que a utilização do tunelamento sem segurança (cenário IP-IP) representou uma queda de aproximadamente 50% na taxa de transferência de bits (em relação ao cenário IP). Na transferência de arquivo via FTP a queda foi próxima de 30%. O impacto do ESP em modo túnel diminuiu em 75% o desempenho da comunicação. O impacto isolado do ESP em relação ao tunelamento sem segurança (IP-IP) foi de 50% e utilizando o FTP a queda foi de 65%. A troca do algoritmo Blowfish pelo DES resultou numa queda da taxa de transferência em 15% associada a eficiência dos dois algoritmos. Na transferência de arquivo via FTP esse impacto foi menor, cerca de 5%. Outro importante dado para transmissões multimídia (não consta na figura 2) são os valores do RTT para datagramas menores que o MTU: 2,9 ms (cenário IP), 4,0 ms (IP-IP) e 8,1 ms (ESP).

A queda da taxa de transferência de bits e o aumento do *Round-Trip Time* são consequências diretas do tunelamento e da criptografia implementados pelo Sistema Operacional.

4 Considerações

Ao analisar os datagramas IP trocados entre estas sub-redes em um roteador intermediário (D4 na fig. 1) as únicas informações relevantes obtidas (em claro) foram os endereços IP dos *security gateways* e o protocolo utilizado (ESP, número 50). O endereço IP e os dados das máquinas que participaram da comunicação fim-a-fim são escondidos na carga

cifrada do ESP, o que impede a revelação não-autorizada. Porém a análise de tráfego (baseada na quantidade de informação) não pode ser impedida com pacotes de tamanho variável. A análise de tráfego tratada pelo IPSec é o desconhecimento das informações das máquinas finais no canal de VPN.

A utilização do ESP em modo túnel protege apenas o tráfego entre os dois *security gateways*. Sendo assim, as sub-redes ainda estão vulneráveis a ataques internos como a interceptação ou introdução de dados.

Destaca-se o fato que a VPN montada entre as duas sub-redes não alterou a configuração de nenhum outro dispositivo presente nas sub-redes.

O pchar indicou que no cenário IP o gargalo da comunicação encontra-se entre D4 e D1. O próximo passo será a substituição de D1 por outro equipamento com especificação mais próxima a N1.

Esta pesquisa pretende prosseguir comparando as técnicas utilizadas para fornecer segurança em videoconferências com a segurança fornecida pelo ESP em modo túnel. Em um trabalho correlato [ANM+00] analisa o impacto do IPSec em redes IPv6 para transmissão de vídeo digital.

Os testes iniciais realizados entre D2 e N2 apenas com áudio codificado em GSM utilizou uma parcela muito pequena da banda disponível (0,013 Mbps) e o resultado qualitativo mostrou que o cenário ESP não afetou a qualidade do som. Os resultados até o momento indicaram a viabilidade do ESP em modo túnel para a segurança da comunicação do tipo audioconferência. Já está em andamento um trabalho que exibe resultados quantitativos envolvendo audio e vídeo.

Referências

[ANM+00] Seiji Ariga, Kengo Nagahashi, Masaki Minami, Hiroshi Esaki, and Jun Murai. Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks. In *Proceedings of the 10th Annual INET Conference*, Yokohama, Japan, Jul 2000.

[DH98] Stephen Deering and Robert M. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Request For Comments (Draft Standard) RFC 2460, Internet Engineering Task Force, December 1998.

[dRHG+99] Theo de Raadt, Niklas Hallqvist, Artur Grabowski, Angelos Keromytis, and Niels Provos. Cryptography in OpenBSD: An Overview. In *Proceedings of the 1999 Usenix Security Symposium*, Jun 1999. `http://www.openbsd.org`.

[GLJH+00] B. Gleeson, A. Lin, J. J. Heinanen, G. Armitage, and A. Malis. A Framework for IP Based Virtual Private Networks. Request For Comments (Informational) RFC 2764, Internet Engineering Task Force, Feb 2000.

[HP99] Orion Hodson and Colin Perkins. RAT - Unicast and Multicast Audio Conferencing Tool, May 1999. `http://www-mice.cs.ucl.ac.uk/multimedia/software/rat`.

[KA98] Stephen Kent and Randall Atkinson. Security Architecture for the Internet Protocol. Request For Comments (Proposed Standard) RFC 2401, Internet Engineering Task Force, Nov 1998.

[Mah] Bruce A. Mah. pchar: Perform Network Measurements Along an Internet path. `http://www.employees.org/~bmah/Software/pchar/`.

[PAM98] Vern Paxson, Guy Almes, and Jamshid Mahdavi. Framework for IP Performance Metrics. Request For Comments (Informational) RFC 2330, Internet Engineering Task Force, May 1998.

[QN98] Lintian Qiao and Klara Nahrstedt. Comparison of MPEG Encryption Algorithms. *Computer & Graphics*, 22(4), 1998.

[Roe] Marty Roesch. snort: Lightweight Network Intrusion Detection System. `http://www.snort.org`.

[Sch93] Bruce Schneier. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). In *Proceedings of Cambridge Security Workshop*, pages 191–204, Dec 1993.

[VLM] Jacobson Van, Craig Leres, and Steven McCanne. tcpdump: dump traffic on a network. `ftp://ftp.ee.lbl.gov`.