ANÁLISE DE SEGURANÇA DOS PROTOCOLOS UTILIZADOS PARA ACESSO REMOTO VPN EM PLATAFORMAS WINDOWS

Edmar Roberto Santana de Rezende[⊗]
Instituto de Computação
Universidade Estadual de Campinas
13083-970 Campinas - SP
edmar.rezende@ic.unicamp.br

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

RESUMO

As Redes Privadas Virtuais (Virtual Private Network – VPN) possuem uma importância cada vez maior para os negócios das organizações, porém trazem consigo sérias implicações de segurança. O acesso remoto VPN, onde o usuário remoto acessa diretamente os recursos da organização, possui implicações de segurança específicas que precisam ser consideradas. A escolha de uma solução adequada para este cenário constitui uma decisão fundamental para a segurança do ambiente cooperativo. Este artigo visa analisar os principais protocolos utilizados para acesso remoto VPN em plataformas Windows, principalmente em sistemas Windows 2000, devido aos seus mecanismos internos de segurança mais capazes e sua maior disseminação em ambientes corporativos.

ABSTRACT

The importance of Virtual Private Network (VPN) to businesses organizations has been steadily increasing, but there are serious security implications involved. The remote access VPN, in which remote user directly access the corporations' resources, has specific security concerns that need to be addressed. The appropriate solutions in this context constitutes a fundamental decision for secure cooperative environment. This paper presents an analysis of main protocols used for remote access VPN in Windows platforms, focusing Windows 2000 systems, due to their more competent internal security mechanisms and its largest dissemination in corporate environments.

1 INTRODUÇÃO

As Redes Privadas Virtuais possuem uma importância fundamental para as organizações, principalmente no seu aspecto econômico, ao permitirem que conexões dedicadas sejam substituídas por conexões públicas.

Economias também podem ser geradas com a substituição das estruturas de conexões remotas tradicionais, como o *pool de modens* e gastos com ligações interurbanas, que podem ser eliminadas em função da utilização do acesso remoto VPN, fazendo-se uso da infra-estrutura de redes públicas, como a Internet.

Porém, essas vantagens trazem uma série de implicações, principalmente quanto à segurança das informações, que passam a correr riscos com relação à sua confidencialidade e à sua integridade, já que as informações das organizações passam a trafegar através de uma rede pública.

Nesse contexto, a utilização de protocolos capazes de suprir as necessidades de segurança impostas torna-se fundamental. É importante também que tais protocolos atendam a requisitos relacionados a performance, flexibilidade, interoperabilidade e escalabilidade.

Este artigo tem como objetivo analisar os principais protocolos utilizados para o acesso remoto VPN em plataformas Windows, principalmente em sistemas Windows 2000, devido aos seus mecanismos internos de segurança mais capazes e sua maior disseminação em ambientes corporativos.

Inicialmente serão apresentados na Seção 2 alguns conceitos relacionados às Redes Privadas Virtuais e uma melhor caracterização do cenário de acesso remoto proposto. A Seção 3 apresenta os protocolos para acesso remoto VPN utilizados em plataformas Windows, analisando suas principais deficiências e vulnerabilidades para sua adequação ao cenário desejado. A Seção 4 apresentada uma conclusão geral sobre a análise realizada, trazendo algumas considerações e sugestões para a adoção de um protocolo que melhor atenda às necessidades impostas pelo acesso remoto VPN.

2 REDES PRIVADAS VIRTUAIS (VPN)

As Redes Privadas Virtuais (*Virtual Private Network* - VPN) são um componente importante dentro de um ambiente cooperativo, e têm como objetivo utilizar uma infra-estrutura de rede pública para a comunicação, em substituição às conexões privadas e às estruturas de acesso remoto, que possuem custos bastante elevados. A VPN permite que uma rede pública, como por exemplo a Internet, seja utilizada como *backbone* para a comunicação entre pontos distintos. Para os usuários que se comunicam através de uma VPN, é como se duas

[⊗] Financiado por Robert BOSCH Ltda.

redes fisicamente distintas fossem logicamente uma única rede, constituindo assim uma rede privada virtual que passa fisicamente por uma rede pública.

Esse tipo de VPN, que é transparente ao usuário, pode ser chamada de *gateway-to-gateway* VPN, e o túnel VPN é iniciado e finalizado nos *gateways* das organizações. Outro tipo de VPN é a *client-to-gateway* VPN, onde o túnel é iniciado no próprio equipamento do usuário, através de um software cliente (Nakamura, 2000).

Esses dois tipos de VPN podem ser utilizadas para caracterizar uma *Intranet* VPN, que conecta departamentos e filiais dentro de uma organização, ou uma *Extranet* VPN, que conecta a organização a parceiros estratégicos, clientes e fornecedores. A *Intranet* VPN exige uma tecnologia de ponta para as conexões de alta velocidade presentes em LANs, além de alta confiabilidade, para assegurar a prioridade em aplicações de missão crítica. A facilidade de gerenciamento para acomodar mudanças com novos usuários, novas filiais e novas aplicações também é importante. Já a *Extranet* VPN requer uma solução padrão para assegurar a interoperabilidade entre as várias soluções de parceiros, sendo que o controle de tráfego é importante para se evitar os gargalos e garantir a rápida resposta aos dados críticos.

Além da economia com as linhas dedicadas, a VPN também pode ser utilizada como solução alternativa aos acessos remotos tradicionais, apresentando nesse caso, características híbridas entre uma *Intranet* VPN, ao fornecer conexão a funcionários em ambientes remotos, e uma *Extranet* VPN, disponibilizando alguns de seus serviços a fornecedores e parceiros estratégicos.

A manutenção dos componentes do acesso remoto, que incluem o *pool de modens* e as linhas telefônicas, pode ser considerada bem mais cara do que uma solução VPN. Essa solução, na qual o túnel VPN é iniciado no cliente, que se conecta a um provedor de acesso à Internet (*Internet Service Provider* - ISP), substituindo os acessos remotos diretos, é conhecida como acesso remoto VPN (*remote access* VPN) e é ilustrada na Figura 1.

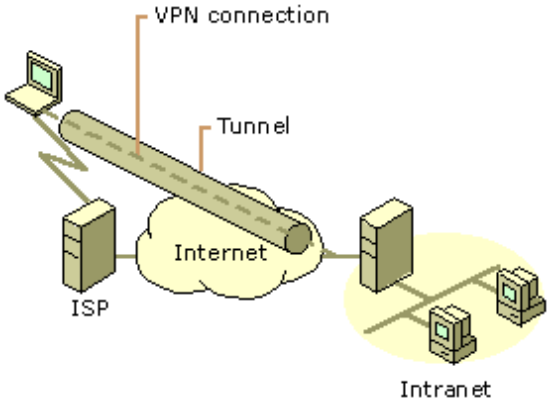

Fig. 1 – Acesso remoto VPN.

O acesso remoto VPN possui uma grande aplicabilidade em um ambiente cooperativo, onde os usuários remotos podem deixar de realizar ligações interurbanas, acessando os recursos da organização utilizando um túnel virtual criado através da Internet. Uma autenticação forte é um requisito importante neste cenário, já que os recursos da organização são acessados diretamente pelos usuários, e a segurança física é difícil de ser implementada em soluções remotas.

Assim, quando a VPN é utilizada, o serviço aparece para o usuário como se ele estivesse conectado diretamente à rede privada, quando na realidade ele utiliza uma infra-estrutura pública. A utilização da rede pública para a comunicação entre matriz, filiais e parceiros comerciais significa custos mais baixos e maior flexibilidade e escalabilidade com relação a usuários móveis e a mudanças nas conexões, se comparado com as conexões privadas, que possuem custos altos para mudanças em sua infra-estrutura. De fato, a utilização da Internet facilita o gerenciamento das conexões, pois não é mais necessário criar um ponto de acesso privado para cada uma das conexões, e sim apenas um, para a Internet, tirando-se vantagem ainda da conectividade global, que é mais difícil de ser alcançada através de conexões dedicadas. Esse conjunto de fatores facilita a conexão entre as organizações, que podem assim buscar a evolução natural em seus processos de negócios.

3 ANÁLISE DOS PROTOCOLOS

Os conceitos que fundamentam a VPN são a criptografia e o tunelamento. A criptografia é utilizada para garantir a autenticidade, a confidencialidade e a integridade das conexões, e é a base para a segurança das soluções VPN. Já o tunelamento, é responsável pelo encapsulamento e transmissão dos dados, sobre uma rede pública, entre dois pontos distintos.

A carência de mecanismos capazes de proteger o acesso remoto VPN culminou na especificação de diferentes padrões. Em determinadas situações, é possível combinar soluções no intuito de obter o conjunto de serviços desejados.

Além disso, os diversos protocolos existentes diferem entre si na camada do modelo ISO/OSI onde atuam, ou no modo em que a criptografia é utilizada, o que influencia diretamente no nível de segurança do acesso remoto VPN.

A seguir serão apresentadas as características básicas e uma análise de segurança dos principais protocolos utilizados atualmente para acesso remoto VPN em plataformas Windows. Apesar de algumas das tecnologias apresentadas serem utilizadas por todos os sistemas operacionais da família Windows, serão enfatizadas as tecnologias VPN suportadas

pelo sistema Windows 2000, devido à sua maior disseminação em ambientes corporativos e à presença de tecnologias VPN mais capazes.

3.1 POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

O PPTP (*Point-to-Point Tunneling Protocol*) (Hamzeh et al., 1999) é um protocolo que foi originalmente desenvolvido por um grupo de empresas chamado *PPTP Forum*, constituído pela 3Com, Ascend Communications, Microsoft, ECI Telematics e US Robotics.

A idéia básica do PPTP era dividir as funções do acesso remoto de tal modo que indivíduos e empresas pudessem utilizar a infra-estrutura da Internet para prover uma conectividade segura entre clientes remotos e redes privadas.

O PPTP tem como finalidade principal prover um mecanismo para o tunelamento de tráfego PPP (*Point-to-Point Protocol*) (Simpson, 1994) sobre redes IP.

Antes do envio de um datagrama IP, o PPTP cifra e encapsula este datagrama em um pacote PPP que, por sua vez, é encapsulado em um pacote GRE (*Generic Routing Encapsulation*) (Farinacci et al., 2000), como mostrado na Figura 2.

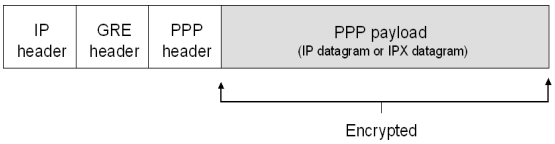

Fig. 2 - Encapsulamento de um datagrama IP feito pelo PPTP.

Da mesma forma que outros protocolos de segurança, o PPTP também requer a negociação de parâmetros antes de, efetivamente, proteger um tipo de tráfego entre duas entidades. Porém, o seu procedimento de negociação é feito sem qualquer proteção, permitindo que um atacante modifique parâmetros ou obtenha dados como o endereço IP dos extremos do túnel, nome e versão do software utilizado, nome do usuário e, em alguns casos, o *hash* criptográfico da senha do usuário (Chapman, Cooper e Zwicky, 2000).

Além disso, as mensagens do canal de controle PPTP são transmitidas sem qualquer forma de autenticação ou proteção de integridade, o que expõe esse canal de controle a um sequestro de conexão (*connection hijacking*) (Nakamura, 2000). Também é possível gerar falsas mensagens de controle ou alterar essas mensagens em trânsito sem qualquer detecção.

Outra vulnerabilidade do PPTP é o fato do cliente só precisar se autenticar após a conclusão do processo de estabelecimento de parâmetros. Esta característica permite que atacantes façam com que um servidor inicie diversos processos de negociação falsos, o que pode resultar em negação de serviço (DoS) (Nakamura, 2000) e até mesmo na total paralisação do servidor.

3.1.1 Considerações sobre a implementação do PPTP pela Microsoft

Implementações específicas de um protocolo podem conter, além dos problemas de segurança detectados na própria especificação, falhas que podem comprometer o uso deste protocolo.

Em relação ao PPTP, a Microsoft possui uma implementação com extensões proprietárias incluída na maioria das versões do Microsoft Windows. Pelo fato deste sistema operacional ser amplamente utilizado e o seu suporte ao PPTP representar uma solução viável e de baixo custo para a configuração de VPNs, análises de segurança desta implementação do PPTP merecem atenção especial.

Uma primeira fragilidade do PPTP da Microsoft está em um dos formatos de armazenamento e transmissão de *hashes* de senhas nas várias versões do Microsoft Windows, conhecido como *LanMan*. Senhas do Windows NT possuem 14 caracteres de extensão. Porém, quando armazenadas no formato *LanMan*, que é *case-insensitive*, todos os caracteres são convertidos para *uppercase*, diminuindo o número de *hashes* possíveis e, conseqüentemente, facilitando ataques de força-bruta. Porém, a maior vulnerabilidade do *LanMan* é a divisão da cadeia de 14 caracteres em duas de 7 caracteres. *Hashes* para cada uma das cadeias são gerados separadamente. Este procedimento reduz um ataque de força-bruta da senha ao esforço necessário para descobrir colisões para duas senhas curtas de 7 caracteres. Caso não ocorresse a divisão da cadeia original, as senhas seriam mais seguras, dado que *hashes* de cadeias de 14 caracteres possuem, aproximadamente, 6 trilhões de possibilidades a mais em relação a um *hash* gerado a partir de uma cadeia de 7 caracteres (Sena, 2002).

Uma vez que os dados do processo de negociação de parâmetros do PPTP são transmitidos sem a proteção de qualquer serviço de confidencialidade, um atacante pode obter o *hash* da senha de um usuário armazenada no formato *LanMan* e, com base neste dado, descobrir a senha original. Deve-se ainda levar em consideração o fato de que muitos usuários escolhem senhas previsíveis e sujeitas a ataques de dicionário (Klein, 1990), o que certamente facilita a violação de senhas representadas e transmitidas em *LanMan*.

Apesar do Windows NT possuir um novo formato para a manipulação de senhas, caso a compatibilidade com o *LanMan* esteja ativa, as senhas serão manipuladas utilizando este formato. Desta forma, o uso do protocolo PPTP certamente representa uma exposição perigosa da senha dos usuários de um ambiente Windows. Vale ressaltar que o ataque a *hashes* de 7 caracteres pode ser

realizado através da utilização de computadores pessoais de baixo custo (Schneier, 1996).

Outra vulnerabilidade grave da implementação do PPTP em sistemas Windows está no tamanho e no processo de geração de chaves criptográficas para o serviço de cifragem. Dois modos de confidencialidade são oferecidos através do algoritmo RC4 (Schneier, 1996): um que utiliza chaves de 40 bits e outro com chaves de 128 bits. No primeiro caso, além da utilização de chaves pequenas, altamente suscetíveis a ataques de força-bruta, as chaves geradas são baseadas nas senhas dos usuários. Em outras palavras, várias sessões de um mesmo usuário irão utilizar a mesma chave, a não ser que este usuário altere o valor de sua senha. Este fato agrava-se ainda mais se o atacante conseguir a senha de um usuário através da obtenção da sua versão no formato *LanMan*.

No segundo modo de cifragem, que utiliza chaves de 128 bits, consideradas atualmente seguras, o valor gerado para uma chave é baseado, novamente, na senha do usuário, porém combinada com um número aleatório específico para cada sessão. Apesar deste procedimento ser mais seguro que o anterior, o uso constante da senha do usuário diminui consideravelmente o número de tentativas que podem compor um ataque (Sena, 2002).

O uso de ferramentas que automatizam o ataque a senhas pode obter sucesso em alguns minutos, considerando o uso de senhas comuns, fragilizando ainda mais o processo de geração de chaves criptográficas baseadas nas senhas dos usuários. No caso de um ataque de força bruta, algumas ferramentas podem obter sucesso num prazo de no máximo 250 horas, caso a senha seja composta somente por caracteres alfabéticos (Sena, 2002).

O conjunto de vulnerabilidades do PPTP implementado em sistemas Windows fez com que a própria Microsoft recomendasse a desabilitação do formato *LanMan* em cenários onde é possível o uso de outras opções. Os resultados de análises de segurança detalhadas sobre a implementação Microsoft do protocolo PPTP podem ser encontrados em (Schneier e Mudge, 1998; Schneier, Mudge e Wagner, 1999).

3.2 Layer Two Tunneling Protocol (L2TP)

O *Layer 2 Tunneling Protocol* (L2TP) (Townsley et al., 1999) foi desenvolvido com base no *Layer 2 Forwarding* (L2F) (Valencia, Littlewood e Kolar, 1998) e no *Point-to-Point Tunneling Protocol* (PPTP), e tem por principal objetivo, assim como o PPTP, o encapsulamento de pacotes PPP.

Uma das diferenças entre o L2TP e o PPTP está no protocolo utilizado na camada inferior. Enquanto o PPTP deve ser sempre utilizado acima do IP, o L2TP pode ser utilizado sobre redes IP, X.25, *Frame Relay* ou ATM (*Asynchronous Transfer Mode)*.

Sob o ponto de vista da segurança da comunicação, dado que o L2TP realiza o encapsulamento de pacotes PPP, ele pode então fazer uso dos mecanismos de autenticação PPP, bem como do Protocolo de Controle de Cifragem (*Encryption Control Protocol* - ECP) (Meyer, 1996) e do Protocolo de Controle de Compressão (*Compression Control Protocol* - CCP) (Rand, 1996) utilizados pelo PPP.

O L2TP provê também suporte à autenticação do túnel, permitindo que ambos os extremos do túnel sejam autenticados.

Contudo, não existem mecanismos de proteção do túnel L2TP definidos, o que expõe tanto os pacotes de dados quanto os pacotes de controle deste protocolo a algumas formas de ataque.

Dentre as vulnerabilidades possíveis podemos destacar: a obtenção da identidade do usuário através da observação dos pacotes; a modificação dos pacotes de dados e controle; o sequestro do túnel L2TP ou da conexão PPP dentro do túnel; ataques de negação de serviço contra a conexão PPP ou o túnel L2TP; a interrupção da negociação PPP ECP com o intuito de remover a proteção de confidencialidade; e a interrupção ou o enfraquecimento do processo de autenticação PPP sendo possível até mesmo conseguir acesso à senha do usuário (Patel et al., 2001).

Diante de todos os problemas de segurança apresentados pelo protocolo L2TP, seu uso em cenários onde existe uma rede não-confiável, como a Internet, entre os extremos de um túnel, deve sempre ser combinado com outros protocolos capazes de suprir a sua ausência de serviços de segurança.

Um conjunto de propostas tem sido desenvolvido para conciliar o uso do L2TP com o IPSec (Patel et al., 2001; Srisurech, 2000).

Na Seção 3.4 são discutidos os aspectos referentes à utilização do L2TP sobre o IPSec em maiores detalhes.

3.3 IP Security (IPSec)

O IPSec (*IP Security*) (Kent e Atkinson, 1998a) é uma arquitetura definida pelo IETF (*Internet Engineering Task Force*), cujo principal objetivo é oferecer mecanismos de segurança a pacotes IP. Tais serviços são providos através de dois cabeçalhos de extensão, o AH (*Authentication Header*) (Kent e Atkinson, 1998b) e o ESP (*Encapsulation Security Payload*) (Kent e Atkinson, 1998c), e através do uso de protocolos e procedimentos para gerência de chaves criptográficas, como o IKE (*Internet Key Exchange*) (Harkins e Carrel, 1998).

O AH foi desenvolvido para garantir a autenticidade e a integridade dos pacotes IP. Sua

utilização oferece proteção contra modificações nos campos de valor fixo do pacote IP, proteção contra *spoofing* (Nakamura, 2000), e opcionalmente, proteção contra ataques de *replay* (Nakamura, 2000).

Já o ESP provê o encapsulamento dos dados com cifragem, para garantir que somente o destinatário possa ler o *payload* do pacote IP. Opcionalmente, também pode garantir a autenticidade e a integridade do pacote, e proteção contra ataques de *replay*.

Os dois cabeçalhos podem ser utilizados separadamente ou podem ser combinados para prover as características de segurança desejadas para o tráfego IP.

A principal diferença entre os serviços de autenticação e integridade providos pelo AH e pelo ESP está na abrangência da proteção. O AH protege todos os campos de um pacote, excetuando-se aqueles cujos valores são alterados em trânsito. Quando oferecidos pelo ESP, esses serviços abrangem somente o próprio cabeçalho do ESP e a porção de dados do pacote.

3.3.1 Algoritmos criptográficos

Diversos algoritmos criptográficos podem ser utilizados pelo AH e ESP, porém existe um conjunto mínimo cuja implementação é obrigatória. São eles: *HMAC-MD5-96 E HMAC-SHA-1-96* para os serviços de autenticação e integridade do AH e ESP; DES-CBC para a confidencialidade provida pelo ESP; e, algoritmos nulos de autenticação e confidencialidade utilizados pelo ESP quando um dos seus serviços não é requisitado. No entanto, este conjunto obrigatório não é suficiente para prover segurança de forma adequada a todos os tipos de informação (Sena, Geus e Augusto, 2002).

Estudos têm mostrado que particularidades do MD5 permitem acelerar o processo para gerar mensagens que produzam o mesmo *hash*, utilizando máquinas de baixo custo (Schneier, 1996).

Em relação ao DES, o tamanho de chave utilizada, 56 bits, é atualmente vulnerável a ataques de força-bruta tornando-o inadequado para preservar informações cujo sigilo é de extrema significância (Bellovin, 1997).

Sendo assim, a implementação de outros algoritmos mais capazes seria de extrema importância, porém se algoritmos mais seguros não estão padronizados, nem todas as implementações os conterão.

3.3.2 Associações de Segurança (SA)

Para que duas entidades consigam enviar e receber pacotes utilizando os serviços do IPSec é necessário o estabelecimento de Associações de Segurança (*Security Association* – SA), que especificam os algoritmos a serem utilizados, as chaves criptográficas, os tempos de vida destas chaves, entre outros parâmetros.

Existem duas formas de estabelecimento de associações de segurança: estática e dinâmica. No primeiro, os parâmetros são inseridos manualmente em ambos os extremos da comunicação. No segundo, os parâmetros são negociados por protocolos como o IKE, sem a intervenção do administrador.

A escalabilidade do IPSec está relacionada ao estabelecimento dinâmico de SAs que devem ser definidas por conexão ou, no máximo, por usuário, para prover maior segurança. Abusar intencionalmente do mecanismo de estabelecimento de SAs pode constituir diversos ataques de DoS.

3.3.3 Modo transporte e modo túnel

Ambos os cabeçalhos, AH e ESP, possuem dois modos de operação: transporte e túnel.

No modo transporte, os cabeçalhos de segurança utilizados por um pacote são inseridos após o cabeçalho IP. Este modo, em geral, é utilizado para proteção fim-a-fim da comunicação entre dois *hosts* e representa uma solução adequada para auxiliar na segurança de pacotes em redes locais.

O modo túnel tem seu uso recomendado na proteção do tráfego entre um *host* e um *gateway*. Antes de ser enviado, o pacote original é inserido completamente na porção de dados de um novo pacote que contém os cabeçalhos de segurança e cujos endereços correspondem aos extremos do túnel.

No modo transporte, os cabeçalhos de segurança provêm proteção primária para os protocolos das camadas superiores. No modo túnel, os cabeçalhos protegem o pacote IP encapsulado, provendo proteção para todos os campos do cabeçalho IP original.

3.3.4 Solução IPSec para o acesso remoto VPN

Uma solução bastante utilizada atualmente para o acesso remoto VPN é o uso do IPSec em modo túnel.

Nesse cenário, o túnel IPSec é estabelecido entre o cliente remoto e o *gateway* VPN da organização, constituindo um canal seguro para o tráfego dos dados sobre a rede pública intermediária.

Todo o tráfego IP é encapsulado pelo IPSec, sendo o pacote IP original transmitido através do túnel, tirando-se proveito de todos os serviços de segurança oferecidos pelo IPSec.

A Figura 3 mostra o uso do IPSec em modo túnel utilizando apenas os serviços do protocolo AH, garantindo a integridade e a autenticidade tanto do pacote IP original, quanto do pacote IPSec utilizado para prover o tunelamento.

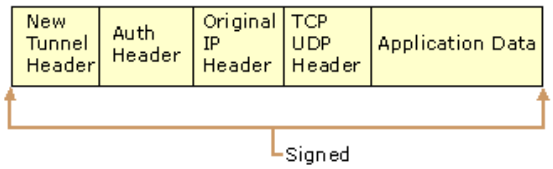

Fig. 3 – IPSec em modo túnel utilizando os serviços do cabeçalho AH.

Na Figura 4 é mostrado o modo túnel do IPSec utilizando os serviços do cabeçalho ESP, provendo confidencialidade a todo o pacote IP original, e integridade e autenticação ao pacote IP original e parte do pacote IPSec utilizado para prover o tunelamento.

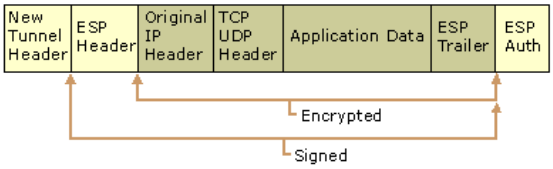

Fig. 4 – IPSec em modo túnel utilizando os serviços do cabeçalho ESP.

No entanto, é importante notar que o uso do IPSec somente com os serviços de autenticação e integridade, ou somente com o serviço de confidencialidade, pode causar uma falsa sensação de segurança na comunicação, tornando o túnel IPSec vulnerável a alguns tipos de ataques. Uma análise detalhada dessas vulnerabilidades pode ser encontrada em (Bellovin, 1996; Sena, Geus e Augusto, 2002).

Apesar dos problemas apresentados constituírem uma ameaça à segurança do túnel IPSec, quando utilizado de forma adequada esse protocolo provê um excelente nível de segurança para a comunicação, sendo uma das principais tecnologias atualmente disponíveis para a implementação de VPNs.

Contudo, alguns aspectos relacionados à utilização do IPSec para o acesso remoto VPN ainda carecem de padronização.

O modo túnel do IPSec não provê suporte à atribuição e configuração de endereços IP, o que se faz necessário no caso do acesso remoto VPN, já que um dos extremos do túnel é um *host* remoto que não possui endereço IP fixo e que após o estabelecimento do túnel precisa estar associado a um endereço IP da rede interna.

Além disso, muitos dos esquemas de autenticação existentes, comumente usados para autenticação de usuários, são de natureza assimétrica, e não são suportados pelo IKE (*Internet Key Exchange*), utilizado pelo IPSec. Apesar do IKE prover um suporte poderoso para a autenticação de máquina, ele apresenta somente um suporte limitado para formas de autenticação de usuário e não provê suporte para autenticação assimétrica de usuário.

Outra característica desejável ao IPSec seria o suporte à múltiplos protocolos, uma vez que esse protocolo só é capaz de transportar pacotes IP em seu modo túnel.

Todos esses itens são requisitos importantes para o acesso remoto VPN. As plataformas Windows atuais não possuem suporte para a solução desses problemas e as soluções proprietárias existentes não apresentam interoperabilidade entre si.

Existem alguns trabalhos em andamento, no sentido de criar uma solução padrão para os problemas envolvendo o uso do IPSec em um ambiente de acesso remoto, que estão sendo discutidos atualmente no IPSec *Working Group*, grupo do IETF (*Internet Engineering Task Force*) que desenvolve mecanismos de segurança para o protocolo IP (Gleeson, 2000).

3.4 L2TP SOBRE IPSEC (L2TP/IPSEC)

Com o intuito de solucionar os problemas de segurança apresentados pelo L2TP, diversas propostas têm sido desenvolvidas, visando suprir as deficiências do protocolo L2TP através dos serviços de segurança oferecidos pelo IPSec.

A utilização do L2TP sobre o IPSec apresenta vantagens significativas para o acesso remoto VPN, pois a comunicação se beneficia dos serviços de confidencialidade, autenticidade, integridade e proteção contra *replay*, providos pelo IPSec, e ao mesmo tempo usufrui da autenticação de usuários, configuração e atribuição de endereços IP nos extremos do túnel, e suporte a múltiplos protocolos providos pelo túnel L2TP.

Quando executado sobre o IP, o L2TP é transportado através do UDP. Desta forma, a aplicação da proteção do IPSec sobre o L2TP pode basear-se simplesmente no uso de seletores que filtram o tráfego L2TP (Sena, 2002). É importante notar que neste caso o IPSec é utilizado em modo transporte, ou seja, não existe a criação de um túnel IPSec.

A Figura 5 exibe o encapsulamento de um pacote IP feito pelo L2TP sendo utilizado sobre o IPSec, protegido somente pelo ESP.

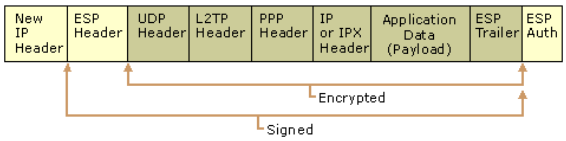

Fig. 5 - Encapsulamento de um pacote IP feito pelo L2TP sob a proteção do cabeçalho ESP do IPSec.

Tal procedimento no entanto implica em um certo custo. Há um *overhead* considerável na pilha de protocolos, particularmente porque o IPSec também é necessário por propósitos de segurança,

dado que o *host* pode estar conectado através de um *link dial-up* de baixa largura de banda.

O *overhead* é causado pela adição de vários cabeçalhos extra no envio de dados e protocolos de controle necessários ao controle da conexão, e pode trazer alguns problemas, como por exemplo, a fragmentação de pacotes IP.

Como consequência da fragmentação dos pacotes, pode-se ter uma queda significativa no desempenho, podendo causar também perda de pacotes e um aumento considerável no consumo de memória no *gateway* VPN, para realizar a remontagem dos pacotes fragmentados, prejudicando assim a viabilidade dessa solução. Além disso, algumas formas de ataque se aproveitavam da fragmentação de pacotes IP para burlar os *firewalls*.

Usando L2TP para o tunelamento, protegido pelo IPSec, teríamos uma aplicação web, por exemplo, rodando sobre a seguinte pilha de protocolos:

HTTP/TCP/IP/PPP/L2TP/UDP/ESP/IP

Enquanto que utilizando apenas o IPSec em modo túnel reduziríamos consideravelmente o *overhead*, usando a seguinte pilha de protocolos:

HTTP/TCP/IP/ESP/IP

Uma área de potenciais problemas também, seria o uso do PPP, devido ao fato que as características de uma camada de enlace implementada através de um túnel L2TP sobre um *backbone* IP são completamente diferentes de uma camada de enlace rodando sobre uma linha serial, como discutido na própria especificação do L2TP (Townsley, 1999). Parâmetros da conexão PPP mal escolhidos, por exemplo, podem levar a frequentes *resets* e *timeouts*, particularmente se a compressão estiver sendo usada. Isso ocorre porque o túnel L2TP pode desordenar ou até mesmo perder pacotes, o que normalmente não ocorre em linhas seriais. A taxa geral de pacotes perdidos pode ser significativa também devido ao congestionamento da rede (Gleeson, 2000).

Outro problema na integração do L2TP com o IPSec é a impossibilidade do segundo levar em consideração os valores dos campos de pacotes IP encapsulados pelo primeiro.

Outros procedimentos de interação entre os dois protocolos têm sido sugeridos no intuito de prover o desenvolvimento de soluções para aspectos ainda não padronizados do IPSec. Apesar destas soluções serem práticas e de baixo custo, pelo fato do protocolo L2TP já ser um padrão definido, existem críticas severas quanto ao uso de um protocolo que não foi projetado para ambientes seguros na execução de procedimentos vitais para um protocolo de segurança como o IPSec (Frankel, 2001).

4 CONCLUSÃO

As Redes Privadas Virtuais possuem uma importância fundamental para as organizações, principalmente em seu aspecto econômico.

O acesso remoto VPN apresenta diversas vantagens em relação aos acessos remotos tradicionais, como por exemplo, a redução dos custos e a escalabilidade que oferece, no entanto, traz consigo diversas implicações de segurança que precisam ser analisadas e solucionadas.

A carência de mecanismos capazes de proteger o acesso remoto VPN culminou na especificação de diferentes padrões.

Com a análise dos principais protocolos utilizados para acesso remoto VPN em plataformas Windows, foi possível observar alguns dos pontos positivos e negativos de cada tecnologia, facilitando assim a opção por uma tecnologia mais adequada às necessidades de cada cenário.

O PPTP, por apresentar uma estrutura bastante simples, pode ser uma solução adequada em situações onde não é exigida uma solução robusta de segurança.

O L2TP não possui mecanismos de proteção do túnel definidos, por isso seu uso em cenários onde existe uma rede não-confiável, como a Internet, entre os extremos de um túnel, deve sempre ser combinado com outros protocolos capazes de suprir a sua ausência de serviços de segurança.

A utilização do L2TP sobre o IPSec é uma alternativa que apresenta muitas das funcionalidades necessárias para o acesso remoto VPN.

O uso da confidencialidade, autenticidade, integridade e proteção contra replay, providos pelo IPSec, unidos a autenticação de usuários, configuração e atribuição de endereços IP nos extremos do túnel, e suporte a múltiplos protocolos providos pelo túnel L2TP, são algumas das vantagens apresentadas por essa solução.

Porém, causa um *overhead* considerável na pilha de protocolos utilizada. Como consequência disso, podem surgir problemas de segurança relacionados à fragmentação de pacotes IP causada, além do impacto direto no desempenho, na disponibilidade e na viabilidade da solução VPN.

O IPSec em modo túnel é uma solução que vem sendo padronizada e que atende perfeitamente aos requisitos de segurança das soluções VPN. No entanto, ainda carece de padronizações em alguns aspectos de funcionalidade e interoperabilidade do acesso remoto VPN, dependendo do término de trabalhos em andamento para a completa viabilidade da solução.

REFERÊNCIAS BIBLIOGRÁFICAS

BELLOVIN, S. M., *Problem Areas for the IP Security Protocols*. In Proceedings of the Sixth Usenix Security Symposium, pp. 205-214, Jul. 1996.

BELLOVIN, S. M., *Probable Plaintext Cryptoanaliysis of the IP Security Protocols*. In Proceedings of the 1997 Symposium on Network and Distributed Systems Security, 1997.

CHAPMAN, B., COOPER, S., and ZWICKY, E., *Building Internet Firewalls*. O'Reilly Associates, Sebastopol, Califórnia, 2nd Edition, 2000.

FARINACCI, D., et al., *Generic Routing Encapsulation (GRE)* , RFC 2784, Mar. 2000.

FRANKEL, S., *Demystifying the IPSec Puzzle*. Artech House, Norwood, Massachusetts, 2001.

GLEESON, B., et al., *A Framework for IP Based Virtual Private Networks*, RFC 2764, Feb. 2000.

HAMZEH, K., et al., *Point-to-Point Tunneling Protocol (PPTP)*, RFC 2637, Jul. 1999.

HARKINS, D., and CARREL, D., *The Internet Key Exchange (IKE)*, RFC 2409, Nov. 1998.

KENT, S., and ATKINSON, R., *Security Architecture for the Internet Protocol*, RFC 2401, Nov. 1998a.

KENT, S., and ATKINSON, R., *IP Authentication Header*, RFC 2402, Nov. 1998b.

KENT, S., and ATKINSON, R., *IP Encapsulating Security Payload (ESP)*, RFC 2406, Nov. 1998c.

KLEIN, D. V., *Foiling the Cracker: A Security of, and Implications to, Password Security*. In: 2nd USENIX Workshop on Security, pp. 5-14, 1990.

MEYER, G., *The PPP Encryption Control Protocol (ECP)*, RFC 1968, Jun. 1996.

NAKAMURA, E. T., *Um Modelo de Segurança de Redes para Ambientes Cooperativos*. Campinas: IC/UNICAMP, 2000. Tese de Mestrado.

PATEL, B., et al., *Securing L2TP Using IPSec*, RFC 3193, Nov. 2001.

RAND, D., *The PPP Compression Control Protocol (CCP)*, RFC 1962, Jun. 1996.

SCHNEIER, B., *Applied Cryptography*. John Wiley & Sons, New York, 2nd Edition, 1996.

SCHNEIER, B., and MUDGE, *Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)*, Proceedings of 5th ACM Conference on Communications and Computer Security, ACM Press, Nov. 1998, http://www.counterpane.com/pptp.pdf.

SCHNEIER, B., MUDGE, and WAGNER, D., *Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)*, *CQRE '99*, Springer-Verlag, Heidelberg, Germany, 1999, pp. 192-203, http://www.counterpane.com/pptpv2.pdf.

SENA, J. C., *Um modelo para proteção do tráfego de serviços baseado em níveis de segurança*. Campinas: IC/UNICAMP, 2002. Tese de Mestrado.

SENA, J. C., GEUS, P. L., and AUGUSTO, A., *Impactos da Transição e Utilização do IPv6 sobre a Segurança de Ambientes Computacionais*. In: II WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS, Maio 2002, Búzios. Anais do 20º Simpósio Brasileiro de Redes de Computadores. Búzios: SBRC'2002, 2002, pp.73-80.

SIMPSON, W., *The Point-to-Point Protocol (PPP)*, RFC 1661, Jul. 1994.

SRISURECH, P., *Secure Remote Access with L2TP*, RFC 2888, Aug. 2000.

TOWNSLEY, W., et al., *Layer Two Tunneling Protocol (L2TP)*, RFC 2661, Aug. 1999.

VALENCIA, A., LITTLEWOOD, M., and KOLAR, T., *Cisco Layer Two Forwarding (Protocol) "L2F"*, RFC 2341, May 1998.