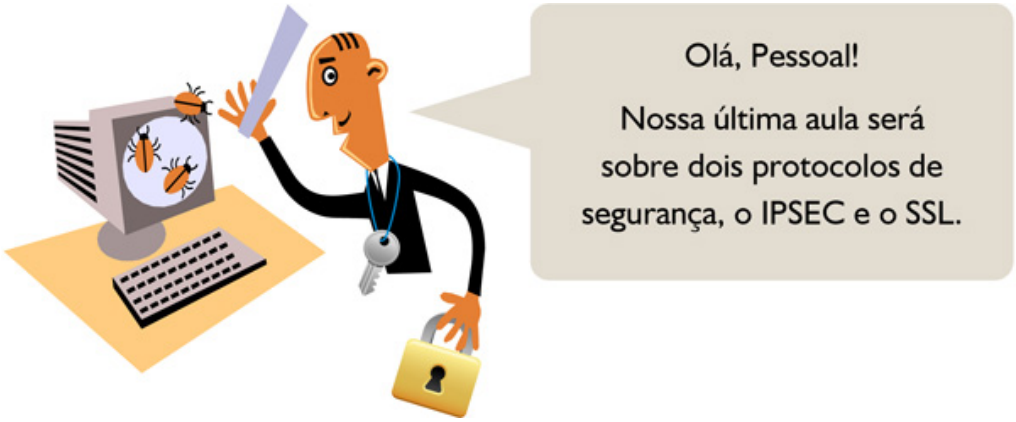
Segurança em Redes

Aula 10 - IPSEC e SSL

Apresentação



Nesta aula, você vai estudar mais uma maneira de adicionar segurança aos sistemas computacionais, em nível de protocolos de rede. Estudaremos o IPSEC e o SSL.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Definir o que é IPSec.
- Descrever o que é SSL.
- Conhecer, de uma forma geral, o funcionamento do IPSec e do SSL.
- Diferenciar SSL e IPSec.

Visão Geral

Um ambiente computacional está sujeito a problemas de segurança, como vírus e invasões, que podem, por exemplo, impedir o seu correto funcionamento ou levar a perda de informações. Como você já estudou durante a disciplina, a segurança computacional tem como objetivo, exatamente, prevenir que usuários mal intencionados realizem ataques que venham a comprometer um sistema. Para uma rede ser considerada segura, ela deve possuir uma forte política de segurança, que defina tanto as condições de acesso de usuário às informações quanto o uso de mecanismos de segurança na mesma.

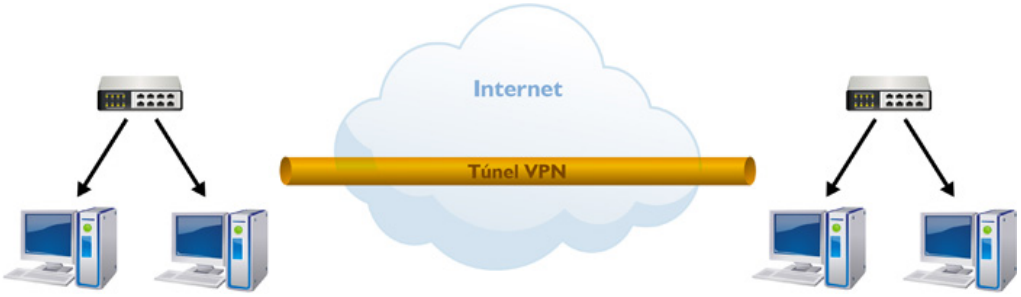
Como mostrado nas aulas anteriores, existem várias soluções para construção de uma infraestrutura segura para a internet: uso de criptografia, de mecanismos de autenticação do usuário, acompanhamento de suas ações, sistemas de detecção de intrusão e auditoria para verificar se a política de segurança da rede está realmente funcionando.

Nesse sentido, esta aula tem como objetivo mostrar o que é SSL e IPSec e como eles são usados para garantir privacidade, integridade e autenticidade de informações com uso de encriptação, certificação digital e autenticação de dispositivos.

Redes Privadas Virtuais (VPN)

Antes de explicar os protocolos de segurança SSL e IPSec, é necessário ter um conhecimento prévio sobre o que são redes privativas virtuais (VPNs). Segundo Martins D. (2000), uma VPN pode ser definida como uma simulação de rede privativa de longa distância. A **Figura 1** mostra um exemplo de VPN em que duas redes privadas se comunicam utilizando um “túnel” criado por uma VPN.

Figura 01 - Visão Geral VPN.



Vídeo 01 - VPN

As VPNs criptografam todo o tráfego que passa por este túnel, fornecendo confidencialidade à informação. Quando adequadamente implementada, uma VPN pode assegurar comunicação segura por meio de redes inseguras.

Atividade 01

1. As VPNs garantem a disponibilidade da informação? Por quê?

Secure Sockets Layers (SSL)

O SSL (ou camada de sockets protegida) é um mecanismo de segurança através do qual podemos garantir segurança na transmissão de dados na internet. O SSL consiste em um método de criptografia por chave pública no qual para haver comunicação entre duas maquinas (normalmente cliente e servidor) é realizada uma etapa de autenticação e, em seguida, é criado um canal de comunicação protegido (criptografado) entre essas máquinas.

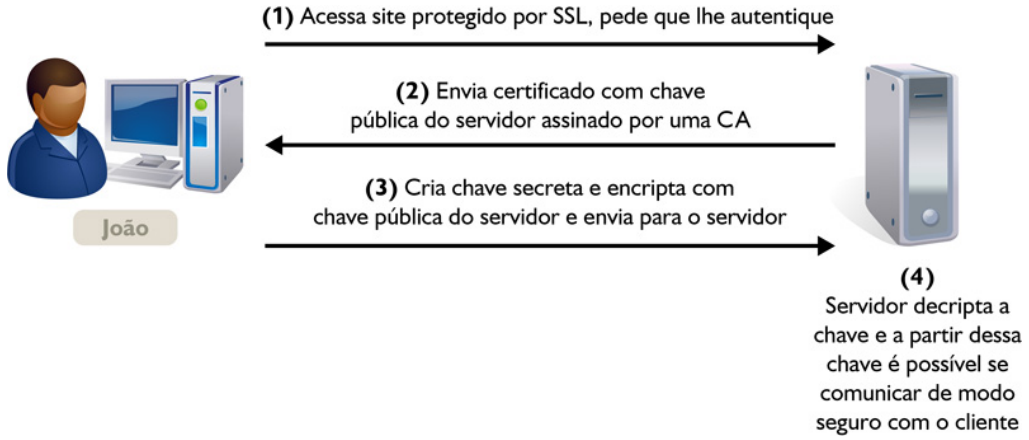
O SSL atua entre as camadas de aplicação e transporte, sendo independente de protocolo de aplicação, ou seja, pode proteger diferentes protocolos como HTTP, FTP, POP3, IMAP etc.

Funcionamento do SSL

O mecanismo de segurança das transações do SSL 2.0 é baseado na troca de chaves entre cliente e servidor, a fim de garantir a integridade e a confidencialidade dos dados trocados. A transação protegida por SSL segue o modelo ilustrado na **Figura 2** e descrito a seguir:

- Inicialmente, o cliente conecta-se ao servidor e pede-lhe que se autentique. O cliente envia também uma lista dos algoritmos de criptografia que suporta.
- Quando o servidor recebe o pedido, envia seu certificado, contendo sua chave pública, assinada por uma autoridade certificadora (CA), bem como o nome do algoritmo de criptografia usado.
- O cliente, por sua vez, verifica a validade e a autenticidade do certificado, e cria uma chave secreta aleatória, conhecida como chave de sessão. Em seguida, encripta a chave de sessão com a chave pública do servidor e envia o resultado para o mesmo.
- O servidor decripta a chave de sessão com a sua chave privada. Assim, as duas entidades estão na posse de uma chave comum da qual são os únicos conhecedores. O restante da comunicação será criptografada utilizando essa chave.

Figura 02 - Modelo de funcionamento básico do SSL.



Vídeo 03 - Conhecendo o IPSec e SSL

Vídeo 04 - Configuração HTTPS

Vantagens e Desvantagens do SSL

O SSL é amplamente utilizado, estando disponível nos principais sistemas operacionais, como Windows, Linux e Mac OS X. Outro ponto positivo do SSL é sua independência (teórica) das aplicações utilizadas, ele, simplesmente, cria um canal seguro que permite que se executem todas as funções que, normalmente, já estão disponíveis no TCP/IP.

Como desvantagem destaca-se o aumento no consumo de banda de rede e CPU. Na prática, apesar de ser independente do protocolo, as aplicações em si, por exemplo, um navegador web como o Firefox, devem inserir o suporte ao SSL em seu código.

Atividade 02

1. Pesquise e cite outras vantagens do uso do SSL.

IPSec

O IPSec (ou protocolo de segurança IP) é um conjunto de extensões do protocolo IP que tem o objetivo de fornecer confidencialidade, integridade e disponibilidade às informações transferidas por meio da internet.

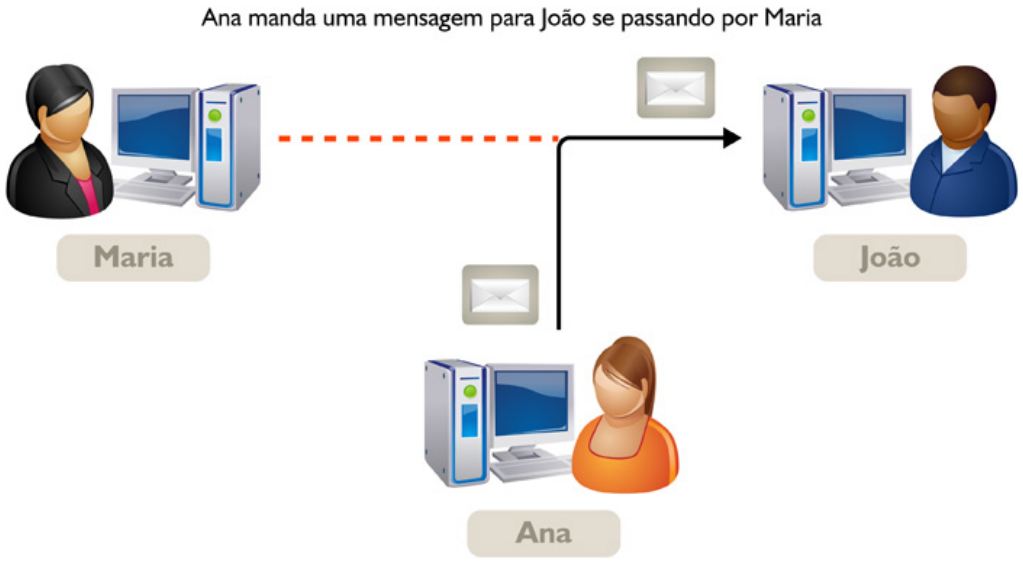
Outros protocolos de segurança da internet, como o SSL estudado anteriormente, operam próximos à camada de aplicação. O IPSec, ao contrário, opera sob a camada de rede do modelo TCP/IP, o que o torna mais flexível, mais complexo (e aumenta o gasto de processamento).

Finalidade do IPSec?

O IPSec cria um canal de comunicação seguro, em que todos os dados trocados entre os computadores com IPSec habilitado são criptografados. O uso de criptografia permite ao IPSec a proteção de seus usuários contra ataques e tentativas de captura dos dados por pessoas não autorizadas, mesmo se estiverem em redes inseguras como a internet.

Em suma, o IPSec é um protocolo de comunicação que serve para garantir privacidade e integridade dos dados, assim como evitar falsificação de identidade (também conhecido como IP spoofing). O IP spoofing consiste em mascarar ou manipular o cabeçalho IP fazendo-se passar por um determinado endereço de origem para enviar pacotes e dados se passando por outra pessoa. A **Figura 3** mostra Ana enviando uma mensagem para João se passando por Maria, ou seja, ela mascara sua real identidade.

Figura 03 - IP Spoofing.



Tecnologias Envolvidas no IPSec

IPSec combina tecnologias diferentes de segurança em um sistema completo que provê confidencialidade, integridade e autenticidade, empregando atualmente (STEPHEN, 1995):

- Protocolo Diffie-Hellman para troca de chaves entre duas partes em qualquer rede pública.

- Criptografia de chave pública para permitir trocas de chaves, garantindo, assim, a identidade das duas partes e evitando ataques do tipo *man-in-the-middle* (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação).

- Algoritmos de criptografia simétricos: como o DES (Data Encryption Standard), normalmente, utilizados em trocas de grandes volumes de dados.

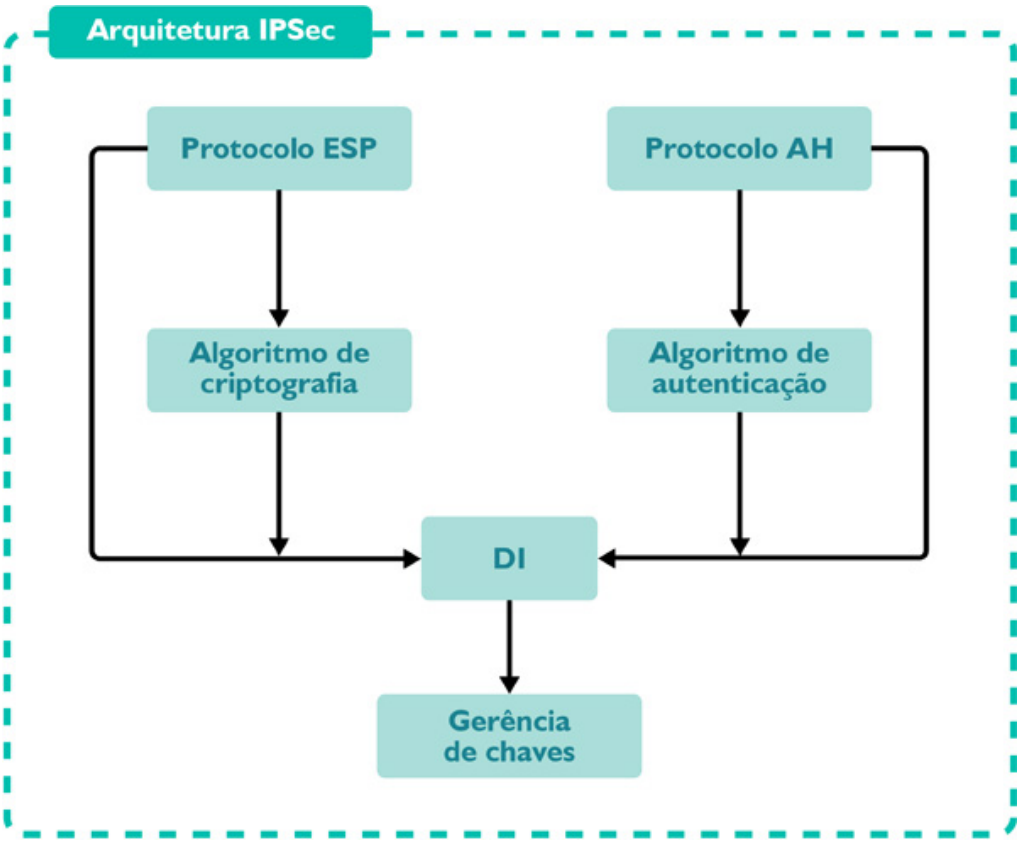
- Algoritmos para cálculo de *hash,* como o MD5 ou SHA, e de autenticação, como o HMAC.

- Certificados digitais assinados por autoridades certificadoras.

Arquitetura IPSec

A arquitetura do IPSec é composta por vários componentes. A **Figura 4** mostra os principais componentes e as suas relações.

Figura 04 - Arquitetura IPSec.



Os principais componentes da arquitetura do IPSec são: o cabeçalho de autenticação (AH), o protocolo de segurança (ESP) e o gerenciamento de chaves.

O protocolo AH (*Authentication Header*) é usado para prover autenticação aos datagramas IP. O cabeçalho AH possui um campo chamado "autenticação de dados", que contém um *hash* da mensagem e uma assinatura digital. A assinatura digital é processada utilizando o algoritmo de autenticação especificado na associação de segurança. O protocolo ESP (*Encapsulating Security Payload*) foi projetado para oferecer autenticação e confidencialidade através de criptografia.

Para padronizar os parâmetros de uma determinada transação segura (SA – Security Association), o IPSec usa o conceito de *domínio de interpretação* (componente DI na **Figura 4**), que funciona semelhante a um banco de dados para armazenar identificadores de algoritmos de criptografias e autenticação, bem como parâmetros operacionais, como a vida útil das chaves dos algoritmos. Esses dados são usados durante o estabelecimento de um canal seguro para a comunicação.

O gerenciamento de chaves do IPSec usa o protocolo IKE (*Internet Key Management*), que é uma combinação de outros protocolos usados para prover serviço de autenticação, permuta de chaves e vários modos de troca de chaves criptográficas.

Usando o IPSec

A implementação do IPSec não requer alteração nos aplicativos existentes. A sua configuração é feita a partir de diretivas de segurança para permitir que o computador use o IPSec. Fazendo isso, automaticamente, todos os programas instalados no computador usarão o IPSec, quando houver transações com outros computadores que também tenham IPSec configurado. Em suma, o IPSec fica totalmente transparente para os usuários finais, sendo sua implementação totalmente realizada no próprio sistema operacional.

De acordo com o que podemos verificar na **Figura 5**, o IPSec utiliza o conceito de tunelamento, ou seja, são criados túneis entre as redes por onde as informações vão passar. Na prática, os administradores de cada rede devem compartilhar uma chave de autenticação entre cada um dos computadores usando IPSec e configurar uma

porta de comunicação e o IP de destino. A chave de autenticação serve para que os dois (ou mais) computadores se autentiquem, sendo idêntica em todos eles. Somente o usuário administrador deve poder acessar ou alterar a mesma.

Figura 05 - Tunelamento IPSec.

Atividade 03

1. Quais os tipos de criptografia suportadas pelo IPSec?

Diferenças SSL e IPSec

Os mecanismos de segurança IPSec e SSL são ambos eficazes e bastante utilizados na internet, porém, esses mecanismos possuem algumas diferenças. O **Quadro 1** realiza um comparativo entre SSL e IPSec.

	SSL	**IPSec**
Aplicações com suporte	Navegadores web, clientes de email	Qualquer
Criptografia	Simétrica e assimétrica	Simétrica e assimétrica
Autenticação	Pode-se usar tokens ou certificação digital	Pode-se usar tokens ou certificação digital

	SSL	IPSec
Facilidade de uso	Alta – O usuário precisa saber usar web browser	Baixa – O usuário precisa ter conhecimento sobre IPSec
Complexidade	Moderada	Alta
Consumo de recursos	Médio	Baixo

Quadro 1 - Comparativo entre SSL e IPSec

Resumo

Nesta aula, aprendemos o que é SSL e IPSEC, como eles funcionam e as diferenças entre eles. Percebemos a diferença entre esse assunto e os anteriores, uma vez que esses são protocolos que atuam em nível de rede ou aplicação.

Autoavaliação

1. Quais as principais desvantagens do IPSec?
2. Cite duas semelhanças entre SSL e IPSec.
3. Nas alternativas a seguir, assinale V para verdadeiro e F para falso:

   ( ) O IPSec é computacionalmente mais leve que o SSL.
   ( ) Ambos os protocolos estudados permitem a autenticação do outro usuário ou computador envolvido em uma comunicação.
   ( ) O SSL é totalmente independente da aplicação, sendo seu uso transparente para elas.
   ( ) O IPSec é implementado pelo Sistema Operacional, como uma extensão das funcionalidades originais da camada de rede.

Referências

GODINHO JUNIOR, Luis; BOGO, Madianita. Análise da Utilização do IPSec como Garantia de Segurança na Comunicação em Redes TCP/IP. In: ENCONTRO DE ESTUDANTES DE INFORMÁTICA DE TOCANTINS, 6., 2004, Palmas. **Anais...** Palmas, 2004. Disponível em: <http://www.focosecurity.com.br/materiais_academicos_arquivo/luisGodinhoIPSECEncoinfo2004.pdf>. Acesso em: 19 out. 2010.

LARGURA, Luiz Aristides Rios. **Monografia sobre SSL para o Curso de Extensão Segurança em Redes de Computadores**: 5a Turma. 2000. Monografia (Trabalho de Conclusão de Curso) – Departamento de Ciência da Computação, Instituto de

Ciências Exatas, Universidade de Brasília, Brasília, 2000. Disponível em: <http://www.cic.unb.br/~pedro/trabs/ssl.pdf>. Acesso em: 23 ago. 2012.

MARTINS, D. **Redes privadas virtuais com IPSec**. Brasília, 2000. Disponível em: <http://www.cic.unb.br/~pedro/trabs/vpn.pdf>. Acesso em: 23 ago. 2012.

NAKAMURA, E.; GEUS, P. L. **Segurança em Redes em Ambientes Cooperativos**. Rio de Janeiro: Editora Novatec, 2007.

STEPHEN, K.; ATKINSON, R. **Security Architecture for the internet protocol**. IETF RFC1825, 1995.

TUTORIAL de TCP/IP. Disponível em: <http://www.juliobattisti.com.br/artigos/windows/tcpip_p18.asp>. Acesso em: 19 out. 2010.