Universidade Estadual de Londrina

KAUEE ROCHA PUERTAS

Segurança, TLS e Certificados Digitais

LONDRINA - PR
2023

Trabalho de Laboratório – 02/05/2023

Questão 01) Qual a função do protocolo IPsec, apresente seu histórico, funções, camadas, em qual RFCs ele foi padronizado?

O IPsec (Internet Protocol Security) é um conjunto de protocolos que oferecem segurança para comunicações de rede IP. Ele foi criado para suprir a necessidade de segurança de redes, garantindo confidencialidade, integridade e autenticidade dos dados trafegados. O IPsec possui dois modos de operação, modo de transporte e modo de túnel. No modo de transporte, a segurança é aplicada apenas aos dados que são transportados pelo pacote IP, enquanto que no modo de túnel, o pacote IP inteiro é encapsulado em um novo pacote IP.

O IPsec é composto pelos seguintes protocolos:

- AH (Authentication Header): responsável pela autenticação dos dados e garantia de integridade;
- ESP (Encapsulating Security Payload): responsável pelo fornecimento de confidencialidade e autenticação;
- IKE (Internet Key Exchange): responsável por estabelecer as chaves criptográficas usadas pelos outros protocolos do IPsec.

O IPsec opera nas camadas de rede e transporte, e é padronizado pelas RFCs 2401, 2402, 2406, 2407 e 2408.

Questão 02) Qual a função do protocolo TLS, apresente seu histórico, funções, camadas, em qual RFC ele foi padronizado?

O Transport Layer Security (TLS) é um protocolo criptográfico projetado para fornecer comunicação segura pela Internet. Ele é frequentemente usado para proteger a comunicação entre aplicativos cliente/servidor, como navegação na web, e-mail e mensagens instantâneas. As principais funções do TLS são autenticação, confidencialidade e integridade.

O TLS foi desenvolvido como uma evolução do Secure Sockets Layer (SSL), que foi originalmente criado pela Netscape em 1994. O SSL foi projetado para fornecer comunicação segura entre clientes e servidores, e a primeira versão do TLS (TLS 1.0) foi criada em 1999 como uma atualização do SSL.

Desde então, o TLS foi aprimorado e atualizado várias vezes para se tornar mais seguro e eficiente. As versões mais recentes incluem TLS 1.1, TLS 1.2 e TLS 1.3. O TLS é padronizado pelo IETF (Internet Engineering Task Force) e é definido pela RFC 5246, que descreve a versão 1.2 do protocolo.

O TLS opera na camada de transporte do modelo OSI, que é responsável por garantir a entrega confiável de dados de um dispositivo para outro. O TLS é implementado entre o protocolo de transporte (como TCP) e o protocolo de aplicativo (como HTTP). Ele usa criptografia simétrica e assimétrica para proteger a comunicação e usa um modelo de chave pública/privada para gerenciamento de chaves. Durante o handshake inicial, as chaves são negociadas entre o cliente e o servidor para estabelecer uma conexão segura.

O TLS é amplamente adotado e é usado em quase todas as transações financeiras na Internet, bem como em muitos outros tipos de comunicação on-line.

Questão 03) Apresente em uma tabela as principais diferenças/características entre o TLS e do IPSEC?

Característica	TLS	IPsec
Nível do Modelo OSI	Camada de Transporte	Camada de Segurança da Internet e Camada de Gerenciamento de Chaves
Finalidade	Comunicação segura entre aplicativos cliente/servidor	Segurança em nível de rede
Padronização	RFC 5246 do IETF	RFCs 2401 a 2412 do IETF
Principais funções	Autenticação, Confidencialidade e Integridade	Autenticação e Criptografia
Usos comuns	Navegação na web, e-mail, mensagens instantâneas	Redes privadas virtuais (VPNs), conexões ponto a ponto
Escopo	Limitado a comunicação entre cliente e servidor	Pode ser usado em toda a rede
Implementação	Principalmente em aplicativos de software	Pode ser implementado em roteadores, firewalls e outros equipamentos de rede
Criptografia	Usa criptografia simétrica e assimétrica	Usa principalmente criptografia simétrica
Chave de segurança	As chaves são negociadas durante o handshake	As chaves são estabelecidas antes da comunicação
Desempenho	Leve e adequado para transações de baixo volume	Mais pesado e adequado para grandes volumes de tráfego
Gerenciamento de chaves	Usa um modelo de chave pública/privada	Usa principalmente um modelo de chave compartilhada

REFERÊNCIAS

https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-vf/ipsec/

https://www.cloudflare.com/pt-br/learning/ssl/transport-layer-security-tls/

https://www.blockbit.com/pt/blog/vpn-ipsec-ou-ssl/