INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Prática 19: Protocolos de Segurança IPSec, SSL/TLS e HTTPS.

Olá, meus alunos!! Como é que vocês vão? Na aula de hoje iremos compreender a importância dos protocolos de segurança na comunicação em redes. Conhecer os princípios de funcionamento e aplicação do IPSec, SSL/TLS e HTTPS. Analisar os cenários de uso, vantagens e limitações de cada protocolo e realizar uma análise prática de uma conexão HTTPS . Vamos lá!!! Preparados???

IPSec

O IPSec (Internet Protocol Security) é um conjunto de protocolos que fornece segurança para comunicações IP ao nível da camada de rede. Ele é amplamente utilizado para proteger dados transmitidos entre computadores, especialmente em conexões de VPNs (*Virtual Private Networks*).

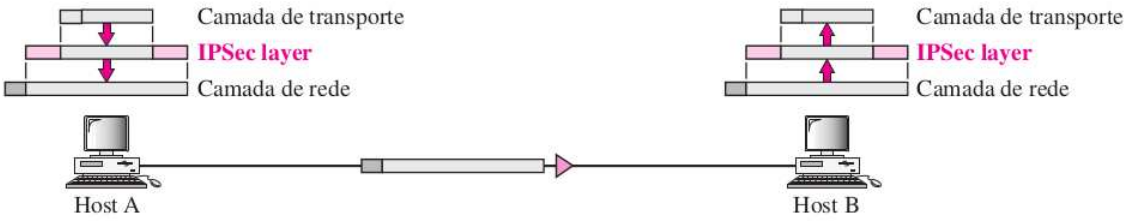
A maioria dos sistemas operacionais modernos, incluindo distribuições Linux e Windows, oferecem suporte nativo ao IPSec.

O IPSec protege o tráfego de dados, oferecendo três serviços principais: confidencialidade, integridade e autenticação. Para isso, o protocolo pode operar em dois modos distintos:

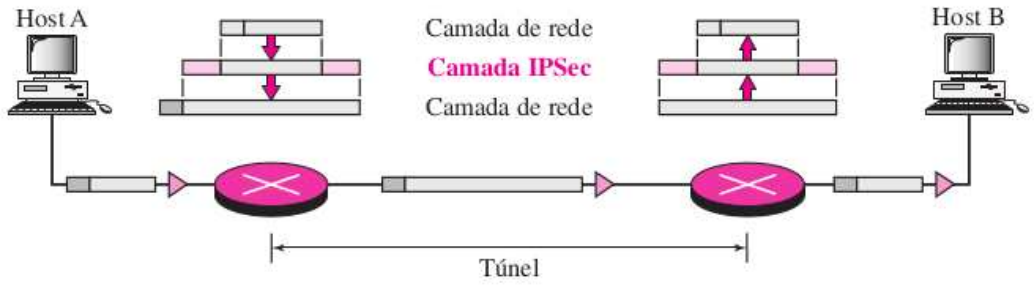
- Modo Transporte: protege a carga útil do pacote IP (dados da camada de transporte), mantendo o cabeçalho original intacto.
- Modo Túnel: encapsula o pacote IP inteiro, incluindo cabeçalho e dados, dentro de um novo pacote. O novo cabeçalho IP tem informações distintas do cabeçalho IP original.

No modo transporte, é calculada a função hash da carga útil do pacote IP é depois a carga útil é criptografada. Isso garante que, se o pacote for interceptado por um atacante, ele não poderá ler ou alterar os dados. O cabeçalho IP original do pacote é mantido e não é criptografado. Isso significa que a informação como o endereço IP de origem e destino permanece visível, mas os dados transmitidos estão protegidos.

Modo Transporte:



Modo Túnel:



No modo túnel, o pacote IP original é encapsulado dentro de um novo pacote IP. Este novo pacote recebe um novo cabeçalho IP, e o pacote original é criptografado e tratado como a carga útil deste novo pacote. Isso significa que as informações de origem e destino no cabeçalho original são ocultadas e protegidas, o que aumenta a privacidade e a segurança da comunicação. Este novo cabeçalho é utilizado para rotear o pacote pela rede, enquanto o cabeçalho original permanece criptografado dentro do pacote. É amplamente utilizado para criar VPNs (Virtual Private Networks) entre dois gateways, como entre duas redes corporativas.

Dois protocolos fundamentais compõem o IPSec:

- O AH (*Authentication Header*): permite a autenticação e a integridade dos dados utilizando a função hash e uma chave simétrica para criar um resumo de mensagem autenticada (HMAC). Ele garante que os dados não foram modificados durante o trânsito e que o remetente é quem afirma ser mas não garante a confidencialidade;

- O ESP (*Encapsulating Security Payload*): implementa autenticação, integridade e confidencialidade dos dados. O protocolo ESP acrescentou a criptografia simétrica.

O AH insere um novo cabeçalho entre o cabeçalho IP e o conteúdo do pacote. Ele inclui um código de autenticação (como HMAC-SHA256) que é verificado no destino. Se alguém alterar o pacote no caminho, o código não baterá, e o pacote será descartado. O ESP ele cifra os dados com algoritmos de criptografia, além de utilizar o HMAC para autenticação e integridade. O ESP é mais utilizado do que o AH. No IPv6 o AH e o ESP fazem parte do cabeçalho de extensão.

SSL/TLS

Foi desenvolvido também protocolos de segurança para a camada de transporte. Entre eles se destaca o SSL (Secure Sockets Layer) e seu sucessor TLS (Transport Layer Security), que garantem a confidencialidade, integridade e autenticidade dos dados trafegados.

O SSL foi desenvolvida em 1994 Netscape para garantir a segurança das comunicações na web. Ele estabelecia um canal seguro entre o cliente e o servidor, criptografando e autenticando os dados transmitidos. No entanto, tinha várias vulnerabilidades significativas.

Em 1999, A Internet Engineering Task Force (IETF) padronizou o TLS como uma versão aprimorada do SSL 3.0. O TLS introduziu melhorias de segurança significativas, como métodos mais robustos de autenticação e criptográficos. TLS 1.3 é a versão mais recente do protocolo.

O uso mais comum e conhecido do TLS é: navegação na web, e-mail, mensagens instantâneas e outras transferências de dados. Estes protocolos garantem: a confidencialidade, a integridade dos dados e a autenticação.

O funcionamento do TLS baseia-se em duas etapas principais. A primeira é o handshake, ou aperto de mão, em que cliente e servidor trocam informações para negociar os algoritmos de criptografia que serão utilizados. Da seguinte forma:

1. O cliente envia uma mensagem "Client Hello" para o servidor, contendo a versão do protocolo, algoritmos de criptografia, hash e compressão de dados suportados e valores aleatório que será usado para gerar chaves criptográficas.

2. O servidor responde com um "Server Hello", contendo: versão, algoritmos de criptografia selecionada pelo servidor, valores aleatórios gerado pelo servidor, também usado para gerar chaves criptográficas, certificado digital do servidor e opcionalmente pode solicitar o certificado do cliente.

3. O cliente verifica o certificado digital do servidor usando uma autoridades certificadoras (CAs). Se o certificado for válido e confiável, a conexão continua.

4. O cliente gera um "pre-master secret", um valor aleatório que será usado para criar as chaves simétricas. Esse valor é criptografado com a chave pública do servidor (obtida do certificado digital) e enviado ao servidor.

5. O servidor usa sua chave privada para descriptografar o "pre-master secret"

6. Tanto o cliente quanto o servidor usam o "pre-master secret", juntamente com os valores aleatórios trocados durante o handshake, para gerar as chaves simétricas para criptografia e de autenticação das mensagens durante a sessão.

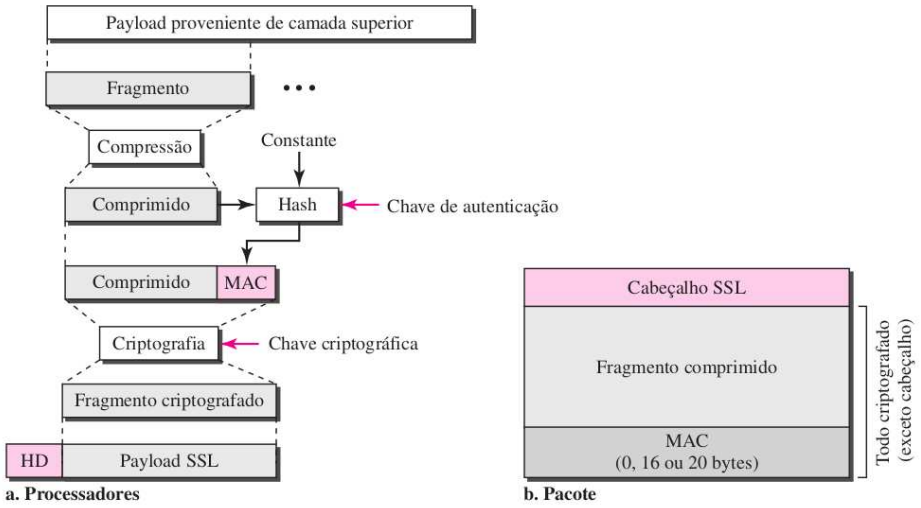
7. Agora, o cliente e o servidor começam a usar as chaves simétricas para criptografar e autenticar os dados trocados durante a sessão.

Depois de garantida a autenticação e obtida as chaves de criptografia, os dados podem ser trocados. Da seguinte forma:

1. A primeira etapa é a fragmentação. Cada mensagem de camada superior é fragmentada em blocos de até 2^{14} bytes.

2. É realizada a compactação, porém ela é, opcional e normalmente não é utilizado.

Encapsulando os dados com SSL/TLS.



3. É calculado um código de autenticação de mensagem (HMAC). Para essa finalidade, é usada uma chave secreta compartilhada e um algoritmo de hash.

4. A mensagem compactada mais o MAC são encriptados usando a encriptação simétrica.

A troca de dados é bidirecional e simultânea: o cliente pode continuar enviando dados criptografados (formulários, credenciais, uploads) e o servidor responde com dados também criptografados (páginas HTML, mensagens, arquivos). Tudo isso ocorre de forma transparente para o usuário.

Os certificados digitais utilizados pelo TLS seguem o padrão X.509 e desempenham papel essencial na autenticação. Eles são emitidos por autoridades certificadoras, como a Let's Encrypt ou a DigiCert, que asseguram a identidade dos servidores e estabelecem uma cadeia de confiança entre as partes envolvidas.

O TLS utiliza uma combinação de algoritmos criptográficos, incluindo algoritmos de troca de chaves como RSA e ECDHE, algoritmos de criptografia simétrica como AES e ChaCha20, e funções de hash como SHA-256. O resultado é uma comunicação segura, resistente a interceptações e manipulações, mesmo em redes públicas ou não confiáveis.

O TLS é utilizado em diversas aplicações, como acesso seguro à web (HTTPS), envio de e-mails (SMTPS), transferência segura de arquivos (FTPS), serviços de voz sobre IP (VoIP) e conexões remotas.

HTTPS

O protocolo HTTPS, sigla para *HyperText Transfer Protocol Secure*, representa a evolução do HTTP para atender à crescente demanda por segurança na navegação web. Com a utilização do protocolo TLS, o HTTPS assegura a confidencialidade das informações, protegendo dados como senhas, informações bancárias e dados pessoais. Além disso, ele garante a integridade dos dados, impedindo que sejam modificados durante a transmissão. Além disso, o HTTPS fornece autenticação, ao permitir que o navegador verifique a identidade do servidor acessado, evitando ataques de falsificação e interceptação (man-in-the-middle).

Na prática, o HTTPS é utilizado em praticamente todos os sites modernos que envolvem algum tipo de troca de informação sensível, como serviços bancários, redes sociais, comércio eletrônico e plataformas educacionais. Além disso, o uso do HTTPS passou a ser um critério de ranqueamento nos mecanismos de busca, incentivando sua adoção ampla.

Quando um usuário acessa um site utilizando HTTPS, o navegador e realiza os seguintes passos:

1. O navegador inicia uma conexão com o servidor IP de destino usando o protocolo TCP na porta 443 (porta padrão do HTTPS). O navegador envia um pacote SYN. O servidor responde com SYN-ACK e o navegador responde com ACK.

2. O navegador envia a mensagem TLS ClientHello com: versões TLS que suporta (ex: TLS 1.3), algoritmos de criptografia (AES), número aleatório e identificador do servidor (SNI).

3. O servidor responde com uma mensagem TLS ServerHello com: versão TLS e algoritmo escolhidos, outro número aleatório e o certificado digital X.509 com chave pública assinado por uma autoridade certificadora.

4. O navegador verifica o certificado digital (validade, domínio, CA confiável). Se o certificado for inválido, exibe um aviso de segurança.

5. Caso o certificado seja validado ou o usuário assuma os riscos, ambos derivam uma chave de sessão simétrica segura para criptografar os dados (usando Diffie-Hellman, por exemplo).

6. Mensagens ChangeCipherSpec e Finished são trocadas para ativar a criptografia.

7. Com a conexão segura ativa, o navegador envia a requisição HTTP de forma criptografada.

8. O servidor envia a resposta HTTP também cifrada. O navegador descriptografa a resposta e começa a processar o conteúdo (HTML, CSS, imagens, scripts).

Atividades

01. Com o Wireshark, acesse: https://portal.ifrn.edu.br e aplique o filtro: "tls && ip.addr == 200.137.1.195". Coloque os resultados em um arquivo de texto.

- **a)** No pacote Client Hello, identifique a versão TLS, cipher suites propostas, algoritmos de compressão (Compression Method) e algoritmos de assinaturas suportado (Signature HASH Algorithm).
- **b)** No pacote Server Hello, identifique a versão do TLS, algoritmo de criptografia selecionado (Cipher Suite), método de compressão selecionado (Compression Method)

02. No seu navegador iremos inspecionar o Certificados HTTPS do site do IFRN. Para isso, clique no cadeado da barra de endereços, em "Conexão segura", "Mais informações" e "Ver certificado". Coloque os resultados em um arquivo de texto.

- **a)** Informações relacionadas ao sujeito (País, Estado, Localidade, Organização e Nome);
- **b)** Informações sobre o emissor do certificado: País, Organização e Nome;
- **c)** Validade do certificado;
- **d)** Informações da chave pública: Algoritmo e Tamanho da Chave;
- **e)** Algoritmo de assinatura.

03. Insira o arquivo com os resultados no Google Sala de Aula.