

**UNIVERSIDADE FEDERAL DE MATO GROSSO - UFMT
CAMPUS ARAGUAIA**

**TAINÁ ISABELA MONTEIRO DA SILVA
WILLYAN JOSUÉ BASTOS SILVA**

**BARRA DO GARÇAS
2022**

Tainá Isabela Monteiro Da Silva
Willyan Josué Bastos Silva

Trabalho escrito apresentado como requisito parcial
para obtenção de nota na disciplina de Rede
de Computadores em Bacharel em Ciência da
Computação do Universidade Federal de Mato
Grosso - UFMT, Campus Araguaia.

Docente: Prof. Dr. Maxweel Silva Carmo

Barra do Garças
2022

SUMÁRIO

1	INTRODUÇÃO	4
2	DESENVOLVIMENTO	5
2.1	Princípios da criptografia, assinaturas digitais e autenticação do ponto final .	5
2.2	Protegendo o e-mail e conexões TCP:SSL	6
2.2.1	Pretty Good Privacy (PGP)	6
2.2.2	Conexões TCP:SSL	6
2.3	IPsec e redes virtuais privadas	7
2.4	Segurança de LANs sem fio	7
2.4.1	Privacidade Equivalente Cabeada (WEP)	7
2.5	Segurança Operacional	8
3	CONSIDERAÇÕES FINAIS	9
	REFERÊNCIAS	10

1 Introdução

Segurança de rede consistem em principalmente poder se comunicar de forma segura. Com a certeza de que a mensagem enviada será recebida pelo destinatário específico e que não será alterada ou interceptada por outros. Para isso existem quatro pilares que são abordados para chegarmos a este resultado.

- Confidencialidade: Consiste em apenas o remetente e o destinatário poderem entender o conteúdo da mensagem transmitida, impedindo assim que outros consigam interceptar a mensagem.
- Integridade: Ter segurança de que o conteúdo da comunicação não foi alterado seja por acidente ou má intenção.
- Autenticação do ponto final: Ter a certeza da identidade da outra parte envolvida, confirmado que esta é quem alega ser.
- Segurança operacional: Impedir que redes conectadas à Internet Pública sofram ataques e sejam comprometidas.

Caso um ou mais desses pilares sejam comprometidos, um intruso pode ter acesso à rede e monitorar usuários, identificando e gravando as mensagens e os dados daquele canal e modificar, incluir e eliminar mensagens ou conteúdos prejudicando os mesmos usuários.

Para evitar esse tipo de situação é necessário tomar contra-medidas adequadas, que serão abordadas neste trabalho escrito.

2 Desenvolvimento

2.1 PRINCÍPIOS DA CRIPTOGRAFIA, ASSINATURAS DIGITAIS E AUTENTICAÇÃO DO PONTO FINAL

As Técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados, porém pra isso é necessário que o destinatário esteja permitido de recuperar os dados originais (CISCO, 2022). Todos os algoritmos criptográficos envolvem a substituição de um dado por outro, tomando um trecho de um texto aberto, calculando e substituindo esse texto por outro cifrado apropriado criando assim uma mensagem cifrada. Para isso existem duas categorizações para estes algoritmos:

1. Criptografia de chaves simétricas: A criptografia simétrica faz uso de uma única chave, que é compartilhada entre o emissor e o destinatário de um conteúdo. Essa chave é uma cadeia própria de bits, que vai definir a forma como o algoritmo vai cifrar um conteúdo. Essa categoria possue outras duas categorias:
 - Cifras de fluxo: Os bits originais são combinados com uma corrente de bits de cifragem vindos de um gerador de dígitos pseudo-aleatório.
 - Cifras de bloco: A mensagem a ser criptografada é processada em blocos de k bits.
2. Criptografia de chave pública/assimétrica: A criptografia de chave pública usa um par de chaves relacionadas matematicamente. Uma mensagem criptografada com a primeira chave deve ser descriptografada com a segunda chave e uma mensagem criptografada com a segunda chave deve ser descriptografada com a primeira chave.

A criptografia ajuda a manter a integridade da mensagem porém não é o único recurso que proporciona isso, as assinaturas digitais e a autenticação do ponto final são utilizadas para este fim também:

- Funções de hash criptográficas: As funções hash criptográficas são algoritmos matemáticos unilaterais usados para mapear dados de qualquer tamanho para uma sequência de bits de tamanho fixo.
- Código de autenticação da mensagem - MAC: MAC é utilizado para garantir a integridade de mensagens enviadas em um canal inseguro. Uma construção bem difundida é a HMAC, que utiliza funções de resumo para a geração de códigos de autenticação.

- Assinaturas digitais: A assinatura digital é uma criptografia “assinada”. Duas mensagens então são enviadas: uma contendo somente a mensagem cifrada e outra contendo a assinatura, essa assinatura pode ser simétrica ou assimétrica.

Além destes recursos, também temos a autenticação do ponto final que é o processo de provar a identidade de uma entidade a outra entidade por uma rede de computadores. O protocolo de autenticação primeiro estabelece as identidades das partes para a satisfação mútua e após isso é que as entidades “põem as mãos” no trabalho real.

2.2 PROTEGENDO O E-MAIL E CONEXÕES TCP:SSL

Embora a segurança na camada de rede possa oferecer “cobertura total” cifrando todos os dados dos datagramas e autenticando todos os endereços IP destinatários, ela não pode prover segurança no nível do usuário. Para isso utilizamos outros recursos mostrados a seguir.

2.2.1 Pretty Good Privacy (PGP)

Esquema de criptografia para e-mail que se tornou padrão. Criando um par de chaves públicas: a chave pública pode ser colocada no site ou em um servidor de chaves públicas, a chave privada é protegida pelo uso de uma senha. A senha tem de ser informada todas as vezes que o usuário acessar a chave privada.

2.2.2 Conexões TCP:SSL

O SSL é usado para oferecer segurança em transações que ocorrem pelo HTTP. Entretanto, como o SSL protege o TCP, ele pode ser empregado por qualquer aplicação que execute o TCP. O SSL provê uma Interface de Programação de Aplicação (API) com sockets, semelhante à API do TCP. Para isso existem três fases que a versão simplificada do SSL faz para iniciar uma sessão de comunicação:

- Apresentação: Estabelecer uma conexão TCP e verificar identidade. Após isso é gerado um Segredo Mestre e Segredo Mestre Cifrado.
- Derivação de chave: Utilização da MS como chave de sessão simétrica para toda a verificação subsequente de criptografia e integridade de dados.
- Transferência de dados : Envio de dados protegidos por meio da conexão TCP validados por números de sequência.

2.3 IPSEC E REDES VIRTUAIS PRIVADAS

O protocolo IP de segurança, mais conhecido como IPsec, provê segurança na camada de rede que protege os datagramas IP entre quaisquer entidades da camada de rede, incluindo hospedeiros e roteadores. Assim, muitas organizações utilizam o IPsec para criar redes virtuais privadas (VPNs). O objetivo de uma VPN é que seus hospedeiros e servidores consigam enviar dados um ao outro de uma maneira segura e sigilosa. Para isso, o tráfego é criptografado antes de entrar na Internet pública:

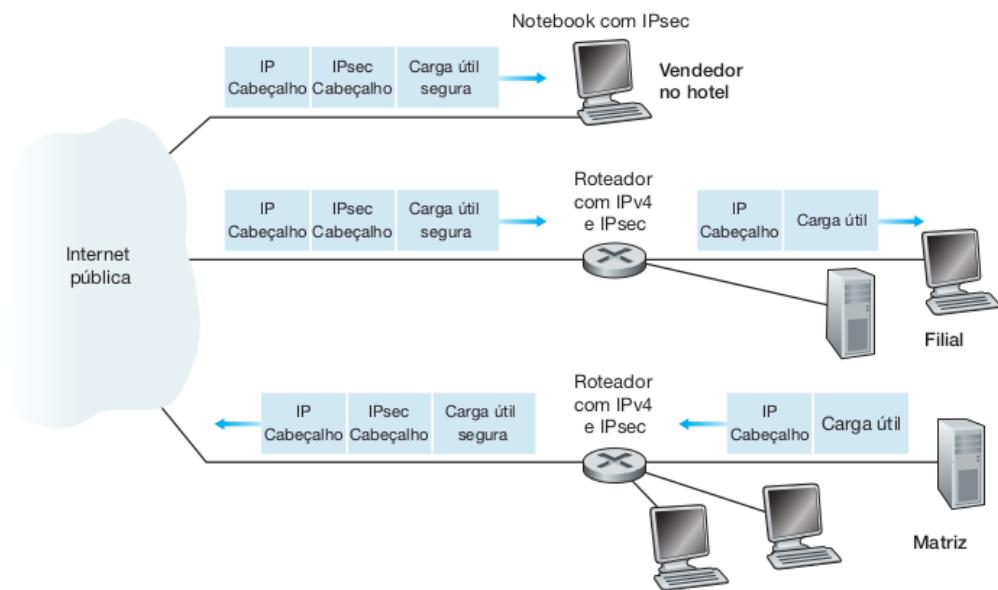


Figura 1 – Rede Virtual Privada (VPN)

Os datagramas IPsec são enviados entre pares de entidades da rede, portanto antes de enviar datagramas IPsec da entidade remetente à destinatária, essas entidades criam uma conexão lógica da camada de rede, denominada associação de segurança (SA). Uma SA é uma conexão lógica simples sendo assim, unidirecional do remetente ao destinatário. Se as duas entidades querem enviar datagramas seguros entre si, então duas SAs necessitam ser estabelecidas.

2.4 SEGURANÇA DE LANS SEM FIO

2.4.1 Privacidade Equivalente Cabeada (WEP)

O protocolo IEEE 802.11 WEP foi criado para fornecer autenticação e criptografia de dados entre um hospedeiro e um ponto de acesso sem fio usando uma técnica de chave compartilhada simétrica (ROSS, 2013), para isso a autenticação é realizada da seguinte forma:

1. Um hospedeiro sem fio requisita uma autenticação por um ponto de acesso.
2. Um ponto de acesso responde ao pedido de autenticação com um valor de nonce de 128 bytes.
3. O hospedeiro sem fio criptografa o nonce usando uma chave simétrica que compartilha com o ponto de acesso.
4. O ponto de acesso decodifica o nonce criptografado do hospedeiro.

Caso o nonce decodificado seja compatível com o valor nonce originalmente enviado ao hospedeiro, então o hospedeiro é autenticado pelo ponto de acesso.

2.5 SEGURANÇA OPERACIONAL

Um firewall é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem enquanto bloqueia outros, o firewall possui 3 principais objetivos; Todo o tráfego de fora para dentro passa por um firewall, somente o tráfego autorizado, como definido pela política de segurança local pode passar e o próprio firewall é imune à penetração. Além disso o firewall pode atuar de três formas:

- Filtros de pacotes tradicionais; Um filtro de pacotes examina 11/18/11, 11/23/11 rossos cada datagrama que está sozinho, determinando se deve passar ou ficar baseado nas regras específicas definidas pelo administrador.
- Filtros de estado; Os filtros de estado rastreiam conexões TCP e usam esse conhecimento para tomar decisões sobre filtragem.
- Gateways de aplicação; Um gateway de aplicação é um servidor específico de aplicação, através do qual todos os dados da aplicação devem passar.

Todavia, para detectar muitos tipos de ataque é necessário realizar uma inspeção mais profunda de pacote, para isso utilizamos os sistemas de detecção de invasão, que são dispositivos que geram alertas quando observa tráfegos potencialmente mal-intencionados (CéSAR, 2020); O sistema de detecção de invasão (IDS) é utilizado para observar tráfegos potencialmente mal-intencionados enquanto que sistema de prevenção de invasão (IP) filtra o tráfego suspeito.

3 Considerações Finais

Com isso podemos observar que atualmente existem diversas ferramentas que possibilitem a comunicação com segurança na internet, entre outras operações que exigem um nível maior de confiabilidade da informação e integridade da mensagem, as quais são primordiais para o funcionamento da internet mundial atual. Sendo assim não apenas a área de segurança é primordial para formação como cientista da computação como também toda a disciplina de Redes de Computadores, que é a base para o entendimento fundamental do funcionamento da internet, das redes de comunicação e sua melhor utilização atual.

Referências

- CISCO. **O que é segurança de rede?** [S.l.]: <https://www.cisco.com>, 2022.
- CéSAR, J. **Segurança de rede.** [S.l.]: <https://www.infosec.com.br/seguranca-de-rede>, 2020.
- ROSS, K. . **Redes de computadores e a internet uma abordagem top-down.** [S.l.]: Pearson, 2013.