Os problemas de segurança das redes podem ser divididos nas seguintes áreas interligadas

* Sigilo: somente usuários autorizados podem ser capazes de entender o conteúdo de mensagens ou de arquivos
* Autenticação: cuida do processo de identificar com quem se está falando antes de se revelar informações sigilosas ou entrar em uma transação comercial
* Integridade e não repudiação: certifica que uma determinada mensagem recebida é realmente legítima, e não algo modificado ou impropriamente criado
* Disponibilidade e controle de acesso: garante que recursos de comunicação possam ser efetivamente utilizados e somente por usuários que tiverem os direitos de acesso apropriados

**Varredura de endereços e de portas:** observa quais endereços respondem a requisições de presença e contata os seus possíveis serviços para ver o que acontece como resposta

**Sniffer de pacotes:** um programa que permite um equipamento conectado a uma rede, receba todos os pacotes que trafegam por ela

**Spoofing de endereço:** trata de através da alteração do software da placa de rede – criar pacotes com endereços IP arbitrários, fazendo parecer que o pacote tenha sido enviado de outro equipamento

**DoS:** tem o objetivo de tornar um equipamento de rede inutilizável criando uma quantidade tão grande de trabalho para a infraestrutura sob ataque, que requisições legitimas não conseguem ser tratadas

**Sigilo**

Para permitir que um remetente disfarce dados de modo que um intruso não consiga obter nenhuma informação desses dados interceptados, utilizam-se técnicas de criptografia

**Texto claro:** mensagem a ser criptografada

**Chave:** parâmetro de uma função para a transformação do texto claro

**Texto cifrado:** saida do processo de criptografia

Utiliza-se **C = Ek1(P)** para denotar que a criptografia do texto claro P, usando a chave K1, gera o texto cifrado C. Da mesma forma, **P = Dk2(C)**representa a descriptografia de C para recuperar-se o texto claro original através da chave K2. A partir daí tem-se que:

**Dk2(Ek1(P)) = P**

**Os algoritmos de criptografia são classificados em função do número de chaves utilizadas, em simétricos e assimétricos. Nos algoritmos simétricos, temos que k1 = k2 e em algoritmos assimétricos k1 != k2**

**Algoritmos de criptografia são públicos! O sigilo é garantido na chave de criptografia e no seu tamanho**

**Des foi um algoritmo muito utilizado pelo setor de informática para o uso em produtos de segurança, criado pela IBM no final da década de 70. Nesse algoritmo o texto claro é criptografado em blocos de 64 bits, produzindo um texto cifrado de 64 bits através de uma função parametrizada por uma chave de 56 bits (mais 8 bits de soma de verificação)**

**No início da década de 80, percebeu-se que a segurança do DES baseado em chaves de 56 bits já estava sendo quebrada. Então a IBM criou uma criptografia tripla, denominado de DES triplo, composto por três estágios de cifras DES ou com duas chaves de 56 bits ou com três chaves de 56 bits**

**Porém, para o uso atual ele já é considerado fraco e possui problemas de velocidade**

Outro conjunto de algoritmos chamados RC4 e RC5, desenvolvidos por Ron Rivest e publicados em 1994, utilizam chaves de tamanho variável (de 128 a 256 bits) em um algoritmo eficiente, proporcionando uma criptografia muito rápida e em alto volume. O uso mais comum é do algoritmo RC4 com chave de 128 bits.

Atualmente, o algoritmo mais robusto e eficaz de chave simétrica é o **Rijndael**,

* Aprovado pelo NIST para ser o novo padrão de criptografia e passou a se chamar AES (Advanced Encryption Standard)
* Publicado em novembro de 2001 pelos pesquisadores belgas Vicent Rijmen e Joan Daemen
* Permite a criptografia de blocos de comprimento de 128 bits e a utilização de chaves de 128, 192 ou 256 bits

Um problema encontrado em algoritmos de criptografia de chaves simétricas é o fato de que as duas partes precisam conhecer a chave e nesse caso, ter que mandar a chave junto para uma requisição no outro lado do mundo não seria algo seguro. Isso porque, uma vez que alguém descobrisse a chave, o sistema acabaria se tornando inútil

Então na década de 70, propôs-se um sistema de criptografia diferente, na qual as chaves de criptografia e descriptografia fossem diferentes assim sendo **Ek1 e Dk2** tais que:

**Dk2(Ek1(P)) = P**

Um grupo de pesquisadores desenvolveu um algoritmo baseado na grande dificuldade de fatoração de números primos muito grandes que satisfaz estes requisitos, conhecido pelas iniciais dos três estudiosos que o criaram: RSA (Rivest, Shamir, Adleman). Este algoritmo usa chaves de pelo menos 1024 bits para manter um bom nível de segurança (ou 2048 bits para garantir uma segurança ainda maior)

* escolher dois números primos extensos, p e q (da ordem de 10150)
* calcular n=pq e z=(p-1)(q - 1)
* escolher um número menor que n e primo em relação a z e chamá-lo de e
* encontrar d de forma que ((ed-1) mod z) = 0

Para criptografar a mensagem P, calcula-se C = Pe mod n. Para descriptografar C, calcula-se P = Cd mod n. É possível provar que as funções de criptografia e de descriptografia são inversas entre si. Para realizar a criptografia, precisa-se de e e n, ao passo que para a descriptografia, são necessários d e n. Portanto, a chave pública k1 consiste no par de números (e, n) e a chave privada k2 consiste no par de números (d, n).

O único problema deste algoritmo é que ele é excessivamente lento para grandes quantidades de dados. Por esta razão, o algoritmo RSA é comumente utilizado para se transmitir de forma segura uma chave secreta, criando-se assim, em seguida, uma sessão segura de chave simétrica sem que tenha sido necessário conhecer previamente a chave secreta de criptografia.

**Autentificação**

Autenticação é uma técnica através da qual um processo confirma que seu parceiro na comunicação é quem ele diz ser, e não um impostor

O **protocolo de autenticação** deve ser utilizado antes que se inicie a comunicação propriamente dita, pois ele é responsável por estabelecer a identidade das partes que irão se comunicar de forma a criar um canal seguro de comunicação

Para uma distribuição segura de chaves de criptografia, é preciso que haja um centro intermediário no qual os interessados em distribuir e obter chaves precisam confiar. Esse centro intermediário costuma ser chamado de cartório virtual

Para os algoritmos de criptografia de chave simétrica o centro intermediário confiável é o **KDC** (uma entidade de rede e de confiança com qual o usuário compartilha a chave) e para algoritmos de criptografia de chave assimétrica o centro intermediário confiável é o **CA** (certifica que uma determinada chave publica pertence a uma determinada entidade)

Fluxo do **KDC**:

* quando o usuário A deseja criar uma sessão segura com um usuário B, ele pede ao KDC, usando a sua chave secreta kA, que crie uma chave de sessão k para ser utilizada entre os usuários A e B;
* o KDC retorna a chave k e uma mensagem, cifrada com a chave kB, contendo a identificação do usuário A e a chave k, de forma que somente o usuário B possa descriptografá-la;
* o usuário A extrai a chave k e encaminha a mensagem cifrada com a chave kB para o usuário B, o qual extrai a chave k e confirma que está se comunicando com o usuário A;
* a partir de então, os usuários A e B podem se comunicar de forma segura através da chave secreta k criada pelo KDC.

Fluxo do **CA**:

O processo segue o seguinte fluxo: quando o usuário A deseja enviar uma mensagem segura ao usuário B, ele pede ao CA que envie a chave pública do usuário B. O CA retorna o certificado digital de B contendo a sua chave pública k1 e, de posse dela, o usuário A pode criptografar a mensagem e enviá-la, estando certo de que apenas o usuário B será capaz de descriptografá-la, já que ele é o único usuário a conhecer a sua chave privada k2. A comunicação entre o usuário A e o CA é feita utilizando-se a chave pública do CA amplamente divulgada.

**O certificado digital, especificado na recomendação ITU X.509 e no padrão IETF RFC 3280, é uma estrutura que contém a chave pública e a informação exclusiva que identifica univocamente o proprietário da chave pública. Exemplos de CA são o Cybertrust e o Verisign.**

**Integridade**

A **assinatura digital** é uma técnica de criptografia que permite identificar quem criou um documento digital, garantir a integridade do seu conteúdo, identificar de quem é um documento digital e/ou comunicar a concordância com relação ao conteúdo de um documento digital

Porém, pelo fato de a criptografia de chave pública ser lenta, não se criptografa o documento digital completo, mas sim um resumo do seu conteúdo, chamado **resumo de mensagem**. Para que estes resumos de mensagem sejam efetivos é importante que sejam os mais aleatórios possíveis e que não permitam reconstituir uma mensagem original a partir do seu resumo

Os algoritmos mais importantes de resumo são MD5 (Message Digest), SHA-1 e SHA-2 (Security Hash Algorithm).

* MD5: produz um resumo de mensagem de 128 bits mas já é vulnerável
* SHA-1: foi desenvolvido a partir do MD5, sendo mais forte e menos vulnerável, produzindo um resumo de mensagem de 160 bits
* SHA-2: inclui mudanças significativas no SHA-1, tornando-o mais forte e não vulnerável e produzindo um resumo de mensagem ainda maior, de 256 ou 512 bits

Para validar a autenticidade do documento, basta comparar se o resumo do texto claro e o resumo descriptografado com a chave publica de quem assinou são iguais

**Controle de acesso**

Um **Fiewall** é uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros

* **Rede externa**: é a internet publica à qual é permitido acessar somente recursos públicos específicos de uma organização que são colocados no segmento **DMZ**
* DMZ: uma parte da rede privada da organização onde estão isolados recursos públicos que podem ser acessados de forma controlada desde a rede externa quanto desde a **rede interna**
* Rede interna: rede privada da organização (LAN) a ser protegida, à qual é permitido acessar qualquer dos demais segmentos de rede