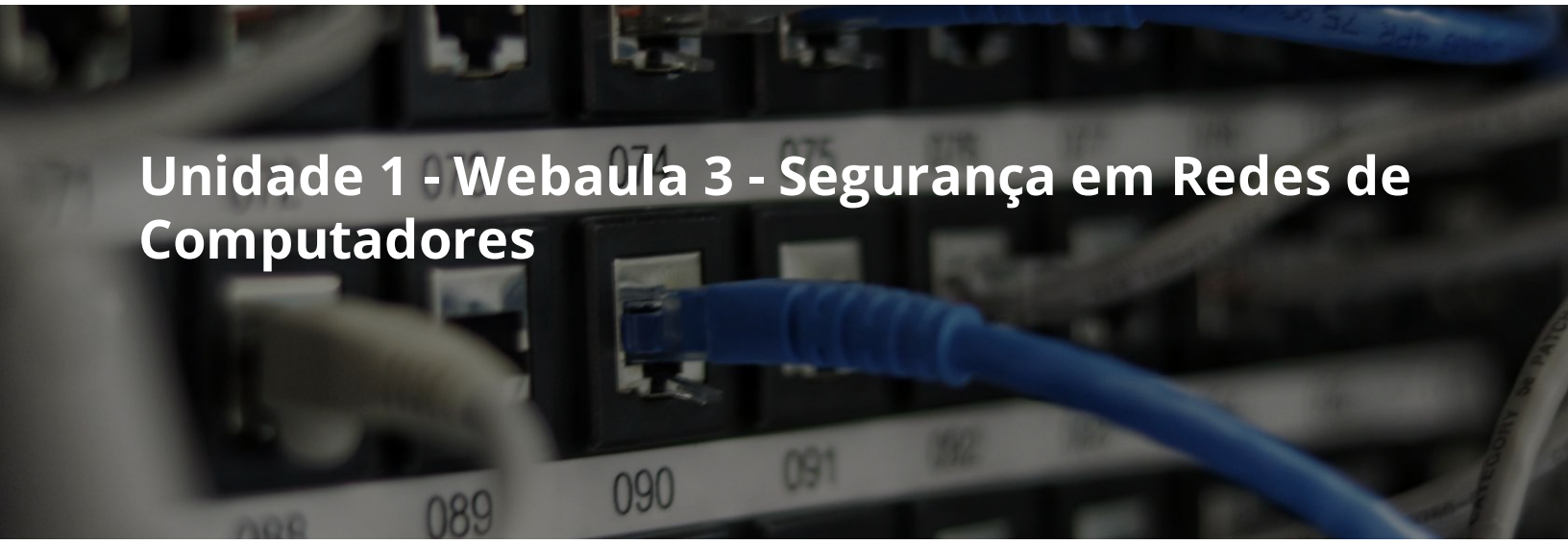


Unidade 1 - Webaula 3 - Segurança em Redes de Computadores

Olá! Tudo bem?

Seja bem-vindo(a) à Webaula 3 de **Redes de Computadores.**

INTRODUÇÃO

- Introdução à Webaula 3

TÓPICO 1

- Sigilo

TÓPICO 2

- Autentificação

TÓPICO 3

- Integridade
- Atividade de Passagem

TÓPICO 4

- Controle de Acesso

Atividade de Passagem

RESUMO

Resumo da Webaula 1

Conclusão da Unidade 1

REFERÊNCIAS

Referências

Créditos

Introdução à Webaula 3

Olá!

A segurança da informação é um assunto abrangente. Em sua forma mais simples, ela se preocupa em garantir que pessoas mal-intencionadas não leiam ou modifiquem mensagens enviadas a outros destinatários. Outra preocupação da segurança se volta para as pessoas que tentam ter acesso a serviços remotos, que elas não estão autorizadas a usar. Ela também permite que se faça a distinção entre uma mensagem supostamente verdadeira e um trote.

Reflita

Você costuma se preocupar com a possibilidade de os dados que disponibiliza na internet sejam um dia acessados por pessoas não autorizadas?

Os problemas de segurança das redes podem ser divididos nas seguintes áreas interligadas (KUROSE; ROSS, 2013):

- **sigilo**: está relacionado à manutenção das informações longe de usuários não autorizados, ou seja, 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, ou seja, é preciso se assegurar da identidade da outra parte com quem se quer trocar informações;

- **integridade e não repudiação**: certifica que uma determinada mensagem recebida é realmente legítima, e não algo modificado ou impropriamente criado, tratando também de assinaturas, ou seja, da garantia de que uma determinada transação foi realmente requisitada naqueles termos;

- **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, ou seja, garante que a comunicação possa ocorrer entre usuários legítimos.

Uma rede de computadores é essencialmente vulnerável a acessos não autorizados, pois permite que qualquer equipamento analise o conteúdo de mensagens que estejam trafegando pela rede mesmo que não sejam direcionadas ao equipamento. Além disso, qualquer equipamento conectado a uma rede pode criar, alterar ou extrair mensagens mascarando a sua operação através de endereços fictícios.

Saiba Mais

Você já sabe que um grave problema de segurança é o vírus de computador. São vários os tipos e eles realmente são uma praga mundial. Milhões de equipamentos são infectados anualmente, o que causa prejuízos gigantescos para empresas e consumidores. Por isso devemos nos proteger usando sempre um programa antivírus e desconfiando de todos os arquivos que recebemos da internet! Assista o vídeo "6 curiosidades, mitos e verdades" e saiba mais sobre problemas de segurança relacionados a vírus.

Você sabia que as redes de computadores possuem vulnerabilidades e não é difícil para um especialista invadi-las? O primeiro passo para invadir uma rede de computadores é saber os endereços das máquinas pertencentes a ela, quais sistemas operacionais elas utilizam e os serviços que estes sistemas estão oferecendo. Uma técnica para se obter estas informações chama-se **varredura de endereços e de portas**, que observa quais endereços respondem a requisições de presença e contata os seus possíveis serviços para ver o que acontece como resposta (SCAMBRAY; MCLURE; KURTZ, 2014).

Um exemplo de intrusão em uma rede é o ***sniffer* de pacotes**. Este programa permite que um equipamento conectado a uma rede, através de uma placa de rede operando em modo promíscuo, receba todos os pacotes que trafegam por ela. Estes pacotes podem então ser passados para programas que tratem de analisá-los.

Outro tipo de intrusão em uma rede de computadores é o ***spoofing* de endereço**. Em uma rede, os equipamentos se identificam necessariamente através do uso de um endereço, o que determina que qualquer pacote que trafegue pela rede é composto de dados e dos endereços dos equipamentos de origem e de destino. O *spoofing* de endereço IP 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.

Por último, um tipo de ataque à segurança de uma rede de computadores é o DoS (*Denial of Service*). O ataque de DoS tem por objetivo tornar um equipamento de rede inutilizável criando uma quantidade tão grande de trabalho para a infraestrutura sob ataque, que requisições legítimas não conseguem ser tratadas. Quando o ataque é feito de maneira coordenada a partir de inúmeros hospedeiros alocados por toda a internet, ele se chama DDoS (*Distributed Denial of Service*), e é particularmente devastador.

Leitura Complementar

Veja mais informações sobre como os ataques DDoS ocorrem aqui.

Nesta aula trataremos das quatro principais áreas relativas à segurança dos dados em redes de computadores: sigilo, autenticação, integridade e controle de acesso, para que você entenda como

essas problemáticas são tratadas e quais técnicas são utilizadas para implementar esses mecanismos de segurança.

CONTINUE

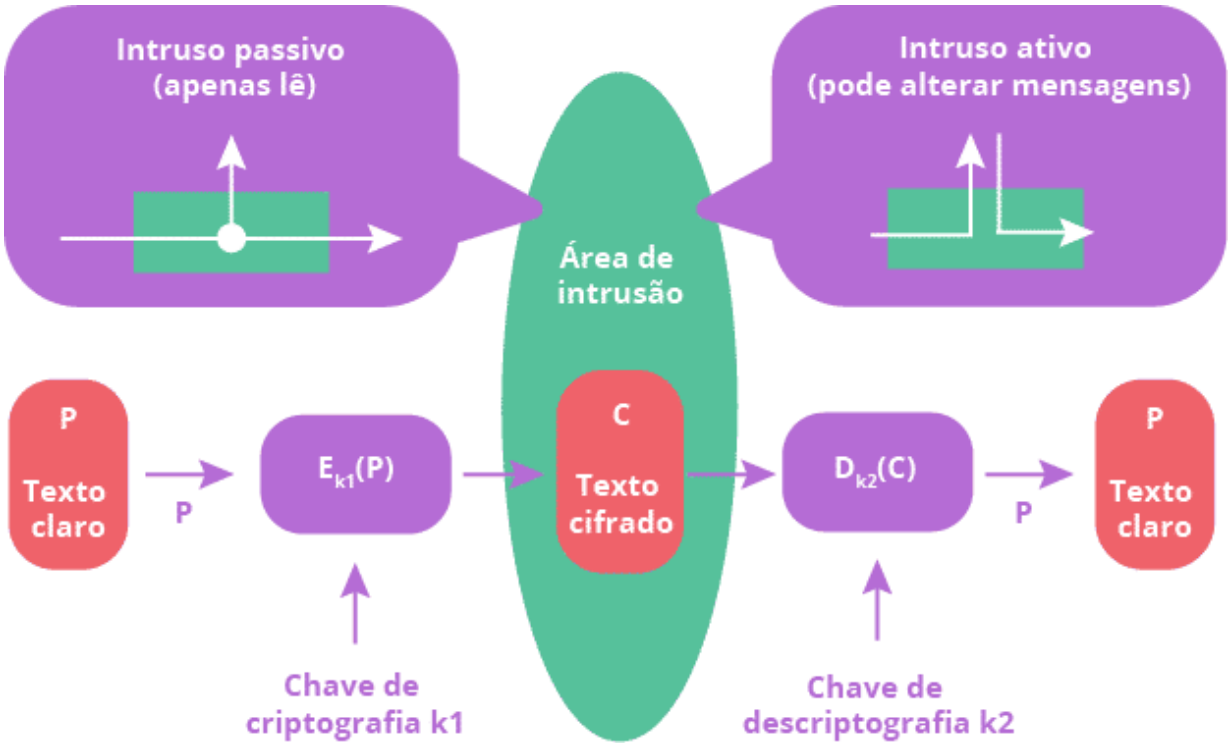
Sigilo

Já que uma rede de computadores é vulnerável, como é que se pode tornar uma comunicação confidencial? 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. Somente o destinatário deve ser capaz de recuperar os dados originais a partir dos dados disfarçados. Este processo garante a confidencialidade dos dados (KUROSE; ROSS, 2013).

1 Criptografia

Na forma tradicional de manter o sigilo de uma comunicação, a mensagem a ser criptografada, conhecida como **texto claro**, é transformada por uma função que é parametrizada por uma **chave**. Em seguida, a saída do processo de criptografia, conhecida como **texto cifrado**, pode ser transmitida para o destinatário. Por fim, o destinatário aplica uma nova função para transformar o texto cifrado no texto claro original através da utilização de uma nova chave. Este processo de transmissão está representado na Figura 1.

Figura 1 - Sigilo de Uma Comunicação pelo Uso da Criptografia



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Usa-se uma notação para estabelecer uma relação entre o texto claro (legível), o texto cifrado e as chaves (BURNETT; PAINE, 2002). 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:

$$D_{k2}(E_{k1}(P)) = P$$

Os algoritmos de criptografia são classificados em função do número de chaves utilizadas, em **simétricos** e **assimétricos**. Nos algoritmos simétricos uma única chave é usada tanto para criptografar quanto para descriptografar (K1 = K2), enquanto nos algoritmos assimétricos uma chave é usada para criptografar, e outra diferente e completamente independente para descriptografar (K1 ≠ K2).

A primeira ideia que vem à nossa cabeça é que uma comunicação segura implica usar um algoritmo de criptografia secreto! Mas não é isso que ocorre, pois hoje os algoritmos de criptografia e descriptografia são públicos, conhecidos, e por isso o sigilo está na chave de criptografia utilizada e no seu tamanho: quanto maior for a chave, mais difícil será descobri-la.

2 Algoritmos de Chave Simétrica

O fato de os algoritmos de criptografia serem públicos não significa que eles devam ser simples. Muito pelo contrário! Hoje em dia o objetivo é tornar o algoritmo de criptografia o mais complexo e emaranhado possível, de tal forma que, através da inclusão de um número de estágios suficientemente grande de chaves de substituição e de transposição, a saída pode ser transformada em uma função excessivamente complicada da entrada.

Um algoritmo que foi muito utilizado pelo setor de informática para uso em produtos de segurança foi criado pela IBM no final da década de 70 e foi denominado **DES** (*Data Encryption Standard*). Neste algoritmo, o texto claro é criptografado em blocos de 64 bits, produzindo 64 bits de texto cifrado, através de uma função parametrizada por uma chave de 56 bits (mais 8 bits de soma de verificação). O algoritmo foi projetado para permitir que a descriptografia fosse feita com a mesma chave da criptografia, só que executando o algoritmo na ordem inversa (BURNETT; PAINE, 2002).

No começo da década de 80, a segurança do padrão DES baseado em chaves de 56 bits já estava sendo quebrada. A IBM percebeu que o tamanho da mensagem DES era muito pequeno e inventou uma forma de aumentá-lo usando a criptografia tripla. O método escolhido, denominado **DES triplo**, é composto por três estágios de cifras DES ou com duas chaves de 56 bits, formando uma chave de 112 bits (mais 16 de soma de verificação), ou com três chaves de 56 bits, formando uma chave de 168 bits (mais 24 bits de soma de verificação).

Entretanto, como o DES triplo é considerado hoje fraco e tem um problema – a velocidade –, você não deve mais utilizá-lo. Para vários aplicativos o desempenho do algoritmo de criptografia é fundamental e por isso novos algoritmos foram propostos.

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**, que, ao ser aprovado pelo NIST (National Institute of Standards and Technology) para ser o novo padrão de criptografia de chave simétrica em substituição dos demais algoritmos, passou a se chamar **AES** (*Advanced Encryption Standard*). Publicado em novembro de 2001 pelos pesquisadores belgas Vincent 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. Este é o algoritmo que hoje todos já estão usando na internet e pelo qual nós também devemos optar, dadas suas características: rapidez, robustez e confiabilidade (KUROSE; ROSS, 2013).

3 Algoritmos de Chave Assimétrica ou Pública

Reflita

Apesar de muito eficientes e seguros, os algoritmos de chave simétrica têm uma característica: as duas partes precisam conhecer a chave de criptografia. Então, ao enviar uma mensagem criptografada para alguém do outro lado do mundo, teríamos que também mandar a chave! Você concorda que não seria possível fazer isso de forma segura?

Historicamente, o problema da distribuição de chaves sempre foi o ponto fraco da maioria dos sistemas de criptografia de chaves simétricas: as duas partes precisam conhecer a **chave secreta** comum. Mesmo sendo robusto, se um intruso pudesse roubar a chave, o sistema acabaria se tornando inútil.

Em meados da década de 70 propôs-se um sistema de criptografia diferente, no qual as chaves de criptografia e de descriptografia fossem diferentes e a chave de descriptografia não pudesse ser derivada da chave de criptografia (BURNETT; PAINE, 2002). O método funcionaria da seguinte forma: uma pessoa, desejando receber mensagens secretas, cria dois algoritmos com chaves diferentes, E_{k1} e D_{k2}, tais que:

$$D_{k2}(E_{k1}(P)) = P$$

Aí, ao se publicarem os algoritmos e a **chave pública** de criptografia **k1**, qualquer pessoa poderia enviar mensagens cifradas de forma que a descriptografia só seria possível de ser executada com o conhecimento da **chave privada** de descriptografia **k2**, não publicada e, portanto, secreta.

Reflita

Você consegue imaginar a complexidade matemática envolvida na criação de um algoritmo de criptografia que criptografa com uma chave e descriptografa apenas com outra completamente diferente?

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) (KUROSE; ROSS, 2013).

Para se utilizar o algoritmo com uma chave de 1024 bits, seguem-se os seguintes passos:

- escolher dois números primos extensos, **p** e **q** (da ordem de 10^{150})

- 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 = P^e **mod n**. Para descriptografar **C**, calcula-se **P** = C^d **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.

CONTINUE

Autentificação

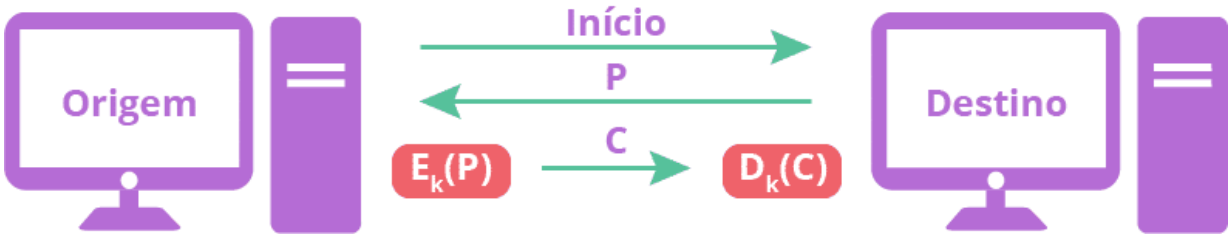
Sempre que acessamos algum conteúdo na internet podemos nos deparar com o seguinte questionamento: será que aquela página é realmente de quem diz ser ou é uma cópia em um servidor de alguém mal-intencionado? Pois este é o propósito da autenticação: uma técnica através da qual um processo confirma que seu parceiro na comunicação é quem ele diz ser, e não um impostor. Confirmar a identidade de um processo remoto através de uma rede de computadores, face à presença de um intruso ativo mal-intencionado, é surpreendentemente difícil e exige protocolos baseados no uso da criptografia (KUROSE; ROSS, 2013).

A autenticação é efetuada através da troca de mensagens constituintes de um **protocolo de autenticação**. Esse 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.

O protocolo de autenticação se baseia no pressuposto de que somente as duas partes interessadas em estabelecer o canal de comunicação conhecem uma chave de criptografia.

Uma vez que se inicia o protocolo de autenticação a partir de um pedido desde um processo de origem, o processo de destino envia ao processo de origem uma informação que nunca tenha sido utilizada (um contador de acessos, por exemplo). O processo de origem criptografa a informação com a chave secreta **k** e a envia ao processo de destino, e este a descriptografa com a chave secreta **k** e compara se o resultado é idêntico à informação enviada. Como somente os dois processos conhecem a chave secreta **k** de criptografia, pode-se garantir que as suas identidades são autênticas. Este processo está representado na Figura 2.

Figura 2 - Processo de Autenticação



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Mas aqui existe um problema complicado inerente ao protocolo de autenticação: como distribuir de forma segura as chaves utilizadas no processo?

1 Distribuição de Chaves e Certificação

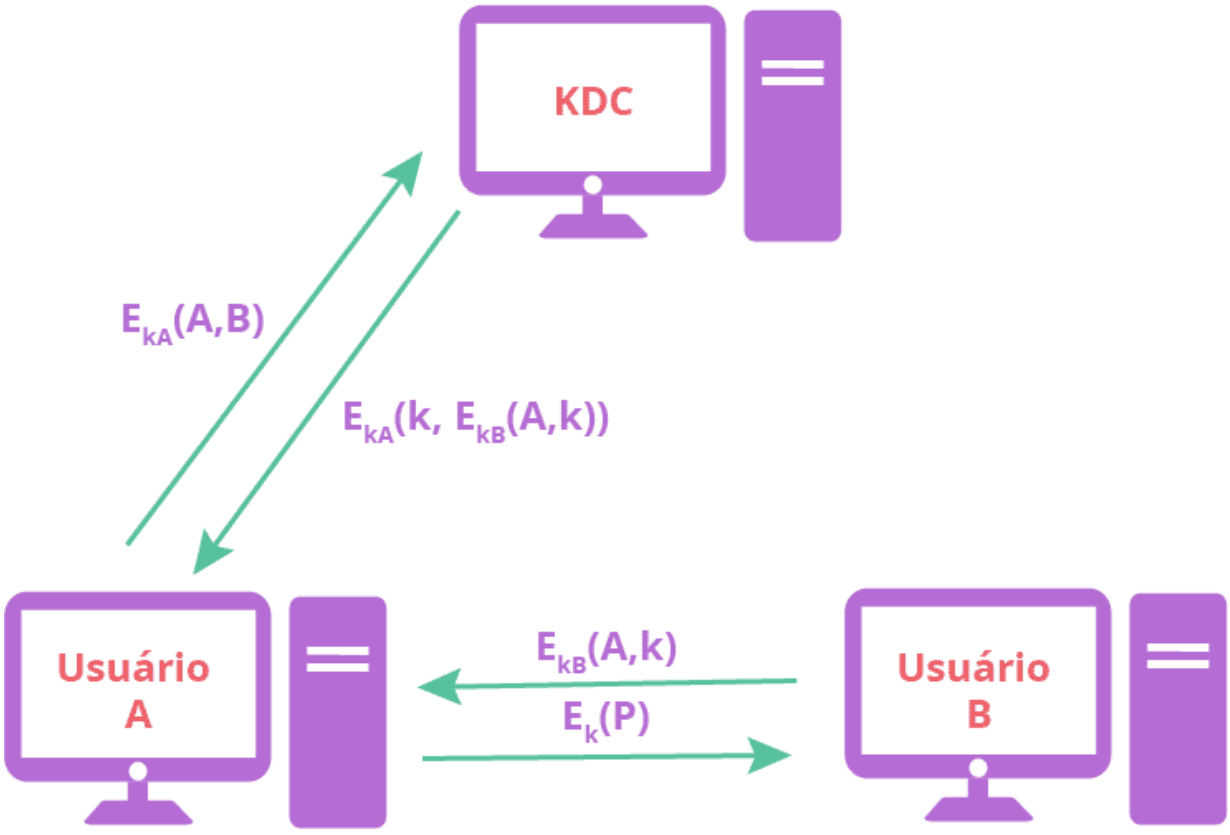
Para uma distribuição segura de chaves de criptografia, é preciso que haja um centro intermediário no qual os interessados em distribuir e obter chaves precisam confiar. Quer dizer então que só é possível transmitir de forma segura uma chave simétrica para o destinatário se houver um intermediário de confiança que me auxilie? Sim, e este centro intermediário faz o papel de um cartório e costuma ser chamado de cartório virtual (KUROSE; ROSS, 2013).

No caso da distribuição da chave com base no algoritmo de criptografia de chave simétrica, o centro intermediário confiável é o **KDC** (*Key Distribution Center*), uma entidade de rede única e de confiança com a qual o usuário compartilha uma chave secreta. No caso da distribuição da chave pública com base no algoritmo de criptografia de chave assimétrica, o centro intermediário confiável é o **CA** (*Certification Authority*), que certifica que uma chave pública pertence a uma determinada entidade (BURNETT; PAINE, 2002).

O KDC é um servidor que compartilha uma chave secreta com cada um dos usuários registrados nele. Portanto, cada usuário pode se comunicar de forma segura com o KDC através desta chave. Um exemplo de KDC é o Kerberos, desenvolvido pelo MIT (Massachusetts Institute of Technology).

A ideia básica do uso de um KDC para viabilizar uma comunicação segura entre dois de seus usuários é ele criar e enviar para cada um dos usuários uma chave secreta a ser compartilhada e utilizada para uma sessão de comunicação. Como cada um desses usuários compartilha com o KDC uma chave secreta, eles se comunicam com o KDC através de um canal seguro. O processo está representado na Figura 3.

Figura 3 - Comunicação Sigilosa Através de um KDC



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

O processo segue o seguinte fluxo:

- 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.

Por outro lado, o CA é um servidor que disponibiliza de forma confiável a chave pública de cada um dos usuários registrados nele na forma de um **certificado digital**. 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.

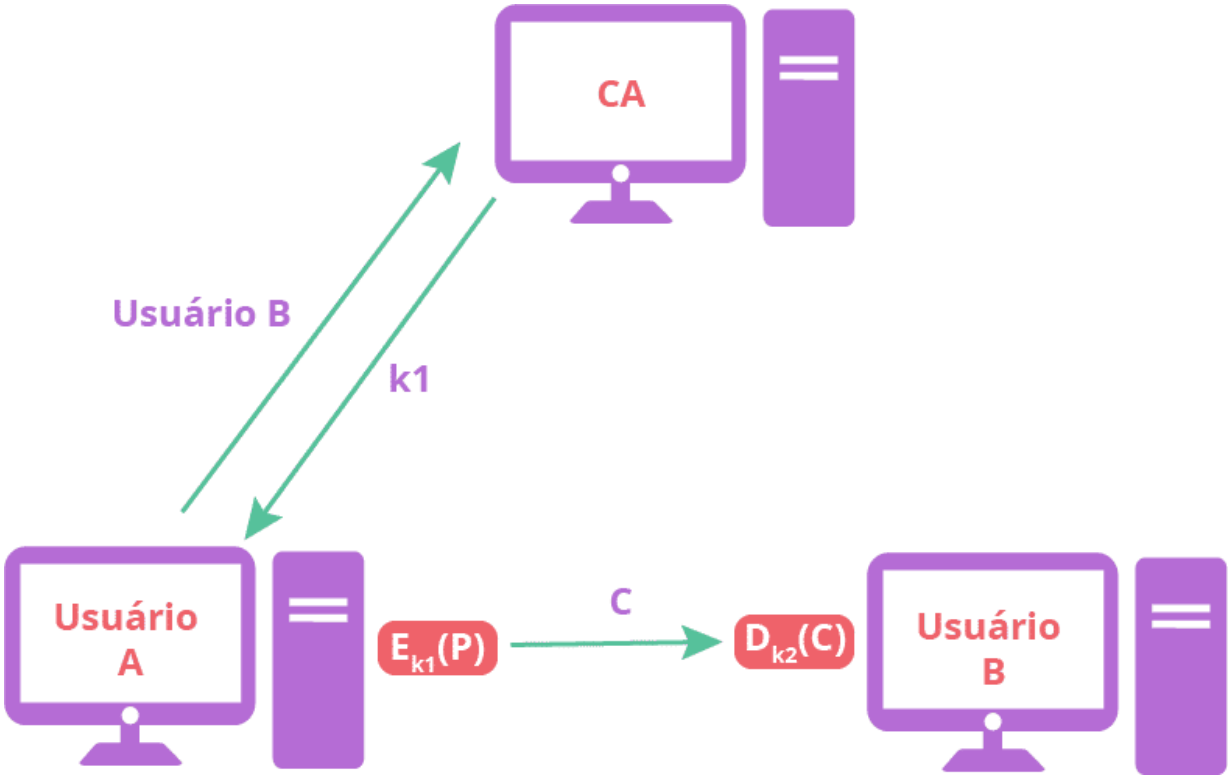
Os certificados digitais podem ser utilizados para autenticar um CA, criando desta forma uma árvore hierárquica de certificação de chaves públicas, identificada pelo nome geral **PKI** (*Public Key Infrastructure*). Assim, o CA de nível superior, chamado de CA raiz, certifica todos os CAs abaixo dele recursivamente. Esta cadeia de certificados que vai do certificado digital do proprietário da chave pública até o certificado digital raiz chama-se caminho de certificação.

Saiba Mais

Observe no site de um CA exemplo os tipos de certificados comercializados e os seus respectivos valores.

O processo de utilização de um CA está representado esquematicamente na Figura 4.

Figura 4 - Comunicação Sigilosa Através do Uso de um CA



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

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.

Mas como é que se fica sabendo que houve um processo de autenticação válido ao se acessar algum recurso da internet? Se for apresentado um certificado digital de um centro intermediário confiável, posso ter certeza de que aquele conteúdo pertence a quem o certificado diz pertencer. Por exemplo, ao se navegar pela internet através de um navegador, sempre que a barra de endereços ficar verde, significa que houve uma identificação válida de um certificado digital que pode ser apresentado.

CONTINUE

Integridade

Outra funcionalidade que temos utilizado cada vez mais é a chamada assinatura digital, que trata da integridade e autenticidade de documentos que são determinadas pela presença de uma assinatura autorizada. 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 (KUROSE; ROSS, 2013).

O problema de se criar um substituto para as assinaturas escritas à mão não é trivial. Basicamente, necessita-se de um sistema através do qual uma parte possa enviar uma mensagem "assinada" para outra parte, de forma que:

- o receptor possa verificar inequivocamente a identidade alegada pelo transmissor;
- o transmissor não possa posteriormente repudiar o conteúdo da mensagem;
- o receptor não possa inventar uma mensagem (não enviada pelo transmissor).

A solução se baseia na utilização de algoritmos de chaves públicas. Para alguém assinar digitalmente um documento, basta criptografá-lo usando sua chave privada. Como somente esta pessoa deve conhecer a sua chave privada e como o conteúdo do documento pode ser conhecido bastando para isso ter a chave pública de quem o assinou, as condições listadas acima são satisfeitas.

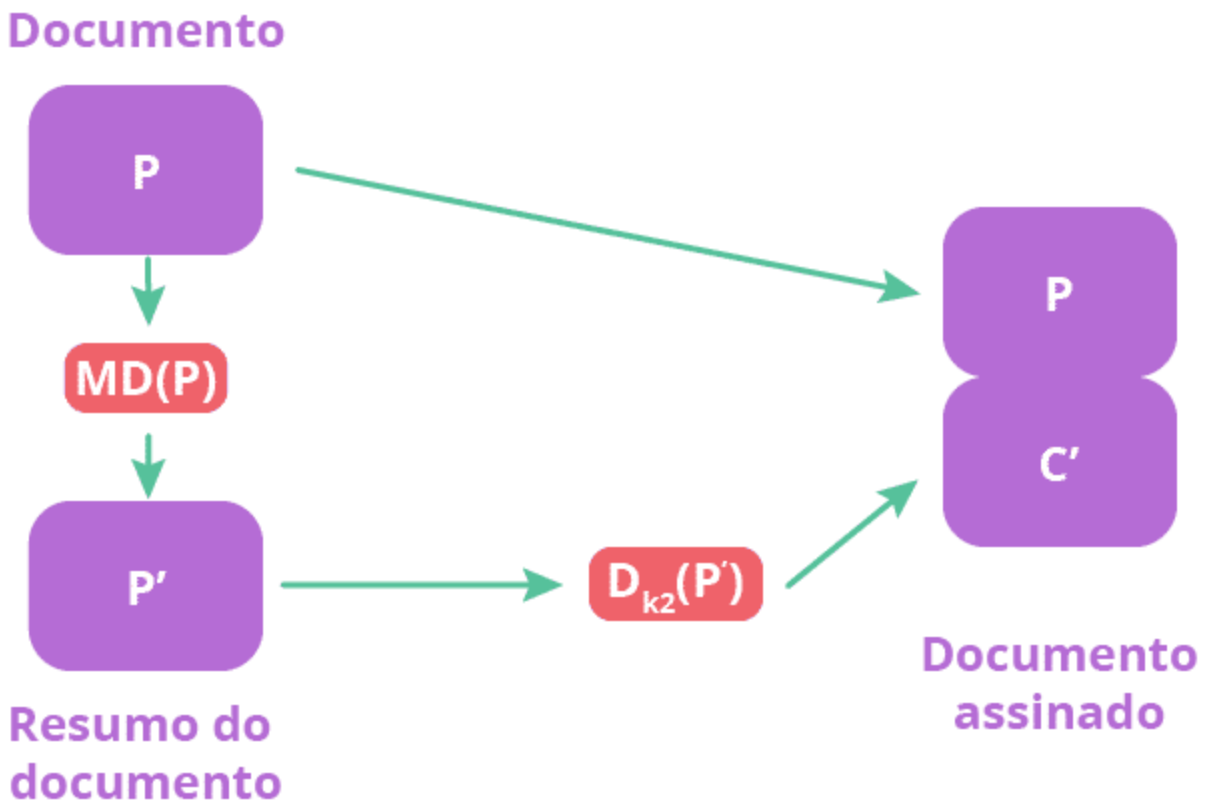
Porém, pelo fato de a criptografia de chave pública ser lenta, não se criptografa o documento digital completo, mas sim um resumo do seu conteúdo, chamado **resumo de mensagem**. Para que estes

resumos de mensagem sejam efetivos é importante que sejam os mais aleatórios possíveis (mesmo para mensagens muito semelhantes, o resumo de mensagem deve ser completamente diferente) e que não permitam reconstituir uma mensagem original a partir do seu resumo (BURNETT; PAINE, 2002).

Os algoritmos mais importantes de resumo são **MD5** (*Message Digest*), **SHA-1** e **SHA-2** (*Security Hash Algorithm*). O algoritmo MD5 produz um resumo de mensagem de 128 bits, mas já é vulnerável. O SHA-1 foi desenvolvido a partir do MD5, sendo muito mais forte e menos vulnerável, e produzindo um resumo de mensagem maior, de 160 bits. O SHA-2 inclui mudanças significativas no SHA-1, tornando-o ainda mais forte e não vulnerável e produzindo um resumo de mensagem ainda maior, de 256 ou 512 bits.

A Figura 5 representa graficamente o processo de assinatura digital de um documento legível (texto claro). O documento assinado é o texto claro com o resumo do texto claro cifrado com a chave privada de quem estiver assinando o documento.

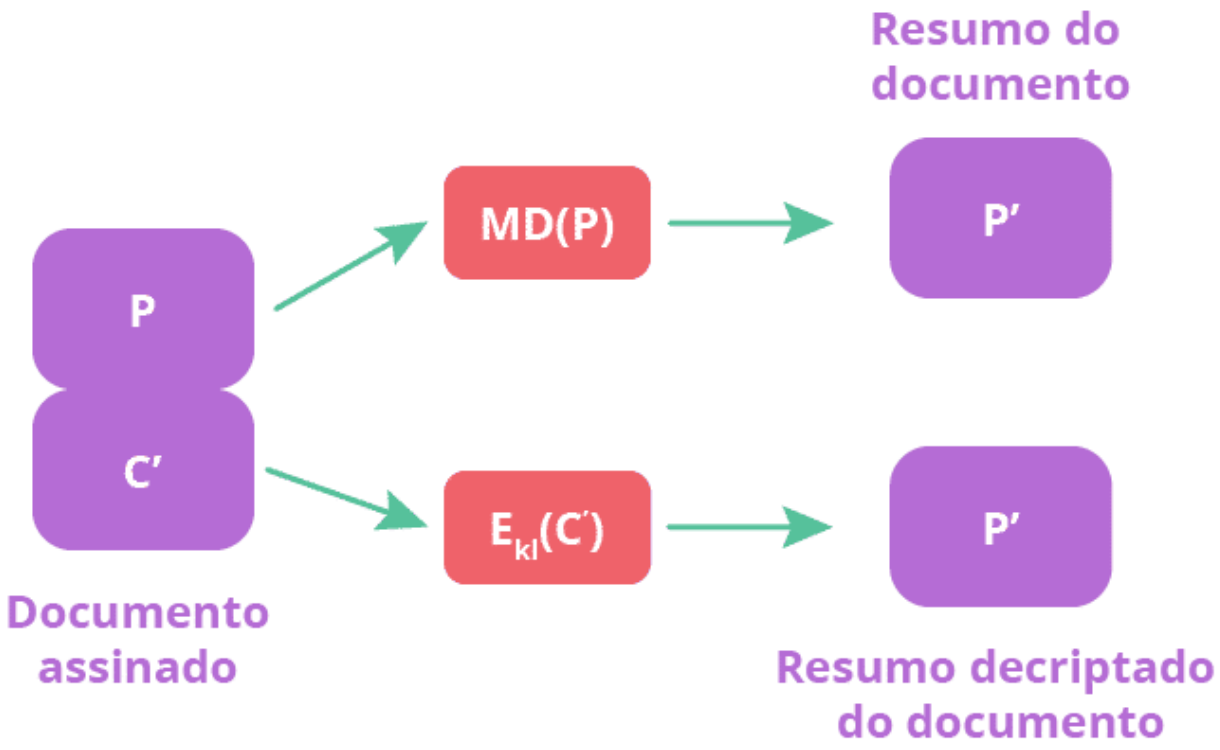
Figura 5 - Assinatura Digital



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

E como é que se faz para verificar se o documento contém uma assinatura digital válida, ou seja, para verificar a integridade e a autenticidade do documento? Basta comparar se o resumo do texto claro e o resumo descriptografado com a chave pública de quem assinou o documento são iguais, conforme representado na Figura 6.

Figura 6 - Verificação da Assinatura Digital



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB (2023).

Com esse procedimento de assinar um documento digitalmente e posteriormente poder verificar sua integridade e autenticidade é que conseguimos transferir para a internet uma funcionalidade fundamental hoje: a garantia de que um determinado conteúdo tem um autor e é autêntico. Essa é a técnica utilizada atualmente no e-CPF/e-CNPJ, nas notas fiscais eletrônicas, nos arquivos assinados etc.

CONTINUE

Atividade de Passagem

(ENADE) Um arquivo confidencial precisa ser enviado de uma empresa A para uma empresa B por meio da Internet. Existe uma preocupação com a possibilidade de interceptação e alteração do documento durante a sua transmissão. Para reduzir a possibilidade de que um hacker tenha acesso ao conteúdo da mensagem, foi adotado um procedimento de criptografia de chave pública e assinatura digital. Considerando a utilização dessas tecnologias para a codificação dos dados, avalie as afirmações que se seguem.

I. Para o procedimento de cifragem do documento, é utilizada a chave pública do destinatário.

II. Para o procedimento de assinatura digital do documento, é utilizada a chave pública do destinatário.

III. Para o procedimento de decifragem do documento, é utilizada a chave privada do remetente.

IV. Para o procedimento de verificação da assinatura digital do documento, é utilizada a chave pública do remetente.

- ◯ I.

- ◯ II.
- ◯ I e IV.
- ◯ II e III.
- ◯ III e IV.

SUBMIT

(ENADE) As transações eletrônicas na Internet precisam de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade das informações. Com relação a esse contexto, avalie as afirmações a seguir.

I. Criptografia assimétrica é um método em que é utilizado um par de chaves: uma pública e uma privada.

II. Certificado digital é um documento eletrônico assinado digitalmente que permite associar uma pessoa ou entidade a uma chave pública.

III. Assinatura digital é um método de autenticação de informação digital tipicamente tratado como análogo à assinatura física em papel.

IV. VPN (Virtual Private Network) é um dispositivo de uma rede de computadores por meio do qual se aplica uma política de segurança a determinado ponto da rede.

É correto apenas o que se afirma em:

- ◯ I e II.
- ◯ I e IV.
- ◯ III e IV.
- ◯ I, II e III.
- ◯ II, III e IV.

SUBMIT

(ENADE) A criptografia de ponta a ponta do WhatsApp garante que somente você e a pessoa com quem você está se comunicando podem ler o que é enviado. Ninguém mais terá acesso a elas, nem mesmo o WhatsApp. As suas

mensagens estão seguras com cadeados e somente você e a pessoa que as recebe possuem as chaves especiais necessárias para abri-los e ler as mensagens. E, para uma proteção ainda maior, cada mensagem que você envia tem um cadeado e uma chave únicos. Com base no texto acima e considerando os conceitos de segurança e criptografia, avalie as afirmações a seguir

I. Se um par de chaves é gerado durante a instalação do aplicativo e a chave pública do usuário é armazenada no servidor, é possível verificar a autenticidade de uma mensagem recebida usando a chave pública do remetente obtida do servidor.

II. A estratégia de utilizar um vetor de inicialização (IV) variável para compor chaves criptográficas diferentes para cada mensagem enviada oculta padrões de dados, além de dificultar os chamados ataques de reprodução.

III. O uso do algoritmo AES nas comunicações entre dois usuários indica o emprego de criptografia simétrica, isto é, aquela que utiliza um par de chaves, uma usada pelo remetente, para encriptar a mensagem, e outra para o destinatário decriptá-la.

IV. A presença do algoritmo SHA-256, no protocolo de comunicação entre cliente e servidor, sugere a verificação de integridade das mensagens, visto que é possível detectar se ocorreu alguma modificação comparando-se os valores de hash da mensagem enviada e recebida.

É correto apenas o que se afirma em:

- ◯ I e IV.
- ◯ II e III.

III e IV.

I, II e III.

I, II e IV.

SUBMIT

CONTINUE

Controle de Acesso

A segurança em relação às informações acessíveis pelas LANs de empresas ou organizações é uma preocupação para os administradores de redes. A forma mais comum de evitar o acesso às LANs por pessoas não autorizadas é através do seu isolamento, utilizando-se os ***Firewalls***. 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 e bloqueando outros. Um Firewall permite que um administrador de rede controle o acesso entre o mundo externo e os recursos da rede que administra, gerenciando o fluxo de tráfego de e para esses recursos (KUROSE; ROSS, 2013).

Observe que a Figura 7 representa a localização de um *Firewall* como o elemento responsável pela interconexão dos três principais tipos de segmentos de rede, apresentando a forma como é controlado o fluxo de informações que pode ou não trafegar por ele:

(Clique nas abas para acessar os conteúdos)

REDE EXTERNA	DMZ (DEMILITARIZED ZONE)	REDE INTERNA

Geralmente é a internet pública à qual é permitido acessar somente recursos públicos específicos de uma organização que são colocados no segmento DMZ;

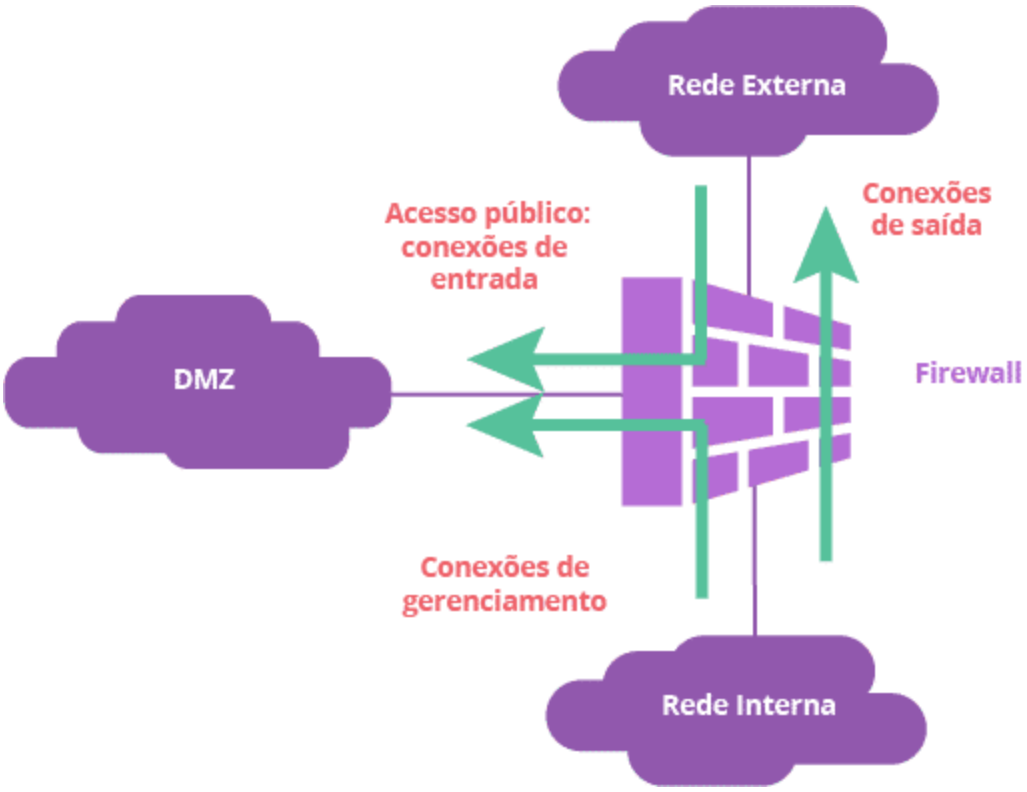
REDE EXTERNA	DMZ (DEMILITARIZED ZONE)	REDE INTERNA

É uma parte da rede privada da organização onde estão isolados recursos públicos que podem ser acessados de forma controlada, tanto desde a rede externa quanto desde a rede interna;

REDE EXTERNA	DMZ (DEMILITARIZED ZONE)	REDE INTERNA

É a rede privada da organização (LAN) a ser protegida, à qual é permitido acessar qualquer dos demais segmentos de rede.

Figura 7 - *Firewall* e os Segmentos de Rede Interconectados

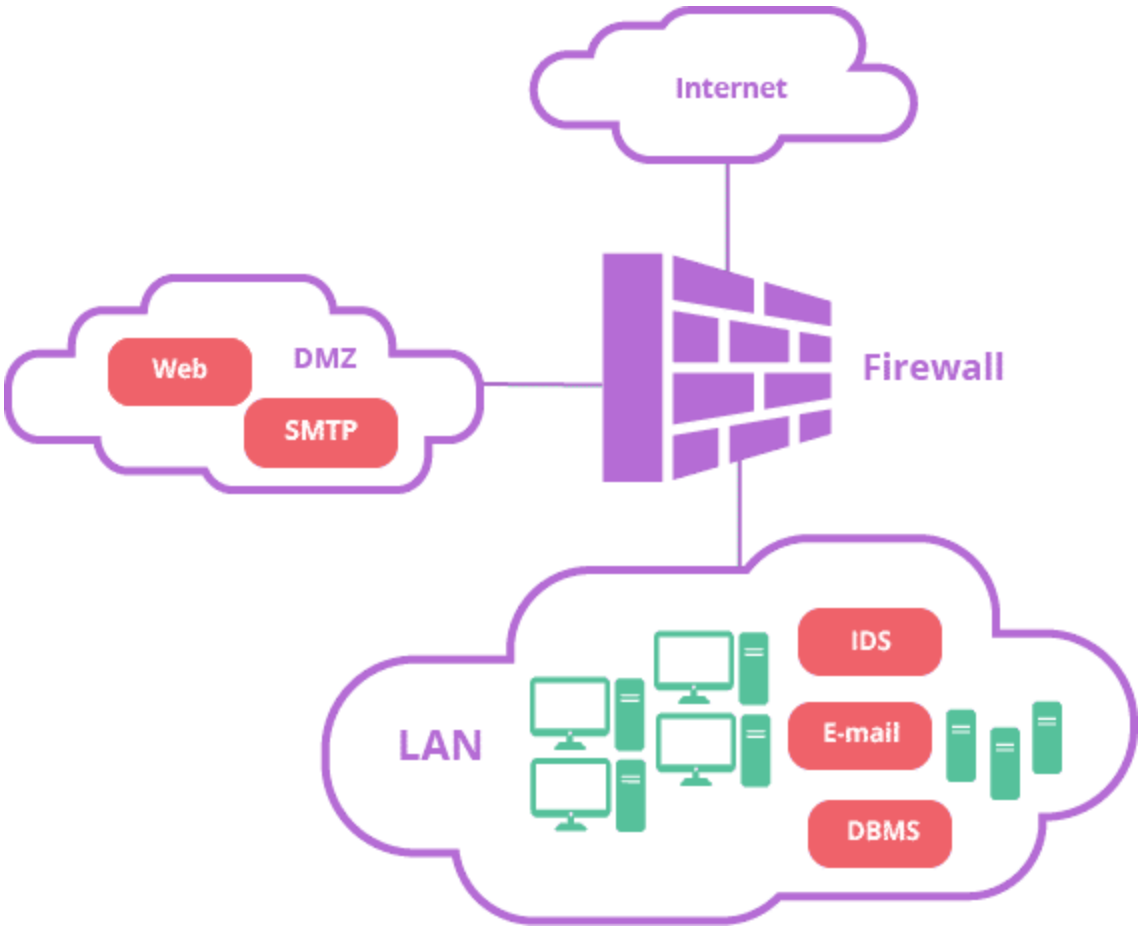


Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB. (2023).

Para isolar as LANs de uma empresa ou organização através de um Firewall, é necessário que, independentemente da forma como elas estejam interconectadas, todo o tráfego de entrada e de saída da empresa ou organização seja feito exclusivamente através dele (FORRISTAL; TRAXLER, 2002).

Um exemplo de topologia de uma rede segura está representado na Figura 8. Neste exemplo, os serviços de servidor de internet e de encaminhamento de correio eletrônico – dois serviços disponibilizados para acesso desde a internet – foram colocados no segmento de rede DMZ. Todos os demais servidores utilizados exclusivamente pela empresa ou organização estão localizados na LAN e isolados em relação à internet de acordo com as regras definidas pela sua política de segurança.

Figura 8 - Topologia Básica de uma Rede Segura



Fonte: Elaboração própria (2022).
Arte/Diagramação: DME/FURB. (2023)

No exemplo de topologia de rede da Figura 8 foi incluído um serviço adicional de segurança na LAN: um **IDS** (*Intrusion Detection System*). O IDS é um software que tem como objetivo monitorar um equipamento ou um segmento de rede, visando detectar atividades suspeitas ou mal-intencionadas em serviços ou arquivos disponibilizados na rede (FORRISTAL; TRAXLER, 2002).

Um IDS é basicamente um sistema passivo de monitoramento e análise do comportamento de usuários da rede a partir do fluxo de dados que trafega por ela. Em função disso é necessário que o administrador da rede acompanhe periodicamente os relatórios do IDS e então atue efetivamente sobre os recursos da rede, buscando bloquear essas atividades suspeitas e sanar eventuais vulnerabilidades.

CONTINUE

Atividade de Passagem

(ENADE) Ao se realizar o acesso a um servidor WWW usando o protocolo HTTPS, uma sessão SSL é estabelecida sobre a conexão TCP, entre o programa navegador do usuário e o processo servidor. Para tanto, usam-se mecanismos baseados em criptografia simétrica e assimétrica para prover serviços de segurança. Em relação ao acesso HTTPS, que serviços de segurança são providos para o usuário?

- ◯ autenticação do servidor e controle de acesso do cliente
- ◯ autenticação do cliente e controle da velocidade de transmissão
- ◯ autenticação da rede e proteção contra vírus
- ◯ autenticação do servidor e confidencialidade das transmissões

autenticação do cliente e temporização das ações executadas

SUBMIT

(ENADE) Um provedor de serviços de segurança de redes e sistemas distribuídos enumerou três componentes de rede essenciais para a garantia da segurança dos dados corporativos: firewall de rede; sistemas de prevenção e detecção de intrusão; e gateways antivírus. Acerca desses componentes de rede, assinale a opção correta.

Os gateways antivírus trabalham no nível da camada de rede e verificam o fluxo de dados em busca de assinaturas de vírus conhecidas

O *firewall* de rede deve ser configurado para detectar transferência de informação através de um canal camuflado (covert channel) baseado em túneis

Um *firewall* de camada de rede (network layer firewall) permite uma filtragem mais detalhada dos dados que

um *firewall* de camada de aplicação (application layer firewall) ao custo de um pior desempenho

Os sistemas de prevenção de intrusão são vistos como uma extensão do firewall e são capazes de detectar anomalias de tráfego ou conteúdo malicioso antes que eles alcancem a rede

O sistema de detecção de intrusão é capaz de identificar ataques iniciados dentro da rede protegida e agir proativamente para neutralizar a ameaça

SUBMIT

CONTINUE

Resumo da Webaula 1

Nessa aula você viu que a problemática de segurança em relação à transmissão de dados ao longo das redes de computadores está dividida em quatro problemas: o sigilo ou a confidencialidade; a autenticação; a integridade e a não repudiação; a disponibilidade e o controle de acesso.

Foram apresentados também os principais algoritmos de criptografia utilizados atualmente: o baseado em chaves simétricas e o baseado em chaves públicas ou assimétricas. As diferentes formas com que esses algoritmos e suas diferentes implementações são utilizados é que permite que se implemente diferentes formas de segurança nas redes de computadores.

Porém é importante ter ciência de que não basta apenas implantar esses mecanismos de segurança, é preciso que os usuários sejam treinados para que se comportem de forma prudente ao lidar com dados sigilosos nas redes de computadores.

CONTINUE

Conclusão da Unidade 1

Nesta Unidade apresentamos para você vários conceitos e termos importantes para o desenvolvimento do estudo de redes de computadores, tanto em relação a aspectos relativos à topologia física quanto à lógica.

Uma definição muito importante para o estudo das próximas Unidades é o das camadas de rede, tanto do modelo de referência especificado pela OSI, com suas sete camadas, quanto do modelo proposto para a arquitetura TCP/IP, com suas cinco camadas.

Outro aspecto importante abordado nesta Unidade trata da história da criação e implantação da rede que hoje chamamos de internet, tanto no contexto mundial quanto aqui no Brasil.

Por fim, foram apresentados também vários conceitos importantes da área de segurança da informação cujas técnicas são atualmente utilizadas para garantir o sigilo, a autenticação, a integridade e o controle do acesso aos dados transmitidos ao longo das redes de computadores.

CONTINUE

Referências

A introdução às redes de computadores e uma referência básica às tecnologias citadas nessa aula podem ser encontradas em:

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

Tópicos aprofundados sobre métodos de segurança em redes de computadores são apresentados em:

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança**: o guia oficial RSA. Rio de Janeiro: Campus, 2002.

FORRISTAL, Jeff; TRAXLER, Julie. **Site seguro**: aplicações web. Rio de Janeiro: Alta Books, 2002.

SCAMBRAY, Joel; MCLURE, Stuart; KURTZ, George. **Hackers expostos**. 7. ed. São Paulo: Makron Books, 2014.

As normas referenciadas nessa aula podem ser obtidas diretamente da página da internet dos respectivos organismos de padronização:

- **IEEE**: ieeexplore.ieee.org/Xplore/guesthome.jsp
- **IETF**: www.rfc-editor.org/rfc-index.html

- **ISO**: www.iso.org/standards-catalogue/browse-by-ics.html
- **ITU-T**: www.itu.int/pub/T-REC

CONTINUE

Créditos

Reitora

Profª. Ma. Marcia Cristina Sardá Espindola

Vice-Reitor

Prof. Dr. Marcus Vinicius Marques de Moraes

Pró-Reitor de Ensino de Graduação, Ensino Médio e Profissionalizante

Prof. Dr. Romeu Hausmann

Pró-Reitor de Administração

Prof. Me. Jamis Antônio Piazza

Pró-Reitora de Pesquisa, Pós-Graduação, Extensão e Cultura

Profª. Drª. Michele Debiasi Alberton

Divisão de Modalidades de Ensino Chefia da Divisão

Profª. Drª. Clarissa Josgrilberg Pereira

Professores Autores

Prof. Me. Francisco Adell Péricas

Design Instrucional

Profª. Drª. Clarissa Josgrilberg Pereira

Prof. Dr. Maiko Rafael Spiess

Prof. Me. Francisco Adell Péricas

Marcia Luci da Costa

Me. Wilson Guilherme Lobe Junior

Revisão Textual

Me. Wilson Guilherme Lobe Junior

Laura Cristina Zorzo

Roteirização

Laura Cristina Zorzo

Produção de Mídia

Gerson Luís de Souza

Gustavo Bruch Féo

Equipe de Design Gráfico

Amanda Kannenberg

Camylle Sophia Teske

Laura Cristina Zorzo

Nicolle Sassella

Renan Diogo Depiné Fiamoncini

Diagramado por Amanda Kannenberg em 06 de Fevereiro de 2023

CONTINUE