SOFTWARES E EQUIPAMENTOS PARA DIMINUIÇÃO DOS RISCOS

Segurança física

Estar conectado à internet nos expõe a diversos riscos, como roubo de informações e de identidade, adulteração de informações etc. De acordo com a norma ABNT 27001:2013, para minimizar os riscos dessa conexão, é necessário implementar mecanismos de controle a fim de garantir a segurança dela.

Esses mecanismos podem ser divididos em dois tipos:

Mecanismos de controle físicos

Evitam ou dificultam as falhas nos equipamentos e instalações.

Mecanismos de controle lógicos

Evitam ou dificultam as falhas relacionadas aos softwares utilizados.

Vejamos agora a aplicação desses mecanismos na manutenção da segurança de uma conexão.

Segurança física abrange todo ambiente em que os sistemas de informação estão instalados. Seu objetivo principal é garantir que nenhum dano físico ocorra nos equipamentos. Por exemplo: roubo de equipamentos, incêndio, inundação e qualquer ameaça às instalações físicas.

A norma ABNT NBR ISO/IEC 27002:2013 divide a segurança física em dois itens principais:

- **Áreas seguras**: Previnem o acesso físico não autorizado, os danos e as interferências em instalações e informações da organização.
- **Equipamentos**: Impedem perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

A segurança física envolve outras áreas da Engenharia, como a civil e a elétrica, ao permitir a projeção de prédios com paredes adequadas à proteção dos equipamentos, sistemas de para-raios, aterramento, limpeza da área para evitar incêndios etc.

Alguns exemplos de **mecanismos de controle físicos** podem ser encontrados no emprego de:

1. Sistemas de refrigeração e de combate a incêndio

Projetados para os equipamentos poderem operar em condições adequadas de temperatura e umidade. Ainda garantem que os casos de incêndio possam ser combatidos o mais rápido possível.

2. Sala-cofre

Espaço construído com paredes corta-fogo, sistemas de refrigeração e de forma hermética para proteger equipamentos críticos de TI.

3. Sistemas de energia redundantes

Funcionam como *no-breaks* (*Uninterruptable Power Supply* - UPS) e geradores. Ambos são necessários ao permitirem que, em caso de queda de energia, os equipamentos permaneçam em operação. Isso garante tanto o fornecimento constante de energia quanto a manutenção dela dentro da tensão recomendada.

4. Preparação do ambiente contra alagamento

No caso de chuvas fortes.

5. Limpeza da área externa

Para evitar incêndios.

Segurança lógica

A segurança lógica **envolve o emprego de soluções** baseadas em softwares para garantir a CID. Entre os diversos mecanismos existentes, destacaremos os oito listados a seguir:

1. Autenticação
2. Sistemas de controle de acesso
3. Criptografia
4. Funções de hash
5. Assinatura digital
6. Certificado digital
7. Redes Virtuais Privadas (VPN)
8. Firewall, sistemas de detecção de intrusão e antivírus

Vamos entender agora o funcionamento de cada mecanismo.

Autenticação

Está relacionada à garantia da propriedade da autenticidade, evitando que terceiros possam fingir ser uma das partes legítimas a fim de acessar sistemas ou informações não autorizadas.

A autenticação diminui o risco de um ataque de personificação ou fabricação. Para realizá-la, podem ser utilizados os seguintes mecanismos: senhas, controles biométricos, *tokens*, certificados digitais.

O mecanismo escolhido deve se adequar ao objetivo de segurança a ser alcançado. Atualmente, os controles biométricos são considerados os mais eficientes, mas é recomendado que seja utilizada a chamada autenticação de dois fatores.

A autenticação de dois fatores utiliza dois mecanismos para autenticar um usuário, por exemplo, utilizando senha e um código enviado por e-mail.

Exemplo

Digitais, reconhecimento de íris, palma da mão e certificados digitais.

Sistemas de controle de acesso

Gerenciam os usuários que podem acessar sistemas e redes, **autorizando apenas** o acesso às informações que lhes couberem. Desse modo, a confidencialidade dos dados está garantida.

Exemplo

O uso de senhas nas redes wi-fi garante que somente as pessoas autorizadas possam utilizá-las.

Para que o controle de acesso seja efetivo, deve-se empregar um mecanismo de autenticação a fim de validar a identidade e – caso o acesso esteja autorizado – restringir os direitos de acesso para cada indivíduo de acordo com o seu perfil de uso.

Criptografia

Assim como a criptoanálise, que não discutiremos aqui, a criptografia é uma vasta área que compõe a criptologia.

A criptografia é uma área que estuda técnicas para esconder não a mensagem real, mas o seu significado. Ela pode ser, inclusive, utilizada para garantir a

CID. A propriedade a ser garantida depende do mecanismo utilizado e de que maneira ele foi empregado.

Funções

Para entendermos o processo criptográfico, iremos, inicialmente, identificar duas funções principais:

Ciframento

Transforma um escrito simples, cujo alfabeto comum é utilizado para compor a mensagem original, em um texto cifrado. Nesse texto, as letras originais são substituídas pelas do alfabeto cifrado, escondendo, dessa forma, o conteúdo da mensagem. A função do ciframento é responsável pela criptografia da mensagem original. Já a substituição das letras da mensagem original é feita pelas cifras (Qualquer forma de substituição criptográfica aplicada ao texto original da mensagem.).

Deciframento

Realiza o processo oposto. Como o texto cifrado é transformado no original, o conteúdo de sua mensagem pode ser entendido. A função de deciframento é a responsável pela decriptografia da mensagem cifrada.

As técnicas modernas de criptografia envolvem o uso de um **algoritmo de criptografia associado a uma chave**. O segredo do processo não está no algoritmo em si, mas na chave utilizada para a realização do ciframento.

Classificação

Quanto ao modelo de chave empregada, os algoritmos criptográficos podem ser classificados como:

- **Algoritmos de chave simétrica ou de chave privada**: Empregam uma **única chave**. Dessa forma, a mesma chave que realiza a cifragem faz a decifragem. Alguns exemplos de algoritmos simétricos: DES, 3DES, Blowfish, RC4, RC5, IDEA, Rinjdael e *Advanced Encrytion Standard* (AES) - Algoritmo padrão adotado por diversos governos e várias empresas para garantir a confidencialidade.
- **Algoritmos de chave assimétrica ou de chave pública**: Utilizam **duas chaves** (pública e privada): uma para cifrar e outra para decifrar. Dependendo da ordem em que ambas são empregadas, o algoritmo pode garantir a confidencialidade ou a autenticidade. A exemplo temos o algoritmo Rivest-Shamir-Adleman (RSA), que é o padrão utilizado para transações comerciais, financeiras etc.

Vamos entender melhor o que ocorre com o uso de cada modelo de chave, de acordo com a ordem na qual são utilizadas:

Chave pública

Quando a chave pública é utilizada na função de cifragem, apenas a privada pode decifrar. Como o nome sugere, a chave privada fica restrita à entidade.

Exemplo: pessoa, empresa ou equipamento.

Neste caso, está garantida a confidencialidade, porque só quem possui a chave privada pode decifrar o conteúdo.

Chave privada

Quando a chave privada é empregada no processo de cifragem apenas a pública pode decifrar. Como a chave usada para decifrar é a pública, qualquer pessoa pode possuí-la e, portanto, decifrar a mensagem.

Neste caso, não há como garantir a confidencialidade, mas sim a autenticidade. A aplicação das chaves nesta ordem permite o emprego da assinatura digital.

Funções de hash

Conhecendo as funções de hash

O objetivo das funções de resumo de mensagem ou de hash é a **garantia da integridade** das informações. Para calcular o resumo, pode ser utilizado qualquer algoritmo que pegue uma mensagem de qualquer tamanho e a mapeie em uma sequência de caracteres de tamanho fixo.

Exemplo

Você tem um arquivo chamado *aula.doc* e quer calcular o resumo dessa mensagem. Uma das funções de hash bastante utilizadas é o *Message-Digest Algorithm 5* (MD5). Então, caso você tenha instalado em seu computador o MD5, pode utilizar o seguinte comando:

md5sum aula.doc

A saída desse comando é uma sequência de caracteres:

5 9 5 f 4 4 f e c 1 e 9 2 a 7 1 d 3 e 9 e 7 7 4 5 6 b a 8 0 d 1

Essa saída será permanente enquanto não ocorrer nenhuma alteração no arquivo. Portanto, toda vez que quiser verificar se ele foi modificado, basta executar novamente a função de hash e compará-la à sequência original. Se ela permanecer a mesma, isso demonstra que o arquivo é íntegro; caso contrário, é uma evidência de que ele foi modificado.

Uma propriedade desejável na função de resumo é que, **diante de qualquer modificação mínima** na informação, o resumo gerado deve ser totalmente

diferente. As funções de resumo também são utilizadas como auxiliares no processo de autenticação.

Alguns sistemas usam o hash para armazenar a senha de um usuário. Portanto, quando ele cadastra uma senha, o sistema calcula o hash e armazena esse valor. Quando o usuário for digitar sua senha para entrar no mesmo sistema, o sistema calculará o hash, enviará essa informação e comparará com o que está armazenado. Se for igual, o seu acesso será autorizado.

A vantagem dessa solução é que a senha do usuário não fica armazenada no sistema nem trafega pela rede. Quem o faz é o hash.

Outra propriedade desejável das funções de resumo é que ela **não é inversível**, ou seja, se temos o hash da mensagem, não conseguimos descobrir a mensagem original. Dessa forma, podemos afirmar que ele configura uma função criptográfica, pois esconde o conteúdo de uma mensagem. Então, quando ocorre o envio do hash da senha, não há como um atacante descobrir a senha original.

Entretanto, o uso isolado dele na autenticação pode gerar uma facilidade para o ataque de reprodução. Um atacante que conseguir obter o hash das assinaturas poderá repetir o seu processo, enviando o resumo e obtendo a autorização de acesso.

Além do MD5, outras funções de resumo muito utilizadas são as seguintes:

1. Secure Hash Algorithm version 1 (SHA-1)

2. Secure Hash Algorithm version 2 (SHA-2)
3. Secure Hash Algorithm version 3 (SHA-3)

Assinatura digital

O que é Assinatura Digital

O objetivo do emprego da assinatura digital é **assegurar a autenticidade** e a integridade das informações. Automaticamente, está garantido o não repúdio. A assinatura ainda garante a validade jurídica dos documentos, pois existe a certeza de que eles não sofreram qualquer adulteração, estando íntegros e completos, e a certeza quanto a sua autoria, asseverando que eles realmente foram assinados por determinada pessoa.

O processo utilizado para realizar a assinatura digital combina o emprego da criptografia assimétrica com as funções de resumo da mensagem. Para que um documento seja assinado digitalmente, o usuário deve seguir estes passos:

1. Calcular

   Calcular o resumo da mensagem.

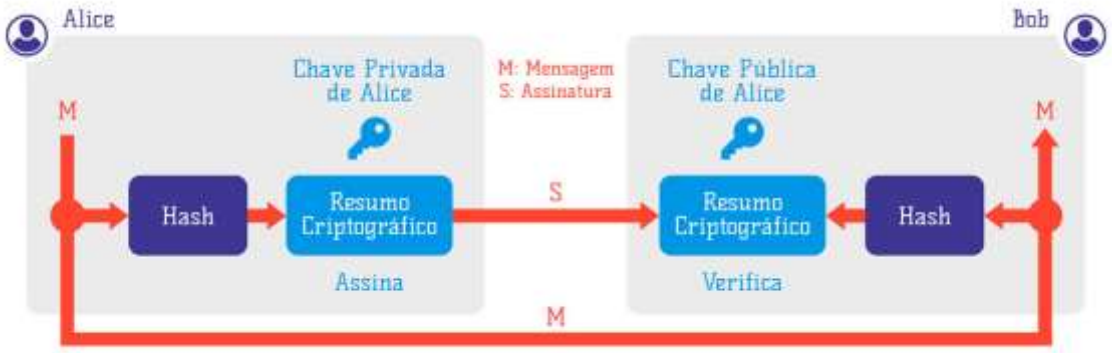
2. Cifrar

   Cifrar esse resumo com a chave privada do emissor do documento.

3. Enviar

Enviar a mensagem com o resumo criptografado, que é a assinatura digital.

O esquema a seguir ilustra esse processo:



Assinatura digital de um documento.

Ao receber o documento, o receptor precisa realizar o seguinte processo para o validar:

O usuário deve calcular o hash da mensagem e decifrar o outro recebido com a utilização da chave pública do emissor. Em seguida, ele vai comparar os dois hashes. Se forem iguais, há a garantia de que o documento não foi modificado e o emissor é autêntico. Caso sejam diferentes, algum problema ocorreu. Mas não é possível garantir se o problema reside na modificação dele ou na autenticidade do emissor. Estabelece-se apenas que o documento não é válido.

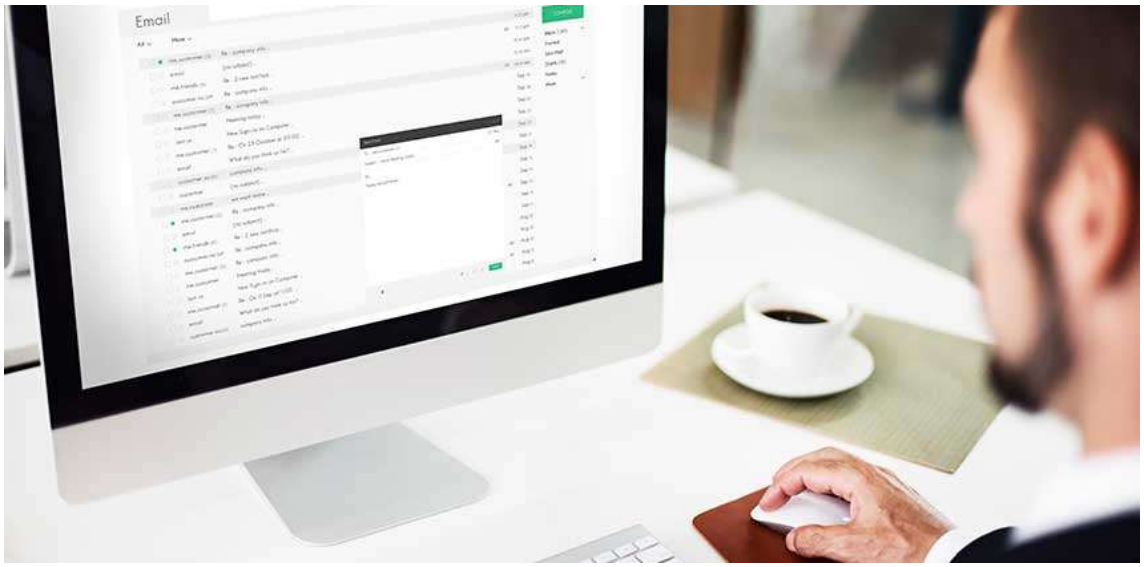
Certificado digital

O que é o Certificado Digital

Ele é utilizado para **vincular a chave pública a uma entidade**, como pessoa, empresa, equipamento etc. O certificado contém a chave pública da entidade, que é assinada digitalmente por uma terceira parte confiável chamada de Autoridade Certificadora (AC).

A existência da autoridade certificadora é importante para garantir um ataque conhecido como “homem no meio” (MITM - *Man In The Middle*). O MITM ocorre quando um atacante pode interceptar o envio da chave pública e ter acesso às informações.

Vejamos a descrição deste problema:



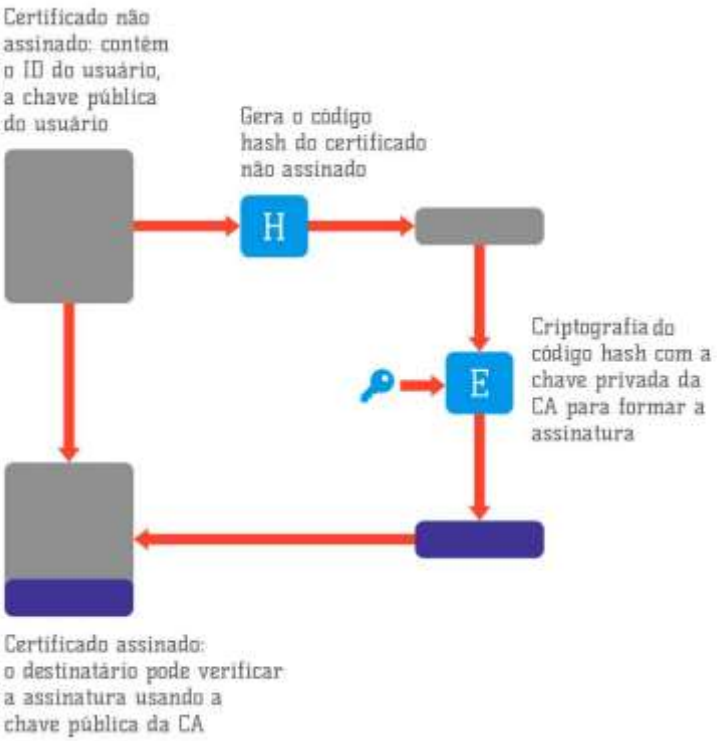
Alice quer enviar um documento para Bob. Ela solicita a chave pública dele para poder cifrar a mensagem.

Darth, enquanto isso, realiza um ataque de interceptação para monitorar a comunicação entre ambos. Quando percebe que houve uma solicitação da chave pública de Bob, Darth envia para Alice a sua chave. Ao mesmo tempo, se fazendo passar por ela, solicita a Bob a chave pública dele, o que caracteriza um ataque de personificação.

Alice, dessa forma, cifra a mensagem com a chave privada de Darth. Obviamente, ele consegue ler as informações enviadas. Para que o processo continue, Darth agora cifra a mensagem com a chave pública de Bob e a envia. Bob, em seguida, recebe a mensagem e a decifra com sua chave privada.

Ao monitorar a troca de mensagens entre Alice e Bob, Darth conseguiu obter as informações, quebrando a confidencialidade desse processo de comunicação.

Para resolver esse problema, é necessária uma terceira parte confiável: a AC, responsável por armazenar as chaves públicas das entidades envolvidas no processo de comunicação. Dessa maneira, a chave fica assinada digitalmente pela autoridade certificadora. Veja o esquema:



Uso do certificado de chave pública.

Voltemos ao exemplo da comunicação entre Alice e Bob. Agora ela já pode solicitar o certificado digital dele para a AC. Ao receber esse certificado, Alice verificará a assinatura digital da AC. Se ela estiver correta, é um indício de que Alice possui o certificado correto de Bob, podendo, dessa forma, realizar a transmissão das mensagens.

O processo para obter a chave privada da AC, contudo, pode esbarrar no mesmo problema. Para o processo funcionar corretamente, o usuário deve ir ao site da AC e realizar o download dos certificados – chamados de certificados raiz –, garantindo, assim, a obtenção da chave pública correta.

Saiba mais

No Brasil, as ACs estão organizadas na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Trata-se de uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão.

Redes virtuais privadas (VPN)

O que é uma VPN

A VPN (*virtual private network*) permite a utilização de um meio inseguro de forma segura. Afinal, quando estamos conectados à internet e desejamos

acessar algum serviço ou rede, ficamos vulneráveis a diversos tipos de ataques.

Para minimizar o risco inerente a esse acesso, podemos empregar uma VPN, que utilizará um **túnel de comunicação entre dois dispositivos**. Considere a topologia desta imagem na qual as redes da matriz e da filial desejam trocar informações por meio da internet:

Ao trafegar pela internet, as informações trocadas entre as redes da matriz e da filial estão sujeitas a diversos tipos de ataque. Na utilização de uma VPN, é criado um túnel virtual entre essas redes. Veja:

Na utilização do túnel, as informações trafegadas ficam protegidas, já que os **dados são criptografados**. Além disso, podem ser utilizados mecanismos de autenticação e integridade para garantir tanto a entrada em cada rede só de pacotes autorizados quanto a manutenção de sua estrutura, ou seja, que eles não sejam modificados.

Firewall, sistemas de detecção de intrusão e antivírus

Confira a seguir os mecanismos de segurança lógica.

Veja o trecho da seguinte notícia:

“PF identifica invasão nos celulares de presidentes de STJ, Câmara e Senado; PGR também foi alvo”. (Fonte: G1, 2019)

Percebemos aqui a importância dos softwares, cuja função é a de garantir a CID nas instituições. Pesquise outras situações similares e procure perceber como foi a intervenção da segurança lógica nesses casos.