5

Controle de Acessos

Para começar

Agora que já apresentamos os princípios da segurança da informação e suas principais ameaças, vamos aprender o que é necessário para que sejam evitados estes ataques e como são mantidos os princípios da Segurança da Informação

5.1 Introdução

Para que os princípios da segurança da informação sejam mantidos e preservados, é necessária a criação de regras de acesso às redes, sistemas e bancos de dados armazenados em servidores de uma rede. É importante, ainda, a definição de padrões de procedimentos, por meio da utilização de ferramentas que possam bloquear ao máximo ataques externos aos computadores da rede, de políticas que estabeleçam os critérios para identificar quem internamente está utilizando os recursos de uma rede de computadores, bem como o registro de quando e o que foi executado ou realizado.

Este conjunto de regras é o que denominamos política de segurança da informação.

5.2 Controle de acessos

Como controle de acesso entende-se o gerenciamento da visualização de informações e da utilização dos recursos digitais de uma rede de computadores, considerando as propriedades da segurança da informação, quais sejam: confidencialidade, integridade e disponibilidade.

A gestão deste controle deve ser realizada para prevenir a visualização não autorizada dos dados e recursos computacionais (confidencialidade) e impedir qualquer modificação não autorizada de dados (integridade). E, paralelamente, assegurar que os dados e recursos gerenciados estarão sempre aptos para uso, quando solicitados por usuários autorizados (disponibilidade).

Quando falamos em controle de acessos, estamos nos atendo primeiramente em dois pontos: a identificação do usuário que se conecta em uma rede e sua autenticidade. Isto é, que existam formas de validar aquele nome de usuário como sendo ele mesmo.

Para que um usuário seja capaz de acessar um recurso de uma rede, deve ser determinado se essa pessoa é quem ela diz ser, se ela tem as credenciais necessárias e se foram dados a ela os direitos e privilégios necessários para executar as ações desejadas.

Em um primeiro momento, deve-se fixar um conceito: a identificação trata-se de um meio de garantir que um sujeito (usuário, programa ou processo) é realmente quem afirma ser.

Uma identificação pode ser verificada com o uso de uma credencial (com nome de usuário e número de identificação pessoal), um cartão inteligente (também conhecido, em inglês, como *smart card*), assinatura digital, número de uma conta ou um atributo anatômico (impressão digital, impressão palmar etc).

Para ser devidamente autenticado, o usuário é, normalmente, obrigado a fornecer uma segunda peça para fechar o seu conjunto de credenciais de acesso.

Esta segunda peça pode ser uma senha, uma frase-senha, uma chave de criptografia ou a informação gerada no momento em um token.

Nadasazh/Shutterstock.com

Figura 5.1 – Um Token.

Estas duas peças de identificação de credenciais são comparadas com as informações previamente armazenadas no sistema pelo usuário. Se essas credenciais coincidirem com as armazenadas, o usuário é autenticado na rede. Mas o processo ainda não está concluído.

Uma vez que o usuário fornece suas credenciais e está devidamente identificado, o sistema que ele está tentando acessar (rede, sistemas, programas etc.) precisa determinar se para este assunto lhe foi dado o direito e os privilégios necessários para realizar as ações solicitadas.

O sistema de gerenciamento da rede (sistema operacional) recorrerá a algum tipo de matriz de controle de acesso, ou fará comparações nos registros de segurança, para verificar se este usuário está realmente apto a acessar o recurso solicitado e a executar as ações desejadas.

Se o usuário estiver registrado e seu acesso liberado nesta matriz, ele será autorizado a executar as ações desejadas e a utilizar os recursos solicitados.

Apesar de identificação, autenticação e autorização possuírem definições próximas e complementares, cada uma tem funções distintas que cumprem uma exigência específica no processo de controle de acesso.

Entretanto, um usuário pode ser devidamente identificado e autenticado para a rede, mas não pode ter a autorização para acessar arquivos no servidor de arquivos da rede.

Por outro lado, um usuário pode ser autorizado a acessar os arquivos no servidor de arquivos. Mas, até que ele esteja devidamente identificado e autenticado, esses recursos estão fora de alcance.

É necessário que o usuário seja responsabilizado pelas ações tomadas dentro de um sistema.

A única maneira de garantir o registro de contas é se o usuário possuir unicamente uma identificação e suas ações no sistema ou na rede forem registradas.

A Figura 5.2 apresenta os três passos para que um usuário possa utilizar recursos de uma rede, no caso uma impressora da rede, e das aplicações desejadas:

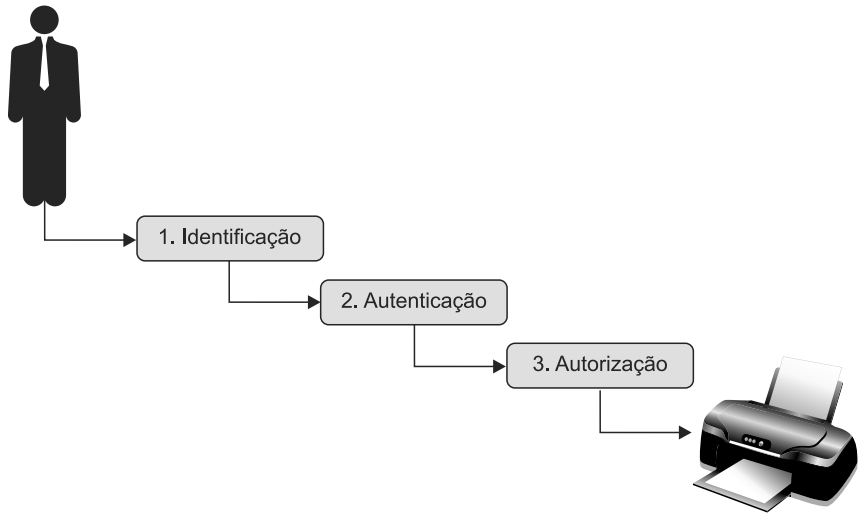

Figura 5.2 – Três passos para acessar um objeto.

Portanto, os três passos para um usuário acessar ou utilizar um recurso da rede são: identificação, autenticação e autorização.

Os chamados controles de acesso lógico são ferramentas de software utilizadas para identificação, autenticação, autorização e registro de atividades de usuários.

Eles são normalmente softwares componentes que realizam medidas de controle de acesso para sistemas, programas, processos e informações.

Os controles de acesso lógico podem ser incorporados nos sistemas operacionais, aplicativos, em add-ons de pacotes de programas de segurança, ou em sistemas de gerenciamento de banco de dados e gerenciamento de telecomunicações.

5.2.1 Identificação

Falaremos agora sobre o primeiro passo de um controle de acesso: a identificação do usuário.

A identidade de um indivíduo deve ser verificada durante o processo de autenticação.

A autenticação geralmente contém um processo de duas etapas: primeiro a inserção de informações consideradas públicas (um nome de usuário, número de funcionário, ou número de conta, identificação de um departamento, ou uma característica biométrica) e depois a inserção de algum tipo de informação privada (uma senha estática, um número de um token inteligente, uma password cognitiva, *one-time password* etc.).

A entrada de uma informação pública é a etapa de identificação e inserção de informação privada. Trata-se da fase de autenticação deste processo de duas etapas.

Normalmente as empresas criam nomes de usuários de rede baseados no nome próprio do funcionário, porém criando regras de formação deste formato de nome.

É comum utilizar-se na formação de nomes de usuário o modelo da Tabela 5.1, considerando-se que temos de adotar critérios para solucionar nomes similares ou até os casos de pessoas homônimas.

Tabela 5.1 – Funcionários e nome de usuários

Nome do funcionário	Username
Alexandre Silva	Asilva
Carlos Santos	Csantos
Carlos Silva Santos	Csilva
Carlos Silva	Silvac
Claudia Ferreira	Claudia
Claudia Souza Ferreira	Csouza
Claudia Souza	Souzac

Algumas empresas, dependendo da configuração dos servidores de rede, utilizam composições com nome, um ponto e sobrenome, mas isto é mais comum na criação de contas de e-mail corporativo.

Como comentamos, podemos também utilizar a matrícula, ou número do funcionário, como identificador público. A opção de utilizar identificadores genéricos como identificação de um departamento é passível de ser utilizada, porém não recomendada. Nesse caso, seria como ter uma identificação para mais de um usuário, ou seja, todos os funcionários do departamento usariam a mesma identificação.

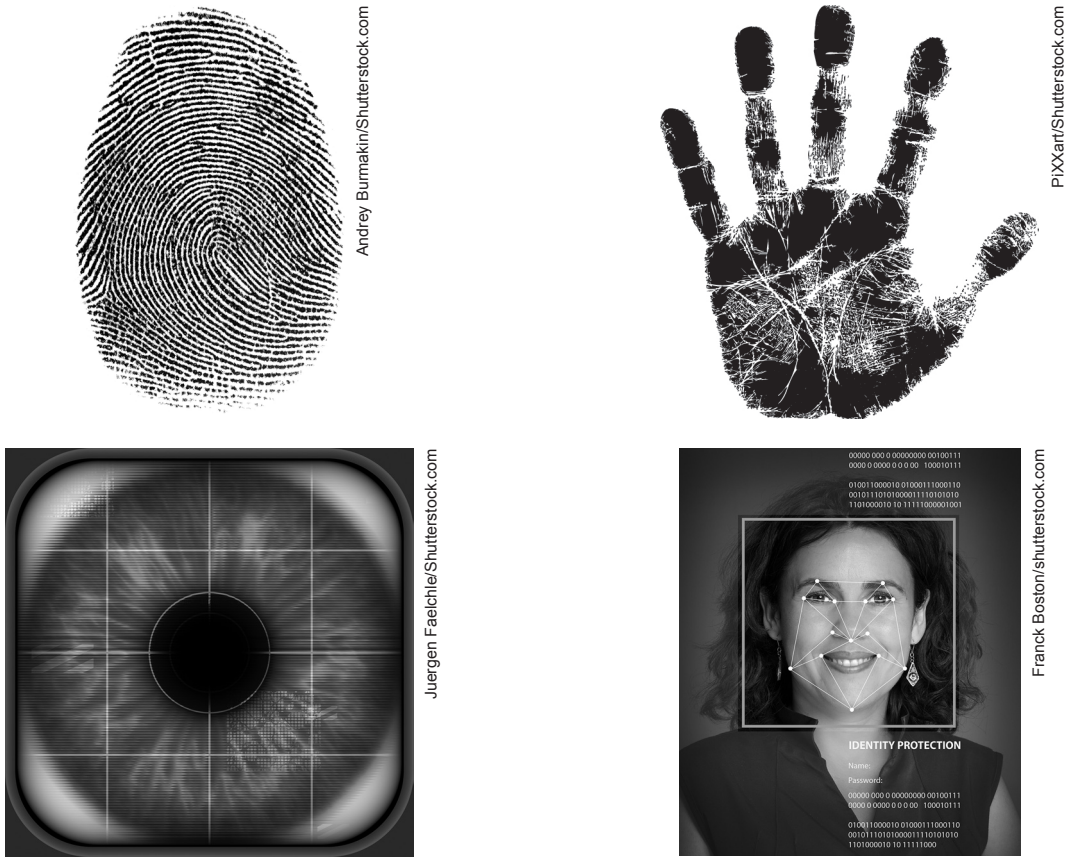

Figura 5.3 – Tipos de tecnologias de identificação biométricas.

Vejamos alguns conceitos de identificação biométrica.

A identificação biométrica verifica uma identificação individual por meio de um único atributo pessoal. Ela é considerada um dos mais acurados e efetivos métodos de verificação de identificação.

É claro que estamos falando de tecnologia sofisticada e cara. Você já deve ter assistido a filmes em que as pessoas são identificadas para acessar um computador por meio de impressão digital, da palma da mão, ou da leitura da retina (quando alguém coloca o olho em frente a uma tela e um raio escaneia o olho).

Uma vez que este sistema verifica as ranhuras de impressão digital, o padrão de retina ou as características de voz de uma pessoa, uma das suas principais características é a extrema sensibilidade. Um sistema deste tipo deve executar medições precisas e repetíveis de características anatômicas ou fisiológicas de um indivíduo. Entretanto, este tipo de sensibilidade pode facilmente provocar falsos positivos ou falsos negativos.

Este sistema de identificação deve ser calibrado para que esses falsos positivos e falsos negativos tenham ocorrências muito baixas e que os resultados sejam sempre o mais precisos possível.

Novamente, recorrendo aos filmes como exemplo, você acreditou que alguém possa cortar o dedo indicador ou a mão de outra pessoa e usá-lo para uma identificação por impressão digital?

A princípio se estivermos lidando com um sistema de identificação biométrico, por meio de impressão digital ou de impressão palmar (mão inteira), isso seria possível com certeza. Mas não recomendamos que você faça isso.

Sistemas de identificação por impressão digital armazenam a impressão digital completa, um volume muito grande de informações que ocupam muito espaço no disco rígido e que tornam o processo para a realização de comparações de dados mais lentos quando um usuário está tentando ser autenticado.

A tecnologia de scanner de dedo, por assim dizer, extrai algumas características específicas da impressão digital e armazena apenas esta informação associada a um usuário, funcionário da empresa. Com isso ocupa menos espaço em discos rígidos e permite pesquisas mais rápidas em banco de dados e as comparações necessárias no processo de autenticação do usuário.

Na verificação baseada em retina ou íris temos o seguinte formato de operação:

5.2.1.1 Scanner de retina

Um sistema que lê a retina da pessoa verifica o padrão dos vasos sanguíneos da retina, que fica na parte de trás do globo ocular.

O padrão tem-se mostrado extremamente único entre as pessoas. Ou seja, não existem duas pessoas com o mesmo padrão de vasos sanguíneos da retina.

Uma câmera é usada para projetar um feixe de luz dentro do olho e capturar o padrão de vasos sanguíneos da retina e compará-lo a um arquivo de referência registrado anteriormente, no cadastramento do funcionário, por exemplo.

5.2.1.2 Scanner de íris

A íris é a parte colorida do olho que envolve a pupila. Ela tem um padrão único, com fendas, cores, anel, coroas e sulcos.

A singularidade de cada uma dessas características dentro da íris é capturada por uma câmera e comparada com as informações obtidas durante a fase de cadastramento do funcionário.

Ao se utilizar um sistema biométrico padrão da íris, o leitor ótico deve ser posicionado de modo que o sol incida sobre a lente. Por isso, quando implementado, deve ser devidamente colocado em um edifício com uma análise da incidência solar no local antecipadamente. A incidência solar sobre a lente irá perturbar o funcionamento correto do sistema de identificação.

Para além das tecnologias estudadas anteriormente, existem outras que não iremos detalhar, quais sejam:

» Geometria da mão
» Impressão de voz
» Escaneamento facial
» Topologia da mão

Amplie seus conhecimentos

Deixo aqui o desafio para ampliação dos seus conhecimentos por meio de pesquisa de campo. Faça um resumo descritivo de cada uma destas quatro outras tecnologias de identificação apresentadas.

5.2.2 Autenticação

Uma vez que uma pessoa foi identificada, ela deve ser autenticada. Deve-se confirmar que ela é realmente quem se diz ser.

Existem três tipos gerais de autenticação para uma pessoa: algo que ela saiba, algo que ela possua, algo que ela seja.

Algo que uma pessoa possa saber pode ser uma password (senha), um número PIN (como em alguns telefones celulares), o nome da mãe ou uma combinação de um segredo tipo de cofre.

A desvantagem deste método é que uma terceira pessoa pode obter o conhecimento desta senha e ter acesso não autorizado a um sistema.

Este é um dos motivos pelo qual as pessoas têm cada dia mais interesse em utilizar identificação e autenticação biométrica, que tem se mostrado um meio mais seguro. Lembre que senhas podem ser perdidas, observadas e copiadas e podem causar danos irreparáveis aos sistemas de informação.

Fique de olho!

Identificação e senha são pessoais e intransferíveis. São confidenciais e nunca se deve emprestar ou dar sua senha para um colega de trabalho, amigo, ou quem quer que seja, independentemente do motivo.

5.2.2.1 Passwords

A autenticação acoplada com uma password (senha) é o mecanismo mais comum de autenticação utilizado.

Password é uma sequência de caracteres protegida utilizada para autenticar um indivíduo, um usuário.

Uma password, esta sequência de caracteres, é baseada unicamente em um conceito ou alguma coisa que o usuário sabe e somente ele sabe.

Muitos usuários não dão importância à segurança até o momento em que um craker invade seu computador.

Já foi muito comum, e ainda é um pouco, em alguns lugares encontrarmos um papel colado no monitor do computador com a password de seu usuário. Ou então encontrarmos password como data de aniversário, nome da mãe, nome do cachorro, da esposa etc.

Usuários não têm muito cuidado na escolha de senhas. É, por exemplo, o que Ashley Feinberg nos mostra em uma compilação feita pelo SplashData (uma lista que puxa dados de milhões de senhas roubadas que se tornaram públicas ao longo do ano).

Apresentamos, a seguir, as vinte senhas mais comuns na rede e que deixam muito a desejar em relação à segurança.

As "vinte mais" imprudentes são:

Tabela 5.2 – As vinte senhas mais usadas

	Senhas mais comuns
1	123456
2	password
3	12345678
4	qwerty
5	abc123
6	123456789
7	111111
8	1234567
9	iloveyou
10	adobe123
11	123123
12	Admin
13	1234567890
14	letmein
15	photoshop
16	1234
17	monkey
18	shadow
19	Sunshine
20	12345

Fonte: http://gizmodo.uol.com.br/as-25-senhas-mais-comuns-de-2013

Se as senhas forem corretamente geradas/criadas, atualizadas e mantidas em segredo, elas podem fornecer uma segurança eficaz.

Fique de olho!

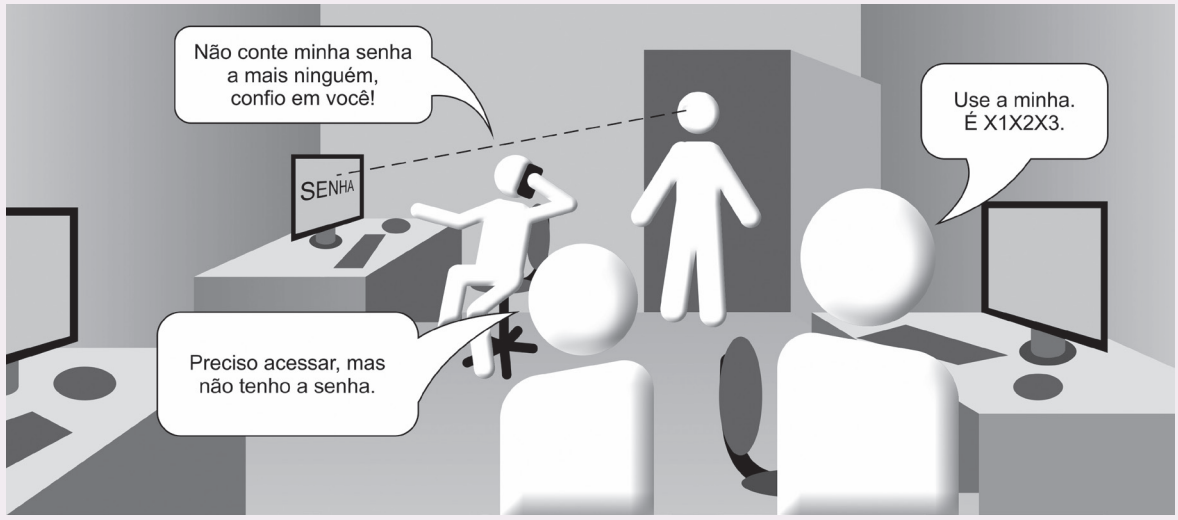

Figura 5.4 – Ambiente sem segurança de senhas.

Tudo o que for executado com a sua senha será de sua inteira responsabilidade. Portanto, tome todas as precauções possíveis para manter sua senha secreta.

Geradores de senha podem ser usados para criar as senhas de usuário.

Isso garante que o usuário não usará "*Maria*" ou "*Teste*" para uma senha. Por outro lado, se o gerador criar uma senha como "*kdjasijew284802h*", o usuário certamente irá anotá-la em um pedaço de papel e colocá-lo colado em seu monitor.

Se um gerador de password for utilizado, as ferramentas que o compõem devem criar "*Não palavras*" pronunciáveis para ajudar o usuário a se lembrar dela. Elas não devem ser tão complexas a ponto de o usuário precisar anotá-las. De nada adiantam senhas difíceis de ser memorizadas pelo usuário.

Caso os usuários possam escolher suas próprias senhas, o sistema operacional deve exigir certos requisitos de senha para garantir maior grau de segurança. Por exemplo, pode exigir que uma senha contenha um determinado número de caracteres, letras maiúsculas, minúsculas e números. Assim, não estará estabelecendo uma senha fraca tampouco de difícil memorização, por parte do usuário.

Normalmente, o sistema operacional, ao verificar as senhas de cada usuário, impede e garante que nenhuma senha seja reutilizada.

Os usuários também devem ser forçados a mudar suas senhas periodicamente. Esta é uma prática comum em empresas, apesar de incômoda para o usuário que tem de usar de criatividade para criar senhas a cada três meses, por exemplo. *Isso chama-se envelhecimento de senha*.

O sistema mantém normalmente uma lista com as cinco últimas senhas, ou mais, e não permite que o usuário repita uma senha utilizada anteriormente.

Todos estes fatores tornam mais difícil para um atacante adivinhar ou obter senhas dentro de um ambiente de rede.

Como outro fator de segurança temos o que denominamos limite de tentativas de login na rede. Um limite pode ser configurado para que apenas um determinado número de tentativas de login sem sucesso possa ser realizado. Após, sem sucesso, atingir este limite de tentativas, a senha do usuário é bloqueada imediatamente.

5.2.2.2 Dispositivo de token

Um dispositivo de token, ou gerador de senhas, geralmente é um dispositivo portátil que tem um display de LCD e teclado.

Dave Clark Digital Photo/Shutterstock.com

Figura 5.5 – Dispositivo de token.

Este dispositivo é uma peça de hardware separada do computador do usuário que tenta acessar a rede ou uma aplicação.

O dispositivo de token (sinal) e o serviço de autenticação têm de ser sincronizados, ou seja, utilizar o mesmo esquema de questão-resposta para ser capaz de autenticar um usuário.

O dispositivo de token apresenta ao usuário uma lista de caracteres para ser inserido, como uma senha ao fazer login em um computador.

Somente o dispositivo de "token" e o serviço de autenticação (uma aplicação desenvolvida para este fim) conhecem o significado dos caracteres apresentados no aparelhinho.

5.2.3 Outros métodos de autenticação

Existem outros métodos de autenticação que serão elencados a seguir. Como este livro não tem como objetivo detalhar o funcionamento destes métodos, sugerimos que você, leitor, pesquise sobre eles. Assim, ampliará seus conhecimentos.

5.2.3.1 Chaves criptografadas

É realizada por meio de uma chave privada, ou uma assinatura digital. O ato de criptografar este valor de "*hash*" com uma chave privada é chamado assinatura digital de uma mensagem. Uma assinatura digital usa uma chave privada para criptografar um valor de "*hash*".

Hash (resumo), uma função do sistema operacional, é qualquer algoritmo que mapeie dados grandes e também de tamanho variável para pequenos dados de tamanho fixo.

Por esse motivo, as funções hash são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos. Assim, os dados do usuário, como nome, matrícula de funcionário, departamento e empresa, podem ser criptografados em uma função "hash", criando, então, sua assinatura digital.

5.2.3.2 Password de frase (passphrase)

É também uma sequência de caracteres, porém mais longa que um password (senha).

Em seu primeiro acesso ao sistema, o usuário entra com uma frase, que o sistema transformará em uma senha virtual.

Por exemplo, o usuário entra com a frase "Gosto de minha privacidade", e o sistema a converterá em uma senha virtual.

Como é sempre mais longa que um password comum, teoricamente ela é mais difícil de ser copiada por um atacante.

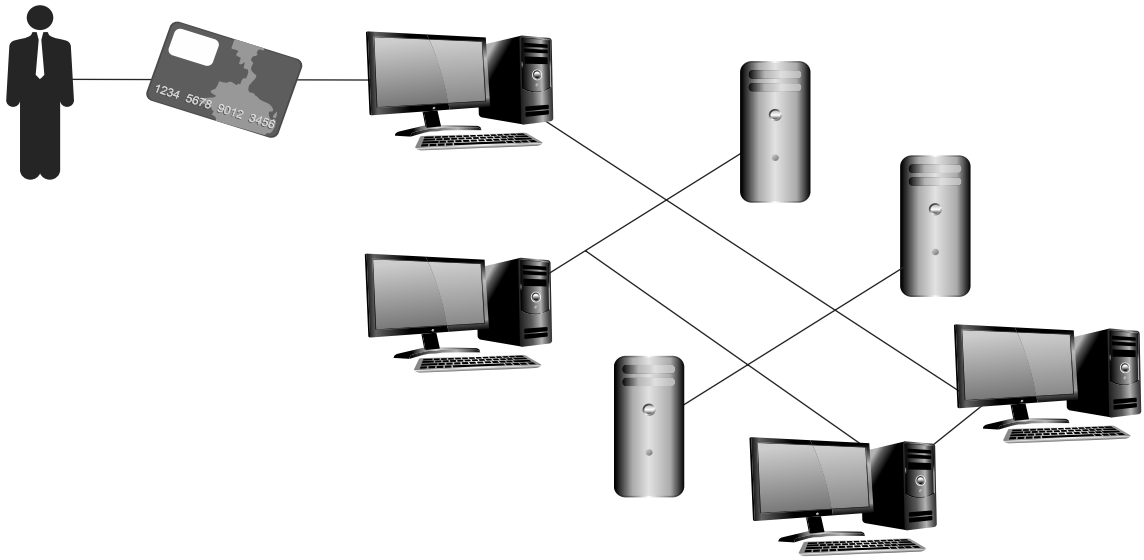

Figura 5.6 – Autenticação com utilização de cartão inteligente.

5.2.3.3 Cartões de memória

A principal diferença entre os cartões de memória e cartões inteligentes é a capacidade de processamento.

Um cartão de memória contém informações de autenticação de um usuário, de modo que este usuário só precisa digitar uma identificação de usuário (ID) ou um número de identificação pessoal (PIN), presente no cartão de memória. Se os dois combinarem, será aprovado pelo serviço de autenticação e o usuário será autenticado com êxito.

5.2.3.4 Cartões inteligentes (smart cards)

Um cartão inteligente tem a capacidade de processamento de informações porque possui um microprocessador e circuitos integrados incorporados no próprio cartão.

Um cartão inteligente fornece um método de autenticação de dois fatores; o usuário tem de digitar uma identificação de usuário ou senha para desbloquear o cartão do leitor.

Isto significa que o usuário deve fornecer algo que ele sabe, como o seu número de identificação pessoal (PIN), e algo que ele tem (smart card).

Isso é o que acontece quando você vai a um caixa eletrônico, fornece o cartão do banco e uma identificação e ele solicita uma senha para desbloquear e liberar o cartão.

Claro que, após realizar suas operações, você terá fornecido o cartão e uma identificação (no caso uma senha e mais um número de um token) para poder utilizar os recursos disponíveis.

5.3 Monitoramento de controle de acesso

Monitoramento de controle de acesso é um método de manter o controle de quem tenta acessar recursos de rede específicos. Trata-se de um importante mecanismo de detecção. Vale destacar que existem diferentes tecnologias que podem realizar esta atividade.

Vamos estudar sobre estas ferramentas e os Firewalls no próximo capítulo.

Vamos recapitular?

Neste capítulo aprendemos os conceitos de identificação, autenticação e autorização, assim como os principais métodos aplicados para identificação e autenticação que possibilitam a realização conjunta de identificação e autenticação, conhecidos como métodos biométricos. Além disso, aprendemos sobre a utilização de cartões inteligentes (smart cards), dispositivos de token e como é realizada a interação de controle entre uma pessoa e um computador ou rede de computadores.

Agora é com você!

1) O que é derivado de um password (senha) de frase?
2) Cite dois tipos de autenticação de controle biométrico?
3) O que uma pessoa sabe é o que proporciona uma melhor autenticação? Explique.
4) O que significa a autenticação?
5) Uma senha é usada principalmente para qual função?
6) Um cartão de crédito ou de débito é um smart card?