Controle de Acesso

"É necessário não apenas proteger o acesso físico e lógico, mas também tem que controlar e auditar o acesso".

Na década de 80, os Sistemas de Controle de Acesso Físico começaram a se popularizar. Isso ocorreu devido ao barateamento dos computadores de pequeno porte, que então obtiveram processamento suficiente para controlar as transações em tempo real.

Atualmente, os sistemas de controle de acesso físico possibilitam a integração de outras funcionalidades, como integração com leitores biométricos, controle de estacionamento, controle de elevadores, integração com alarmes de incêndio, controle de ronda, emissão de crachás para visitantes, integração com CFTV, etc.

Outra tendência é o Acesso Universal, isto é, a integração do controle de acesso físico com controle de acesso lógico.

Isso permite a criação de regras especiais, como permitir o acesso à estação de trabalho apenas a usuários que se autenticaram na entrada do departamento e a utilização da mesma credencial biométrica para todos os dispositivos.

Biometria

As tecnologias de autenticação biométrica estão cada vez mais acessíveis e já vêm sendo utilizadas em muitas empresas e entidades governamentais. As principais dúvidas relacionadas a esta tecnologia estão ligadas à segurança, à facilidade de seu emprego e ao tipo de biometria que será adotada.

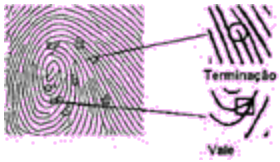
A definição de Biometria é "característica física única e mensurável de uma pessoa". Os indivíduos possuem algumas dessas características que podem ser unicamente identificadas, como por exemplo, a impressão digital, a retina, a formação da face, a geometria da mão, o DNA e outras. O ponto diferencial em relação a outras formas de identificação como a senha ou o cartão inteligente é que não podemos perder ou esquecer nossas características biométricas.

A tecnologia digital cada vez custa menos e assim possibilita a introdução no mercado de dispositivos que fazem a autenticação biométrica. Alguns mecanismos como leitor de impressão digital, da geometria da mão e até mesmo de retina, já se tornaram conhecidos através de filmes, além de também já podermos ver em algumas empresas.

A identificação biométrica se dá em duas fases:
. primeiro o usuário é registrado no sistema, permitindo a captura de suas características biométricas, as quais são convertidas em um modelo que as representa matematicamente.
. a segunda fase é a autenticação, onde o usuário apresenta suas características biométricas, que são comparadas e validadas com o modelo armazenado

Tecnologias

Impressão Digital



A impressão digital é composta por vários sulcos, que em sua formação apresentam diferenças chamadas de pontos de minúcias, ou seja, aquelas partes em que os sulcos se dividem (vales) ou onde terminam abruptamente (terminação). Cada um desses pontos tem características únicas, que podem ser medidas. Ao compararmos duas digitais podemos determinar seguramente se pertencem a pessoas distintas, baseados nos pontos de minúcias. Há muitos anos os institutos oficiais de identificação de diversos países já realizam o reconhecimento de pessoas através do sistema de análise da impressão digital. Na Europa, judicialmente, são necessárias 12 minúcias para saber quem é uma pessoa. Os leitores biométricos são capazes de identificar mais de 40 minúcias de uma impressão digital.

Existem três tipos de leitores de digitais:

• Ópticos: O dedo é colocado sobre uma plataforma de vidro e uma imagem do dedo é capturada. Estes dispositivos tornaram-se pequenos e baratos;
• Ultra-som: O dedo é colocado sobre uma plataforma de vidro e uma varredura de ultra-som é efetuada;
• Baseados em chip: O usuário coloca seu dedo direto em um chip de silício.
Diversas empresas estão realizando grandes investimentos na evolução dessa tecnologia. Um dos empregos que já se nota

é o acesso de usuários a sistemas operacionais, no lugar de se fornecer uma identificação e senha.

Veja mais adiante um exemplo sobre o uso da impressão digital.

Retina

A biometria da retina é baseada na análise da camada dos vasos sanguíneos no fundo dos olhos. Para isto utiliza uma luz de baixa intensidade, que faz uma varredura para encontrar os padrões singulares da retina. É uma técnica de muita precisão e praticamente impossível de ser adulterada devido a forte relação com os sinais vitais humanos. Não é comumente bem aceita por seus usuários porque requer que este olhe em um visor e focalize um determinado ponto, trazendo alguma dificuldade se o usuário estiver de óculos.

Geometria da Mão

Os dispositivos biométricos da mão são rápidos, de fácil operação e se baseiam nas medidas da mão do usuário. Ideal para ambiente onde o acesso a áreas restritas necessita ser rápido e seguro como no controle de acesso de funcionários de uma empresa.
Esta técnica já é utilizada desde a década de 70. Considera-se que é baixíssima a probabilidade de que existam pessoas com a geometria da mão idêntica e que o formato da mão, a partir de uma determinada idade, não sofre alterações.

Neste tipo de técnica realiza-se uma análise tridimensional do comprimento e largura da mão para que seja possível a

identificação de um indivíduo. Após o reconhecimento de voz e da impressão digital, a geometria da mão é a técnica mais utilizada. Para a captura, o usuário posiciona sua mão no leitor, alinhando os dedos, e uma câmara posicionada acima da mão captura a imagem. Medidas tridimensionais de pontos selecionados são tomadas e o sistema extrai destas medidas um identificador matemático único na criação do modelo.

Íris

Baseada nos anéis coloridos do tecido que circunda a pupila, é considerada a menos intrusiva das tecnologias que envolvem o uso dos olhos para identificação, pois não requer um contato muito próximo com o dispositivo de leitura como no caso da retina. Outro fator que agrada aos usuários é que não é necessário retirar os óculos para fazer a leitura da íris.

Facial

O uso de reconhecimento facial em sistemas de CFTV tem sido adotado desde 1998, mas apenas recentemente se tornou bastante procurado devido aos ataques terroristas nos EUA.
A autenticação é realizada através de uma câmera digital, que captura as características da face e de sua estrutura óssea e codifica a imagem da face em uma credencial biométrica.
Essa credencial é então comparada com uma lista de credenciais biométricas faciais previamente cadastradas. Essa lista pode ser composta de criminosos ou simples usuários, dependendo da finalidade da aplicação.

Um dado interessante é que os grandes cassinos investiram muito nesta tecnologia e criaram um banco de imagens de celebridades para sua rápida identificação, de forma a garantir sua segurança pessoal. O uso de óculos, por exemplo, pode dificultar o processo de reconhecimento.

Voz, assinatura e digitação

São métodos menos utilizados, mas que também vêm sendo pesquisados. O reconhecimento do timbre de voz é pesquisado como ferramenta de autenticação em aplicações como phone-banking. Além da senha, o sistema reconheceria a voz do usuário.

Entre os desafios para a consolidação desse método estão a identificação de voz do usuário que enfrenta uma crise de rouquidão e reconhecer a voz mesmo em ambientes barulhentos, no caso de a ligação ser feita de um telefone público, por exemplo.

Os reconhecimentos de digitação e assinatura analisam comportamentos do usuário. No caso da assinatura, além do desenho, é analisada a pressão que o usuário faz sobre o papel e os movimentos. A digitação segue lógica parecida

O processo de autenticação consiste em analisar características tais como velocidade e pressão de uma assinatura. Os usuários desta tecnologia se identificam bastante com o processo, por já estarem acostumados a utilizar a assinatura como meio de autenticação. Existe uma outra forma de reconhecimento através da assinatura que se constitui na dinâmica da assinatura. Nesse método o equipamento utilizado é a caneta óptica.

Apesar desta tecnologia ser de baixo custo e de boa precisão, surpreendentemente, poucas aplicações no mercado a adotam.

Aplicações da Biometria

A utilização da biometria tem basicamente dois propósitos: validar e identificar usuários. A identificação é um processo mais complexo, devido à necessidade da existência de uma base de informações com dados para autenticação de usuários e sua administração. As aplicações de biometria contemplam basicamente os seguintes tipos de acesso:

1 – Controle de Acesso físico

Já há alguns anos, ambientes que exigem alta segurança vêm utilizando biometria para controle e acesso. Durante os jogos olímpicos de 1996, 65.000 pessoas passaram por um rigoroso controle de acesso usando biometria. O Congresso Nacional está utilizando a impressão digital para garantir a autenticidade dos deputados nas votações. Leitores da íris estão sendo amplamente avaliados para uso em aeroportos. Alguns aeroportos nos EUA já estão testando esta tecnologia com passageiros voluntários e especialistas arriscam a previsão de que esta tecnologia poderá substituir os passaportes no futuro. No Serpro, a sala-cofre da Autoridade Certificadora utiliza leitores de impressão digital no seu controle de acesso.

2 - Controle de Acesso lógico

A redução drástica dos preços dos dispositivos biométricos e a forte necessidade de maior segurança da informação vem atraindo muitas empresas a utilizarem a biometria para controlar o acesso às suas redes e aplicações. O grande atrativo é trocar as senhas por uma chave mais segura e protegida, onde você é sua própria chave, que ninguém pode roubar ou pegar emprestada.

A Procuradoria-Geral da Fazenda Nacional, em conjunto com o Tribunal Regional Federal de São Paulo, investiu no uso de biometria no Projeto de Execução Fiscal Virtual. Toda vez que um juiz precisa assinar um documento deverá utilizar seu smart card em conjunto com sua impressão digital.

O Serpro está desenvolvendo um projeto de estação segura, onde será utilizado um leitor biométrico conjugado com smart cards, para aumentar a proteção dos dados e aplicações.

O Supremo Tribunal Federal já conta, desde maio de 2001, com o reconhecimento da impressão digital na identificação de seus funcionários, para acesso a seus computadores.

No comércio Eletrônico:
O número de fraudes nesse setor, cresce a cada dia, sendo imperioso o uso de mecanismos mais eficazes para a identificação de clientes do que os cartões magnéticos com senha. Os smart cards já são mundialmente reconhecidos como um dispositivo de alta segurança para substituírem os cartões magnéticos. Além disso, a possibilidade deles guardarem os dados biométricos para a identificação do usuário torna esta combinação perfeita para as transações comerciais. O usuário pode assinar digitalmente as transações com um certificado presente no cartão, que só é liberado mediante a identificação biométrica com a impressão digital. Assim, aplicações bancárias, aplicações na Web e em postos de vendas, ofereceriam muito mais segurança aos seus usuários e reduziriam substancialmente os prejuízos com fraudes.

Escolhendo uma Tecnologia

Existem vários aspectos que devemos observar ao selecionar uma solução tecnológica envolvendo biometria. É importante observar o nível de rejeição que a tecnologia causa a seus usuários. O tipo de aplicação de biometria também deve ser levado em conta, por exemplo, para controlarmos a entrada de pessoas autorizadas em uma empresa. A tecnologia de geometria da mão é adequada porque tem boa precisão na identificação, não toma tempo dos usuários e é bem aceita. Em um microcomputador é mais adequado o leitor de impressão digital, pelo seu preço, precisão e tamanho do dispositivo.

Embora muitas empresas já façam uso da biometria, para autenticação em muitas aplicações, a indústria continua evoluindo muito. Em 1995 foi criado o Biometric Consortium, para orientar e dar apoio a esta tecnologia. A última conferência mundial desse organismo, enfocou duas áreas de importância:

1- Padronização

Devido à diversidade de produtos de biometria, cada qual com sua interface proprietária, algoritmos e estruturas de dados, sentiu-se a necessidade da criação de padrões para uma interface comum, que permita compartilhar templates (modelos gerados a partir da representação matemática das biometrias) biométricos e possibilitar a comparação efetiva entre diferentes tipos de tecnologia.

A BioAPI é um padrão aberto, desenvolvido por um consórcio de 60 entidades, que define um método comum de interface com as aplicações que usam biometria e que define funções básicas tais como: inscrição de usuários, autenticação e pesquisa de identidade.

2- Uso de tecnologias híbridas

Uma nova forma de utilização desta tecnologia é a conjugação dos leitores de impressão digital com os smart cards. O template gerado na captura da digital é armazenado dentro da área segura do cartão. O cartão é inserido em um leitor híbrido, integrado com o do smart card, que possui as duas funcionalidades: leitor de smart card e biométrico, sendo o processo de autenticação realizado inteiramente dentro do dispositivo. Além disso, o usuário também pode ter armazenado o seu certificado digital dentro do cartão, garantindo que somente ele, o dono da impressão digital, poderá usá-lo. O processo de autenticação da digital usando o template no smart card é conhecido como match-on-card.

Exemplo de Uso

Veja como funciona o sistema biométrico do Detran-SP

Fonte: Site da UOL de 21/07/2005 – 18h00.

1 - Cadastro

Para que o sistema possa, mais tarde, reconhecer o candidato através de sua digital, é necessário, primeiramente, cadastrá-lo. Isso acontece durante o exame médico. A impressão digital é incluída na ficha virtual do candidato, como mais um dado seu. A impressão digital é capturada três vezes. O sistema escolhe a imagem mais nítida, identifica as minúcias da digital e envia o arquivo para o banco de dados de Detran, o Gefor.

O scanner deve ter resolução superior a 500dpi, para que as vilosidades da pele possam ser capturadas. A transmissão de dados para o computador é feita via USB.

2. Identificação

O arquivo com a impressão digital do candidato é baixado pela escola em que ele faz as aulas teóricas, e incorporado à base de dados local. Antes de iniciar a aula, a escola seleciona no sistema a próxima turma, para que o software agrupe as digitais dos alunos que chegarão.

Assim, quando os alunos encostam o dedo no leitor, a imagem do seu dedo é comparada às que já estão selecionadas. É o processo chamado, em biometria, de "identificação". O computador identifica quem é a pessoa que apresenta aquele dedo, dentre todos os dedos disponíveis para a busca.

Se um aluno da manhã, colocar a digital no leitor e no software tiver sido selecionada a turma da noite, o sistema não o identificará, ainda que sua digital faça parte da base de dados da escola.

Essa foi a tática adotada para reduzir o tempo de processamento dos dados -tão maior quanto a base de arquivos. Em vez de pesquisar a digital de todos os alunos da escola, o sistema só analisa os dados dos que devem comparecer à aula naquele horário.

A configuração mínima para que o equipamento biométrico possa ser instalado é: processador Pentium, placa USB, Windows, versão 98 ou superior, e 64 MB de memória RAM

Em uma auto-escola da capital visitada pela reportagem na semana de implantação da biometria eletrônica, o desempenho do sistema era baixo. Levava-se mais de 1 minuto para o computador receber a imagem da digital coletada no sensor e identificar o aluno. Com cerca de 60 alunos, a auto-escola gastava mais de 1 hora apenas para registrar presença na hora da entrada.

3 - Envio de dados

Em até 5 dias, a escola envia os dados para o Detran, que autoriza os alunos que cumpriram a carga horária obrigatória a fazer os exames.

Controles de Acesso Lógico

Considerando-se que controles de acesso físico não são suficientes para garantir a segurança de informações de um sistema computacional, são necessários controles de acesso lógico, representados por medidas de segurança

implementadas por hardware e por software para impedir acessos não autorizados ao sistema.

O principal objetivo do controle de acesso lógico é o de que apenas usuários autorizados tenham acesso aos recursos computacionais e que esse acesso seja apenas aos recursos realmente necessários à execução de suas tarefas. Isto significa que, usuários devem ser impedidos de executar transações incompatíveis com suas funções ou além de suas responsabilidades.

Na tentativa de acesso ao sistema, entram em ação os controles de acesso lógico, envolvendo o fornecimento da identificação do usuário e de uma senha que serve de autenticação, provando ao sistema que o usuário é realmente quem diz ser. O identificador de cada usuário deve ser único, ou seja, cada usuário deve ter sua identidade própria.
Como autenticação podem ser usadas senhas, cartões inteligentes, características físicas como impressão digital, voz ou retina (características biométricas de uma pessoa).

A identificação baseada em uma característica física do usuário (identificação biométrica) visa suprir deficiências de segurança de senhas que podem ser reveladas ou descobertas e de objetos, como cartões magnéticos ou cartões inteligentes, que podem ser perdidos, roubados ou reproduzidos.

O nível de segurança desejado dependerá muito da forma biométrica escolhida, já que umas são mais seguras que outras.

A identificação utilizando a íris ou a retina são as formas mais eficazes apresentadas até o momento. A relação custo benefício também deve ser levada em consideração na escolha da forma biométrica.

Portanto, os sistemas de reconhecimento biométrico têm sido utilizados tanto nos controles de acesso físico, quanto nos controles de acesso lógicos de um sistema computacional.