PROVENDO SEGURANÇA ATRAVÉS DA BIOMETRIA

Juliana Michele Vicentin[1], Fernanda Ferreira de Barros Barreto[2], Daniele Dickel[3], Patrícia Viturino dos Santos[4]

[1] Gerencia de Arquitetura Tecnológica – Diretoria Tecnológica
Banco do Brasil S.A.
STN 716, Conjunto C, Ed. Sede IV, 1º subsolo, Asa Norte – Brasília – DF – Brasil

[2]Coordenação Geral de Informática – Ministério do Desenvolvimento Social e Combate a Fome
Setor Comercial Sul, Ed. Toufic 6º andar – Brasília – DF – Brasil

[3]Stefanini IT Solutions
SHCGN 712/13 Bloco B Loja 8 – Brasília – DF – Brasil

[4]Brasil Telecom
SNC, Quadra 02, Ed. Telebrasília – Brasília – DF – Brasil

juliana.michele@gmail.com, fernanda.barreto@mds.gov.br,
dani_dickel@hotmail.com, patriciaviturino@ibest.com.br

Resumo. *A biometria é uma das bases do tripé de autenticação do usuário, formado por informações que o indivíduo sabe (senhas), as que possuem (cards ou chaves) e as contidas no próprio corpo, encaixando-se a biometria nesta última categoria. Os dispositivos biométricos vão desde a verificação de digitais, geometria das mãos e leitura de retina e íris até o reconhecimento facial e de padrões de voz. O registro é feito com o auxílio de scanners, leitores óticos ou mesmo gravadores no caso dos padrões de voz.*

"Nos nossos dias, a biometria tem se tornado um assunto polêmico e bastante discutido, devido aos atentados ocorridos nos EUA. O tema Segurança e Identificação Pessoal não é visto mais como futurista e sim como um assunto de extrema importância, sobretudo nos setores de aviação, controle de informações e Internet."

1. A Biometria

Biometria é a ciência que realiza a verificação de identidade, é mais bem definida como sendo as mensurações fisiológicas e/ou características de comportamento que podem ser utilizadas para verificação de identidade de um indivíduo. As mensurações incluem impressões digitais, voz, retina, íris, reconhecimento de face, imagem térmica, analise de assinatura, palma da mão e outras técnicas. Elas são de grande interesse em áreas onde realmente o importante é verificar a real identidade de um indivíduo.

Inicialmente, estas técnicas eram empregadas em aplicações especializadas de alta segurança. Entretanto, agora sua utilização é proposta de uso em uma grande e crescente gama de situações, incluindo utilizações públicas no nosso dia a dia.

2. Origem da Biometria

O primeiro método de identificação biométrico aceita oficialmente foi desenvolvido por Alphonse Bertillon no final do século XVIII. Também chamada de antropometria, o sistema se baseava numa combinação de medidas físicas tiradas de acordo com elaborados procedimentos. As métricas junto com cor de cabelo, de olhos e fotos de frente e de costas eram arquivadas. Bertillon criou 243 categorias.

A técnica foi adotada pela polícia de Paris em 1882 e rapidamente copiada por toda a França e Europa. Em 1887 os Estados Unidos aderiram ao sistema. O fracasso do método de Bertillon deveu-se a dificuldade no armazenamento e na consulta dos dados e ao complicado método para coletar as medidas.

O método de Bertillon foi substituído pelo sistema de impressões digitais, criados pelo oficial britânico William Herschel. Em missão na Índia, Herschel estava descontente com os comerciantes locais, que não cumpriam contratos. O oficial passou a pedir que colocassem além das assinaturas, a impressão das digitais nos documentos. A idéia, segundo o próprio, era "assustar os comerciantes, de modo que não pudessem repudiar sua assinatura".

Outros pesquisadores também começaram a estudar as impressões digitais na mesma época. Em 1870, o cirurgião Henry Faulds começou a vislumbrar nas digitais um caminho para comprovar identidades. Mas a classificação final ficou por conta do oficial Edward Richard Henry, que criou e adotou o sistema em 1897, na cidade indiana de Bengal. O sistema funcionou tão bem que foi adotado em toda Índia.

Pouco tempo depois, um comitê da Scotland Yard testou e aprovou o sistema, implantado na Inglaterra em 1901. O sistema antropométrico de Bertillon estava ultrapassado, apesar de algumas agências o terem usado até a década de 30.

3. Funcionamento da Biometria

Basicamente existem duas formas de se trabalhar com biometria: a primeira é chamada de captura da imagem biométrica e a segunda é chamada de captura de pontos biométricos. Em ambos o caso, é necessário tirar uma "foto" ou imagem digital do usuário e armazená-la em um meio magnético qualquer, que pode ser um banco de dados ou outro dispositivo.

A grande diferença entre as formas de captura são os algoritmos aplicados e a forma de captura da biometria, no primeiro caso, onde aplicamos a captura da imagem

biométrica, é retirada uma imagem da impressão digital do usuário. Essa imagem poderá variar até 70% da imagem original de sua biometria, ou seja, o software de autenticação trabalhará por probabilidades e aproximação da imagem da impressão armazenada. No segundo caso, onde aplicamos a captura de pontos biométricos, o software deverá especificar quais são os pontos de biometria que serão utilizados para gerar a identificação do usuário. Através de um algoritmo matemático tridimensional e gráfico, será possível definir sua identidade, não importando se você está com machucado ou até mesmo esfolamento. Extraindo somente as minúcias significativas para composição de sua identificação, será possível fazer a identificação.

4. Vantagens e Desvantagens

As vantagens deste sistema face aos habituais são inúmeras. Uma delas tem a ver com o fato de as características biológicas serem realmente pessoais e intransmissíveis. Não há forma de dizer o seu código a terceiros ou de lhes emprestar o seu cartão. É a única forma de segurança que implica realmente a presença física da pessoa em causa.

Outro fator importante é o fato de a biometria não estar dependente de um computador específico, na qual o nosso fornecedor já instalou um certificado digital. Com a biometria, não há cookies nem qualquer tipo de vínculo ao computador utilizado. Para David Fernandes, da Proglobo, empresa que desenvolve soluções biométricas, as vantagens deste tipo de sistemas resumem-se em duas palavras: "Segurança e conveniência", as quais não pode existir uma sem a outra.

Mas a biometria também tem suas desvantagens. Quando nos referimos à autenticação em grandes massas de trabalho, sua performance não é tão boa quanto deveria ser. Dependendo da quantidade de usuários em um banco de dados biométrico, a autenticação do usuário se torna lenta e inviável para utilização.

Pensando em todas essas características, foram criados cartões que comportam a tecnologia biométrica e também outros níveis de segurança para as aplicações, não só dos cartões, mas também em redes corporativas e projetos de segurança em geral, tornando um sistema único. O uso de uma quantidade muito maior de informações para cada impressão digital, ao invés da simples verificação de impressões digitais, mostra a capacidade de trabalho dessa tecnologia.

5. Vulnerabilidades

Como qualquer mecanismo de segurança, os dispositivos biométricos estão sujeitos a falhas. São três os tipos de erros:

- Falsa rejeição do atributo físico de um usuário. O sistema não reconhece o padrão mesmo estando correto. É classificado na taxa de falsa rejeição;
- Falsa aceitação de um atributo físico. Neste caso, o sistema aceita a pessoa errada. O tipo de erro é classificado na taxa de falsa aceitação;
- Erro no registro de um atributo físico. São casos onde a variação de características físicas pode dificultar a operação do sistema. Alguém com problemas de voz, por exemplo, pode atrapalhar o funcionamento do dispositivo, aumentando a taxa de erro.

Por isso, dependendo do nível de segurança desejado, especialistas recomendam o uso de pelo menos dois tipos de autenticação. Outro ponto fundamental para tirar melhor proveito das ferramentas é o treinamento/conscientização dos funcionários. Se eles estiverem desconfortáveis com a tecnologia, é provável que os erros apareçam numa taxa superior aos índices considerados normais.

Outra recomendação é de que os sistemas que armazenam dados biométricos devem ser protegidos com o uso de criptografia. No tráfego das informações pela rede é fundamental a implementação de PKI (Public Key Infrastructure) para evitar ataques do tipo "man-in-the-middle".

6. Soluções

A) Verificação de Digitais

No final do século XVIII, um policial britânico estabeleceu a primeira classificação de impressões digitais. Atualmente, a comparação de impressões é feita baseando-se em "minutiae" (características únicas da impressão). Em média, a imagem de uma digital tem entre 30 e 40 detalhes únicos. Segundo estudos do FBI, duas pessoas não apresentam mais do que 8 pontos coincidentes.

B) Geometria das Mãos

Nesse método são usadas medidas das mãos e dos dedos a partir de uma perspectiva tridimensional. Esse tipo de método oferece uma boa performance e é relativamente fácil de ser usado. Já é utilizado no controle de acesso e na verificação de identidades em muitos aeroportos, empresas e usinas nucleares.

C) Padrão de Voz

Esse tipo de reconhecimento envolve a gravação de um "modelo" para o padrão de voz que será usado na autenticação. O usuário deverá repetir determinada frase para que seu padrão de voz seja gravado.

D) Leitura de Retinas

Tecnologia em que os padrões dos vasos sangüíneos da retina são "lidos" por uma luz infravermelha com o auxílio de um leitor ótico. Os vasos absorvem mais rápido a luz que o tecido ao redor, formando uma imagem única que será analisada seguindo alguns pontos característicos. A quantidade de dados obtidos por esse processo é semelhante à da análise através de impressões digitais.

Esse método é bastante preciso, entretanto tem algumas desvantagens. A retina é mais suscetível à doenças como catarata, por exemplo, que alteram as características oculares; O método para obter os dados é bastante inconveniente - a luz deve ser direcionada diretamente para a córnea; A obtenção de uma imagem correta da retina vai depender da habilidade do operador e da capacidade da pessoa que está sendo scaneada em seguir os procedimentos.

A identificação exige que o usuário fixe o olhar em determinado ponto, o que não é muito prático, nem confortável. Por isso, esse método tem pouca aceitação entre os usuários, apesar de sua precisão.

E) Leitura de Íris

Considerado menos intrusivo, esse método baseia-se nas características da íris dos olhos. O usuário deve manter-se à distância de 14 polegadas de uma câmera ccd (usada para criar imagens em bit map). Esse dispositivo não requer contato entre o usuário e a câmera o que o torna mais confortável.

F) Padrões de Assinatura

Esse processo não se baseia apenas na comparação entre as assinaturas, mas sobretudo na dinâmica da assinatura do usuário, velocidade, direção, pressão e tracejado das letras. A restrição desse método é que se baseia no padrão de comportamento. Ninguém assina do mesmo modo sempre, o que permite maior margem de erros na autenticação.

G) Reconhecimento Facial

Dois padrões de tecnologia são aplicados. O escaneamento da imagem num padrão bidimensional, baseado na medida de ângulos e distâncias entre traços da fisionomia como olhos, nariz e boca. No entanto, as medidas podem variar de acordo com o movimento do usuário. Num primeiro momento, a aplicação deste método revelou-se pouco eficaz na identificação de nuances do rosto.

O desenvolvimento da captura de imagens do rosto com uso do padrão tridimensional, entretanto, supre essa deficiência significando a percepção de mais detalhes, como a estrutura óssea ao redor dos olhos e do nariz. Uma vez capturada, a representação em três dimensões pode ser construída a partir de um simples frame de gravação de vídeo. Grupos de defesa da privacidade questionam o uso desses dispositivos.

7. Conclusões

De acordo com uma pesquisa do instituto Meridien Research, feita em janeiro, o uso de mecanismos biométricos tende aumentar nos próximos anos, devido ao barateamento da tecnologia, e devem se tornar cada vez mais integrados a diferentes tipos de hardware. Há pelo menos duas razões apontadas para o sucesso do método: é mais seguro e permite o acesso rápido e descomplicado à informação, sem a necessidade de senhas - muito mais vulneráveis à falhas de segurança.

O estudo revela ainda a divisão do mercado americano por tipo de dispositivo. A verificação de digitais fica com 39%; a identificação pelas mãos com 31% e a de rosto com 7,1%. O scaneamento dos olhos responde por 4,3% e de verificação de assinaturas tem 2,7% do mercado. Dados da organização americana International Biometric Industry Association (IBIA) mostram que no ano 2000 foram gastos 100 milhões de dólares em dispositivos biométricos. A expectativa é de que esse valor chegue a 600 milhões em 2003.

Ser mais segura faz parte da própria natureza da biometria, já que o usuário é identificado por características únicas, pessoais e intransferíveis, que não podem ser roubadas, compartilhadas ou esquecidas, como senhas e cards. Apesar de serem facilmente administradas, as senhas estão longe de manter alto grau de segurança.

Empresas vão desenvolver tecnologia biométrica para integração em futuras versões do Windows. A Microsoft e a I/O Software Inc., empresa líder em software de segurança, sediada em Riverside, na California, EUA, anunciaram sua cooperação para

ampliar o uso da Biometria através da integração da tecnologia de autenticação biométrica nas versões futuras do sistema operacional Windows. A Microsoft adquiriu as tecnologias Biometric API (BAPI) e de autenticação SecureSuite da I/O Software para oferecer aos usuários o mais alto nível de segurança na rede baseado em um método de autorização pessoal confiável. A integração da autenticação biométrica permitirá aos usuários logarem-se em seus computadores e conduzirem transações seguras de e-commerce utilizando uma combinação de impressão digital, da íris ou reconhecimento de voz e um código privativo ao invés de uma senha.

Referências

Dicionário da Lígua Portuguesa

Sites:

www.timaster.com.br

www.fingersec.com.br

www.modulo.com.br