Como funciona a leitura biométrica?

Biologia & Ciências

Enviado por: _rogeriofvi@seed.pr.gov.br

Postado em:17/10/2012

Fonte: Rafael Moco / TechTudoNa tentativa de aumentar a segurança de seus clientes, alguns bancos brasileiros têm adotado sistemas de leitura biométrica em caixas eletrônicos e agências. Mas será que esses sistemas realmente eliminam por completo as chances de fraudes?Nenhum sistema de segurança é totalmente livre de falhas, costumam dizer os analistas do ramo. Não há como negar tal afirmação. O tempo passa, e as informações sobre senhas roubadas e acesso não autorizado a contas em bancos só aumenta, sempre partindo de diferentes direções.Como eles funcionam?Existem diferentes sistema de reconhecimento biométrico disponíveis, cada um levando em conta alguma característica específica do usuário. É possível analisar o timbre de voz, o formato da íris de um olho, a assinatura de um cliente e até mesmo a geometria das veias de uma mão. Cada um possui suas próprias particularidades, como você vai conferir a seguir:Escaneamento da impressão digital: Sem dúvidas, o dado biométrico mais conhecido, por conta da sua presença frequente em filmes e séries. Como alguns já devem saber, cada ser humano possui sua própria digital, não se repetindo de qualquer forma em outra pessoa. Apesar de visualmente semelhantes, cada uma possui um padrão de linhas e curvas, e é justamente estas diferenças que são utilizadas nos sistemas de segurança.Tudo o que o sistema faz é entender os padrões da impressão digital utilizada e criar uma espécie de código único que represente estas linhas e curvas. Para isso, alguns sistemas utilizam equipamentos capazes de tirar fotos em altíssimas resoluções somente das digitais, enquanto outros contam com uma superfície super sensível, ao ponto de conseguir detectar as linhas e sulcos dos dedos, de forma individual. Toda esta tecnologia permite uma leitura quase sempre livre de erros, garantindo assim a segurança dos usuários.Geometria vascular: Como o nome indica, o sistema de geometria vascular detecta a posição das veias do usuário, capturando este padrão e convertendo-o em um código único. Geralmente ele utiliza como base a palma da mão de seus usuários, em um processo de escaneamento bastante simples.Uma câmera especial tira uma foto utilizando uma luz infravermelha. A hemoglobina presente no sangue absorve esta luz, fazendo com que as veias apareçam escuras na foto tirada. Com base nesta captura, o software cria um padrão único, garantindo assim o reconhecimento do usuário.Escaneamento caligráfico: Não é de hoje que a assinatura de uma pessoa é utilizada como forma de garantir a autenticidade de um documento ou até mesmo sua identidade. Porém, o sistema de verificação de assinatura ou escaneamento caligráfico, age de forma muito mais precisa.Os sensores de reconhecimento de caligrafia detectam não só a forma escrita, mas também como ela é escrita. É medida até mesmo a pressão da caneta durante o processo, de uma forma que dados suficientes sirvam para que um padrão de detecção único seja criado. Isso evita, por exemplo, que uma assinatura possa ser falsificada por alguém habilidoso.Teste de timbres de voz: Você já deve ter ouvido que cada ser humano possui seu próprio timbre de voz. E apesar de algumas pessoas terem uma capacidade incrível de imitar a voz de outra pessoa, é praticamente impossível reproduzir com exatidão todas as nuances presentes em um mesmo timbre.O que este sistema faz é justamente medir, por meio de um espectrograma, a frequência do som emitido por uma voz no eixo horizontal e vertical. A principal qualidade deste método é permitir que uma pessoa possa provar sua identidade à distância, sem a necessidade de estar frente a frente com o equipamento de reconhecimento, como ocorre com o sistema de detecção dos padrões da íris por exemplo. Por isso mesmo, é um método

que pode dar margens a fraudes, e dificilmente seria utilizado em um caixa eletrônico, por exemplo.Escaneamento da Íris: Há muito tempo atrás, utilizava-se um sistema que refletia uma luz na retina do usuário, e garantia sua identificação por conta do padrão de reflexos obtidos. Este método acabou se mostrando ineficiente com o passar do tempo, já que a retina de algumas pessoas acabou sofrendo modificações, levando a leituras inexatas. Porém, o exame da Íris acabou se mostrando muito mais eficiente.O que ele faz é simplesmente tirar uma foto em alta resolução da íris do usuário, analisando seu modelo visualmente e traduzindo em seguida os padrões obtidos em um código único. Este tipo de sistema tem se tornado cada vez mais comum, e alguns bancos já estudam a possibilidade em adotá-lo como medida de segurança em caixas eletrônicos e agências.Mas será que isso é o suficiente para garantir a segurança?O mercado de leitura biométrica tem aumentado junto com a necessidade constante de segurança de dados pessoais. No Brasil, já existem alguns bancos que contam com leitores biométricos em seus caixas. Mas apesar da tecnologia avançada, ela acaba servindo de complemento na hora de assegurar a identidade do usuário.Outro ponto importante é que, hoje em dia, é bem difícil burlar qualquer um destes sistemas. Existem sim, técnicas bem avançadas que podem ou não resultar na quebra de identidade, mas a maioria é complexa demais para que sejam adotadas por qualquer um.No fim, vale lembrar que qualquer aumento na segurança é válido, já que isso pode reduzir bastante os prejuízos no caso de roubo de cartão de crédito, dentre outros eventos. Pode até ser mais complicado usar caixas eletrônicos com sistemas deste tipo, mas é melhor prevenir do que remediar, não é verdade?Esta notícia foi acessada no dia 17/10/2012 no site TechTudo. Todas as informações são de responsabilidade do autor.