4 Dedos São Melhor Que Um

Uma Renovação no Reconhecimento de Mão

VERIDIUM
HANDS ON SECURITY

Segurança na Palma da Sua Mão

Mais Companhias de serviços financeiros estão aderindo à biometria para autenticação de usuários em aplicativos todos os dias. De Visa a bancos pequenos, usar a impressão digital para validar um pagamento ou transferência é muito mais seguro do que simplesmente uma senha. Mas um dos primeiros bancos virtuais, bunq, escolheu um recurso biométrico ainda mais seguro – o reconhecimento da mão.

O bunq precisava de um jeito fácil e conveniente de autenticar transações que eram de alta segurança. Eles optaram por um tipo de biometria que eliminava riscos de segurança e ainda assim era fácil e conveniente de usar – O 4 Fingers Touchless ID.

Agora, não importa quando um cliente bunq quer realizar uma transação que requeira um alto nível de segurança, ele é solicitado a escanear suas 4 impressões digitais para autenticação. Isto combina a facilidade de uso, experiência descomplicada com a otimização prática de segurança.

Nós escolhemos 4 Fingers com a Veridium ID porque ele atende nossa garantia de uma experiência bancária fácil e segura usando tecnologia de autenticação biométrica de ponta no Mercado.

- Ali Niknam, CEO e Fundador do bunq

O Nascimento da Digitalização da Impressão Digital

Enquanto o uso moderno de impressões digitais existe desde o final dos anos 1800, a invenção do computador e a digitalização de imagens é o que realmente levou à adoção em massa de impressões digitais como ferramenta de segurança. Movendo-se para além do uso de impressões digitais pelas autoridades para identificar criminosos, a digitalização de imagens digitais permitiu que os sistemas de segurança biométrica fossem construídos. Os primeiros modelos eram grandes e caros, exigindo sistemas de computador caros embarcados em scanners de mão montados na parede ou numa mesa, mas funcionavam. Você pode perder uma chave ou esquecer uma senha, mas você sempre tem sua biometria na mão.

No entanto, o nascimento da comunicação global e a ascensão do computador forneceu o catalisador necessário para lançar impressões digitais em uma tecnologia cotidiana, onde usamos para desbloquear uma ferramenta que os primeiros adeptos da impressão digital não poderiam sonhar em ter - os computadores em miniatura que carregamos em nossos bolsos.

A Ascensão da Biometria Mobile

Quando a Apple lançou o iPhone, a empresa revolucionou a industria do celular. Movendo-se além de telefonemas e mensagens de texto para poder ler e-mails, ouvir música e fazer download de jogos em um único dispositivo foi uma virada de jogo, e é fácil esquecer que foi há apenas 10 anos que este incrível dispositivo foi lançado.

Certamente a Apple não inventou o smartphone, mas eles criaram o primeiro popular, fácil de usar, amplamente adotado, e essa tendência seria transferida para a adição de sensores biométricos para dispositivos móveis. Em 2013, a Apple mais uma vez entregou uma tecnologia revolucionária com o Touch ID. Na época, o iPhone já era o smartphone mais vendido, e essa popularidade generalizada significava que milhões adotariam a autenticação de impressão digital móvel praticamente de um dia para o outro.

O Touch ID ofereceu aos consumidores cuja única experiência com biometria estava nos filmes a oportunidade de usar a tecnologia em primeira mão e ficar confortável com isso. Sobre tempo, a Apple expandiu seu uso para além de apenas desbloquear o iPhone para permitir recursos de segurança e autenticação em Transações ApplePay e outras fabricantes adotaram a mesma característica. No entanto, o sensor de impressão digital do celular está muito atrás em relação a segurança da mais tradicional captura digital de impressões digitais.

O Que há de Errado com o Touch ID?

Há vários problemas com o Touch ID e seus semelhantes baseados no Android. Estas fraquezas na tecnologia, enquanto eles não negam seu uso como uma ferramenta biométrica, deve deixar com o pé atrás aqueles que estão pensando em implantar biometria mobile para mais necessidades avançadas de segurança.

Sensores de Impressão Digital Embarcados Capturam parcialmente a Impressão Digital

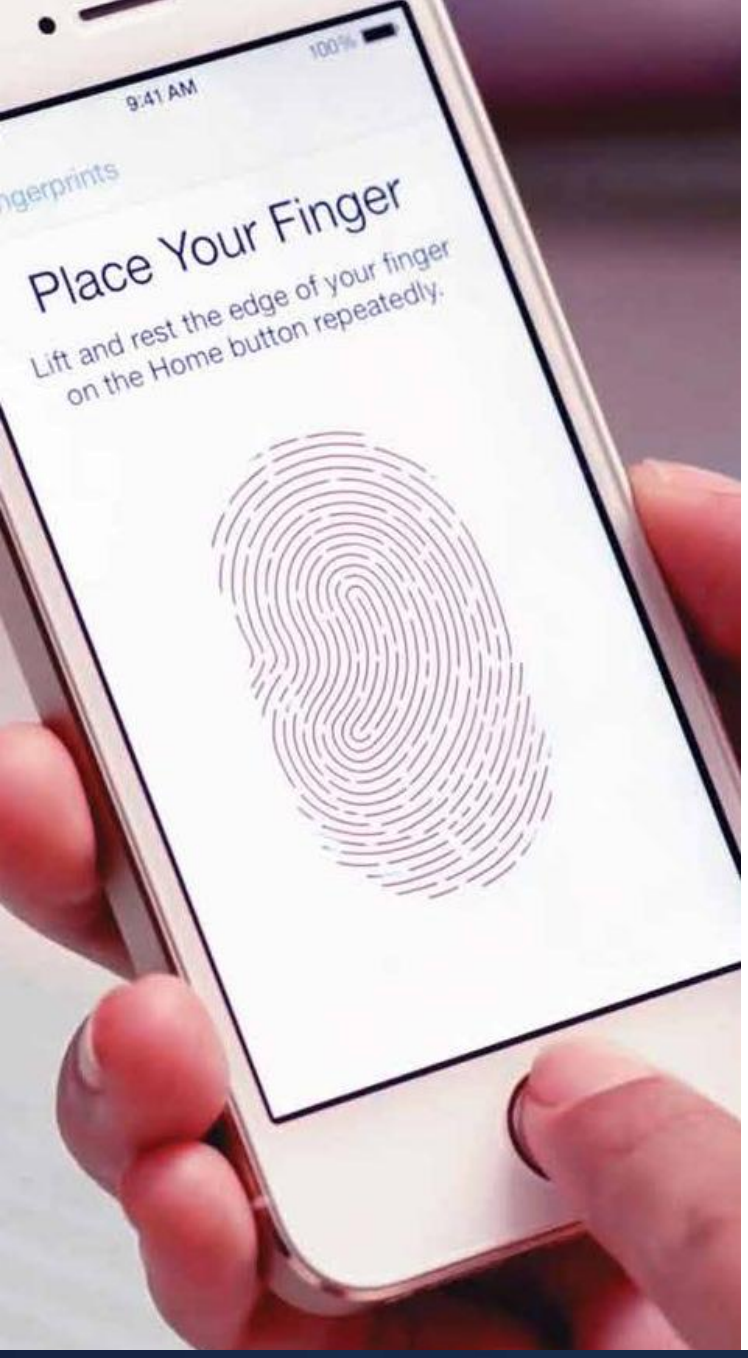
Os sensores de impressão digital usados nos celulares são, por necessidade, muito pequenos. Se você olhar para os botões em que eles estão incorporados, eles são fração do tamanho da nossa ponta do dedo. Isso só permite autenticar uma pequena parte das minúcias na ponta do dedo. Em última análise, isso significa que o número de pontos que podem ser comparados para autenticar a impressão digital é muito menos do que nas impressões digitais tradicionais, o que torna a biometria menos precisa e, pior ainda, mais fácil de falsificar.

As minúcias são os principais pontos de interesse em uma impressão digital, incluindo as bifurcações (uma linha dividida em duas) e terminações de linha, bem como quaisquer cicatrizes ou outras características distintivas.

Impressões Digitais Parciais São Vulneráveis a Ataques

O molde de uma impressão digital, mais conhecido como molde de silicone, é um dos métodos de ataque mais comuns para biometria. Na maioria dos casos, fazem uso de uma cópia, seja uma foto ou molde da impressão digital de uma pessoa para enganar um sistema de autenticação biométrica e liberar o acesso. Há uma variedade de técnicas usadas para parar este tipo de ataque, mas os pesquisadores mostraram que driblar um sensor de impressões digitais de um celular é algo muito fácil.

Em 2016, os pesquisadores de ciência da computação Kai Cao e Anil Jain, da Universidade do Estado de Michigan, mostraram que é possível falsificar um sensor de impressão digital de um celular por menos de U$ 500, usando uma impressora comum e tinta condutiva. O processo leva apenas 15 minutos e requer uma imagem com qualidade de 300 dpi da impressão digital em questão. O que faz este processo de falsificação ser especial é que o uso da tinta condutiva ignora as verificações de dedo vivo do dispositivo.



A Usabilidade é Determinada Pelo Dispositivo

Outra desvantagem para as soluções de impressão digital existentes para celular é que o uso da impressão digital capturada é muitas vezes fortemente afetado pelo dispositivo que você possui. O Apple ID de toque funciona apenas com uma seleção de aplicativos da Apple e de terceiros, e o mesmo vale para os vários equivalentes no Android. Isso faz o seu uso fora da segurança pessoal e autenticação extremamente limitado. Por exemplo, mesmo que sua empresa integre a API do Touch ID em um aplicativo corporativo para usá-lo como uma solução de segurança para entrar no email da empresa, nem todo funcionário terá um iPhone, limitando seu uso em toda a organização.

Como a adoção de segurança biométrica em dispositivos móveis continua a crescer, indivíduos e empresas precisam de uma solução biométrica que permita um maior nível de segurança. Isso pode ser alcançado através do aumento do número de minúcias capturadas, muito além de uma impressão digital parcial, ou mesmo uma única impressão digital, com o reconhecimento de mão.

Por Que Reconhecimento de Mão?

O reconhecimento de mão, ou a captura de todas as quatro impressões digitais de uma vez, fornece significativamente mais detalhes e, portanto, complexidade, para autenticação biométrica. Quanto mais complexa a biometria, mais difícil é falsificar e, com mais precisão ele pode autenticar o usuário, reduzindo taxas de falsa rejeição. Com o reconhecimento de mão você pode capturar quatro impressões digitais em uma única captura, multiplicando o número de minúcias exponencialmente para segurança.

Taxa de Falsa Aceitação (FAR) - A probabilidade de um sistema de segurança biométrica aceitar a tentativa de autenticação por um usuário não autorizado. FAR normalmente é descrito como a razão entre o número de falsas aceitações dividido pelo número de tentativas de identificação.

Taxa de Falsa Rejeição (FRR) - A probabilidade de um sistema de segurança biométrica rejeitar a tentativa de autenticação por um usuário autorizado. FRR normalmente é descrito como a razão entre o número de falsos reconhecimentos dividido pelo número de tentativas de identificação.

Por exemplo, a média de FAR para o 4 Fingers Touchless ID é de 0,1%, com um FRR de 1%.

	UNIVERSALIDADE	UNICIDADE	PERMANÊNCIA	COLECTABILIDADE	PERFORMANCE	ACEITABILIDADE	SEGURANÇA
	MÉDIA	ALTA	ALTA	MÉDIA	ALTA	MÉDIA	MÉDIA
	ALTA	ALTA	ALTA	ALTA	ALTA	ALTA	ALTA

Reconhecimento de mãos via Mobile é o Próximo Passo

Claro, a primeira pergunta que você está fazendo é: mas se o sensor de impressão digital no meu smartphone captura apenas uma impressão digital parcial, como faço o reconhecimento de mãos? Simples, não usando o sensor embutido.

A chave para realizar o reconhecimento de mão *mobile* é usar um dos mais poderosos sensores já no dispositivo, em vez de um sensor dedicado de impressão digital – a câmera. As câmeras modernas para smartphones são mais do que poderosas para capturar fotos com alta qualidade suficiente para extrair minúcias de impressões digitais. Isso permite uma captura de impressões digitais sem contato e reconhecimento de mão em qualquer smartphone, com integração perfeita com o aplicativo certo em toda a equipe de uma empresa ou base de clientes.

O mesmo dispositivo pode permitir o reconhecimento facial usando a câmera frontal, mas há desvantagens em usar um tipo de biometria que não é tão difundido como reconhecimento de impressões digitais. Por um lado, os algoritmos de reconhecimento facial não são tão precisos quanto as impressões digitais por natureza. Em segundo lugar, a câmera frontal na maioria dos smartphones não é tão poderosa quanto a câmera traseira, que é usada para reconhecimento de mão, garantindo mais detalhes capturados na imagem. Também é mais fácil obter falsas rejeições devido a problemas com o ambiente. Problemas como pouca iluminação. Usando sua mão, a câmera traseira e um flash de LED você pode eliminar a iluminação e outros problemas do ambiente ao usar uma biometria confiável em primeiro lugar.

	UNIVERSALIDADE	UNICIDADE	PERMANÊNCIA	COLECTABILIDADE	PERFORMANCE	ACEITABILIDADE	SEGURANÇA
	ALTA	BAIXA	MÉDIA	ALTA	BAIXA	ALTA	BAIXA
	ALTA	ALTA	ALTA	ALTA	ALTA	ALTA	ALTA

Apresentação: 4 Fingers TouchlessID

Tomando as vantagens combinadas de reconhecimento de mão e o potencial das modernas câmeras de smartphones, percebemos que há a necessidade de uma biometria poderosa que não exige que o usuário toque em um sensor e seja compatível com uma ampla variedade de dispositivos, em vez de um único fabricante. O reconhecimento de mão forneceria uma muito mais poderosa e segura biometria *mobile*, e tornando-a sem toque, seria extremamente conveniente para o usuário realizar a autenticação.

4 Fingers TouchlessID.

Vantagens do 4 Fingers TouchlessID

Há muitas vantagens no 4 Fingers TouchlessID. É rápido e fácil de usar. Você não precisa de nenhum hardware especial no dispositivo *mobile*, apenas uma câmera de no mínimo 5MP e um flash de LED, tornando-o compatível com smartphones mais antigos que podem não ter um sensor de impressão digital. Isso oferece uma variedade de casos de uso de alto valor para:

- **Uma autenticação biométrica mais segura em transações bancárias via app.**
- **Aplicação da lei para capturar impressões digitais em campo.**
- **Hospitais para fornecer uma maneira sanitária de autenticar em estações de trabalho (sem contato)**
- **Adicionando camadas adicionais de segurança aos sistemas biométricos corporativos existentes**

Na verdade, estamos trabalhando em parceria com o Instituto Nacional de Padrões e Tecnologia para incluir o 4 Fingers TouchlessID em seu programa de certificação federal com captura sem contato de impressões digitais, configurando-o para se tornar um padrão em algumas dessas áreas, como aplicação da lei e imigração.

Conclusão

O desenvolvimento de um reconhecimento de mão fácil de implantar será um importante ponto de partida tanto na adoção como na aceitação da autenticação biométrica. Com suporte para as mais avançadas demandas por segurança e compatibilidade universal com a maior gama de dispositivos, mais empresas vão aderir a autenticação biométrica para as suas necessidades de acesso seguro. Usando biometria como parte de uma solução de login do Active Directory ou como parte de um aplicativo *mobile* para validar transações financeiras, você precisa de um recurso seguro, conveniente e flexível, como o reconhecimento de mão, para atender estes inúmeros casos.

VERIDIUM
HANDS ON SECURITY
www.VeridiumID.com
info@VeridiumID.com

100 Hancock Street
10th Floor
Quincy, MA 02171
877.301.0299

Distribuidor Autorizado no Brasil:
Computer ID Soluções em Informática
info@computerid.com.br
www.computerid.com.br