White Paper

Lidando com a crescente ameaça de ataques de apresentação, “deepfakes” e “morphs”

AWARE

781.687.0300 | sales@aware.com | www.aware.com

A Aware é uma empresa líder global de produtos de software e soluções para identificação e autenticação biométrica. Os mesmos são utilizados em uma variedade de aplicações, incluindo serviços financeiros, segurança empresarial, gestão de fronteiras e segurança pública. A Aware é uma empresa de capital aberto (NASDAQ: AWRE) com sede em Burlington, Massachusetts.

É de vital importância para as organizações garantir meios para proteger seus sistemas, ativos e dados, próprios e de clientes, contra ameaças externas e acesso indesejado. No mundo de hoje, isso fica ainda mais evidente com a apropriação indevida da identidade de terceiros em um nível nunca antes visto, e com as violações de sistemas e dados crescendo em torno de 17%[1] desde 2020.

Historicamente, senhas formam a espinha dorsal da maioria dos métodos de autenticação e das medidas de segurança para a proteção do acesso a sistemas e dados. Porém, com 61%[2] das violações ocorrendo como resultado de senhas fracas ou roubadas, as organizações estão procurando alternativas mais seguras. A autenticação biométrica, que aproveita as características físicas únicas de uma pessoa para conceder acesso a informações ou benefícios em geral, praticamente elimina os problemas associados aos métodos de autenticação baseados em senha, fornecendo uma alternativa muito mais segura e conveniente

Porém, uma vez estabelecido este novo patamar de segurança, baseado em autenticação biométrica, "hackers" e pessoas com a intenção de cometer fraudes surgem com novos métodos de ataque. Esses métodos incluem ataques de apresentação, "deepfakes" e "morphs", cujos aumento de frequência tem chamado a atenção das organizações. Porém, tem havido muita confusão a respeito desses métodos e sobre o qual a ameaça que os mesmos realmente representam. Organizações bem informadas sobre a natureza de cada uma dessas ameaças, e de como elas tem evoluído, podem se proteger com eficácia e garantir que os ativos de seus clientes permaneçam assegurados.

Como funcionam, o que são, e qual a motivação dos ataques de apresentação

Também conhecidos como "spoofs", os ataques de apresentação são tentativas de partes mal-intencionadas de subverter os sistemas biométricos. Os ataques de apresentação geralmente envolvem um fac-símile de um usuário autorizado sendo apresentado a um dispositivo de imagem, geralmente uma câmera conectada a um aplicativo ou "software" biométrico. O objetivo do usuário não autorizado é induzir o dispositivo de imagem a "acreditar" que está lendo o rosto, a íris ou a impressão digital de uma pessoa autorizada para que ela possa obter acesso de forma fraudulenta.

O tipo mais simples de ataque de apresentação se dá através de uma representação do indivíduo alvo da fraude, como uma fotografia física ou a imagem do mesmo sendo exibida na tela de um dispositivo digital. Aqui, o invasor usa uma foto em vez de seu próprio rosto durante o processo de reconhecimento facial, na esperança de que o "software" biométrico seja enganado e pense que ele é a pessoa autorizada.

Tentativas mais sofisticadas envolvem máscaras 2D ou 3D em vez de uma foto. Aqui, um invasor cortaria os olhos de uma fotografia e apresentaria seu rosto ao dispositivo de imagem ou até mesmo produziria uma máscara 3D especificamente para essa finalidade. A esperança aqui é que a vivacidade dos olhos e, pelo menos no caso das máscaras 3D, a qualidade da máscara, aumentassem as chances de enganar o "software" biométrico.

Um terceiro tipo de ataque de apresentação envolve gravações de vídeo no lugar de fotografias ou máscaras. Aqui, um invasor obtém uma gravação de vídeo de um indivíduo autorizado e a apresenta ao dispositivo de capture de imagens, geralmente em um dispositivo móvel, como um tablet ou smartphone. Ao fornecer uma imagem em movimento do indivíduo real, o fraudador espera que o dispositivo seja enganado e pense que a gravação exibida é do usuário autorizado.

Os “deepfakes” e ataques de injeção

A proliferação dos “deepfakes” aumentou significativamente nos últimos anos, assim como o entendimento de que eles continuam evoluindo com o passar do tempo. Originalmente, os “deepfakes” se referiam ao processo pelo qual os algoritmos de “deep learning” criavam, de forma sintética, uma versão animada de uma pessoa a partir de imagens estáticas da mesma. Esses algoritmos posteriormente possibilitariam criar animações realista em vídeo, de forma a simular falas e comportamentos associadas àquela pessoa. Exemplos comuns incluem vídeos de autoridades políticas e celebridades dizendo coisas que na verdade não disseram, criando grande preocupação com a desinformação e as “fake news”, e trazendo os “deepfakes” para o conhecimento do público em geral.

Atualmente, “deepfakes” normalmente se referem a qualquer geração sintética de uma imagem de uma pessoa, independentemente de como ela foi produzida. Além disso, a tecnologia em torno dos “deepfakes” tem evoluído rapidamente, com melhor qualidade, aparência mais realista e tempo de criação mais rápido. Essas melhoras têm representado uma ameaça crescente aos métodos de autenticação biométrica.

“Hackers” ou indivíduos mal-intencionados podem tentar utilizar “deepfakes” para comprometer as medidas de segurança biométrica de duas maneiras diferentes. A primeira seria simplesmente reproduzir um vídeo do “deepfake” para o dispositivo de imagem, como em ataques de apresentação de vídeo. O segundo seria um tipo inteiramente novo de método de ataque, ou seja, ataques de injeção. Esse tipo de ataque se propõe a substituir a informação oriunda do dispositivo de imagem injetando a informação “deepfake” no próprio “software”. O objetivo é convencer o programa a aceitar a entrada como válida e alterar a execução do programa. Nesse cenário, essa execução resultaria na concessão de acesso ao usuário não autorizado.

Portando, os “deepfakes” não são uma categoria de ataques à parte. Em vez disso, os “deepfakes” podem ser empregados como um ataque de apresentação semelhante a fotos e máscaras, ou como ataques de injeção que fornecem informações de origem não confiável ao “software” biométrico. Os ataques de apresentação e injeção exigem diferentes tipos de contramedidas, respectivamente de ordem biométrica e de segurança de sistemas.

Os ataques “morph” e o que os torna diferentes

“Morphs” são outro tipo de método de ataque biométrico cuja incidência cresceu nos últimos anos. Simplificando, os metamorfos utilizam a tecnologia para combinar os rostos de dois ou mais indivíduos na criação de um rosto novo e único, porém artificial. Frequentemente, o objetivo dos “morphs” é comprometer o reconhecimento facial combinando os recursos faciais de um usuário autorizado com os de um usuário não autorizado. Como há elementos do rosto de cada pessoa no “morph”, o reconhecimento facial poderia, em tese, ser enganado para fornecer acesso de forma fraudulenta.

“Morphs” podem ser usados para a obtenção de documentos de identidade, como passaportes, para indivíduos que não poderiam obtê-los de forma legal. Nesse caso, um “morph” seria criado combinando as semelhanças da pessoa que não pode obter um passaporte com uma pessoa que pode. que o passaporte fosse obtido, o viajante não autorizado poderia usá-lo na tentativa de burlar a segurança da fronteira.

Outro exemplo envolve “hackers” criando “morphs” de usuários já autorizados com eles mesmos – os fraudadores – para enganar o reconhecimento facial e conceder-lhes acesso. Dessa forma, os “morphs” são muito semelhantes aos ataques de apresentação e “deepfakes” descritos acima. Assim como os “deepfakes”, os “morphs” não devem ser considerados como uma categoria própria. Em última análise, esses ataques também se enquadram em ataques de apresentação ou de injeção, e as organizações se beneficiarão se alinharem os recursos corretos para combater essas duas categorias.

Protegendo organizações contra ataques de apresentação e injeção

Felizmente, existem opções disponíveis para as organizações que procuram proteger seus sistemas, dados e ativos das ameaças em constante evolução, como as descritas acima:

Detecção biométrica de vivacidade

Ao implementar ou melhorar uma solução de autenticação biométrica, a inclusão da detecção de vivacidade é vital em qualquer cenário em que a segurança seja fundamental. Simplificando, a detecção de vivacidade determina se o usuário é uma pessoa viva, e fisicamente presente em relação ao dispositivo de imagem, ou se é uma um ataque de apresentação tentando violar o sistema. Ele serve como uma linha de defesa muito importante contra qualquer ataque de apresentação, seja uma simples fotografia impressa, seja um vídeo "deepfake" ou "morph", graças à sua capacidade de distinguir uma pessoa viva de um fac-símile de uma pessoa viva.

Como a conveniência do usuário também é uma consideração importante ao implementar novos recursos de segurança, a detecção de vivacidade pode ser determinada através de um processo totalmente passivo. Embora alguns detectores de vivacidade requeiram que o usuário siga uma série de instruções, como virar a cabeça, ou piscar os olhos, detecção de vivacidade altamente eficaz também pode ser realizada de forma transparente, sem incomodar o usuário de forma alguma. Para organizações comprometidas em se proteger contra ataques de apresentação, a detecção passiva de vivacidade é a combinação ideal de segurança e conveniência.

Segurança de software

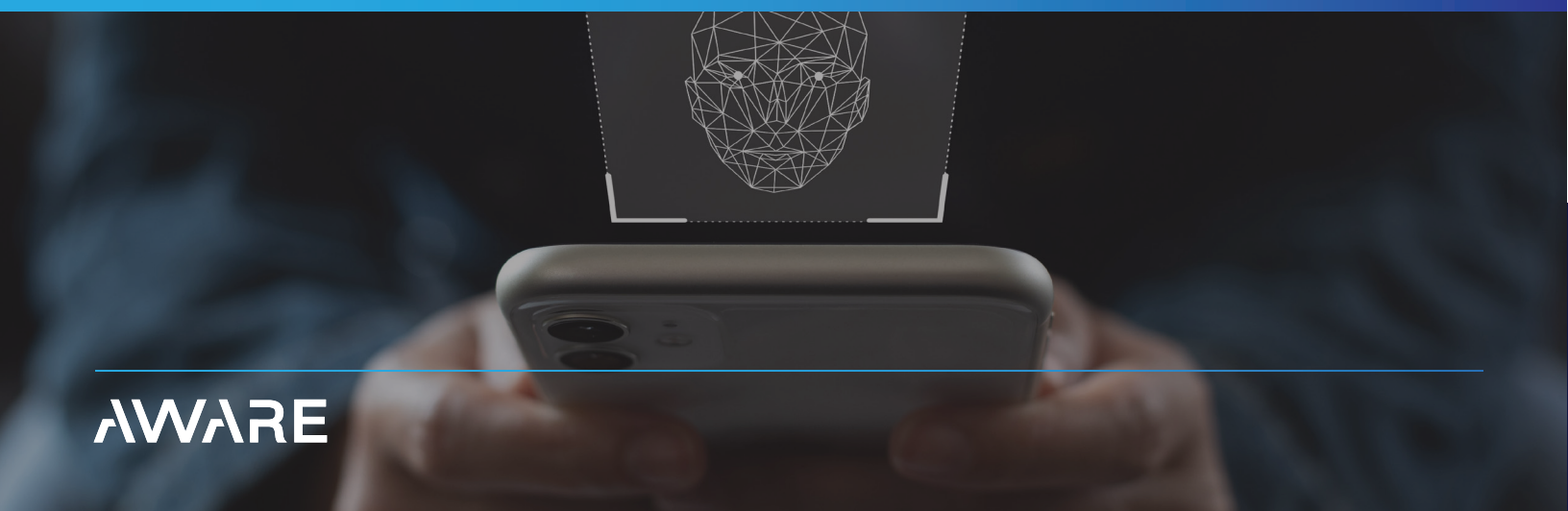
Embora os ataques de apresentação possam ser tratados com detecção de vivacidade biométrica, os ataques de injeção – sejam eles "deepfakes", "morphs" ou qualquer outro tipo de ataque que vise introduzir dados não obtidos através de entrada confiável (por exemplo, não oriundos da câmera do dispositivo móvel) no aplicativo ou "software" biométrico – podem ser tratados totalmente fora do domínio biométrico. Em última análise, os ataques de injeção devem ser endereçados através de medidas de segurança de "software".

As organizações podem detectar vulnerabilidades de injeção em seu sistema e evitar ataques por meio de uma variedade de métodos de teste, software e produtos projetados exatamente para essa finalidade. Profissionais de segurança experientes e treinados nesses tipos de ataque de injeção podem proteger as organizações que queiram se prevenir contra essas ameaças em evolução.

Adicionando outros impedimentos

Embora essa categoria possa variar muito com base nas políticas individuais da empresa, adicionar impedimentos aos seus procedimentos de autenticação também pode servir como uma forte linha de defesa. Exemplos de impedimentos comuns incluem bloquear usuários de uma plataforma após várias tentativas malsucedidas, limitar o número de tentativas de acesso para bloquear endereços IP de fraudadores conhecidos.

Embora esses impedimentos não sejam tão poderosos quanto a detecção biométrica e as medidas de segurança de "software", eles são fáceis de implementar, podem ser empregados de várias maneiras diferentes e podem servir como um meio simples de induzir os "hackers" a acreditar que simplesmente não vale a pena o esforço.



Detecção de vivacidade segura e conveniente com Knomi®

Para empresas e organizações que procuram proteger seus sistemas, ativos, e dados, próprios e de seus clientes, contra ataques de apresentação, o Knomi® da Aware é uma solução ideal. O Knomi fornece uma solução de vivacidade robusta, para uma vasta gama de dispositivos, que é verdadeiramente passiva e transparente para o usuário, proporcionando uma experiência conveniente, que, ao mesmo tempo, não dá pistas ao fraudador de como comprometê-lo.

Quer saber mais? www.aware.com/pt/knomi/

Fontes:
1 - https://www.idtheftcenter.org/post/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020
2 - https://www.verizon.com/business/resources/reports/dbir/

AWARE

© 2022 Aware, Inc. Todos os direitos reservados. Este documento é somente para fins informativos e está sujeito a alterações sem aviso prévio. A Aware, Inc. não assume nenhuma responsabilidade pela acuracidade das informações aqui apresentadas. A AWARE NÃO OFERECE GARANTIAS, EXPRESSAS OU IMPLÍCITAS, NESTE DOCUMENTO. "Aware" é uma marca registrada da Aware, Inc .. Referências a outras empresas e marcas, nomes de produtos e serviços são marcas comerciais, marcas de serviço, marcas registradas ou marcas de serviço registradas de seus respectivos proprietários.

Presentation-Attacks-Knomi_White-Paper_Portuguese