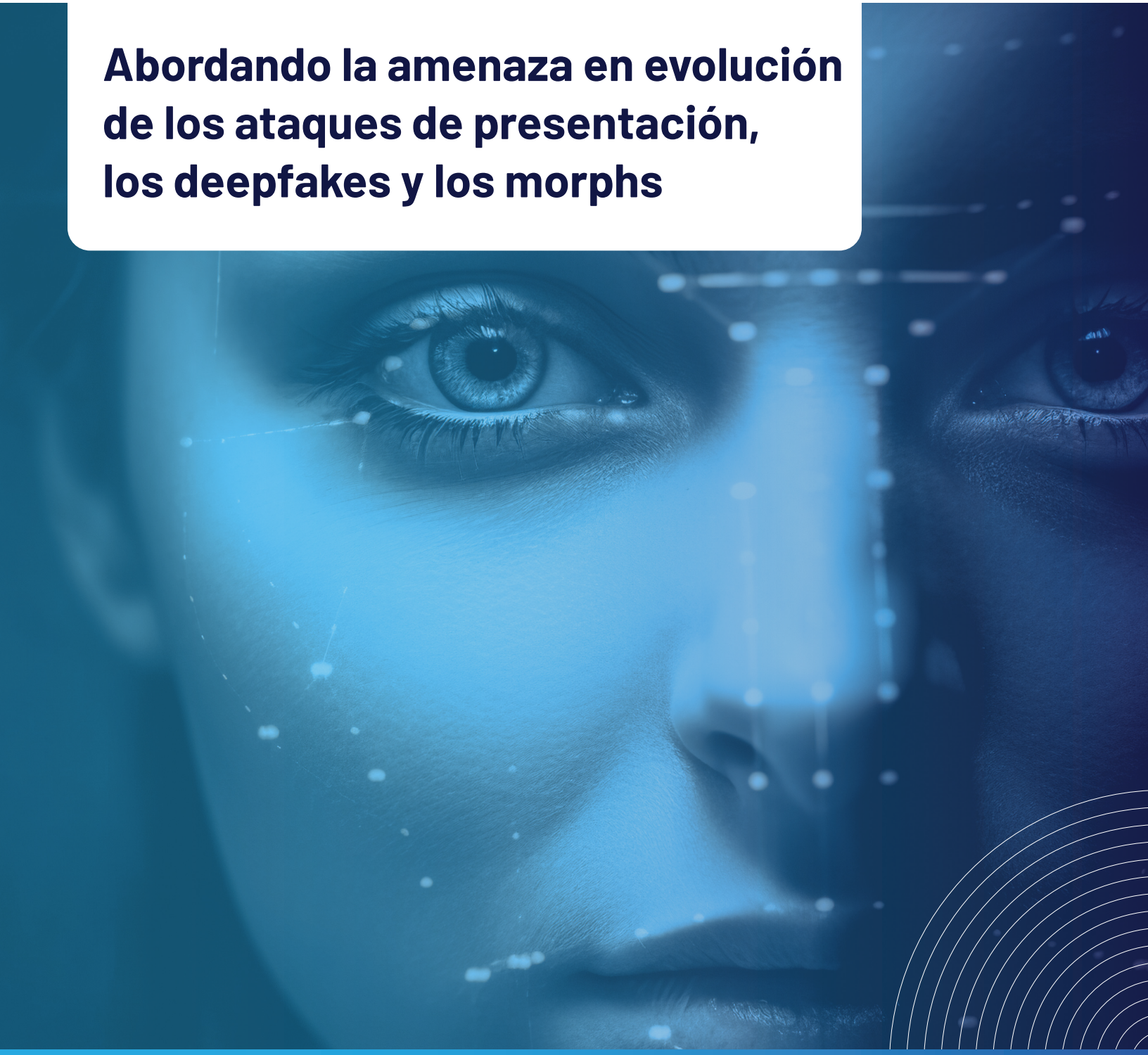
White Paper

Abordando la amenaza en evolución de los ataques de presentación, los deepfakes y los morphs



AWARE

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

Aware es el principal proveedor mundial de productos y soluciones biométricas. Las soluciones de gestión y verificación de identidad de Aware son utilizados en servicios financieros, seguridad empresarial, atención médica, recursos humanos, identificación de ciudadanos, control de fronteras, cumplimento de la ley, defensa e inteligencia. La tecnología Aware líder en la industria ayuda a las organizaciones a recopilar, administrar, procesar y comparar imágenes y datos biométricos para la ayuda de identificación y autenticación.

Siempre ha sido de importancia vital proteger los activos sensibles y valiosos de las organizaciones y sus clientes de amenazas externas y accesos no deseados. En el mundo actual, esto es aún más pronunciado con el robo de identidad en su nivel más alto de todos los tiempos y las filtraciones de datos aumentando en un 17%[1] solo desde 2020.

Las contraseñas suelen formar la fuerza de la mayoría de los métodos de autenticación de seguridad de acceso, pero con el 61% de las filtraciones de datos como resultado de contraseñas débiles o robadas[2], las organizaciones buscan alternativas más seguras. La autenticación biométrica, que aprovecha las características físicas únicas de una persona para otorgar acceso a información o activos seguros, elimina virtualmente los problemas asociados con los métodos de autenticación basados en contraseña, brindando a las organizaciones una alternativa mucho más segura.

Sin embargo, ahora que se está produciendo un cambio de la autenticación basada en contraseña a la biométrica para mejorar la seguridad, los piratas informáticos externos y las partes maliciosas han intentado hacer lo mismo con nuevos métodos de ataque diseñados para frustrar estas medidas de seguridad mejoradas y obtener acceso de manera fraudulenta. Estos métodos incluyen ataques de presentación, deepfakes y morphs, y su aumento en frecuencia ha resultado en una mayor conciencia y temor sobre ellos. Afortunadamente, existen muchos conceptos erróneos sobre estos métodos y la amenaza que realmente representan. Las organizaciones armadas con información sobre cada una de estas amenazas en evolución pueden protegerse de manera efectiva y asegurar a los clientes y grupos interesadss que sus activos permanecen seguros.

El cómo, qué y por qué de los métodos de ataque de presentación

También conocidos como "spoofs", los ataques de presentación están diseñados específicamente para subvertir los sistemas biométricos. Los ataques de presentación generalmente involucran un facsímil de un usuario autorizado que se presenta a un dispositivo de imágenes, como una cámara de reconocimiento facial. El objetivo del usuario no autorizado es engañar al dispositivo de imagen haciéndole creer que está leyendo el rostro, el iris o la huella dactilar de una persona autorizada para que pueda obtener acceso de forma fraudulenta.

El tipo más simple de ataque de presentación incluye una falsificación de una sola imagen, como una fotografía física o una imagen de una persona autorizada que se muestra en la pantalla de un dispositivo. Aquí, el atacante usa una foto en lugar de su propio rostro durante el proceso de reconocimiento facial con la esperanza de que el sistema biométrico se engañe y piense que es la persona autorizada. Por lo general, los atacantes con falsificaciones de una sola imagen tendrán varias fotografías o imágenes a su disposición, ya sea del mismo individuo o de varios individuos, para aumentar sus posibilidades de éxito.

Las parodias más sofisticadas involucran máscaras 2D o 3D en lugar de una foto. Aquí, un atacante cortaría los ojos de una fotografía y mostraría su rostro al dispositivo de imágenes, o incluso haría que se produjera una máscara 3D específicamente para este propósito para un nivel de calidad aún mayor. La esperanza aquí es que la vivacidad de los ojos y, al menos en el caso de las máscaras 3D, la calidad de la máscara les dará una ventaja para pasar el dispositivo de imagen.

Un tercer tipo de ataque de presentación involucra grabaciones de video en lugar de fotografías o máscaras. Aquí, un atacante obtendría una grabación de video de una persona autorizada y la presentaría en el dispositivo de imágenes, generalmente en un dispositivo móvil como una tableta o un teléfono inteligente. Al proporcionar una imagen en movimiento del individuo real, queda la esperanza de que el dispositivo se engañe y piense que la grabación que se muestra es el usuario autorizado.

La amenaza añadida de deepfakes y ataques de inyección

La conciencia de los deepfakes ha crecido significativamente en los últimos años, con la definición de lo que realmente están cambiando con el tiempo. Originalmente, los deepfakes se referían al proceso mediante el cual los algoritmos de aprendizaje profundo creaban una versión falsa y sintética de una persona usando imágenes fijas. Estos algoritmos luego manipularían a esta persona sintética en video para hacer y decir una variedad de cosas. Los ejemplos comunes fueron videos de funcionarios políticos y celebridades que decían cosas que en realidad no dijeron, lo que generaba una mayor preocupación por la información errónea y ponía las falsificaciones profundas en primer plano en la mente de muchas personas.

Actualmente, los deepfakes generalmente se refieren a cualquier generación sintética de una persona, independientemente de cómo se haya producido. Además, la tecnología en torno a los deepfakes está mejorando rápidamente, con mejor calidad, personas sintéticas más realistas y un tiempo de creación más rápido. Estas mejoras han llevado a una mayor sensación de temor acerca de cómo podrían eludir los métodos de autenticación biométrica.

Los piratas informáticos o las personas malintencionadas podrían intentar utilizar una falsificación profunda para eludir las medidas de seguridad biométrica de dos maneras diferentes. La primera es simplemente reproducir un video del deepfake en el dispositivo de imágenes, como con los ataques de presentación de video. El segundo es un tipo de método de ataque completamente nuevo: ataques de inyección. Este tipo de ataque no implica la presentación de una imagen, grabación o falsificación profunda a un dispositivo de imágenes. En cambio, omite el dispositivo de imágenes por completo, inyectando la entrada falsa en el propio software. El objetivo es convencer al programa para que acepte la entrada como válida y altere la ejecución del programa. En este escenario, esta ejecución daría como resultado que se concediera acceso al usuario no autorizado.

En última instancia, las organizaciones que tienen o están considerando métodos de autenticación biométrica deben considerar las falsificaciones profundas y no como su propia categoría de ataque. En cambio, los deepfakes se pueden emplear como un ataque de presentación similar a las fotos y las máscaras, o como ataques de inyección que brindan información no confiable a un programa subyacente. Tanto los ataques de presentación como los de inyección requieren diferentes tipos de contramedidas, y las organizaciones harían bien en centrarse en esas dos categorías, en lugar de las falsificaciones profundas como su propia categoría distintiva.

Ataques Morph y lo que los hace diferentes

Los morphs son otro tipo de método de ataque biométrico que ha crecido en prevalencia en los últimos años. En pocas palabras, los morphs utilizan la tecnología para combinar las caras de normalmente dos, pero posiblemente más, personas diferentes en una cara nueva y única. A menudo, el objetivo de los morphs es vencer el reconocimiento facial al combinar las características faciales de un usuario autorizado con las de un usuario no autorizado. Debido a que hay elementos de la cara de cada persona en el morph, el reconocimiento facial podría ser engañado para proporcionar acceso de manera fraudulenta.

Los morphs se pueden usar para proporcionar documentos de identidad, como pasaportes, a personas que no pueden obtener uno legalmente o cruzar fronteras. En este caso, se crearía un morph combinando las semejanzas de la persona que no puede obtener un pasaporte con una persona que sí puede. Esta imagen transformada podría usarse para inscribirse para un nuevo pasaporte. Una vez que se recibe el pasaporte, el viajero no autorizado podría usarlo en un intento de eludir la seguridad fronteriza.

Otro ejemplo involucra a los piratas informáticos que crean morfos de usuarios ya autorizados consigo mismos para engañar al reconocimiento facial y otorgarles acceso. De esta forma, son muy similares a los ataques de presentación y deepfake descritos anteriormente. Sin embargo, al igual que con los deepfakes, los morphs no deben considerarse como una categoría propia con fines defensivos. En última instancia, los ataques caen en ataques de presentación o de inyección, y las organizaciones obtienen mejores resultados alineando sus recursos hacia esas dos categorías en lugar de morphs y deepfakes individualmente.

Protección contra ataques de presentación e inyección

Afortunadamente, hay opciones disponibles para las organizaciones que buscan proteger sus valiosos activos de las amenazas en evolución descritas anteriormente:

Detección biométrica de vida.

Al implementar o mejorar una solución de autenticación biométrica, la inclusión de la detección de vida es vital en cualquier escenario donde la seguridad es primordial. En pocas palabras, la detección de vida determina si el usuario es una persona viva que respira y se presenta en vivo al dispositivo de imágenes, o si es una presentación o un ataque falso diseñado para violar el sistema. Sirve como una línea de defensa muy sólida contra cualquier ataque de presentación, ya sea una simple parodia de fotos, una falsificación profunda o un video morph, gracias a su capacidad para distinguir entre una persona viva y un facsímil de una persona viva.

Debido a que la conveniencia del usuario también es una consideración importante al implementar nuevas funciones de seguridad, la detección de vida también está disponible como un proceso pasivo en muchos casos. Si bien algunas detecciones de vida requieren que el usuario siga una serie de indicaciones, como giros de cabeza, la detección de vida altamente efectiva también se puede realizar completamente en segundo plano, sin molestar al usuario de ninguna manera. Para las organizaciones comprometidas con la protección contra los ataques de presentación, la detección pasiva de vida es la combinación ideal de seguridad y comodidad.

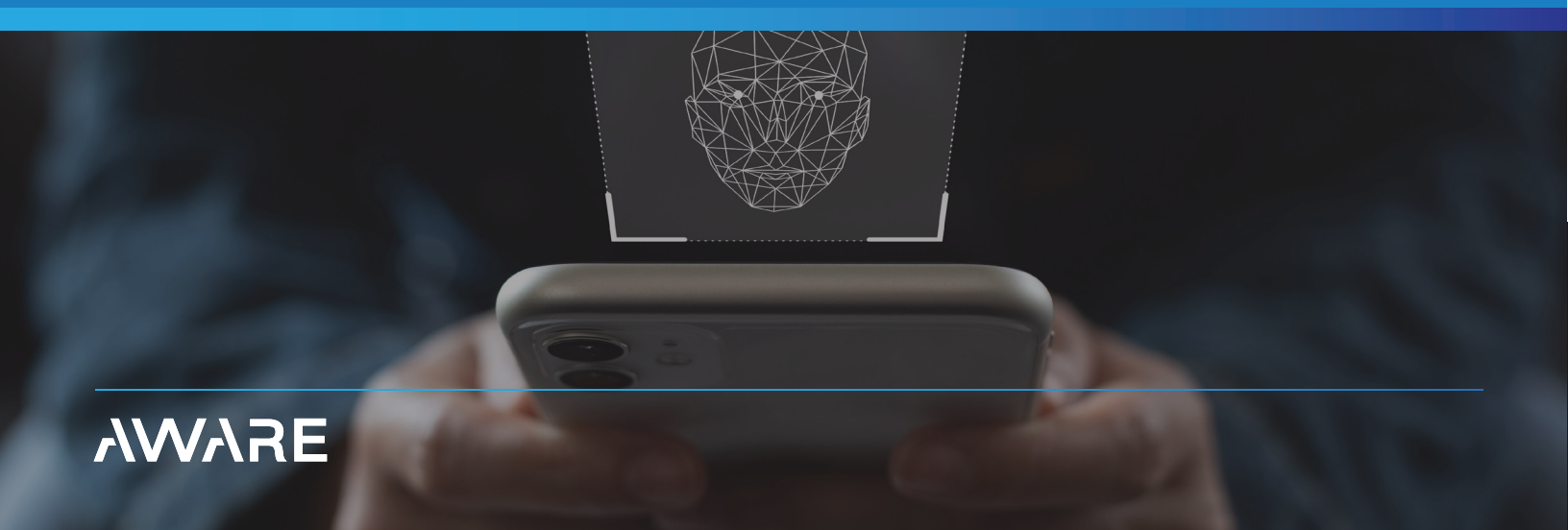
Seguridad del software.

Si bien los ataques de presentación se pueden manejar con detección de vida biométrica, los ataques de inyección, ya sean deepfakes, morphs o cualquier otro tipo de ataque que proporcione información no confiable a un programa, se pueden manejar completamente fuera del ámbito biométrico. En última instancia, los ataques de inyección se frustran mejor con una red sólida y una seguridad de software.

Las organizaciones pueden detectar vulnerabilidades de inyección en su sistema y evitar ataques por completo a través de una variedad de métodos de prueba, software y productos diseñados solo para este propósito. Los profesionales de seguridad capacitados y con experiencia en los últimos tipos de ataques de inyección pueden y deben ser de gran interés para las organizaciones que buscan protegerse contra estas amenazas en evolución.

Adición de disuasivos.

Si bien esta categoría puede fluctuar enormemente según las políticas individuales de la empresa, agregar medidas disuasorias a sus procedimientos de autenticación también puede servir como una sólida línea de defensa. Los ejemplos de disuasivos comunes incluyen bloquear a los usuarios de una plataforma después de varios intentos fallidos, limitar la cantidad de intentos de acceso para empezar y bloquear las direcciones IP de los estafadores conocidos.



Proporcione una detección de vida segura y conveniente con Knomi®

Para empresas y organizaciones que buscan proteger sus activos seguros y los de sus clientes de ataques de presentación, Knomi® de Aware es una solución ideal. Knomi proporciona la solución de actividad independiente del dispositivo de mejor rendimiento disponible que es verdaderamente pasiva, con una experiencia de usuario opaca que no indica a un estafador cómo puede ser derrotado.

El marco de autenticación biométrica móvil de Knomi ofrece detección de vida de rostro y voz de alto rendimiento y probada en campo, con una familia de algoritmos basados en aprendizaje automático que detectan y previenen prácticamente todos los tipos de ataques de presentación biométrica. Knomi detecta ataques que intentan suplantar a la víctima, así como aquellos que intentan ocultar la identidad, lo cual es especialmente importante para la incorporación. Los algoritmos de vivacidad facial de Knomi detectan obstrucciones y distorsiones, y funcionan en condiciones de luz escasa y brillante en todo tipo de rostros.

La solución Knomi también brinda capacidades únicas para proteger todo el flujo de trabajo transaccional, al permitir el cifrado de extremo a extremo, garantizar la integridad de los datos y proporcionar una variedad de contramedidas sofisticadas y opacas diseñadas para frustrar los ataques de inyección.

Para mayor seguridad, la autenticación de voz y la vivacidad se pueden agregar y fusionar opcionalmente con la cara para hacer que la suplantación de identidad sea exponencialmente más difícil para los estafadores. Knomi detecta una variedad de tipos de suplantación de voz, incluidas suplantaciones de voz grabadas, filtradas y sintéticas.

Los SDK y las API de Knomi también se pueden incorporar a una aplicación móvil, de navegador o basada en quiosco, o implementarse con una arquitectura basada en servidor o dispositivo. Knomi Web basado en servidor permite la captura de rostros y la detección de vida desde un navegador en un dispositivo móvil o computadora de escritorio.

En combinación con disuasivos inteligentes y una sólida seguridad de software, la detección pasiva de vida de Knomi brinda a las organizaciones un medio de protección altamente seguro y conveniente contra las amenazas en evolución presentes en la actualidad.

¿Desea saber más? www.aware.com/es/knomi/

Fuentes:
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/