White Paper

Presentation Attacks, Deepfakes and Morphs

AWARE

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

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Burlington, Massachusetts.

It has always been of vital importance to protect the sensitive and valuable assets of organizations and their customers from outside threats and unwanted access. In today's world, this is even more pronounced with identity theft at an all-time high level and data breaches increasing by 17%[1] since 2020 alone.

Passwords have typically formed the backbone of most access security authentication methods, but with 61% of data breaches taking place as a result of weak or stolen passwords[2], organizations are looking for more secure alternatives. Biometric authentication, which takes advantage of a person's unique physical characteristics to grant access to secure information or assets, virtually eliminates the problems associated with password-based authentication methods, providing organizations with a much more secure alternative.

With a shift from password-based to biometric authentication now taking place to improve security, however, outside hackers and malicious parties have attempted to follow suit with new attack methods designed to thwart these increased security measures and gain access fraudulently. These methods include presentation attacks, deepfakes and morphs, and their rise in frequency has resulted in heightened awareness and fear about them. Thankfully, many misconceptions exist around these methods and how much of a threat they truly pose. Organizations armed with information on each of these evolving threats can effectively protect themselves and assure customers and interested parties that their assets remain secure.

The how, what and why of presentation attack methods

Also known as "spoofs," presentation attacks are designed to subvert biometric systems specifically. Presentation attacks typically involve a facsimile of an authorized user being presented to an imaging device such as a facial recognition camera. The goal of the unauthorized user is to trick the imaging device into thinking it's reading the face, iris or fingerprint of an authorized person so they can gain access fraudulently.

The simplest type of presentation attack includes a single image spoof, such as a physical photograph or image of an authorized individual displayed on a device screen. Here, the attacker uses a photo instead of their own face during the facial recognition process in the hope that the biometric system will be fooled into thinking they're the authorized person. Typically attackers with single image spoofs will have multiple photographs or images at their disposal, either of the same individual or multiple individuals, to increase their chances of success.

More sophisticated spoofs involve 2D or 3D masks instead of a photo. Here an attacker would either cut the eyes out of a photograph and present their face to the imaging device, or even have a 3D mask produced specifically for this purpose for an even higher level of quality. The hope here is that the liveness of the eyes and, at least in the case of the 3D masks, the quality of the mask will give them an advantage in getting past the imaging device.

A third type of presentation attack involves video recordings in place of photographs or masks. Here, an attacker would obtain a video recording of an authorized individual and present it to the imaging device, typically on a mobile device such as a tablet or smartphone. By providing a moving image of the actual individual, the hope remains that the device will be fooled into thinking the displayed recording is the authorized user.

The added threat of deepfakes and injection attacks

The awareness of deepfakes has grown significantly in recent years, with the definition of what they actually are changing over time. Originally, deepfakes referred to the process by which deep learning algorithms created a fake, synthetic version of a person using still images. These algorithms would then subsequently manipulate this synthetic person in video to do and say a variety of things. Common examples were videos of political officials and celebrities saying things they didn't actually say, creating heightened worry about misinformation, and bringing deepfakes to the forefront of many peoples' minds.

Currently deepfakes typically refer to any synthetic generation of a person, regardless of how it was produced. Additionally, the technology around deepfakes are rapidly improving, with better quality, more realistic synthetic people and faster creation time. These improvements have led to a greater sense of fear about how they could bypass biometric authentication methods.

Hackers or malicious individuals could attempt to use a deepfake to bypass biometric security measures in two different ways. The first is to simply play a video of the deepfake to the imaging device, such as with video presentation attacks. The second is an entirely new type of attack method: injection attacks. This attack type doesn't involve presenting an image, recording, or deepfake to an imaging device. Instead it bypasses the imaging device entirely, injecting the deepfake input into the software itself. The goal is to convince the program to accept the input as valid and alter the execution of the program. In this scenario, this execution would result in the unauthorized user being granted access.

Ultimately, organizations that have or are considering biometric authentication methods need to look at deepfakes not as their own category of attack. Instead, deepfakes can be employed as either a presentation attack similar to photos and masks, or as injection attacks that provide untrusted input to an underlying program. Both presentation and injection attacks require different types of countermeasures, and organizations would be well served focusing on those two categories, instead of deepfakes as their own distinctive category.

Morph attacks and what makes them different

Morphs are another type of biometric attack method that have grown in prevalence in recent years. Simply put, morphs utilize technology to combine the faces of typically two, but possibly more, different individuals into one new, unique face. Often the goal of morphs is to defeat facial recognition by combining the facial features of an authorized user with those of an unauthorized user. Because there are elements of each person's face in the morph, facial recognition could potentially be tricked into providing access fraudulently.

Morphs can be used to provide identity documents, such as passports, to individuals who cannot lawfully get one or cross borders. In this instance, a morph would be created combining the likenesses of the person who cannot get a passport with a person who can. This morphed image could then be used to enroll for a new passport. Once the passport is received, the unauthorized traveler could then use it in an attempt to bypass border security.

Another example involves hackers creating morphs of already authorized users with themselves to trick facial recognition into granting them access. In this way, they are very similar to the presentation and deepfake attacks described above. Like with deepfakes, however, morphs should not be considered as their own category for defensive purposes. Attacks ultimately fall into either presentation or injection attacks, and organizations are best served aligning their resources toward those two categories instead of morphs and deepfakes individually.

Protecting against presentation and injection attacks

Fortunately, there are options available for organizations looking to protect their valuable assets from the evolving threats described above:

Biometric Liveness Detection

When implementing or improving a biometric authentication solution, the inclusion of liveness detection is vital in any scenario where security is paramount. Put simply, liveness detection determines whether the user is a living, breathing person being presented live to the imaging device, or if it's a presentation or spoof attack designed to breach the system. It serves as a very strong line of defense against any presentation attack, whether it is a simple photo spoof, or a deepfake or morph video, thanks to its ability to distinguish between a live person and a facsimile of a live person.

Because user convenience is also an important consideration when implementing new security features, liveness detection is also available as a passive process in many instances. While some liveness detection requires a user to follow a series of prompts such as head turns, highly effective liveness detection can also be performed entirely in the background, without inconveniencing the user in any way. For organizations committed to protecting themselves against presentation attacks, passive liveness detection is the ideal blend of security and convenience.

Software Security

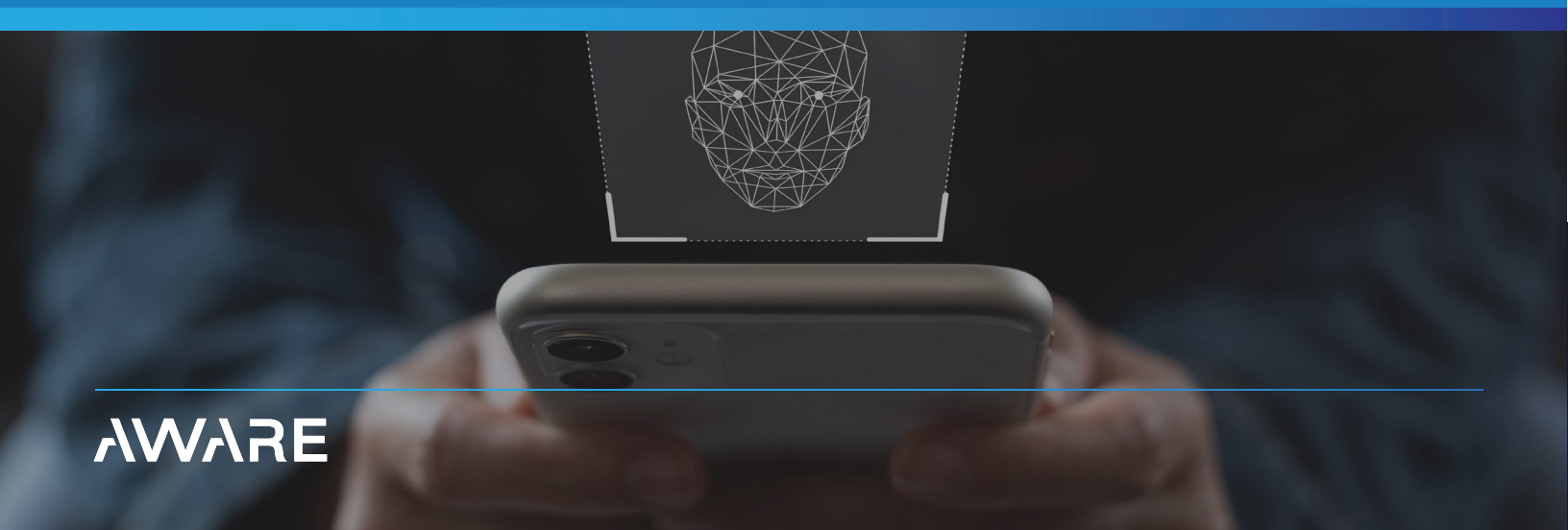
While presentation attacks can be handled with biometric liveness detection, injection attacks—whether they be deepfakes, morphs, or any other type of attack that provides untrusted input to a program—can be handled entirely outside the biometric realm. Ultimately injection attacks are best thwarted by strong network and software security.

Organizations can both detect injection vulnerabilities in their system and avoid attacks altogether through a variety of testing methods, software and products designed for just this purpose. Security professionals trained and practiced in the latest injection attack types can and should be of significant interest to organizations looking to protect against these evolving threats.

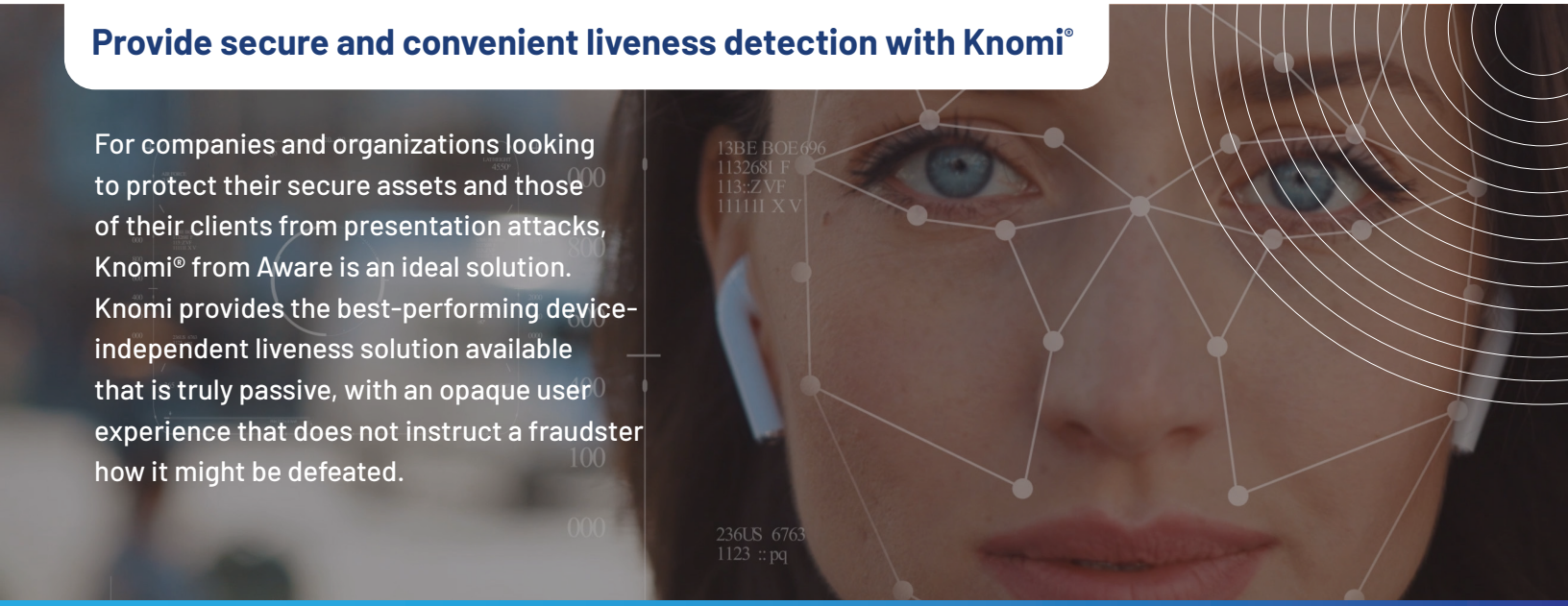
Adding Deterrents

While this category may fluctuate wildly based on individual company policies, adding deterrents into your authentication procedures can also serve as a strong line of defense. Examples of common deterrents include locking users out of a platform after a number of failed attempts, limiting the number of access attempts to begin with, and blocking the IP addresses of known fraudsters.

While these deterrents are not as powerful as biometric liveness detection and software security measures, they are easy to implement, can be employed in a variety of different ways, and can serve as a simple means to convince a hacker that it's simply not worth the effort.



Provide secure and convenient liveness detection with Knomi®



For companies and organizations looking to protect their secure assets and those of their clients from presentation attacks, Knomi® from Aware is an ideal solution. Knomi provides the best-performing device-independent liveness solution available that is truly passive, with an opaque user experience that does not instruct a fraudster how it might be defeated.

The Knomi mobile biometric authentication framework offers high-performance, field-proven face and voice liveness detection, with a family of machine learning-based algorithms that detect and prevent virtually all types of biometric presentation attacks. Knomi detects attacks attempting victim impersonation as well as those attempting identity concealment, which is especially important for onboarding. Knomi's face liveness algorithms detect obstructions and distortions, and work in low-light and bright-light conditions on all types of faces.

The Knomi solution also provides unique capabilities in securing the entire transactional workflow, by enabling end to end encryption, guaranteeing data integrity and providing a variety of sophisticated and opaque countermeasures designed to thwart injection attacks.

For added security, voice authentication and liveness can be optionally added and fused with face to make spoofing exponentially more difficult for fraudsters. Knomi detects a variety of voice spoof types, including recorded, filtered, and synthetic voice spoofs.

Knomi SDKs and APIs can also be incorporated into either a mobile-, browser-, or kiosk-based application, or implemented with a server-, or device-based architecture. Server-based Knomi Web enables face capture and liveness detection from a browser on a mobile device or desktop.

Combined with smart deterrents and strong software security, Knomi's passive liveness detection provides organizations with both a highly secure and convenient means of protection from the evolving threats present today.

Interested in learning more about Knomi? Visit www.aware.com/knomi/

Sources:
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