White Paper

How Aware Helped a Leading Brazilian Bank Stay Ahead of Evolving Attack Vectors Targeting Facial Authentication

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.

While passwords are still the most common authentication method for online banking and mobile financial services applications, they are also highly prone to misuse. Moreover, friction created by the password reset process continues to be a very real pain point for users.

Enter facial authentication which is inherently more secure and effective in preventing fraudsters from setting up fake accounts for money laundering and stealing money from others, with the benefit of improving the user experience.

In recent years, the use of facial biometric authentication has become dramatically more accurate, fast and resilient to environmental and user variables. However, the reality is that banks can still be attacked and subverted if the right technology and support services are not in place. The most common type of attack, often referred to as a "spoof" or presentation attack, can possibly dupe facial authentication systems by presenting a "face artifact" of a legitimate user, which can be readily generated through the easy availability of images and videos of people on social networks.

With over 60 percent of data breaches owing to cases of weak or stolen passwords, organizations are looking for more secure alternatives like biometrics. However, with a shift from password-based authentication to biometric authentication often comes escalations in breach attempts.

A case in point is Aware's work with a large Brazilian bank's facial biometrics authentication system which was very popular among its users due to its high efficiency and accuracy. However, the bank began noticing instances of presentation attacks, and shortly after injection attacks, that were penetrating and evading the facial authentication component of its enrollment system.

In this white paper, we'll explore how Aware's lightning-fast response to implement a multi-layered system of both biometric and non-biometric security enhancements provided multiple lines of defense against these attacks.

The Bank's Problem

Like many industry-leading financial services firms, this leading bank was using facial authentication to provide its customers with both high security and ease of use.

In fact, this bank had a facial biometrics authentication system in place before beginning its work with Aware, and had previously been targeted by bad actors using photographs of others to spoof the system. In some cases, account holders were having their pictures or identification cards stolen and used by attackers to create fraudulent accounts. As a first step, Aware worked with the bank to implement Knomi Liveness Detection to ensure that only living people could set up accounts.

> Presentation attacks typically involve a facsimile of an authorized user – such as an image taken from someone's identification card or even a social media profile – being presented to a camera or another imaging device. The goal of the hacker or unauthorized user is to trick the device into thinking it's reading the face of the authorized person so they can gain access fraudulently.

However, as time went on, the sophistication of these presentation attacks kept increasing. Instead of using photos to set up fraudulent accounts, fraudsters began producing higher-quality presentation attacks as well as deep-fakes and morphs.

More sophisticated presentation attacks involve masks instead of a photo. An attacker might 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. The goal here is to ensure that the liveness of the eyes and/or the quality of the masks will give the bad actor an advantage in getting past the biometric checkpoint.

And then, about nine months ago, the bank started seeing a different kind of attack: injection attacks aimed at foiling the client enrollment system. Injection attacks represented a whole different attack vector from the real-world presentation attacks the bank had initially experienced. Instead of attacking the presentation of the user and the algorithms analyzing that presentation, they instead attacked the software performing the capture itself.

Injection vulnerabilities allow attackers to insert malicious inputs into, or relate malicious code through, an application into another system. During an injection attack, untrusted inputs or unauthorized code are injected into a program, where they're interpreted as part of a query or command. The program is then altered, and that alteration redirects the program for a nefarious purpose.

Injection attacks are particularly frightening because the attack surface is enormous, and the attack can touch an entire system. Injection attacks are also an incredibly well-understood vulnerability class, which means there are many easily accessible resources and tools that allow even inexperienced attackers to exploit those vulnerabilities.

Aware's Solution

Aware implemented three layers of additional protection to thwart attempts to circumvent the facial authentication component of the bank's enrollment system. The first layer was securing the application so that the integrity of the biometric capture process is preserved. The second layer was the analysis of the biometric data for presentation attacks.

The third layer relied on non-biometrics best practices to verify the security of users' biometric data at each of the following steps. Aware addressed the security aspects for all these different pieces of the onboarding pipeline even though they did not technically fall within the company's scope of work, and includes:

- **Data acquisition:**
  The moment the device accepts data from a user.
- **Data transfer security:**
  Ensuring data from the user is encoded and transferred to where it will be processed.
- **Data processing:**
  Keeping data encoded and secure until i t's returned with the answer.

As a result of the measures implemented by Aware, the bank immediately saw a significant decrease in the injection attack vector.

Best Practices and Takeaways

There are several lessons from Aware's work with this bank that others should consider when faced with evolving biometric authentication attack vectors:

Approaching Biometric Authentication Holistically:

Presentation Attack Detection (PAD) is a critical component, but only one element in a complex biometric authentication system that needs to provide a careful balance between security and usability. A successful solution must provide a comprehensive set of defenses that minimizes friction but maximizes the likelihood of an accurate result, and one that can adapt to evolving threats.

This includes:

1. An effective method for quality control that motivates users to optimize their presentation for the most accurate analysis, as provided by Aware's outstanding auto capture capability
2. A primary suite of sophisticated PAD algorithms to detect presentation attacks before they even enter the biometric subsystem, provided as part of Aware's leading Knomi liveness solution
3. A secondary suite of sophisticated hacking attack detection algorithms to safeguard the system from emulator, injection and function attacks that might include deep fakes, morphs or replay inputs
4. A secure end-to-end method that verifies the integrity of the entire transaction
5. Lastly, a solution design infrastructure that allows for a highly responsive and adaptive approach to constantly evolving threats, the success of which is reflected in Aware's leading position in biometric authentication today

Additional institutional safeguards such as monitoring device IDs (or IP addresses) that are associated with frequently rejected transactions, maintaining a memory of the number of different accounts accessed by the same device ID (or IP addresses) and/or using matchers to verify identities of account holders can all contribute to securing financial transactions that want to take full advantage of biometric authentication technology.

In this regard, the importance of actively collaborating with participating institutions cannot be overstated, as striving towards the common goal of highly accurate and secure facial authentication can provide synergistic opportunities for advancing the state of the art. Aware excels in developing and nurturing relationships that can be mutually beneficial, necessary for succeeding in the complex and dynamic environment of biometric authentication.

Learning from Operational Realities:

It's easy to outline what can theoretically be done in the event of a biometric authentication attack, but that's very different than applying solutions in the real world and in real-time. When working with this bank, Aware was able to access these attack vectors and apply protection measures directly and extremely quickly.

Additionally, Aware was able to enhance the effectiveness and accuracy of its algorithms based on the data on the attack vectors supplied by the bank. This synergistic relationship benefitted both Aware's efforts and the bank's security work as attack vectors evolved.

Balancing Security and Usability:

Addressing complex security issues while maximizing the usability of the system can be a hard balance to strike. Most banks recognize the need to make trade-offs between customer convenience and security, in fact, many view it as just the cost of doing business. As an example, VISA writes off an estimated $6 billion in fraud per year to keep its authentication systems easy to use.

In another example, many banks deploy additional protection mechanisms such as matching capabilities. This is when, once an individual has accessed an account, a matching engine continuously matches the user's facial image against the account holder image on file. The matching threshold at many banks is very lenient, so much so that even if a spoofer gets through the initial authentication checkpoint, the matching engine still fails to determine that the spoofer is not the account holder. This is done specifically to ensure an easy experience for legitimate users.

The bottom line is that when implementing security protections, usability needs to be valued as much as the security aspect. Fortunately, Aware supplied the bank with the auto capture capability for the interaction which provided opportunities to directly impact usability in a positive way.

Ensuring a Quality Partnership:

Aware prioritizes true partnerships with its customers, especially in this digital age, with cyberattacks increasing in frequency and maliciousness. This is particularly true in Brazil, which experienced an enormous rise in mobile interactions in the wake of COVID-19, and in turn, a large increase in more aggressive attack vectors.

Aware's close partnership with this bank—one that involved cooperation at both the technical and enterprise security levels, and transactional data sharing—was one of the key components to a successful collaboration and has allowed the bank to stay ahead of evolving attack vectors in order to realize the full benefits of its investment in biometric authentication.

Summary

Passwords are still the most common authentication method for most online banking and mobile financial services applications, but they are prone to misuse and the password reset process continues to be a major frustration point for users. As banks increase their receptivity to newer biometric authentication technologies, they need to collaborate with their technology partners to stay one step ahead of emerging threats.

Aware provided this bank with guidance within as well as beyond the realm of biometric security, and delivered a high degree of success. Aware will do whatever it takes to help, as nothing is more important to the company than protecting the sensitive and valuable assets of its enterprise customers and their users from insidious threats.

This kind of partnership is essential to the future of biometric security, especially in the world of banking and fintech. As these organizations continue to evaluate biometric authentication, it's vital that they strongly consider the choice of partner, and most will benefit from one invested in consistent communication and real-time, proactive threat responsiveness. Working together, the right technology partner can help organizations achieve the maximum benefits of biometric authentication - superior security combined with the ultimate convenience that keeps users loyal to the brand.

Interested in learning more? Visit www.aware.com

AWARE

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