White Paper

Mobile biometric authentication:

Multimodal approaches for improved matching and spoof detection

AWARE

Table of Contents

Introduction

Multifactor authentication aims to maximize both security and convenience.

The vast majority of modern authentication implementations strive to maximize both security and convenience; that is, to:

- Make it as difficult as possible for a fraudster to steal or spoof the rightful user's authentication factors (e.g. device, password, token, biometric).
- Avoid interference with access to the protected asset or service for the rightful user.
- Dissuade the user from circumventing the intended security mechanisms.

Multifactor authentication (MFA) aims to meet these objectives by making it harder for fraudsters to defeat security mechanisms without adding inconvenience for the user.

Mobile authentication methods often use two authentication factors to boost security:

- **Possession:** something you have, such as the smartphone itself.
- **Knowledge:** something you know, such as a password.

They can also be used in an "out-of-band" fashion, where authentication on (an authenticated) device is used to gain access through another channel, such as through a website via a browser on a laptop.

Passwords: The Chink in MFA's Armor

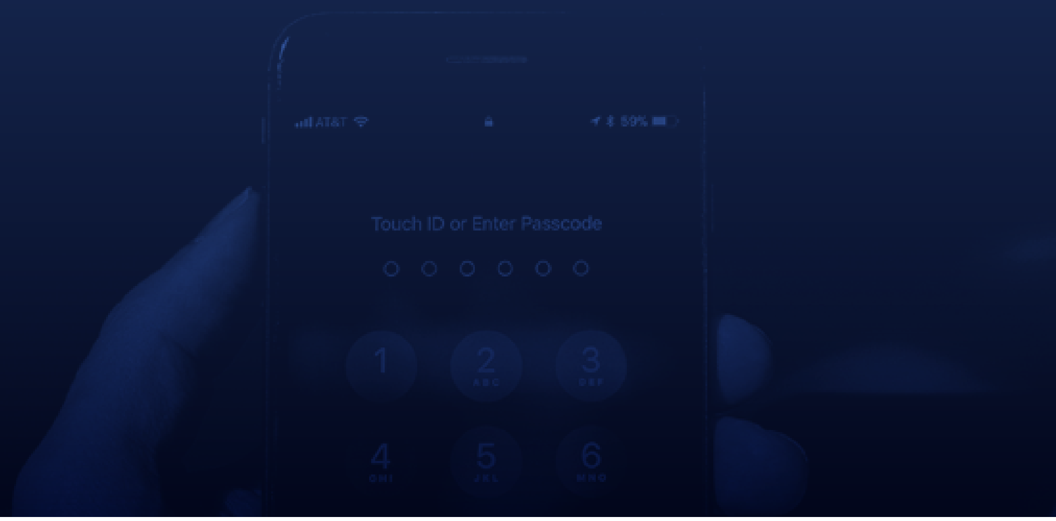
Password protection is a 50-year-old technology that was conceived for a far simpler digital world. They are the shining suits of armor of the cyber-defense world – antiquated, clunky, and ineffective against modern hacking arsenals.

First, passwords are vulnerable to phishing, interception, guessing, brute-force attacks, and large-scale data breaches. Fraudulent email requests for password resets, fake web pages meant to steal credentials, and keylogger malware (which records physical keystrokes) are just a few examples of the phishing and spying techniques that are used to steal passwords or PINs.

Second, passwords are often stored in a central location. In September 2017, Deloitte Digital experienced a data breach that resulted in **emails and passwords being exposed** belonging to as many as 350 corporate and government clients. Earlier in 2017, hackers also exposed HBO administrator passwords in a **1.5 terabyte data theft.**

Third, users have an increasing number of web-based accounts and are relying on more digital services than ever. Best practice is to have different passwords for all of them. However, the only way to feasibly remember them all is with a password manager (most of which cost

Use of passwords on smartphones is inconvenient and insecure.



money). But even password managers have vulnerabilities, such as “clipboard sniffing” (reading the copy-and-paste engine), according to **research** by Fraunhofer Institute’s TeamSIK. Use of passwords on smartphones is even more inconvenient and insecure than with other devices that provide some reasonably secure means to store passwords.

Finally, other knowledge-based factors such as security questions and one-time-passwords are also inadequate. A security question can be guessed through research on social media or even stolen through other means of social engineering (pretending to be someone else to request knowledge). One-time passwords succumb to a different flaw: They can be intercepted.

Considering the radical evolution of our networks and computing devices that has taken place since passwords were invented, it is plainly obvious that they are woefully insecure and inconvenient. Authentication needs to be rethought, yet we remain heavily reliant on them today, according to a recent **report** by Javelin Strategy & Research.

Biometrics as an Alternative

Biometrics are an attractive alternative to passwords as a second authentication factor because they are inherently convenient and unique. They are easy to use but difficult to steal and to spoof. But each biometric modality has unique characteristics that bring advantages and disadvantages in terms of both security and convenience.

Cue Multimodal Biometrics for Authentication

Multimodal biometrics have traditionally been seen as a way to improve biometric performance in terms of false match and false non-match scores; the more data that can be used for biometric matching, the better the performance. But multiple modes can also be used to improve

Multimodal authentication methods improve the biometric performance.

their resistance to fraud. By using multiple biometric modalities in concert, the advantages of each biometric can be exploited, while neutralizing their respective disadvantages. This combination of multiple modalities will be crucial as spoofing methods become more sophisticated.

To better illustrate this point, consider some of the following multimodal methods and how they help with spoof detection as well as biometric performance:

Voice Biometrics Enhanced With Facial Recognition
A facial analysis is conducted while the user is speaking to determine the liveness of the speaker. Real-time analysis of how the mouth moves when the user speaks a random passphrase helps ensure that the voice and facial recognition scan match and that the sample is not an audio/video recording of the targeted victim played from a device.

Keystroke Dynamics Enhanced With Facial Recognition
Keystroke dynamics use the unique keying cadence of the user as a behavioral biometric. A facial image can be captured while the user is typing a username or PIN. This adds facial recognition to the analysis without increasing time to the capture. Together, they add barriers to spoofing and fraud only possible with multiple modalities.

These multimodal authentication methods not only improve the biometric performance but also make it more difficult for fraudsters to spoof biometric scans. They also avoid negatively impacting the user experience by operating simultaneously.

Strong Authentication Just Got Stronger

Biometrics are rapidly evolving, and adoption is increasing at an exponential pace.

Biometric authentication promises to provide a suitably modern replacement for password protection, security questions, and one-time passwords. While they may be in their infancy, biometrics are rapidly evolving, and adoption is increasing at an exponential pace. By simultaneously improving both security and convenience, multimodal biometrics are largely expected to replace password-based MFA and permanently improve authentication as we know it.

Multimodal biometrics reduce the possibility of spoofs by making it much harder for fraudsters to attack with non-live, stolen biometrics. Their precision also reduces the likelihood of false matches and false non-matches, improving the performance and convenience for end users.

In Our Next Article:

Device- Versus Server-Centric Architecture

Effective liveness detection is critical to the successful implementation of biometrics, but so is the underlying security of the biometric sample storage and matching engine, which can be implemented using either a device- or server-centric architecture. The decision of which to implement depends on numerous factors:

- **Security of devices:** What is the level of confidence in the ability of the device and app to secure biometric data?
- **Security of server:** What is the level of confidence in the ability to secure biometric data centrally? What is the risk of a breach?
- **Utility of server-side data:** Can biometric data be used for other purposes, such as training of algorithms or verification against other data (e.g. driver's license or employee ID photos)?
- **Scalability:** How many people will be using the mobile app? Is it more attractive to add complexity to an app or to the backend?
- **Wireless network capacity:** What is the maximum size of an app for convenient download? What is the impact on speed of authentication?
- **Device memory and processing power:** Do many customers use less powerful devices that will benefit from server-side processing?
- **Standards:** How desirable is use of standards-based technology such as FIDO?
- **Cross-device capability:** How important is it for users to be able to use multiple devices?

Subscribe to Aware's Biometrics Blog to receive our next article, which will compare and contrast different biometric authentication architectures. The right architecture for a given application and environment depends on the answers to the above questions and the weight of consideration given to each based on business priorities.

AWARE

www.aware.com/contact