Exploring the applications of passwordless authentication

NomiDio

Contents

Why passwordless authentication?

Both consumers and employees frequently need to log-on to digital systems, quickly and securely. There is already widespread agreement that today's method of allowing people to prove 'they are who they say they are', the humble password, does more harm than good.

In addition to passwords being hard to remember, offering a poor user experience and requiring significant help desk support for resets, they simply aren't secure. In fact, passwords are the root cause enabler for the majority of today's most common cyber security attacks.

Consider this table of common threats from Alex T Weinert, Microsoft's Director of Identity Security where he explains why even strong passwords are no longer effective[1] .

Attack	Frequency	Difficulty: Mechanism	User assists attacker by...	Does your password matter?
Credential stuffing	**Very high** 20M+ accounts probed daily in Microsoft's ID systems	**Very easy** Purchase creds gathered from breached sites with bad data at rest policies, test for matches on other systems. List cleaning tools are readily available	Being human. Passwords are hard to think up. 62% of people admit reuse.	**No** The attacker has exact password
Phishing	**Very high** 0.5% of all inbound emails	**Easy** Send emails that promise entertainment or threaten, and link user to doppelganger site for sign-in. Capture creds. Use Modlishka or similar tools to make this very easy	Being human. People are curious or worried and ignore the warning signs	**No** User gives the password to the attacker

[1] https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Attack	Frequency	Difficulty: Mechanism	User assists attacker by...	Does your password matter?
Password spray	**Very high** Millions of accounts probed and hundreds of thousands broken daily	**Trivial:** Use easily acquired user lists, attempt the same password over a very large number of usernames. Regulate speed and distributed across many IPs to avoid detection. Tools are readily and cheaply available	Being human and using common passwords	**No** Unless it is in the handful of top pass-words hackers aren't trying
Keystroke logging	**Low**	**Medium** Malware records and transmits usernames and passwords entered, but usually everything else too, so attackers have to parse things	Clicking links and failing to screen for malware	**No** Malware intercepts exactly what is typed

The answer is to move beyond passwords. By moving from passwords to quick and easy biometric authentication; security, efficiency and user experience can all be enhanced.

Nomidio: the basics

Nomidio is a passwordless multi-factor authentication service. It allows a user to log-in to virtually any application or cloud service quickly and easily using their voice and face.

The technology is entirely cloud based and delivered as a true service, requiring no on-site infrastructure and minimal IT resources. Nomidio is available from the AWS Marketplace and the Azure Marketplace and can be up and running within a matter of hours.

Nomidio has been designed to prioritise user experience and authentication takes place within the browser, drawing on biometric matching capabilities in the cloud. Therefore it doesn't matter if the user loses their mobile phone or it runs out of battery, they can log-in from any device. The Nomidio sign-in process takes circa 30 seconds.

Introducing a multi-factor biometric check for authentication eliminates the vast majority of common attacks like credential stuffing and phishing. Credentials can't be lost, stolen or shared when they are your own face and voice patterns - the legitimate user must actually be present to log-in.

High levels of security, scalability and certification for industry standards like OpenID Connect mean Nomidio is suitable for both employee and consumer use cases.

Use cases:

Frontline workers

Workers in the field e.g. delivery drivers, taxi drivers, retail staff, cleaners, nurses, utilities engineers and many other professions are increasingly empowered by technology. These frontline workers need access to rotering, payroll, delivery, inventory and operational systems to log updates and prepare for their next day of work. Log-in might be infrequent, perhaps only a few times a week.

This access is typically on-the-go from the van or shop floor and from a mobile or tablet, suggesting a browser-based authentication is an advantage. People in these roles are busy completing real-world activities, yet another reason why logging-in needs to be simple, quick and friction-free.

Providing a username and password for such access is hugely inefficient as people forget and need to reset their passwords. At a basic efficiency level, this places increased strain on administrators in head-office whilst frustrating workers on the frontline who are focused on completing their work.

Replacing passwords with a simple biometric check removes the friction when frontline workers log-in, supporting business continuity and recovery. In addition, a biometric check greatly reduces the potential for job-sharing, where an unaccredited (potentially uninsured) worker sub-contracts a job from the legitimate employee - a particular concern in the gig-economy.

Remote workers

Traditionally a company would have a high degree of certainty about who was logging-in to its systems because employees needed to physically come to the office or the call centre. The company checks who has entered its building and knows it is the person in the seat that's using the credentials to access the system.

Neither of these checks are possible with remote workers, for example a remote contact centre agent could easily share their credentials with a friend to undertake their job for a day or it could simply be an attacker that has obtained the username and password. In both cases, it's hard for the company to be sure who's accessing its systems.

Nomidio solves these challenges by ensuring it is the rightful employee that's logging-in to the system with a multi-factor biometric check. When a company no longer has 'a perimeter' it's more important that users are effectively challenged when logging-in.

Extended workforce (supply-chain)

Most large organisations today are interconnected and operate with an 'extended' workforce. These people might be agents or brokers that help to sell and distribute a product, common in travel and financial services, or they might be suppliers like farmers or manufacturers that are interconnected with retailers. In each case, a company will need this extended workforce to access its systems.

An extended workforce is largely outside your control, they may not have been through your training programmes and there is generally less visibility of their cyber security capabilities. Consider a small broker that sells asset-finance loans on behalf of a lender. If an attacker obtained a broker's log-in credentials they might be able to authorise a significant loan on behalf of the lender.

By replacing a proxy for a specific extended worker (their username and password) with an actual digital representation of that person (their biometric identifiers) it is possible to drastically enhance security and auditability.

Privileged access

Most companies have a subset of users with privileged access to a wide range of systems, for example, company executives or administrators in the IT department. These people are trusted not to abuse their position but remain vulnerable to all the classic cyber security attacks like phishing, where they may inadvertently divulge their password, or credential stuffing where a password they've used elsewhere is breached.

A successful attack on a privileged user represents a significantly higher risk to the organisation and that's driving companies to insist on higher authentication standards. This user group can easily create a Nomidio identity which they can use to access a wide number systems but only if they can successfully pass a multi-factor biometric check each time they log-in.

Subscription businesses

Any company offering a digital product on a subscription basis needs to carefully manage access to that product. From games to online video and newspapers, media owners and distributors face a constant battle against credential sharing.

Whilst a limited amount of credential sharing might be tolerated by a firm like Netflix, where others within a household have legitimate rights to access the platform, it's not accepted that a newspaper subscription can be shared by multiple people.

A classic username and password approach to consumer authentication leads to widespread credential sharing and revenue leakage. Similarly, attackers too are able to steal credentials to consume digital products for free (at the expense of legitimate users).

Nomidio offers a scalable authentication solution that can link any account or digital service to the legitimate subscription holder using biometrics. If a user is asked to sign-in with Nomidio they actually need to present their face and speak a passphrase with their own voice.

Being able to link a digital account to a single user might actually allow some subscription businesses to offer a lower price for those consumers that opt-in for biometric identification.

Nomidio – Company Overview

Nomidio is a UK company specialising in passwordless multi-factor authentication using biometrics. The company is a subsidiary of the Post-Quantum Group, which has a mission to protect the world's information against current and future threats. We want to ensure that everyone can live safely and securely, with trust and confidence in all their activities.

Nomidio's technology is already used by Hitachi Capital to verify its customers before asset-finance loans are agreed as well as by Avaya, which has selected Nomidio as the authentication technology of choice for its widely used contact centre systems.

www.nomidio.com

+44 (0)20 3871 3001