1KOSMOS

Identity Based Authentication

An approach to eliminate passwords that improves security, reduces operational overhead, and enhances user satisfaction

Whitepaper

Password-Based Attacks: Data Breach, Phishing, Ransomware, and More

It seems almost every day our news feed is flooded with reports of ransomware attacks and breaches that lead to millions of dollars in lost revenue and payments to criminals. According to a recent ransomware report[1] by a leading Cyber Insurance broker, the average ransomware payment was $1,450,00 and the average business loss (interruption of business activities) was $5,005,297.

In 2020, 1,001 Data Breaches exposed 155.8M records[2]

Breached companies underperformed NASDAQ by about 5% after six months[3]

We are talking about materially significant impacts here. A common element underlies these attacks: usernames and passwords. Organizations still place the security burden on their employees and customers. The assumption is, they are creating secure credentials and that they are not using them in other locations. We know now that this is simply not true. To be fair, it is a lot to ask of users (workforce, customers, and citizens) to ensure their passwords are secure. They have too many to remember and each and every rule governing their credentials is different.

Everyone knows passwords are painful. On the one hand they cause tremendous inconvenience in our personal and business lives, but the problems with passwords go much deeper than a few hours of lost productivity per month. For starters, those ransomware attacks and breaches are being enabled by this weak form of authentication.

A recent report by Verizon demonstrated that 61% of all data breaches are caused by compromised credentials.[3]

Of highest concern, our critical infrastructure is at risk because of a reliance on passwords. Commercial entities may be attacked for money, but our government is losing citizen data, trade secrets and actual lives are at risk when organizations such as hospitals cannot function and federal, state, and local computer systems are shut down or sabotaged.

In 2021, Ransomware damage costs will rise to $20B[4]

The average cost of a ransomware attack in 2020 was $4.44 million[5]

1 The Lockton Companies, "Ransomware Impact July 2021"

2 Stastica

3 Verizon

4 Cybersecurity Ventures

5 IBM

2FA, KBA, and the Heavily Burdened IAM Tech Stack

To mitigate the inherent risk of passwords, organizations are layering on "band-aids" to give attackers one more hurdle to jump through. The terminology for this is "Two-Factor Authentication". These tools include text and email-based onetime codes, hardware tokens such as Sec rID fobs, and app-based authenticators.

However, the combination of a password and a code does NOT solve the root problem - a lack of true user identity to prove who is accessing the system. If a user can know a password and receive a code, then so can an attacker, and they have proven this time and time again.

Common methods to intercept these extra layers of security are sim-jacking (cloning someone's cell phone sim card) as well as email phishing and "man in the middle" attacks which give the attacker a code before the legitimate user knows what is happening.

Another form of two-factor password mitigation includes the use of "Knowledge-based authentication", or KBA. This method uses information that only the user is likely to know to help prove they are who they say they are.

If you have ever been asked for the name of your elementary school or your mother's maiden name, you have used KBA. However, due to the myriad of breaches by credit bureaus, KBA data has been leaked and is available for pennies per user on the dark web. For these reasons, KBA is often jokingly referred to as "Known by Anyone" and considered by many to be a near useless form of authentication.

If you have ever been asked for the name of your elementary school or your mother's maiden name, you have used KBA.

However, due to the myriad of breaches by credit bureaus, KBA data has been leaked and is available for pennies per user on the dark web.

Again, the reason that organizations are trying to use two factors is to help mitigate the risk of passwords. Using two factors is the right approach - however, the types of factors are broken.

There are three common types of authentication or factors:

Two-Factor Authentication verifies access to an additional and presumably private communication channel, but impedes workers and alienates customers.

Unless biometrics are verified, the identity behind the login is assumed.

We still don't know who is accessing corporate IT systems and services.

Something you know

(passwords or KBA)

Something you have

(token or one time password)

Something you are

(your biometric proof such as a fingerprint or face)

The centralization of "something you know", has to be reconsidered, because if you can know it, so can someone else, and that is the main problem that passwords create.

Replacing the Password with Identity

Identity online is misunderstood and misrepresented. Organizations determine proof of identity through usernames and password. While it is believed that passwords prove identity on the other side of the digital connection, it actually proves is that someone knows the username and the password, and that could be anyone.

Let's take a minute to look at how we think about identity in the physical world. When someone needs to prove who they are, they provide two factors: Something they have, such as a driver's license or passport, andsomething they are - their face.

Their face is matched to the image on the credential, and the requesting party (i.e. a bank manager, police officer, or customs agent) approves the identity. The credential is trusted and difficult to impersonate. The same goes for the face match. Note how there is no "secret" involved in this transaction. This has been proven effective as billions of people prove their identity in person every day.

It was very difficult to utilize factors such as these for remote authentication for two reasons.

First, giving someone a trusted credential remotely was expensive and very difficult to use. The most common form of remote trusted credential was a smart card containing a chip with a cryptographic secret. These chips are nearly impossible to clone (like a good passport).

However, smart cards never achieved wide adoption because they are expensive and they require specific hardware attached to a computer to function. This made their use nearly impossible in commercial settings. How do you take a smart card reader with you from one location to another, and try to get it to function? Government employees have used smart cards (called CAC or PIV cards) for years but their use is not for the faint of heart.

Second, verifying someone's face or fingerprint remotely was just as problematic. How do you enroll their biometric remotely? How do you prove who that biometric belongs to? How do you overcome the challenges of having a fingerprint reader or facial scanner in someone's home or remote office?

The Tipping Point for Identity Based Authentication

The world we live in today is much different than that of 10 years ago. Advances in several standards and technologies now make remote Identity not only possible but cost-effective and have a marked improvement in user experience.

This is where Identity Based Authentication (IBA) comes into play. In order to make IBA widely adopted, the industry would need to standardize two important aspects of identity: 1) Identity Proofing, and 2) Passwordless Authentication.

Identity proofing can be completed from something as simple as an email to an existing employee, to verifying a user's likeness against government issued IDs. Once a user is verified the path to a strong passwordless experience can begin because each access event is associated with a real, verified identity. This concept is the cornerstone for a zero-trust framework, as it enables high identity assurance for every user authentication attempt.

Identity Standards Mature and Define Strict Specifications

NIST 800-63-3 for Remote Identity Proofing

In 2017 the NIST government standards body released a standard called NIST 800-63-3. This standard defines strict criteria for the management and technical operations for how you enroll an identity and use that identity in a secure fashion. There are three "sections" in this standard.

As previously mentioned, until recently it was very difficult to prove someone's identity remotely. Now with billions of people having very capable smartphones and computers, users can enroll their physical identity documents with a high degree of security and accuracy.

A typical method is to have a user take a picture of their drivers license and/or passport and validate them via their overt and covert security features such as watermarks and holograms. They can also be verified with the issuing authority such as a DMV or state department.

Then, the user takes a live "selfie" photo or video that is used to compare the holder's real face to the face on the government documents. This selfie can be used as an authentication factor called "LiveID™" that we will cover later.

When you enroll two forms of strong identity documents, you can achieve 800-63-3A "IAL2" or Identity Assurance Level 2.

Kantara NIST 800-63-3 Full-Service Provider Certification

An organization called Kantara conducts conformity assessments to the 800-63-3 standard and provides a grant of Trust Mark when all requirements of the standard have been met.

Banks, for example, as part of compliance with Know Your Customer (KYC) mandates would need to perform IAL2 identity verification at a minimum for remote new account creations. Certification to 800-63-3 by Kantara versus the lesser standard of conformity to the guideline would be required to support this requirement.

Remote identity proofing has many business applications. Generally, these fall into two categories: 1) Business-to-consumer, and 2) Business-to-worker.

We've mentioned the KYC requirements in banking, which is a legal requirement implemented in part to help fight the funding of terrorism and money laundering. There are several other industry use cases typically characterized by long-term B2C relationships where it is essential to establish trust with individuals interacting with the organization remotely before engaging in commerce. These include remote learning/higher education, telco, online gaming, government, travel, healthcare, utility, real estate, and legal services.

Convergence of Identity Proofing and Passwordless Authentication

It is the combination of these two functions, proofing and passwordless, that allow for IBA. Certified identity proofing to the NIST 800-63-3A guideline combined with certified FIDO2 authentication provides authentication with a high level of certainty of the identity at the other end of the connection.

This effectively brings identity into the security perimeter of the organization in a way that has not been possible for much of the past six decades since the password was invented, removing anonymity behind compromised credentials. With IBA, credentials cannot be borrowed.

This leaves two other threat vectors that need to be defeated. First, the biometric needs to be to the greatest extent possible, sophisticated and non-hackable. A "live selfie" with technology to detect depth of field, specific facial movements, and telltale signs of photo and video manipulation and that provides application-specific authentication (versus device-level) is an absolute must.

Second, biometrics among all other personally identifiable information are by nature extremely personal and represent a high value target for hackers. Anytime they are collected and stored they represent a target. Centralized storage and administration provides the biggest target of all, even if encrypted because administrators can be tricked and are under near continuous attack from all possible angles. This makes distributed storage and access via cryptographic private key a vastly superior model. Private blockchains (AKA distributed ledgers) are ideally suited to this use case. Private blockchains (AKA distributed ledgers) are ideally suited to this use case because the data is encrypted, only accessible via the user's public/private key pairs, and it places ownership of the identity on the user.

Conclusion

The convergence of Identity Proofing and Passwordless Authentication results in a convenient user experience that is impervious to credential theft, removing significant threats posed by unauthorized users logged into the corporate IT network including data breaches, ransomware, commercial espionage, financial fraud, and more.

Modernizing customer and worker onboarding with identity proofing eliminates administrative overhead, reduces business process cycle time, eliminates data key errors, and drives downstream efficiencies for any business process where user information is required. Organizational agility improves to respond more quickly to change or to new user demands.

But, let's circle back to basics.

Only recently have our electronic devices become able to identify us by physical characteristics and true to the course of innovative technologies, standards bodies have evolved to help define the best way for those devices and the various technologies surrounding them to interoperate.

Without a doubt, authenticating with identity simplifies the IAM IT architectures that revolve around passwords and all that is required to store, protect and add 2FA security layers on top of them, but which still fail to protect the organization from catastrophic attacks. To some, this represents a threat. They want to continue to tweak the existing password-based approach.

But for organizations that are no longer willing to expose their operational plans to the threat of disruption that comes from identity-based attacks, Identity Based Authentication provides a path to unwind the highly complicated IAM IT infrastructures that has grown out of control over the decades.

They have come to realize that password-based authentication relies on the hope that the password is kept secret, but it survives because of fear, uncertainty, and doubt about how to change to passwordless authentication and out of sheer denial that the basic "shared secret" approach they represent is a deeply flawed and limiting approach. Identity Based Authentication gives the organizations a path to simplify along a journey that is easy to deploy, highly effective, and that users prefer.

Using Identity Based Authentication ensures legitimate new account creations, prevents account takeover (ATO), and secures financial transactions against fraud by servicing as a strong user authenticator, but it does this in a highly scalable way because the standards on which it is based (specifically NIST 800-63-3) provides for a high level of off the shelf connectivity via APIs without the need for custom coding.

But, maybe most importantly, legitimate users generally like to be recognized. Criminals do not. And that seems to make all the difference for organizations who are deciding they will no longer be held hostage to threats posed by identity deception.

About 1Kosmos
1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.

1KOSMOS