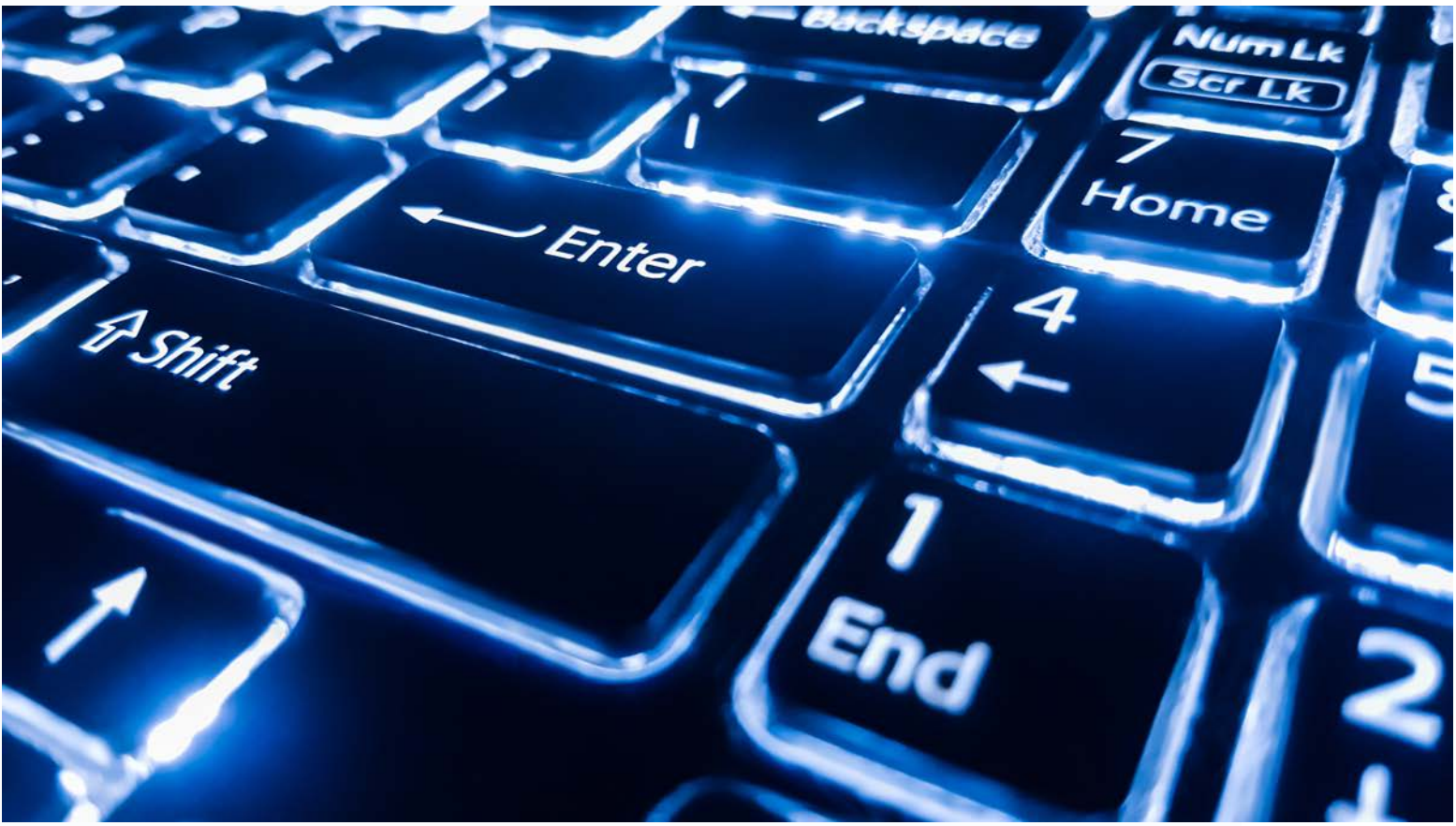
Biometric Typing and Other Multi-Factor Authentication Methods

WHEN PASSWORDS ARE NOT ENOUGH

CO-AUTHORED BY:

typingdna

Optimal IdM

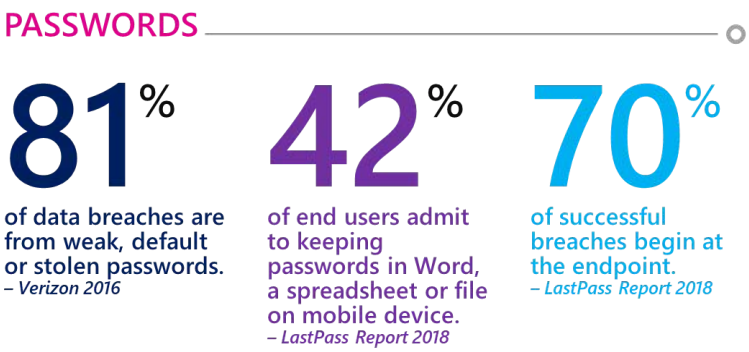


Background

Password policy and hygiene have long challenged even the best I.T. shops. It is not just end users who are to blame for using weak and reused passwords, phishing scams and storing passwords where they can easily be accessed are culprits. I.T. also bears responsibility for not properly, monitoring and securing their Identity Provider (IdP), usually Active Directory (A.D.) as well as the lack of enforcement and visibility into security measures to properly protect passwords.

Many of today's security threats target user passwords/PINs. Username + Password (U/P) requires only one secret – the password. Password/PINs as the only secret to access resources (applications, files, objects, etc.) are insufficient security for access to most resources. They represent a single point of vulnerability.

The I.T. Security industry recognizes that username and password combinations as a single source of authentication are inadequate authentication methods for access to important resources.



Problems With Passwords

- **Passwords are guessable.** They are subject to dictionary and brute force attacks – especially weak ones. Even complex passwords with 'adequate' encryption are vulnerable because compute is cheap in today's cloud world. It's not difficult to leverage the power of the cloud to quickly guess passwords.
- **Passwords are rarely changed** – even when known to be already compromised.
- **Passwords are often reused** from/for other sites. End users mix their personal passwords with their work passwords. It's normal user behavior, but extremely risky, especially when leveraging SSO. Breached passwords absolutely should not be used again.
- **Passwords are written down**. How many times have you written down a password on a Post-It note or seen someone else's passwords on one? There are documented instances of attacks against passwords that were written down and exposed through a picture posted online.
- **Passwords are shared with others** – with friends, family, with helpdesk, and 3rd parties via phone.
- **Passwords are sometimes freely given to hackers** by end users through phishing attacks – usually through email.
- **Passwords left at their vendor default values** - some administratively privileged accounts have been set to a default value provided by the hardware and software vendor and not changed by the organization. These 'secrets' are well known in the hacking community and put the enterprise at risk.
- **Passwords are sent over open networks** constantly open to impersonation attacks
- **Passwords are vulnerable from insufficient encryption** at the corporate level, also vulnerable when stored in bulk databases with weak admin passwords and man-in-the-middle attacks.

Complex Passwords

Many 3rd party consumer services (applications and IdPs) and corporate environments have taken steps to require more complex passwords. More complex passwords are recommended; however, complex passwords, by themselves, can give a false sense of security.

Password complexity requirements mitigate risks of passwords being easily guessed; however, passwords still represent a single secret needed to gain access. Phishing attacks, malware, keystroke loggers, man-in-the-middle attacks, password reuse and a host of other potential attack vectors are still not mitigated by a more complex single (password) secret.

Single Sign On and Passwords

Single Sign On (SSO) often relies on a single source to store credentials. SSO with a complex password, can provide some mitigation against certain attacks. A single trusted provider can provide the secure credential storage foundation to leverage SSO relatively safely. SSO, in a secure Identity Provider (IdP), represents a reduced attack vector versus having your credentials spread out and stored at dozens of sites.[3]

Facebook, LinkedIn and Google+ are examples of consumer IdP services, while familiar corporate IdPs include, Active Directory, Salesforce, Azure A.D. and Optimal IdM's The OptimalCloud.

Corporate IdPs are considered secure, but they certainly are not impenetrable. Good companies, like LinkedIn, have had historically giant password breaches. Even Mark Zuckerberg had his credentials leaked. He, like many users, reused a password he used at other social media sites.

Secure storage of credentials is essential to password security; however, although credentials may be stored safely in an IdP, that won't help if the password is weak, already breached, reused, shared, phished, etc. SSO leveraged with already compromised credentials, weak or reused passwords put individual and corporate assets at high risk. What is needed is greater assurance that the password truly[4] belongs to the rightful owner of the identity.

The answer seems obvious. Require an additional secret before granting access to resources. An additional authentication factor provides greater proof of ownership thereby mitigating risk of an impersonator reusing your credentials.

Identity is today's firewall

Mitigation of Password/PIN Single Secret Vulnerabilities - Why Another Factor

Users cannot control the security of the storage of their credentials in IdPs but can take immediate steps to mitigate the inherent weakness of using only a single secret (password). Leverage MFA when it's offered.

Password/PIN vulnerabilities as the only authentication secret is unnecessarily risky in today's enterprises. The risks of using only a single U/P secret is big enough that several regulatory bodies require additional factors for authentication. Even without regulatory compulsion, security conscious organizations leverage additional authentication factors, because the risks are too high not to. Password breaches can devastate an organization. It's not just the obvious asset and monetary losses, but additionally the reputation of the organization. Reputational damage is something that some organizations cannot fully recover from.

> **Enterprises rarely track successful logins. Therefore, a successful breached password login allows a hacker unreported access to critical resources. That's one of the reasons that most hacks go unreported for nearly 200 days.**

Usernames and passwords (U/P) with at least a second factor is the authentication standard for many security conscious enterprises. It's this additional layer of 'proof' that mitigates the risk of impersonation and provides the proper identity assurance for enterprises. The additional authentication factor(s) go beyond what you know (password) to what you have (a device, smartcard, token, etc.) and/or something you are (biometrics).

An additional factor of authentication allows security to be maintained by an additional, separate, system. Even if the password is breached, the impersonator would have to possess the additional authentication factor to access resources.

At a minimum, a second factor should always be leveraged with privileged digital identity accounts, when any user access private confidential resources or when users perform certain operations (e.g. add, change, delete data). The MFA security challenge to access privileged data and privilege operations in your enterprise dramatically reduces the risk to the organization.

When the risk of the impersonation outweighs the cost of the MFA solution, implement MFA.

Forrester Research estimates 80% of today's security breaches involve privileged credentials.

[1] Forrester Wave: Privileged Identity Management, Q3 2016

MFA Lessens the Attack Vector

Multifactor Authentication (MFA) extends the organizations cybersecurity footprint and significantly lessens the attack vector for digital identity impersonation attempts. MFA does so by requiring additional verification (proof) that the digital identity trying to authenticate is, in fact, the one intended.

Common methods of MFA provide visual cues for end users to view and enter information and require additional user interaction – like approving a PUSH notification on their device and/or entering a generated PIN secret to login.

What If My Application Doesn't Support MFA

Specific applications don't have to natively support MFA to leverage it. Most applications, both on-premises and cloud, can leverage MFA during the login authentication process through SSO vendors.

Look for vendors that have a robust MFA offering to provide enterprises flexibility of choice between security and usability.

Common Customer Requested MFA

- SMS Passwordless authentication
- Strong-Authentication via E-Mail (MFA)
- Strong-Authentication via SMS/Text Message (MFA)
- Strong-Authentication via VOICE (where a call is placed to a number) (MFA)
- Strong-Authentication via TOTP (MFA)
- Strong-Authentication via PUSH (alert to a mobile device) (MFA)
- Basic Authentication + Strong-Authentication via PUSH (alert to a mobile device) (Fingerprint authentication to iOS and Android) (MFA)
- Universal Second Factor (U2F)
- RADIUS
- Client Certificates
- Common Access Card (CAC)
- Native REST Web
- Other methods with the Optimal IdM built-in API extensible framework

* All are Optimal IdM supported MFA methods

Deployment

To provide maximum agility for organizations, an identity vendor should offer multiple MFA deployment methods to onboard users. Options include automatic provisioning through policy, bulk onboarding of users, or requiring end users to use the self-service options in their SSO portal – which takes the burden off your helpdesk.

> **Consider that shared, multi-tenant SaaS MFA services (which make up a bulk of the MFA vendors) can only offer simple configuration choices between MFA options. However, Optimal IdM can offer deep, granular customized authentication workflow rules to enforce MFA based on your business needs and regulatory requirements. Optimal IdM can do this because we provide each customer a completely separate, single-tenant IDaaS MFA service.**

Choice Factors for MFA

Common decision factors for MFA include:

- Cost
- Inclusivity of support for applications on-premises, hybrid and cloud applications
- Customization and workflow options
- Regulatory compliancy of the MFA solution
- Complexity to deploy
- Delivery of tokens (portability)
- Maintenance cost (e.g. of additional hardware tokens),
- End user experience (usability)

Why Not Require Multifactor for Every Authentication Attempt?

If MFA is more secure than a simple username + password (and it is), why not require MFA for every authentication attempt?

There are a few enterprises and many government agencies that do require MFA for, at least, the initial login attempt. Even so, few require MFA for each authentication attempt against a new resource or actually requiring a second factor reauthentication within a session.

The issue for enterprises is that MFA can provide a substandard and frustrating user experience, especially if the end user is constantly prompted to enter additional information. A poor user experience affects productivity and pits the end-users against I.T. Politically, often the end users win – even at the cost of corporate security.

MFA should be as transparent and user-friendly as possible, while still providing maximum risk aversion for the organization.

Step-up Authentication

Even extremely secure networks are aware of the poor user experience that MFA sometimes provides. It's not just the user interface, but the interruption of the end user's productivity. Therefore, it's common to leverage MFA as an additive method at selective times. This is known as "Step-up Authentication."

The MFA challenge required to access a resource, beyond the standard U/P, is considered "step-up authentication." Step-up authentication allows the organization to place security policy to control access to important resources selectively through additional MFA challenges.

To be clear, step-up authentication is not MFA. Rather it is a selective, evaluative process to determine when MFA is going to be invoked. An agile step-up authentication policy may invoke different types of MFA depending upon business and regulatory needs. Examples of step-up authentication include static policy and dynamic policy expressions.

Both static policy based and dynamic, risk-based authentication are examples of step-up authentication.

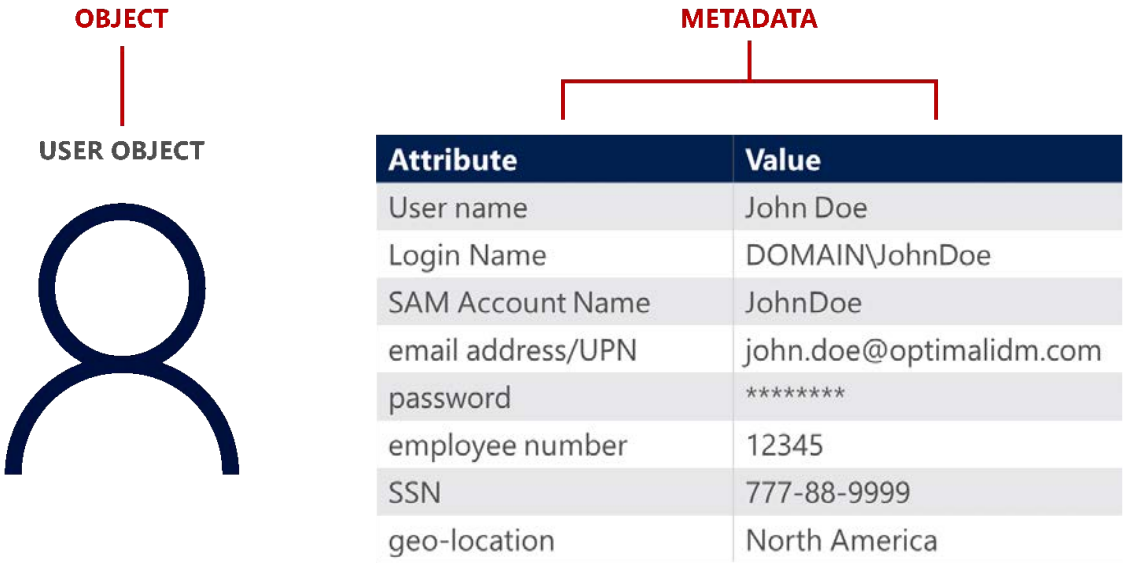
Rule-Based Multifactor Authentication

One simple way MFA is deployed is as a static (IF-THEN-ELSE) policy against certain resources. For example, IF a user tries to access the payroll app, THEN require MFA.

Role based access control (RBAC) is an example of static, rule-based policy – sometimes referred to as 'coarse grained' authentication. IF a user is a part of 'admin-group' THEN require MFA at login.

Unfortunately, the state of cybersecurity and the needs of today's enterprises render such simplistic rules as too narrow in some circumstances and too broad in others.

A policy based on conditions, sometimes complex conditions, would be an appropriate choice for enterprises that want to balance the need between security, user productivity and end-user experience.



Risk-Based Policy - Adaptive Authentication

Many have chosen to implement levels of AuthN challenges based on relevant conditions of the AuthN. There could be dozens of possible AuthN 'conditions.' Each 'condition' is given a score based on the risk it carries and when the score is tallied by the system each time that access to a resource is requested by an identity.

When a resource is considered low priority, a simple U/P may be enough. Other resources, like accessing payroll website (or file or app), are considered higher risk to the organization and should require an additional authentication/access check before allowing access.

A 'risk score' is the sum of calculated risk factors (from metadata). The resultant score from a risk calculation is evaluated against a set threshold to determine whether access should be granted, denied or challenged from an additional authentication factor (require MFA).

Each 'risk' is assessed by scoring metadata. The metadata can be from one or multiple sources – e.g. directory services, databases, etc. The metadata is going to be used strategically digital authentication attributes.

For example, risk can be measured against metadata stores from directories, employee information, readable information returned in a SAML token, and even derived based on user behavior analytics. Other scores can be applied to where and how the digital identity is authenticating from – e.g. geo-network location, originating IP addresses, recognized/trusted devices, recognized browsers, suspicious networks.

Four (4) simple, example risk factors include:

Criteria	Example
Source of User's Identity Provider	SSO user coming in from a social network login will be considered less 'secure' than those leveraging the corporate IdP.
Device	Is the device registered and recognized as 'trusted'?
Roles	User's assigned certain roles, like Admin, have higher risk scores.
The Resource Being Accessed	Confidential resources will have higher risk scores.

'Risk scores' can be a secretive, proprietary formula from a vendor or can be customized to an organization's business and regulatory risks.

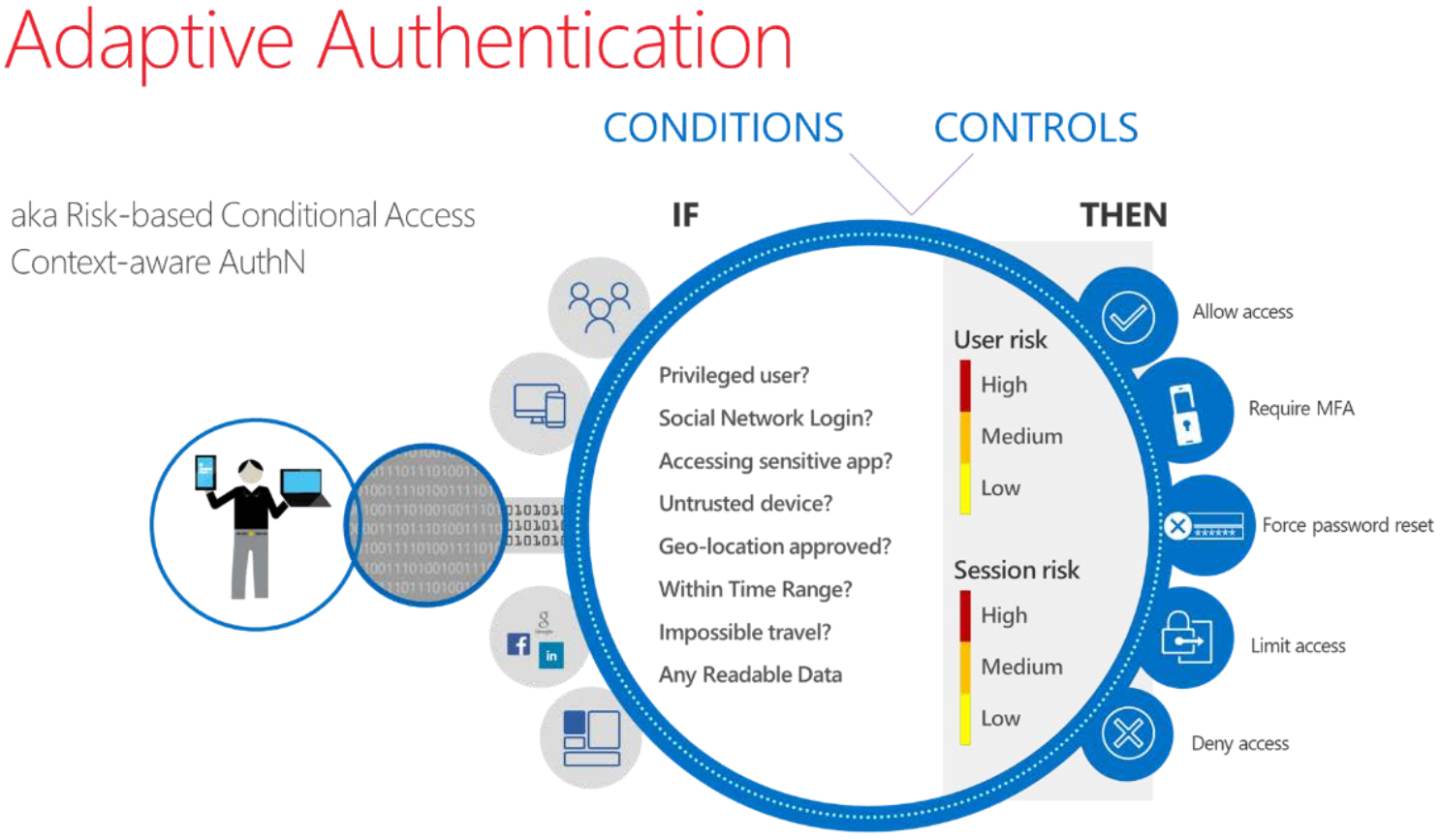
The terms Adaptive Authentication, Context-Aware Authentication, Risk-based Authentication, Attribute Based Access Control, Conditional Authentication, Conditional Access, and Dynamic Access Control are different, but are sometimes used interchangeably. Make certain you compare apples to apples when researching between vendors.

Adaptive Authentication

There is a concept of access control that evaluates the context of where the user is coming from and evaluates the conditions of the user login in relation to the resource (application) it's attempting to access to make access decisions. Adaptive authentication goes a step beyond the risk-based policy expression authentication to one where additional factors are invoked during the authentication session.

Reputable vendors can evaluate the context of the login based on a multitude of metadata factors such as geolocation, IP Address range, browser, known device, within a time range, type of user (privileged user), if originating AuthN came from a social network (e.g. Facebook, etc.) as well as other possible conditions before invoking MFA, to provide a balance of user experience while protecting corporate assets.

Each time a 'condition' is evaluated, a 'control' is possibly implemented. The value of this approach is that MFA is leveraged based on a risk calculation. This method contrasts with traditional login and reauthentication as it provides more controls to determine risk to determine if/when reauthentication is invoked. Also, because reauthentication challenges only happen when really needed, the user experience is massively improved.



Adding MFA within a Login Session

MFA can be leveraged multiple ways during a user's session (after successful login). This can be a static, fixed period reauthentication requirement, or based on user's inactivity during the session. The latter is called a 'sliding session.' The sliding session is basically a token based on some time interval (say, 5 minutes) that will count down only when there is no user interaction. After the countdown, the session is expired, and the user logged out. These examples are considered more secure than a persistent login that doesn't require reauthentication. Sliding sessions are often found in the financial industry, whether through a mobile app, or through a webpage.

Reauthentication During a Session

The benefits of enforcing reauthentication due to user inactivity are straightforward.

Reauthentication during a session, regardless of user activity is also considered a best practice. A security challenge beyond the U/P enforced at some interval gives the authenticator a higher assurance that the identity is still from the initial claimant.

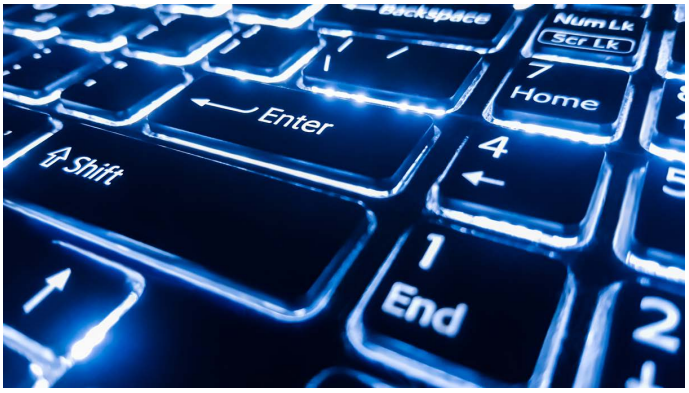
The U.S. Government NIST Standards for Authenticator Assurance mandates that reauthentication is enforced when user inactivity is detected within a session. The session timeout is based on the Authentication Assurance Level (AAL) being enforced – Level 1, 2 or 3. AAL1 requires reauthentication only every 30 days regardless of user activity within a session. AAL2 requires reauthentication at least once every time the sliding session reaches 30 minutes due to user inactivity and at least once every 12 hours even if the user is active in the session. For AAL3, the highest defined assurance level, requires reauthentication with an additional factor every 15 minutes during a session where there is user inactivity and reauthentication with an approved additional factor must be invoked a minimum of once every 12 hours.

Therefore, the expanded use of MFA within sessions are going to provide an additional layer of assurance and mitigate risk associated with impersonation.

Better Biometrics Through Your Keyboard

The challenge to any MFA solution is to minimize end-user disruption and maximize security. It's a balancing act that all I.T. environments consider.

What if gathering unique identity data, used to enable MFA, was invisible to the end user? This could be accomplished through some type of artificial intelligence (AI) that could, for example, evaluate a unique and trusted trait of the end-user – like their typing behavior.



People type differently. Uniquely and individually. Look around your office: Someone is hunting and pecking, someone is mashing keys like they were punishing their keyboard, and a touch typist is flying along with speed and grace. Those variations in personal style are unique to each individual – one keyboard masher won't pound the keyboard exactly like another, and they are nearly impossible to copy.

A good typing biometric company can capture and record each individual's unique keystroke typing signals and turn them into typing patterns. Then, their API engine analyzes and leverages machine learning (AI) against previous patterns to prevent impersonation. This learning process can build a secure user profile pattern in as few as one or two initial typing samples.

It is important for these typing biometric vendors to not store the password, only record how the password was typed. On the backend, encrypting and storing all relevant behavioral data and associates it only with credentials.

Typing Biometric Login Experience

The benefit to this approach is that nothing is replaced in the user's normal login experience. The typing biometric authentication happens passively while users type in their credentials.

When a login page is presented to a user, they type in their credentials. As they do so, their credentials are sent to the identity provider (e.g. Active Directory, Optimal IdM, Facebook), and, as an additional factor of authentication, the user's typing behavior is evaluated against the biometric company's recorded unique known typing patterns for that user. If both match, authentication is successful. This is all done invisible to the end user.

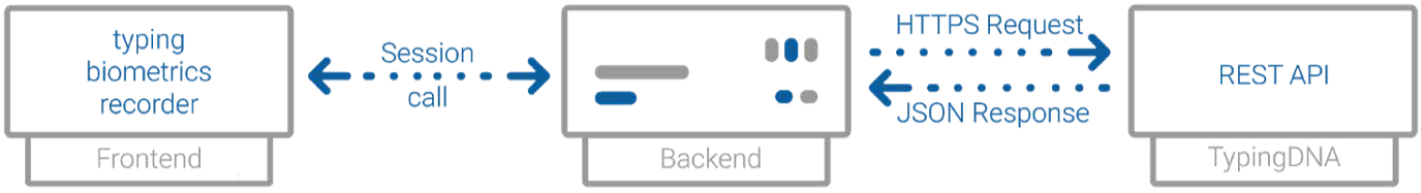
Typing Biometric MFA For Any Organization

Typing biometrics is an authentication method that can be part of an MFA suite or as part of an adaptive authentication system.

The biometric firm, TypingDNA, integrates a data recorder with an organization's authentication system. The recorder listens for events or behaviors. When a typing pattern is detected, a proprietary algorithm checks to see if it matches any records in the database of user typing profiles.

Leveraging typing biometrics as an additional authentication factor provides an excellent user experience because the user has no additional hardware to purchase, carry, maintain and replace. The user doesn't have to remember an additional secret.

Typing DNA can be leveraged in nearly any MFA authentication model – static policy-based, dynamic risk-based, adaptive, within a session, etc. TypingDNA's agility would be an asset to any organization's security policy.



Replay Attacks

A replay attack is an attack that maliciously repeats or delays a valid data transmission. For a replay attack against typing biometrics to be successful, the attackers would need the exact string of characters their target had typed. If attackers just find the typing pattern but don't know the pattern is for J-O-H-N, they won't know what characters to type to match the pattern.

When TypingDNA detects typing activity outside the baseline stored for a user, TypingDNA will not complete the authenticate process. This provides resistance to impersonation attempts.

Best Practices for More Secure Authentication

- Implement password policies
- Require complex passwords
- Require unique passwords for every IdP and site
- Enforce password changes for breached passwords
- Choose a vendor that can support single-tenant, granular customization to your identity and cybersecurity SSO implementation
- Revoke employee passwords after they leave the organization
- Log, audit, report and monitor authentication activity
- Implement and leverage multifactor authentication immediately as additional authentication assurance
- Leverage Step-up authentication to provide a better user experience
- Leverage Adaptive Dynamic Risk Policies to challenge access to important assets
- Enforce additional factors of authentication every AuthN for specific roles/groups – e.g. administrative accounts and groups
- Leverage MFA for in-session reauthentication based on user inactivity – sliding sessions
- Leverage reauthentication within a session regardless of user activity for in-session based on an agreed corporate policy

Typing biometrics provides a frictionless additional factor authentication experience.

ABOUT TYPING DNA

TypingDNA (a Techstars backed company) is an established, innovative behavioral biometrics SaaS company that offers highly accurate typing biometrics solutions. This AI-based technology makes it easier to prevent fraudulent activity such as identity fraud, through keystroke dynamics. TypingDNA's existing commercialized product recognizes people based on the way they type, which offers a non-obtrusive security measure that doesn't require any special equipment.

The company's approach to login authentication has garnered a lot of praise, including being named the Best Newcomer Company from the CESA Regional Awards and earning a spot on the EUTOP50 for Driving the Future of Tech in Europe. Visit www.typingdna.com for more information.

ABOUT OPTIMAL IdM

Optimal IdM is a provider of innovative and affordable identity access management solutions. Optimal IdM partners with clients to provide comprehensive and customizable cloud and hybrid identity solutions that meet their specific security and scalability needs. Customers include some of the largest corporations and government agencies around the globe. Visit www.optimalidm.com for more information.