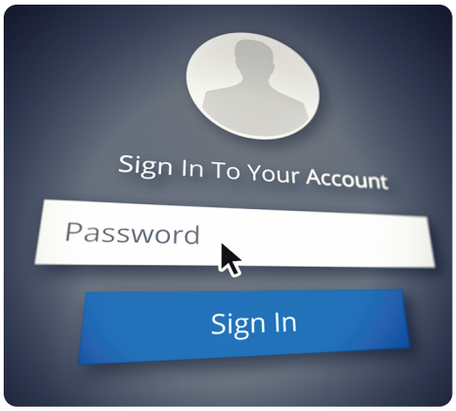
WHITE PAPER

Securing the Enterprise with Advanced Adaptive Multi-Factor Authentication

Contents



INTRODUCTION

As government and regulated industries migrate to the cloud, they require advanced, multi-factor authentication and identity attestation to maintain compliance, fend off data breaches, and prevent fraudulent transactions. This paper describes how organizations can secure credentials from theft and misuse, by employing advanced adaptive multi-factor authentication technologies.

THE CHALLENGE: SECURING CREDENTIALS IN REGULATED INDUSTRIES

Cloud computing offers organizations the ability to develop new technologies in less time, with a lower barrier to entry. As security leaders in government and regulated non-government enterprises migrate to public, private or hybrid cloud, they require strong security to prevent data breaches, protect sensitive information, and maintain compliance.

The implementation of the General Data Protection Regulation (GDPR) in 2018 inflicts penalties for a data breach on any company that holds data on European Union citizens—regardless of where the company actually does business.

Organizations in regulated industries must adhere to even stricter guidelines on how they treat sensitive data, such as financial or healthcare records. A data breach can result in penalties as severe as federal investigation, fines, prosecution and even shutdown. This higher level of liability means that organizations need to take a more deliberate approach to moving applications, systems and data to the cloud. They may choose to keep some sensitive applications and data on-premises or migrate them to a private cloud over time.

Stolen credentials continue to be the leading cause of data breach[1], and this trend is widespread in both healthcare[2] and financial services. Securing credentials and improving how users gain access to sensitive systems and applications should be the highest priority for regulated industries.

Password-based authentication
Most people can remember only a few passwords and tend to reuse them across different accounts. Attackers know this, so using stolen credentials to log into other web applications is their primary method of attack[3].

Cybersecurity experts recommend using a password management tool to generate and store unique, strong passwords. But a recent survey of US online adults found that only 12% of respondents use password managers. 65% rely on memorizing passwords, 41% share the credentials to their online accounts with friends or family members, and 39% reuse their passwords across multiple accounts[4].

Phishing relies on habit and human error
People are accustomed to entering their username and password to authenticate to cloud applications. Phishing campaigns rely on this habit and human error to trick their targets into clicking on a link or opening an attachment in an email or text. The web page—maybe a spoofed email or bank account— appears to be valid, so they enter their credentials and open the doors to data breach.

Weak applications invite attack
Cloud applications are also weak. The Open Web Application Security Project (OWASP) Foundation's 2017 Top 10 lists broken authentication as the second most common security risk[5]. When applications in the cloud have broken authentication, they may allow weak passwords, permit using default credentials (such as "admin/admin"); or allow authentication with plain text, encrypted or weakly hashed passwords. Credential stuffing botnet attacks inject breached password lists and password cracking dictionaries to gain access to accounts. This type of brute force attack is commonly experienced on retail and financial services sites[6].

[1] 2017 Verizon Data Breach Investigations Report
[2] https://www.healthdatamanagement.com/list/assessing-the-10-largest-healthcare-breaches-of-2018
[3] 2018 Verizon Data Breach Investigations Report
[4] Americans and Cybersecurity, http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
[5] 2017 OWASP Top 10, https://www.owasp.org/index.php/Top_10-2017_A2-Broken_Authentication
[6] Akamai: State of the Internet / Security: Credential Stuffing Attacks, vol 4 issue 4, 2018.

Many applications are also built with out-of-date components. OWASP cites "applications using components with known vulnerabilities" as the 9th most common security problem found[7]. Unpatched systems make it possible for an attacker to impersonate any level of employee—not just the CISO or IT director—and move laterally through the network, elevating their privilege levels to gain access to sensitive and potentially lucrative information.

Even single sign-on has its problems

Enterprises use single sign-on (SSO) and identity federation to enable passwordless access to cloud and on-premises applications, VPNs and system resources. But vulnerabilities can exist even in Single Sign On protocols like SAML 2.0, allowing attackers to login as other users without even entering an SSO password[8].

STRONG AUTHENTICATION

Organizations can reduce the risk of data breach from credential theft by reducing or eliminating the username & password combination and using strong authentication technologies as additional layers of protection. They can apply different authentication methods and policies based on risk signals—such as logins from unusual locations or devices. Strong, or "multi-factor," authentication requires users to identify themselves with at least two mutually independent factors that are difficult to guess, find, steal or manipulate.

TYPES OF AUTHENTICATION FACTORS—PROS AND CONS

Knowledge: something you know [Passwords, security questions, PIN codes]

- **Pros:** Knowledge factors can be secure if they are used with another authentication factor before a user is granted access to a system. For example, someone can enter a PIN code to authenticate to their device's embedded cryptographic module. Separately, the device can attest to the user's identity for the service they are requesting access to, without transmitting the PIN over the internet.
- **Cons:** Security questions—such as your mother's maiden name—can be retrieved from public records. PINs and passwords are often reused across accounts—increasing the potential attack surface to other sites.
- **Recommendations:** If you must use knowledge factors, combine them with other authentication factors.

Inherence: something you are [Biometric identifiers: fingerprint, voice print, retina scan, facial recognition, behavioral biometrics]

- **Pros:** Biometrics are harder to duplicate and are unique to each individual. More advanced biometrics, such as behavioral biometrics, can also be used to authenticate to cloud, web, mobile, and on-premises applications[9].
- **Cons:** Biometrics are permanent; fingerprints can't be changed. Biometrics templates stored on a server can also be hacked. Many biometrics templates have been available across multiple databases for a long time and are vulnerable to attack. Raw fingerprint scans of 5.6 million current or former US government employees were stolen in the 2015 Office of Personnel Management hack, for example[10]. Biometrics don't rely on an exact match, as with a password, and don't work for all situations and populations. They are mostly used for convenient unlocking of mobile devices. Other biometric factors, like iris scanners, may be faked by a high quality photograph.
- **Recommendations:** Use biometrics to identify a user to hardware with an embedded cryptographic module—e.g. the Trusted Platform Module (TPM)—on

[7] https://www.owasp.org/index.php/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities

[8] https://duo.com/blog/duo-finds-saml-vulnerabilities-affecting-multiple-implementations

[9] https://www.crossmatch.com/press-release/hid-global-acquires-crossmatch-expand-biometric-identity-management/

[10] https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/

a laptop, iOS Secure Enclave, or Android Trusted Execution Environment. The biometric identifies the user to the device, but the isolated encryption modules do not send biometric information over the Internet. An authentication service can use this biometric identification, along with trusted device status and mobile authentication methods, to allow access to certain cloud applications.

Possession: something you have [Hardware token, smart card, mobile device with push notification, mobile device or hardware token with One Time Passcode]

- **Pros:** Tokens are hard to duplicate. Authentication credentials are stored in the device. Hardware tokens can authenticate users to workstations, cloud applications and buildings. They can also be used to sign transactions in finance and pharmaceutical prescriptions or encrypt hard disks and emails. Mobile device authenticators are convenient because most people with smart phones carry them at all times.
- **Cons:** Tokens and fobs are easy to lose. One Time Passcodes (OTP) sent to phones are vulnerable to man-in-the-middle attacks if credentials are not secured. Soft OTP tokens on mobile are more vulnerable to attack if the OTP seeds can be extracted from the device. The networking protocol used for SMS is vulnerable to attack[11].
- **Recommendations:** Choose the possession factors based on your organization's objectives and compliance requirements. If using mobile devices for OTP authentication, choose a solution that generates the OTP seeds independent of the device ID and add a mobile application security feature (since generating an OTP on a hacked mobile is useless). Avoid SMS. Choose solutions that have been independently certified for compliance with standards bodies like the National Institutes of Standards and Technology (NIST).

Adaptive and risk-based authentication: where you are, what you do

Additional context can help determine the validity of an authentication request. Multi-factor authentication policies that consider factors such as the user's location, IP network and trusted device are the basics of an adaptive authentication framework.

Financial services organizations that are required to comply with cybersecurity regulations such as PSD2[12] and NYCRR PART 500[13] have begun using risk-based analytics solutions to determine whether an authentication attempt is valid. This type of analysis examines hundreds of behaviors—invisibly to the end user— and records and assigns a risk profile. Based on the risk profile, policy can be assigned to determine whether to allow, require step-up authentication/require internal manual review, or deny access.

- **Pros:** Context-based authentication adds more information to the authentication request to determine if the user is valid and puts little to no burden on the user in normal circumstances.
- **Cons:** Not all organizations can afford an advanced risk analytics solution. Static context-based policies can be spoofed.
- **Recommendations:** Create context-based policies broad enough to account for different situations and use them as part of a layered cybersecurity strategy—not as the main authentication method.

COMBINING MFA METHODS

It is important to choose the right combination of authentication methods and understand the security benefits and risks of each.

Least secure: combining two things you know

Many cloud applications require more than one factor of authentication, often in the form of username+password and security questions. Since passwords and security

[11] https://pages.nist.gov/800-63-3/sp800-63b.html
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015L2366
[13] https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

What is FIPS certification?

The Federal Information Processing Standard (FIPS) is a United States Government computer security standard that is essential for many branches of the US government and federal contractors, and also corporations in the private sector that work with the federal government to collect and transmit sensitive information.

FIPS 140-2 has three levels of security for cryptographic modules.

Level 1: cryptographic security with no requirements for physical protection. Examples: software on a computer or mobile device.

Level 2: hardware with tamper resistance to the cryptographic module. Examples: USB authentication tokens.

Level 3: adds secure communication between a physical device and the software applications.

Example: HID ActivID Authentication Server with optional FIPS Level 3 Hardware Security Module

FIPS 201 is the United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

Example: Credential management systems for PIV smart cards.

questions are both knowledge factors, they are considered "dual single factor" rather than multi-factor authentication. MFA should combine different factor types, such as something you know with something you have.

More secure: something you have + something you know

Combining two or more authentication methods of different types is more secure.

Organizations supporting cloud applications can require users to authenticate to a single sign-on service, then be prompted to provide another way to assert identity. This could mean inserting a registered cryptographic hardware token into your computer USB port or responding to a push notification on a trusted mobile device before being granted access to various applications.

Smart cards or mobile smart cards with a user's digital certificate are also considered effective two-factor authentication because they combine the hardware card or mobile device, digital certificate and a PIN that the user has to enter.

Most Secure: advanced adaptive multi-factor authentication

Advanced adaptive multi-factor authentication is a practice that employs secure credential management, digital credentials including PKI certificates, contextual access policy and risk-based authentication methods.

Advanced adaptive MFA is recommended for government and other regulated industries that collect, store, transfer, share and disseminate sensitive information—such as finance, insurance and healthcare. Entities that protect critical infrastructure like power plants, gas pipelines and defense systems can also benefit from implementing advanced adaptive multi-factor authentication that includes logical IT access and physical access controls.

Striking the right balance: security, cost and user experience

When choosing an advanced adaptive multi-factor solution, consider how it will fit into your organization's overall security policy. Which applications and systems require the highest security? When should the authentication methods be restrictive or permissive? How many security experts are available to design and maintain authentication policy? Is physical access control part of your cloud access strategy?

ADVANCED ADAPTIVE MULTI-FACTOR AUTHENTICATION SOLUTIONS FROM HID GLOBAL

HID Global offers a broad range of advanced authentication, credential management and analytics solutions that meet a wide range of security requirements.

AUTHENTICATION SOLUTIONS

Each HID authentication solution is certified by independent third party labs to be compliant with the National Institute of Science and Technology (NIST) and the Federal Information Processing Standard (FIPS).

HID Approve mobile authentication app

HID Approve™ is a Mobile Multi-Factor Authentication app that provides secure and easy-to-use authentication using a mobile device. HID Approve offers push notifications or secure One Time Passcode authentication and transaction verification to protect VPN, cloud and on-premises applications. HID Approve can also be used as the first authentication factor to applications or single sign-on portals, for organizations wishing to eliminate password-based authentication. HID Approve is certified FIPS 140-2 Level 1.

ActivID Authentication Server

ActivID® Authentication Server is available as a virtual appliance, hardware appliance and cloud service, and supports authentication to VPNs, and on-premises and cloud applications. ActivID supports a large range of authentication methods, custom integrations via APIs, and standards-based authentication via public/private key cryptography, RADIUS, SAMLv2, OpenID Connect and SCIM provisioning. The

ActivID Authentication server is FIPS 140-2 Level 2 certified, with an optional Hardware Security Module that is FIPS 140-2 Level 3 certified.

Use case: multi-factor authentication flow to single sign-on portal with HID Approve and ActivID Authentication Server

1. Dr. Moss, a physician, logs into her healthcare group's Single Sign On portal from her work laptop on her home network.
2. The SSO portal utilizes the domain in her username (email address) to redirect her browser to the HID ActivID authentication service.
3. The HID authentication service sends an authentication request to the HID Approve mobile authenticator on her work-issued smart phone.
4. She receives the notification on her phone and swipes to approve.
5. In the background, HID Approve uses its private key to authenticate to the ActivID server. ActivID will connect Dr. Moss to the application and grant access using her public key from the HID Approve app.
6. Her browser redirects back to the SSO portal, where she gets 1-click access to her provisioned apps.

CREDENTIAL MANAGEMENT

ActivID Credential Management System

ActivID® Credential Management System (CMS) offers simple, central and scalable distribution of authentication credentials onto smart cards, virtual smart cards, smart tokens, Windows PCs and mobile devices. These credentials enable secure access to individual workstations and servers within the firewall and on VPNs, on-premises or cloud applications. Using ActivID CMS, organizations replace traditional usernames and passwords with digital identities based on public key infrastructure (PKI). The ActivID CMS also enables organizations to securely manage a large number of end users in heterogeneous, dispersed locations and update their credentials at any point in the life cycle. ActivID CMS is FIPS 201-certified.

PKI-ENABLED AUTHENTICATION DEVICES

HID Crescendo

HID Crescendo® is family of smart cards that secures employees' access to buildings and rooms, and authenticates them to IT systems and applications both in the cloud and on premises. Crescendo combines two of the most secure authentication factors: Something you have (the card) and something you know (a PIN code that you enter onto the laptop, PC or other secure device to identify yourself as the smart card owner). HID Crescendo is FIPS 140-2 Level 2 certified.

HID ActivKey

HID ActivKey USB tokens offer strong authentication for employees accessing corporate IT systems—at a lower cost than smart cards. They support all of the functionality of a PKI-based smart card without the need for a card reader. ActivKey is FIPS 140-2 Level 2-certified, with an optional deployment mode for FIPS 140-2 Level 3.

The HID ActivID BlueTrust token offers OATH OTP authentication over Bluetooth using a one-click button. It uses Bluetooth and Near Field Communication (NFC) for frictionless access and supports FIDO Universal 2nd Factor (U2F) authentication to multiple online applications.

Use case: restricting cloud access to on-premises employees

1. John, an IT administrator, enters his office building using the Crescendo smart card.
2. At his desk, he inserts the Crescendo card into his laptop's card reader to authenticate to his network.

3. He navigates to the accounting system in company's private cloud. Since his Crescendo smart card has already recorded his presence in the facility and logged him into the network, his access request is immediately approved.
4. When he requests privilege elevation to configure the accounting system, he inserts his HID ActivKey USB token to re-assert his identity at the higher access level.

CONTEXT-BASED AUTHENTICATION USING BEHAVIORAL ANALYTICS AND RISK SCORING

HID Risk Management Solution

HID Global's Risk Management Solution (RMS) gives businesses and consumers a new defense against cybercrime. Its threat management option does three things:

- Identifies every device on the network using device fingerprinting
- Uses behavioral biometrics to detect anomalies in user actions such as keystroke, mouse or swipe patterns
- Detects malware, phishing, bots and unsecure configuration.

RMS combines all of these attributes to generate a risk score.

Risk scoring provides an additional layer of protection to the authentication flow. The HID Authentication Server can be configured with policies to allow, require step up authentication/require internal manual review, or deny access for each individual based on their risk score. This analysis runs in the background and is invisibly to the end-user.

CONCLUSION

As enterprises in regulated industries begin migrating some key systems to the cloud, they need to examine their authentication strategy as part of their overall security posture and determine the appropriate level of strong authentication support required. A simpler multi-factor authentication strategy based on mobile app and authentication services may suffice for many situations. However, sensitive applications and systems may require more advanced levels of authentication and lifecycle management for regulatory compliance.

HID Global offers the most flexible and comprehensive authentication solutions—for both cloud and on-premises applications and systems—to prove compliance and mitigate the threat of data breaches.

For more information, visit www.hidglobal.com/.

hidglobal.com

2018-12-04-hid-dv-adaptive-multi-factor-auth-wp-en

PLT-04141