IDC PERSPECTIVE

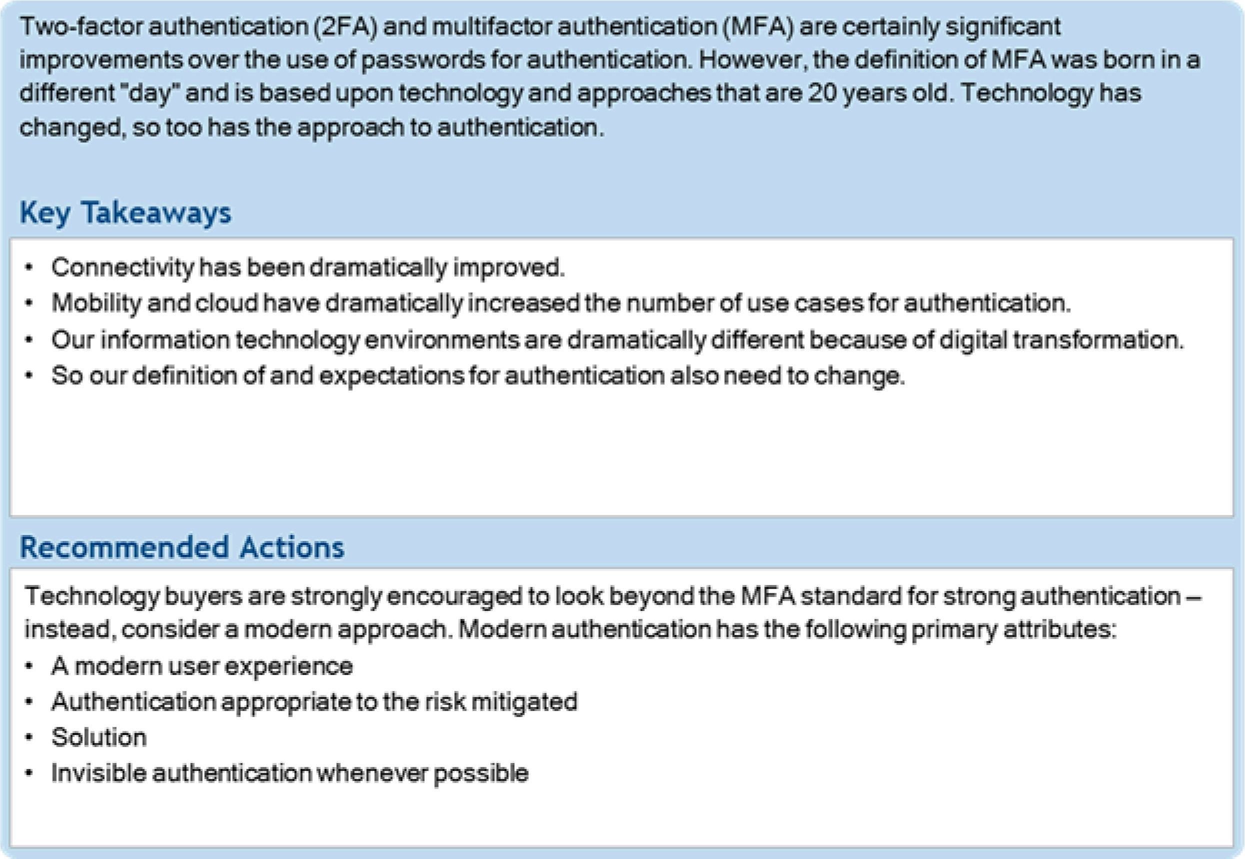
The Death of 2FA and the Birth of Modern Authentication

Frank Dickson

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: The Death of 2FA and the Birth of Modern Authentication



Two-factor authentication (2FA) and multifactor authentication (MFA) are certainly significant improvements over the use of passwords for authentication. However, the definition of MFA was born in a different "day" and is based upon technology and approaches that are 20 years old. Technology has changed, so too has the approach to authentication.

Key Takeaways

- Connectivity has been dramatically improved.
- Mobility and cloud have dramatically increased the number of use cases for authentication.
- Our information technology environments are dramatically different because of digital transformation.
- So our definition of and expectations for authentication also need to change.

Recommended Actions

Technology buyers are strongly encouraged to look beyond the MFA standard for strong authentication – instead, consider a modern approach. Modern authentication has the following primary attributes:

- A modern user experience
- Authentication appropriate to the risk mitigated
- Solution
- Invisible authentication whenever possible

Source: IDC, 2017

August 2017, IDC #US42965617

SITUATION OVERVIEW

No conversation regarding authentication can be complete without the sobering statistic that is brought to us from Verizon's *2016 Data Breach Investigations Report (DBIR).* The report states that "63% of confirmed data breaches involved weak, default, or stolen passwords." The 2017 DBIR was even more sobering as Verizon found that 81% of hacking-related breaches in its data set leveraged either stolen or weak passwords.

In *The Era of the Password Has Passed* (IDC #lcUS41963216, November 2016), IDC articulated many of the issues that plague passwords. IDC also stated in that document that "continuing to use the password for authentication unfairly shifts the responsibility for security from IT and security professionals to end users. Not only is the shift of responsibility unfair but it is also unwise as the focus of end users is getting their jobs done with convenience and expediency, often trumping the need for security." Simply put, in spite of the sophisticated security measures that enterprises are putting in place, something as fundamentally simple as a password is tripping us up.

Identification of the weakness of passwords is clearly not new. Awareness of the problem predates Y2K. In fact, in August 2001, the Federal Financial Institutions Examination Council (FFIEC) guided banks offering internet-based financial services to use "enhanced authentication" and advocated (and defined) multifactor authentication (MFA).

Two-factor authentication (2FA) and MFA authentication methodologies involve three basic "factors":

- Something the user knows (e.g., password and PIN)
- Something the user has (e.g., ATM card, smart card, smartphone, and token)
- Something the user is (e.g., biometric characteristic, such as a fingerprint)

The FFIEC stated that "authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents."

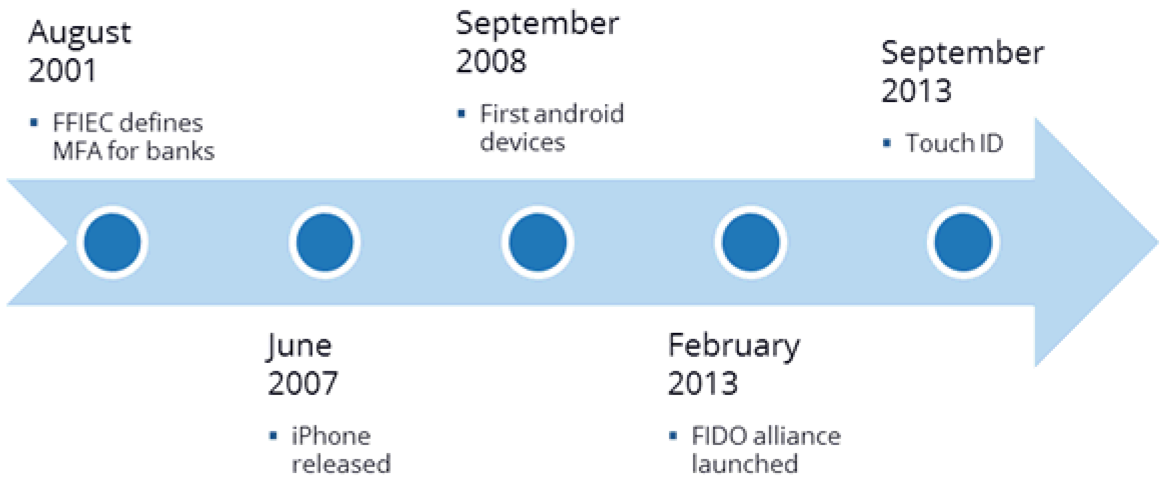
The FFIEC later clarified its position that multifactor authentication requires the use of solutions from two or more of the three categories of basic factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication."

The turn of the century MFA solution to passwords and its definition have become integral to almost all standards that look for authentication beyond passwords. For example, the 2010 Drug Enforcement Agency (DEA) rule for "Electronic Prescriptions for Controlled Substances" mandates that two-factor authentication be used for controlled substances.

2FA or MFA are certainly significant improvements over the use of passwords for authentication. However, the definition of multifactor authentication was born in a different "day" and is based upon technology and approaches that are 20 years old. Consider some of the events and developments that have occurred since MFA was advocated by the FFIEC in 2001 (see Figure 2).

FIGURE 2

Time Line of the 2FA Era



Source: IDC, 2017

ADVICE FOR THE TECHNOLOGY BUYER

Technology has changed. Connectivity has been dramatically improved. Mobility and cloud have dramatically increased the number of use cases for authentication. So our definition of and expectations for authentication also need to change. Technology buyers are strongly encouraged to look beyond the MFA standard for strong authentication – instead, consider a modern approach.

Modern authentication has the following primary attributes:

- A modern user experience
- Authentication appropriate to the risk mitigated
- Solution
- Invisible authentication whenever possible

Modern User Experience

Today's users have a higher user experience expectation than in the past. Devices such as the iPhone changed the belief that technology has to be complicated to be sophisticated. From the perspective of the organization deploying modern authentication, a solution must fit multiple authentication workflows. The technology fits the business – not the other way around!

A common misconception has been propagated by security professionals, and it needs to be dispelled. End users are not lazy. However, they will rebel. Continuing to force the use of unmanageable password hygiene practices or clunky and inappropriate methods for strong authentication unfairly shifts the responsibility for security from IT and security professionals to end users. This shift in responsibility is not only unfair but also unwise, as the focus of end users is getting their jobs done, with convenience and expediency often trumping the need for security.

Modern authentication begins with the fundamental premise of choice. In the past, the options were limited to either a password or a one-time password (OTP) token. Today, authentication options abound, creating a spectrum of options between a very insecure password and a secure OTP token. User experience is about leveraging this new spectrum of technology and context to take that burden back from the end user.

Thus end users are empowered to participate. Choice of challenges must be a fundamental component. Authenticators and/or authentication methods should include:

- Biometrics, including fingerprint, face recognition, voice, iris, palm, eye vein, palm, and retina
- Physical cards or tokens, including common access card, OTP token, Bluetooth tokens, and PIV cards
- Device recognition, including certificates
- OATH tokens
- OTP, including email, SMS, and telephony
- Push notification, including multiple-party authorization
- USB tokens
- Knowledge-based methods, including passwords, grid authentication, and PIN codes

See *IDC TechScape: Worldwide Advanced Authentication, 2017* (IDC #US42418917, April 2017) for an in-depth look at authentication technologies.

The primary emphasis of modern authentication is choice. The mobile phone has become a marvelous authentication platform. Aside from the cell phone being something you have, it is an "authenticator" for establishing trust via fingerprint, SMS, telephony, mobile apps, device recognition, push, and so forth. In addition, risk analysis of the phone and number itself becomes important to ensure we can trust the "thing" we are using to establish some level of trust!

However, many use cases exist for which the mobile phone is inappropriate. Some portion of the user population may not have or may not be able to use a smartphone. Areas with intermittent, challenged, or no service may be an issue. Users and/or organizations may feel authenticating using bring your own devices (BYODs) would be inappropriate to privacy, trust, or content control concerns.

In contrast, the OTP token has been maligned for an awkward and inconvenient user experience; however, the OTP token has long fulfilled the need for strong authentication when a large amount of risk needs to be mitigated — such as in a large monetary transaction. With advances in technology, end users should not feel that added security is unnecessarily or inappropriately burdensome, and when appropriate, should have an improved experience.

Finally, choice is about strengthening authentication and not "counting factors." The FFIEC later clarified its position that multifactor authentication requires the use of solutions from two or more of the three categories of basic factors. The rationale for this was not that two biometrics or two physical tokens did not provide sufficient strength of authentication. The goal was to indicate that multiple knowledge-based methods (passwords) were insufficient, as many banks at the time were implementing a multiple password strategy (or other knowledge-based approaches) for compliance. Multiple "something you have" factors may be appropriate for certain use cases. Granted, unique risks may present themselves in using multiple authenticators from a single factor. For example, multiple "something that you have" tokens present a physical theft risk to consider. The key issue is to consider the risk to be mitigated and then apply authentication challenges in layers to appropriately mitigate that risk.

Authentication Appropriate to the Risk Mitigated

Authentication has far too long been thought of as a binary event (authenticated versus not authenticated). Once authenticated, a user seemingly has unfettered access, regardless of resource or network location. Although the antiquated MFA approach strengthens the authentication event, it also generally suffers from a binary authentication event approach. In addition, it requires users to participate in an authentication test such as providing an OTP from a token for activities that may have relatively low risk such as viewing a bank balance.

Modern authentication changes the view of authentication from a binary event (authenticated or not authenticated) to viewing authentication as a risk score. The activity that a user is performing has a measured level of risk. In this context, risk is essentially the product of the likelihood something is going to happen and the impact if it does. The risk mitigated from the cumulative authentication challenges must sum to offset that amount of risk. The National Institute of Standards and Technology (NIST) is now using the word "assurance" in this context. As previously stated, the key issue is to consider the risk to be mitigated and then apply authentication challenges in layers to appropriately mitigate that risk:

$$\sum \text{Risk mitigation by authentication challenges} = (\text{Probably of compromise}) \times (\text{impact})$$

It is important to acknowledge and identify that risk is not static; it is dynamic and changes throughout a user's session. For example, if an online banking customer wants to view banking activity and balances, that activity will have a certain amount of risk associated with it. Transferring money or paying bills will have a higher level of risk that will require mitigation. If the amount of money to transfer exceeds certain thresholds, there may even be a larger amount of risk to mitigate. Authentication challenges need to be dynamic and appropriate to provide a high amount of risk mitigation to high-risk activities while not burdening the user with onerous authentication challenges for low risk or even benign activities.

Note that the foundational premise of a risk score approach to authentication fundamentally changes the constructs of authentication as the user is never trusted. The user has only satisfied authentication challenge tests to permit him/her to do a certain activity. Thus risk assessments must be continuously assessed throughout a session, as risk is dynamic. If user activity begins to deviate from a manner that is incongruent with past behavior or begins to perform activities that are indicative of behaviors by fraudsters, such activity may increase the required risk score to be satisfied. Likewise, consistent behavior that is congruent with past activity may lower the cumulative risk score.

Inherent in this risk analysis approach to authentication is that the "when" of risk analysis changes. Risk analysis is not a one-time pre-authentication event or continuous; it is both. With each application access and interaction, federated protocols provide the opportunity to perform continuous authentication by reevaluating risk each time a token is generated.

Solution

Security, overall, struggles with an issue of point products. Identity and access management (IAM) acutely suffers from mismatched components, and an integrated solution is critical to address the overall need. Thus even optimal components often do not integrate and work well together, leading to a suboptimal solution.

First and foremost, modern authentication solutions need to be appropriately designed, installed, and configured to solve the use case that the solution is looking to address. Administration, reporting, installation, and maintenance must be appropriate for the market vertical. Healthcare, financial, and government verticals often have very specialized compliance and governance requirements. In addition, the size of organization is exceptionally relevant. Solutions must be highly customizable for enterprise use cases, which tend to have a diversity of needs, and standardized for small and medium-sized businesses, which tend to cybersecurity staffing challenges.

Mobility, big data, cloud, and social media make up the four pillars of today's compute reality that created a massive transformation in our digital lives. Modern authentication, thus, must provide broad coverage and application diversity, which is where many organizations and solution providers stumble. Having MFA is an upgrade over knowledge-based authentication alone, but MFA suffers if the coverage is not comprehensive. An authentication strategy must cover all use cases, including:

- VPN
- Single sign-on applications/portals
- Endpoint devices (Windows, Mac, iOS, Android, Linux, etc., log in)
- APIs for tie-in to homegrown applications and consumer portals (if relevant)
- SaaS applications
- Cloud infrastructures (AWS, Azure, and private clouds)
- Traditional infrastructure (firewalls and network infrastructure)
- Privileged access management solutions

In addition, modern authentication platforms embrace open standards. Authentication is only one of the four critical functions of identity and access management (authentication, identity management, federated provisioning, and governance). Open standards allow for cohesive solutions be to implemented. Standards that must be supported by modern authentication solutions include:

- ACE – Authentication and Authorization for Constrained Environments
- FBA – Forms-Based Authentication
- FIDO U2F – Fast IDentity Online Universal Second Factor
- FIDO UAF – Fast IDentity Online Universal Authentication Framework
- OATH – Initiative for Open Authentication
- OAuth – Open Authorization
- OpenID 2.0 – Simple identity layer on top of the OAuth 2.0 protocol
- OpenID connect – Simple identity layer on top of the OAuth 2.0 protocol
- PKCE – Proof Key for Code Exchange
- RADIUS – Remote Authentication Dial-In User Service
- RESTful – Representational state transfer
- SAML – Security Assertion Markup Language
- SCIM – Simple Cloud Identity Management
- SOAP – Simple Object Access Protocol
- WS-Federation – SAML for Microsoft-centric organizations
- WS-Trust
- XACML – eXtensible Access Control Markup Language

Modern authentication platforms are complete solutions that best address the individual use case but also force vendors to "own" the implementation and integration of the individual parts. When one goes to a grocery store for bread, a person most often does not return home with flour, water, yeast, and sugar and "own" the responsibility of making the bread. This same mindset needs to be taken to the selection of identity and access management platforms.

For example, it has been reported that in the 2014 JPMorgan Chase data breach, an OTP authenticator was deployed, but attackers found one Windows (terminal) server that was unprotected at Windows log-in and used stolen credentials to gain access. In this instance, JPMorgan Chase did not tie that "something you have" into its authentication solution.

Many products may have modern authentication capabilities, but they only protect one type of "thing" such as web apps typically in the cloud, which provides little benefit for other use cases such as VPN or privileged access. Point authentication offerings turn these various "destinations" into islands of identity; thus a user will soon have a potpourri of authenticator applications or many different "experiences" based on what he/she is accessing. As for the user experience, it was just killed. In addition, the ability to achieve true invisible authentication is limited because the risk profile is limited to one type of interaction the offering can see.

Invisible Authentication Whenever Possible

In introducing the concept of modern authentication, we mentioned that technology has changed. Connectivity has been dramatically improved. Mobility and cloud have dramatically increased the number of use cases for authentication. So our definition of and expectations for authentication also need to change.

The same technology that makes authentication use cases challenging also needs to be leveraged to make authentication stronger. Risk-based authentication needs to be a fundamental component of modern authentication. Risk-based authentication measures attributes of the activity that a user is performing and calculates a risk score. Attributes that can be measured include IP address (location and reputation), GPS location, device health, and known device attributes. A key component of the analysis is comparing current attributes with attributes of the activity during the previous authentication session.

Advantages of this approach include:

- Authentication is invisible to the end user since it happens in the background.
- The more factors that are considered by the platform, the stronger the authentication.
- Risk-based authentication is compelling as it is wonderfully complementary to other authentication methods, especially in adaptive authentication use cases (i.e., risk-based authentication is used to allow an individual to view balances in a financial institution account, but an additional authentication method is required to transfer funds).

Modern authentication leverages modern analytics; modern technology for modern authentication. Some of the risk-based test are:

- **Behavior analytics.** Check whether behavior is outside the norm.
- **Device recognition.** Determine whether the device is recognized and associated with a known user — can include web browser configuration, language, installed fonts, browser plug-ins,

device IP address, screen resolution, cookie settings, and time zone and associate this relatively unique "device fingerprint" with a specific user.

- **Directory lookup.** Check group membership and user attributes; credentials created by attackers often lack appropriate group membership and other attributes.
- **Geofencing.** Determine whether access requests come from within or outside a geographic barrier set by the customer.
- **Geographical location.** Determine whether a request is coming from a known good location.
- **Identity governance.** Take an access rights score from IAM and utilize that score in determining the riskiness of access requests.
- **Velocity check.** Look at whether an improbably travel event has occurred by using the user's geolocation and log-in history together.
- **IP reputation.** Compare the IP address of an authentication request with known white and black lists.
- **Jailbreak detection.** Detect whether mobile phone is rooted or "jailbroken."
- **Phone fraud prevention.** Negate the security flaws with one-time passcodes sent via SMS/text with ability to block carrier networks, number class (e.g., virtual, landline, and mobile), and mobile phone numbers that are involved in phone porting fraud.
- **User input analysis.** Gather keystroke dynamics and cursor movements with a particular user on a particular device and stop authentication attempts that fall outside established behavioral templates.
- **Known fraud checking.** Consider known fraudulent elements from security intelligence providers reflected through case markings during risk assessment.

Conclusion

Moving to modern authentication is not an insignificant effort. Standards and regulations will need to evolve to adjust to the new vernacular. Europe's General Data Protection Regulation (GDPR) includes requirements for MFA. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) guidelines for member banks recommend MFA. NIST not only recommends 2FA but also does not consider all 2FA equal, advising against SMS OTP because of security issues. NIST also defined that any self-service and password reset capability around changing the cell phone number for which SMS was being sent must be secured with MFA.

There are recent standards that have come a long way. For example, NIST Special Publication 800-63-3 addresses a better user experience and shifting the burden to the verifier. However, the standards generally do not talk about risk, and they do not consider risk analysis as a component of authentication.

Just as standards bodies have recommended 2FA, same standards bodies can play a role in defining modern authentication. NIST's recommendation to deprecate SMS OTP had a powerful impact on the industry. Recommendations for modern authentication can have a similar impact on the market.

In addition, modern authentication is not just about solving today's issues but laying a foundation for looming use cases. Modern authentication solutions for users must coexist/support authentication for IoT devices and physical access, as people and things will need to operate within a trusted system. Devices, buildings, cars, apps, and the world around will be much more responsive to our physical presence and preferences. Security and authentication are critical in such a reality, as security is a foundational enabler.

Finally, business-to-employee (B2E), business-to-consumer (B2C), and business-to-business (B2B) dynamics need to be considered when implementing modern authentication solutions. Technology and demands actually line up well in terms of session-based and the risk conversation. Differences in use cases and scale must be considered.

LEARN MORE

Related Research

- *Worldwide Identity and Access Management Market Shares, 2016: Identity Is the Core of Security* (IDC #US42575717, May 2017)
- *IDC TechScape: Worldwide Advanced Authentication, 2017* (IDC #US42418917, April 2017)
- *Identity and Access Management: The 3rd Platform Foundation of Cybersecurity* (IDC #US42422517, March 2017)
- *Implementing Microsoft Office 365: User Identity Access and Management* (IDC #US42385817, March 2017)
- *Managing Identity in a Digitally Transformed World* (IDC #DR2017_T3_FD, February 2017)
- *Key Rationale and Criteria for Identity Access Management: A Security Practitioner's Perspective* (IDC #US42058616, December 2016)
- *Best Practice Guide: Reevaluate Vendor Selection Criteria to Accelerate Business Outcomes* (IDC #250453, September 2014)

Synopsis

This IDC Perspective provides insights into modern authentication compared with multifactor authentication (MFA) and two-factor authentication (2FA) for strong authentication. Modern authentication has the following primary attributes:

- A modern user experience
- Authentication appropriate to the risk mitigated
- Solution
- Invisible authentication whenever possible

"The definitions for 2FA or MFA were born in a different 'day' and based upon technology and approaches that are 20 years old," according to Frank Dickson, research director, Security Products. "However, technology has changed. Connectivity has been dramatically improved. Mobility and cloud have dramatically increased the number of use cases for authentication. So our definition of and expectations for authentication also need to change. Technology buyers are strongly encouraged to look beyond the MFA standard for authentication – instead, consider a modern authentication approach."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com