IBM Security

IBM

Upgrade your security with mobile multi-factor authentication

Keep systems secure with best practices—and best user experience—in mind

IBM Security White Paper

Authentication and its future: The virtual front door

Authentication is the beating heart of security. The most fundamental action in all of IT is to identify "who you are"—and authentication is the building block that answers that question. Now more than ever, IT teams must do everything they can to ensure that users are who they say they are, and that their credentials have not been stolen. IT is in state of crisis, with hundreds of millions of identities stolen annually. For system administrators, it's crucial to know which users have the right to access a given resource, and whether unauthorized users have tried to get in.

In a world of distributed workforces, customers and data—and equally distributed, sophisticated cybercrime—vetting users and access also means asking important questions about authentication, such as which authentication method is most appropriate given a resource, channel or specific risk factor.

Authentication, though, is increasingly about more than system security. It's also about meeting user expectations for ease of use, privacy and overall experience—especially in financial and healthcare enterprises. For connected organizations, the authentication process is like the front door. To users, it's important not only to smoothly reach the systems or data they need, but to know that their own account access and data is secured. Authentication is crucial, but it needs to be frictionless to avoid frustrating users—whether they are customers, partners or employees.

A data breach today costs an ***average of USD4 million*** *—that's USD158 per lost or stolen record.*[1]

▸ Read more from IBM about taking control of access management.

1 "2016 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, June 2016.

Multi-factor authentication: Why passwords alone aren't enough

In isolation, passwords are a brittle measure. Even strong credentials can be stolen, cracked through brute force or slyly coaxed from end users. Given today's threat landscape, good security requires strong authentication practices, one of which is multi-factor authentication (MFA). MFA systems have employed telephone calls, one-time passwords, physical tokens (active or passive) and image recognition—and in some cases, user access may require no passwords at all.

Using multiple independent factors multiplies the effort that cybercriminals must exert to break in, and access attempts that fail for lack of additional factors can raise immediate red flags among end users and the enterprise security team alike.

Appropriately-named *mobile* multi-factor authentication (MMFA) skips single-purpose tokens or complicated, tiered passwords, and leverages application programming interface (API)-linked mobile software using the sensors and familiar interfaces already in the hands of authorized users. MMFA employs fingerprint, voice and face biometrics—identifiers cybercriminals can't easily fake. With its ease of use, it is no surprise that MFA has found much popularity within the mobile channel, and this paper will focus mostly on multi-factor authentication as it pertains to mobile.

All that said, it is important to emphasize that good security takes layers—and MFA should not work as a standalone authentication measure. It is in three components that organizations can find strong authentication: mobile and MFA, continuous authentication and advanced fraud protection.

Weak or stolen passwords are used in more than

60%

of known data breaches.[1]

▸ Learn more about why ordinary passwords are vulnerable.

1 "2016 Data Breach Investigations Report," *Verizon*, April, 2016.

Best practices for user authentication

Best practices evolve constantly, but for truly comprehensive authentication, we consider the following three layers essential:

Mobile and multi-factor authentication. The ability to authenticate a user with MFA—and in particular using biometrics, such as fingerprint or face recognition—isn't a new concept, but it is often misunderstood. MFA is not meant to be used in isolation. It is only most effective when traditional authentication factors are also considered, along with risk-based access policies, ID proofing, step-up authentication, and checks for operating system version and device type.

Continuous authentication. Consider the ways that users will interact with the system being secured, and be sympathetic to their needs and expectations. With continuous authentication, the system constantly assesses risk factors and authenticates users without interrupting their experience.

Behavioral/Fraud analysis. Taking a holistic approach to fraud protection and authentication is key because at its core, fraud is an identity problem—and fraud is exactly what we plan to avoid with strong authentication. Ideally, the two systems are complementary. For example, the fraud protection platform indicates instances of fraud risk in a user session—at which point the platform can stop the fraud attempt at its tracks, or request the access management solution to require further authentication. The real value here is in the fraud solution's ability to leverage gathered threat intelligence and apply it to each login attempt.

NIST standards now advise against using text messages alone to send ***one-time passwords.***[1]

- Learn more in the IBM white paper on fighting fraud with intelligent access management.

1 "DRAFT NIST Special Publication 800-63B, Digital Authentication Guideline: Authentication and Lifecycle Management," *National Institute of Standards and Technology*, August 17, 2016.

Best practices: Making MMFA make sense

MMFA requires system designers to consider the realities of mobile device use—and to follow practices that keep those realities in mind.

Authenticate humanely: Require users to provide "just enough" authentication to access the resources they're authorized to use. In the face of complex authentication procedures, users may store sensitive information locally, favor weak passwords, reuse passwords or leave systems unsecured.

Design for mobile: Mobile devices are used under conditions that may mean lower privacy, insecure or unreliable networks, and environmental hazards such as precipitation or glare. What happens if a fingerprint scanner balks, or a challenge-response test is too hard to read? Consider the circumstances within which authentication will be required and ensure that your access management solution can provide strong authentication alternatives.

Consider technical and regulatory limitations: Multiple strong biometrics or other authentication factors may be appropriate in some cases; a simple "Yes/No" challenge might work in others. In deciding which biometric option is best for you, consider that—depending on your industry, country and data set—you may need to comply with certain regulations. Additionally, technical limitations of your users' devices, such as operating systems and hardware differences, might make some biometrics more appropriate than others for you and your users.

Plan for the inevitable: Device theft, loss, breakage or obsolescence are near certainties in the long run. So are changes in product or vendor availability. Avoiding lock-in by device type or operating system helps preserve flexibility.

▸ Read more from IBM Research about creating usable MFA.

In a 2015 study,

65%

of respondents said mobile applications are sometimes put at risk because of customer demand or need.[1]

1 "The State of Mobile Application Insecurity," *Ponemon Institute*, February 2015.

Three MMFA use-case scenarios

The increase in distributed and mobile workforces, along with increasingly capable mobile hardware and software, means there are many plausible scenarios in which MMFA may be appropriate. Here are three access scenarios and how MMFA might be employed to help secure each:

Scenario #1—Local desktop login

- User enters username and password on local computer
- Login attempt triggers a notification pushed to an authentication application on the user's mobile device
- User responds via mobile device with a simple confirmation, biometric identifier, or one-time or secondary password to complete authentication and unlock the computer

Scenario #2—Remote access login

- User enters username and password on remote computer, through a form
- Form completion triggers a notification pushed to an authentication application on user's mobile device
- To complete authentication, user responds with a Yes/No confirmation, biometric identifier, or one-time or secondary password to complete remote-access authentication

Scenario #3—Mobile login

- User launches a phone or tablet application that could access potentially sensitive data or systems
- User selects and uses an authentication method such as a biometric identifier, a one-time password or a challenge question
- Notification is pushed to an authentication application on user's mobile device, which allows access to the chosen data or resource

By early 2015,

74%

of organizations had adopted or planned to adopt bring-your-own-device policies.[1]

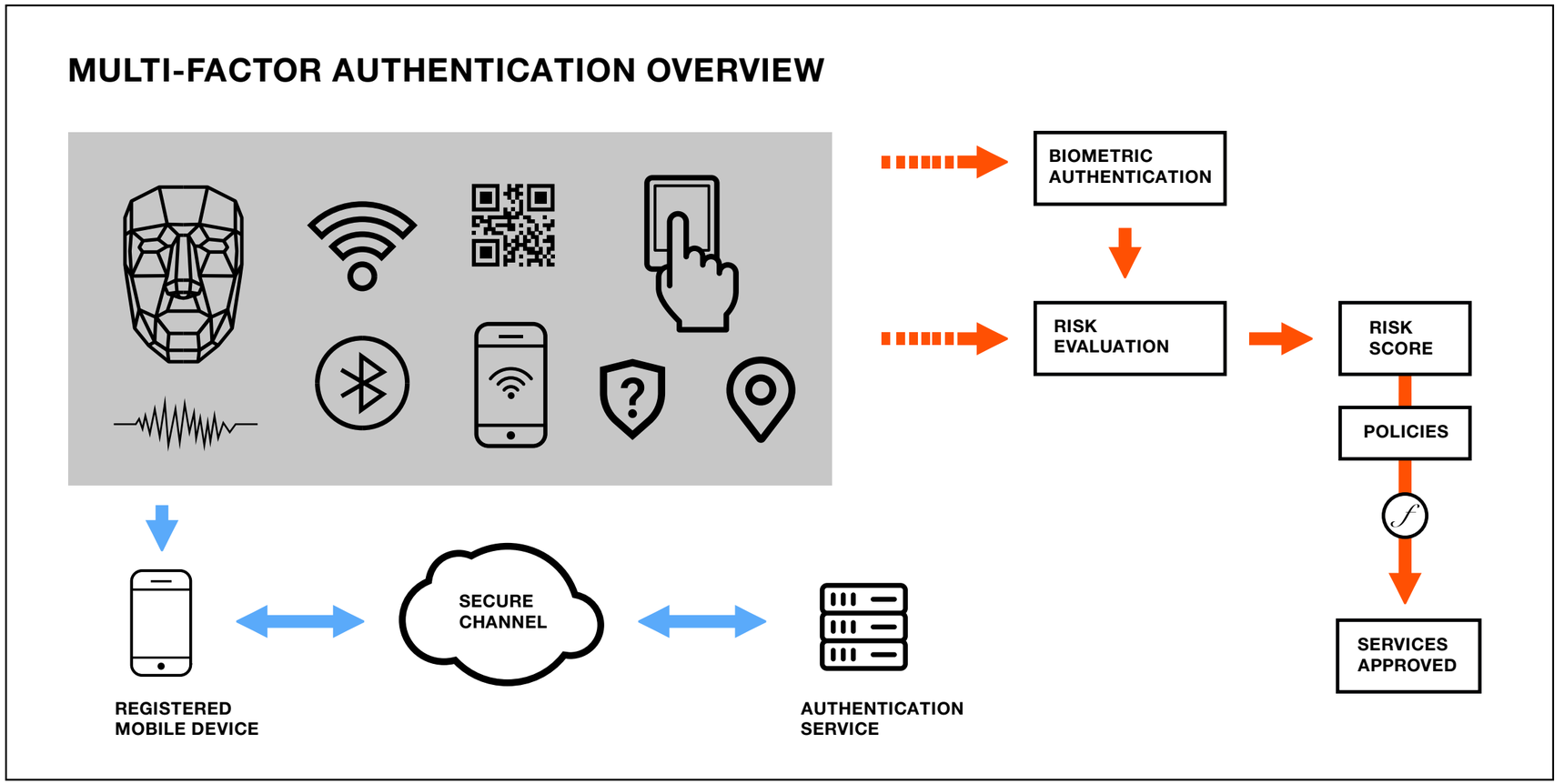
▸ Learn more from IBM about managing mobile device security.

1 Teena Maddox, "Research: 74 percent using or adopting BYOD," *ZDNet*, January 5, 2015.

MMFA overview: Sensors and data flows

MFA relies on factors that go beyond login/password pairs; in the case of MMFA, the sensors and communications capabilities of a user's mobile device are used to provide an independent means of verifying a user's identity.

- Learn about using context-based access to protect websites in this paper from IBM developerWorks®.



MMFA benefits and IBM Verify

MMFA helps organizations balance security with usability. IBM recognizes the importance of MMFA and has now deployed IBM Verify, the MMFA capability forming part of the IBM Security Access Manager solution. To establish strong authentication that is both less intrusive and more affordable, enterprises need risk-based access control over mobile devices and activities. IBM Verify helps organizations integrate flexible and intelligent MFA into applications via two main methods:

- **IBM Verify App**—Out-of-the-box MFA
- **IBM Mobile Access SDK**—MFA easily integrated into a mobile application

IBM Verify helps organizations:

- Deploy adaptive access management that steps up authentication requirements in high-risk contexts
- Adopt user-centric authentication methods, including biometrics
- Utilize mobile as a second authentication factor where one-time passwords, biometric indicators, and action confirmations can act as a stronger line of defense
- Leverage contextual information about a device, user identity, environment, resource and past user behavior to determine required level of authentication
- Reduce user frustration with accessing resources on mobile while increasing security

Wherever you are on the mobile authentication spectrum, it is important to consider the market and technological factors that can influence the success of your mobile security programs. These factors make it more important than ever to take a tiered approach to mobile authentication—one that does not hinge solely on biometrics, but that also considers contextual and known fraud and risk factors.

Users who reuse passwords face the ***greatest risk*** *of account takeover attacks.*[1]

▸ Learn more about IBM Security Access Manager and the authentication mechanisms it offers.

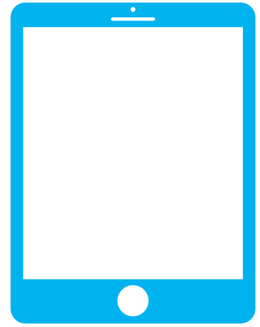
1 "IBM X-Force Threat Intelligence Report 2016," *IBM Corp*., February 2016.

Market factors driving MMFA adoption

It's a complex multi-device, multi-channel world. In the US, as in many other countries, there are more active mobile connections than people.[1] Worldwide, cell phone penetration tops 50 percent even in some developing countries—and the trend points only upward, with greater adoption by young people than older ones.[2] It's also a world of rampant malware and cybercrime. Thousands of intrusions and insider attacks each year cause many millions of dollars' worth of economic and reputational damage. Authentication is key to reducing that damage.

Customer-facing organizations use MFA as an implicit selling point, and effective authentication is increasingly expected by users. Users wary about security risks can rest easier if authorization or account recovery messages arrive through a trusted channel. And whether internal or external, users need systems that are secured yet convenient, and MMFA fits the bill. When done right, it's simpler and faster than many other approaches for elevated access or account recovery.

And for administrators, MMFA such as IBM Verify delivers vital advantages in cost and labor savings. By simplifying access for users, MMFA can reduce the need for human intervention, and free busy IT staff from dealing with important but ordinary tasks such as password recovery or responding to permission-elevation requests.



63%

of enterprises surveyed by IBM have deployed bring-your-own-device policies.[3]

▸ Read about appropriate considerations when adopting two-factor authentication and why a multi-layered approach works.

1 "CTIA Annual Wireless Industry Survey," *CTIA – The Wireless Association*, December 2015.

2 "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," *Pew Research Center*, February 2016.

3 "2016 Mobile Security & Business Transformation Study," *Information Security Media Group, sponsored by IBM Corp.*, 2016.

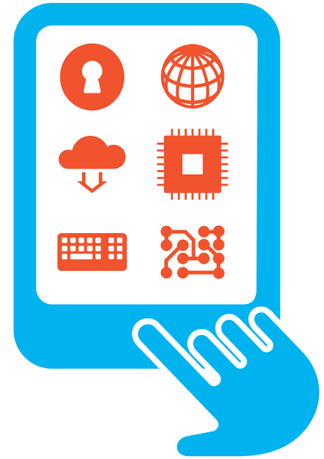
Technical factors affecting MMFA adoption

Like any security measure, implementing MMFA requires awareness of and integration with the systems being protected. Implementing MMFA also means integrating with existing security systems and practices. Failure could mean a major disruption, if a chosen solution is wholly new and does not coordinate well with a previous one. Or it could mean a simple, modular addition to an existing framework. Even at its simplest, however, MMFA is not as easy to use as sending an automated message to a user's mobile device, and the user responding to that message.

Context matters. Users' needs for access to data and systems vary tremendously, as does the complexity of systems themselves. MMFA systems must be designed to accommodate multiple contexts and constraints of mobile interfaces, regulations and other limitations. Because MMFA systems may be used under a wide range of access scenarios, they must take into consideration:

- User mobility limitations (permanent or temporary)
- Installed biometric sensors and their standards
- Screen size and resolution (as they affect usability)
- Possibility of reduced privacy (affecting visual or audio observation)
- Environmental factors that can impede use or function (such as weather, glare or service reception)
- Regulatory limitations (based on industry, geolocation and data sets)
- Biometric data storage (client vs. server-side storage)
- Biometric authentication types (some biometrics are more appropriate than others for certain resources)

Ultimately, MMFA systems must be designed to maintain or improve user experience, making it smooth and uninterrupted.



Learn how IBM supports BIO-key MFA for strong authentication.

How organizations are using MMFA and IBM Security Access Manager

Nearly 60 percent of enterprise security leaders say their organizations are partially or fully mobile—and nearly the entirety of today's enterprise workforce uses Apple iOS or Google Android mobile devices in some way to perform their jobs.[1] Most say that security concerns are the biggest factor that inhibits greater mobile deployment, and nearly a third of organizations named access and fraud security (securing transactions end-to-end, authenticating mobile users, analyzing transactions for possible fraud risk) their top spending priority for mobile.[1]

Two real-world mobile security solutions based on IBM expertise show what can be possible in your organization with IBM Security Access Manager:

- An online file-sharing and personal cloud content-management company in the US has empowered customers to expand their knowledge of security risks and vulnerabilities, improve data protection and bolster mobile security through a strategic partnership with IBM to use IBM Security solutions software to accelerate secure sharing, collaboration and analytics on mobile devices.
- A credit union in the US supports a new mobile application and heightened digital presence that it uses to boost agility and improve member loyalty by working with IBM Premier Business Partner Computer Sciences Corporation and IBM Advanced Business Partner Sapient Corporation to develop and deploy a technology platform featuring IBM analytics and security software.

IBM won

Frost and Sullivan's 2015 Global Identity and Access Management (IAM) Market Leadership Award.[2]

▸ Learn more from IBM about IBM Security Access Manager.

1 "2016 Mobile Security & Business Transformation Study," *Information Security Media Group*, sponsored by IBM Corp., 2016.
2 "2015 Global Identity and Access Management (IAM) Market Leadership Award," *Frost & Sullivan*, July 2015.

For more information

To learn more about IBM Security Access Manager, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
January 2017

WGW03256-USEN-02