IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Yubico

Despite years of investment in educating end users on phishing schemes and the enforcement of early two-factor authentication (2FA) mechanisms, attackers are finding ways to take over user accounts in rising numbers. The time has come for better security standards. Fortunately, they are here.

Modernizing Authentication: A Passwordless Future Is Within Reach

December 2019

Written by: Jay Bretzmann, Program Director, Security Products

Introduction

Multifactor authentication (MFA) and seatbelt usage are both recommended activities for safeguarding our presence — one for our cyber well-being and one for our physical well-being. We know we should always buckle up, and most of us would agree that authenticating to all external IT services is good for us too. In reality, though, these tasks can be annoying and yield somewhat latent user benefits; therefore, we don't do them as well or as often as we should.

Not long ago, the stewards of most IT environments could survive with multiple security disorders in their midst. A server wasn't patched; a website wasn't adequately protected; a default administrator password wasn't changed somewhere — all vulnerabilities. Yet in the scheme of things, the total number of network users was both definable and containable, and intrusions were consequently detectable. Passwords were pretty much good enough.

AT A GLANCE

WHAT'S IMPORTANT

A passwordless future is within reach for most. Fear not though, open and future-proof identity alternatives are readily available. Three cheers to remembering less in the near future.

KEY TAKEAWAYS

Data access secrets stored in the form of passwords are often either knee-jerk, crazy constructions aligned with a format or, worse yet, reuses of old favorites. Human-generated password dependency is costly and unsecure. The answer is only a tap or swipe away.

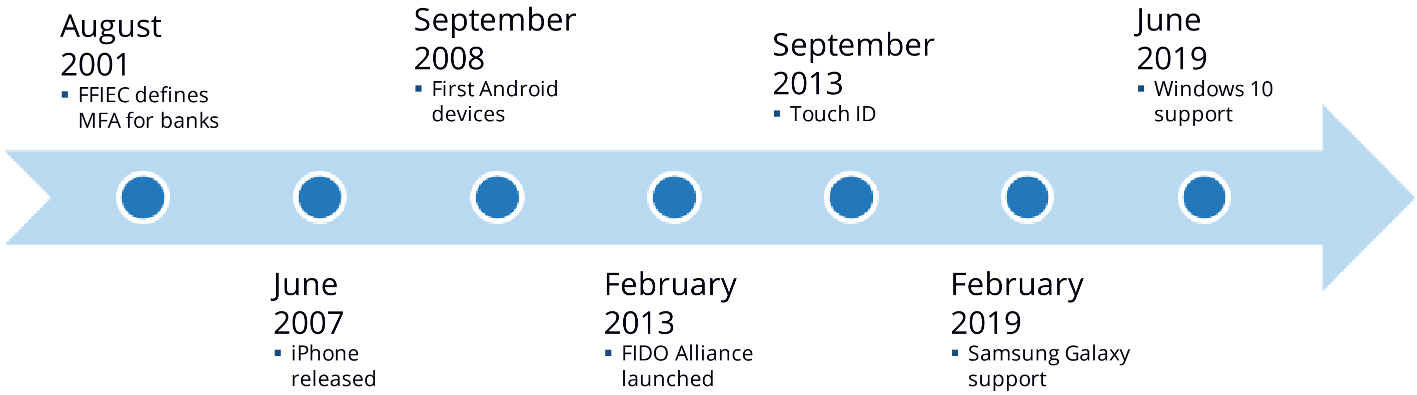
Times have changed, and in case you missed it, most high-profile data theft stories from the past few years have the culprits pursuing a new "way in" via credentials theft. Humans and their weaknesses are just softer targets, and besides, the attack is an easier task than directing malware against zero-day vulnerabilities. People can be fooled, and leaving an identity "root of trust" (RoT) in their hands is no longer an acceptable practice.

Here's the evidence. According to the _2018 Verizon Data Breach Investigations Report_, the top 2 attack vectors for data breaches are phishing and stolen credentials. Despite years of investment in educating end users on phishing schemes, and the enforcement of early two-factor authentication (2FA) mechanisms, attackers are finding ways to take over user accounts in rising numbers. Leveraging real-time man-in-the-middle (MITM) attacks, many second-factor methods are easily captured and replayed. Short message service (SMS) one-time passcodes (OTPs) are among the most popularly used 2FA methods and perhaps also the weakest. Rising numbers of SIM swap and MITM attacks have put phone-based authentication at such risk that NIST has deprecated the practice (SMS) as a recommended authentication method.

These rudimentary authentication activities inject unnecessary user friction and further promote bad identity practices. A good MFA system needs to be more automatic and transparent while beating any requirement for improved data security measures. Tap, swipe, or push your identity troubles aside. People generally do things (repeatedly) that are easier.

Digital transformations deliver a broader reach while exposing a broader attack surface. To maintain an equilibrium — defend the environment if you will — security teams need stronger, more scalable identity solutions. Here's the good news: Recent industry agreements and technological advancements are bringing to a close the 2FA era (see Figure 1). Passwords are becoming as passé as secret decoder rings, and geospatial or biometric measurements are further displacing personal identification numbers (PINs) and SMS as painless n-factor identity proof points.

Figure 1 ***Timeline of the 2FA Era***



Source: IDC, 2019

Challenges Associated with Current Authentication Methods

Today people have a higher user experience expectation than what was permissible in the past. Devices such as the iPhone changed the belief that technology must be complicated to be effective. Solutions must accommodate multiple authentication workflows so that 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 against unmanageable password hygiene practices or clunky and inappropriate methods for strong authentication that unfairly shift the responsibility for security from IT and security professionals to themselves. This shift in responsibility is problematic because end users are focused on getting their jobs done. Convenience and expediency often trump the need for security — and most of us don't need a seatbelt to go around the block.

Modern authentication begins with the fundamental premise of choice. Yesterday's options were limited to either a password or an OTP token. Today, authentication techniques abound, offering relief to users who can readily and transparently be identified by the device, token, or key they possess. Thus end users are empowered to participate with authenticators and/or authentication methods, including:

- Biometrics, including fingerprint and voice recognition, as well as face, iris, palm, eye vein, and retina

- Physical cards or tokens, including common access cards, OTP tokens, Bluetooth tokens, and personal identity verification (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 for an in-depth look at authentication technologies

Again, the primary emphasis of modern authentication is choice. The mobile phone has become a popular authentication platform; however, many use cases exist for which the mobile phone is inappropriate because some portion of the user population may not have or may not be able to use a smartphone, and areas with intermittent, challenged, or no service may be an issue. Some organizations may also decree that authenticating with bring your own devices (BYODs) would be inappropriate to privacy, trust, or content control concerns; nevertheless, the OTP token has, fortunately or not, long fulfilled the need for stronger authentication (better than nothing) when a large amount of risk needs to be further mitigated.

In addition, choice is about strengthening authentication and not counting factors. The Federal Financial Institutions Examination Council (FFIEC) went on record to clarify its position that MFA 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 failed to provide sufficient strength of authentication but that multiple knowledge-based methods (passwords) were insufficient because many banks at the time were implementing a multiple password strategy (or other knowledge-based approaches) for compliance.

Definitions

- **Client to Authenticator Protocol (CTAP).** CTAP is an application layer protocol for communication between a roaming authenticator (security key or mobile phone) to communicate strong authentication credentials locally over USB, Bluetooth, or NFC with a relying party (e.g., website or native application) on some platform (e.g., PC or server). CTAP and WebAuthn underlie the FIDO2 specification.
- **FIDO and FIDO2.** The Fast IDentity Online (FIDO) Alliance was founded in 2012 by PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon, and Agnitio to work on a passwordless authentication protocol based on public key cryptography. Today, the FIDO U2F/FIDO2 specification is accepted by all manner of hardware devices and operating systems as the de facto means for biometric authentication using roaming authenticators (smartphones or key dongles). FIDO2 is the combination of WebAuthn and CTAP.

- **Public key infrastructure (PKI).** PKI is an arrangement that binds public keys with respective private identities of entities (such as people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, certificate issuance may be carried out by an automated process or under human supervision. Any PKI system is far more secure than something based on user-generated passwords.

- **Root of trust.** A RoT is a critical component of PKIs designed to use linked pairs of cryptographic keys — one that is private and one that can be safely published in the form of a public digital certificate. PKIs facilitate the secure transfer of data across the internet and are a means of identifying computer systems and users. The RoT stores and supplies the private key and can be implemented as hardware, firmware, and/or software — including stored passwords. When queried, it must always behave in an expected manner because its misbehavior cannot be detected. A RoT is the ultimate foundation for verifying a user's identity.

- **WebAuthn.** WebAuthn is a World Wide Web Consortium (W3C) standard web API that can be incorporated into browsers and related web platform infrastructure, which gives users new methods to securely authenticate on the web, in the browser, and across sites and devices. It defines the format for communicating with a RoT, allowing a website, a service, or an application to authenticate a user's site-specific credential without storing or sharing the user's private credential itself, and was designed (principally) to eliminate the risk of stolen passwords.

Key Benefits

Any organization still dependent upon secrets rooted in classically constructed passwords is — I'll bet you — wasting money in addition to creating an environment exposed to most classic hacking attacks. It's the rare human who can create and remember more than a couple dozen passwords used across all the online resources he or she touches daily. Password reuse is common, and resets are a costly problem for most. According to IDC survey research, help desk personnel spend most of their time on the following:

- Password resets
- Virtual private network (VPN) access problems
- Application availability issues

Most conservative estimates of help desk costs put the expense at $25 per each instance, and IDC research has identified costs that are triple that figure. Users can physically lose a key (tip: register multiple keys in addition to smartphone keys), but users cannot permanently lose or forget an assigned certificate number.

Most security teams have heard that using some sort of MFA technology eliminates data breach and account takeover risks. At its industry conferences, Google has shared its experiences requiring every employee to use hardware tokens for identity. Phishing attacks became nonexistent — not one occurrence across thousands of users since a security key technology built on the FIDO standard was deployed. That's really justification enough for the average chief information security officer (CISO) to consider upgrading to PKI certificate pairs in a painless, passwordless manner.

Beyond password elimination, hardware security keys also upgrade the RoT that underpins a user's core identity. Hardware security keys are much better than a PIN and impossible for cybercriminals to research as with knowledge-based identity factors (like your pet's name). The key or device that holds the certificate can't be compromised via remote attacks or hacked databases. Furthermore, FIDO uses a batch attestation model that proves the authenticity of the security key without compromising the privacy of the user.

Another benefit to using more modern MFA technologies is the resulting immunity to MITM attacks. Compliance with any FIDO U2F/FIDO2-enabled application or website requires support for:

- PKI cryptographic keys
- Device presence attestation capabilities
- Service registrations or destinations

A user log-in is bound to the client origin through a registration process, meaning that only the real site (previously contacted) can authenticate with the private client key. Fake sites don't know the paired public key component. MITM attacks have been used in various contexts for years and will remain a favorite tactic until the identity vulnerabilities they exploit are eliminated.

A generation from now, no one will believe passwords were once forced upon or entrusted to the user. Biometrics and artificial intelligence/machine learning (AI/ML) will help continuously authenticate users to each interaction or session because an endpoint will know its holder is or isn't the owner based upon what is done, when, and where. Simple one-time registrations will create secure cryptographic exchanges between data owners and data processors, ensuring both privacy and access to application audit trails.

Key Trends

Trust Is Improving

The technology to implement trusted environments is improving and will become more widely adopted as the costs to deploy such environments decrease. Make it easy and everyone will do it; impede business agility or erode employee productivity and users will find ways to get around most lightly funded barriers. No authentication technique is truly foolproof or unhackable, but putting one or two more barriers in place will address most business needs and regulatory requirements if only you can do it without getting sacked.

APIs and Standards Make Markets

In a highly fragmented market — such as the market for identity and access management (IAM) solutions — the ability to collect and share session data with other security technologies is increasingly important. Identity, authentication, privileged access management, and governance offerings are stronger when they're integrated, giving rise to an abundance of vendor API definitions. New industry standards are being defined to help with this information passing and hopefully reduce compatibility issues until something just changes and applications break.

Passwordless Practices Are Increasing

Significant credit is due to Apple for developing Touch ID into an authentication system most people just readily accept. It met the basic criteria for 2FA systems being easy to use and ubiquitous. The emergence of all these smart device applications has served to make the smartphone a device few can put down for long, something Microsoft understood as it developed FIDO2 support for Windows 10 devices and Azure cloud accounts. USB technology has made it just as easy to secure desktop devices using a tap or touch on something that also holds a certificate key.

Reports from the field suggest passwordless systems using FIDO2 keys are effective, and wildly so. High-tech companies have been the early leaders with Google publicly in front and Microsoft following suit — every employee will now implement MFA as soon as possible. It's easy; beyond an initial registration, no one shares a password or passcode again. Simple MFA systems can be assembled including biometric devices, and everyone benefits from PKI certificate pairs all down the line.

Federated Single Sign-On (SSO) Provides Flexibility

People don't want to log on to multiple accounts or services if they can possibly avoid it, and all it takes is a little up-front effort. The Security Assertion Markup Language (SAML), which enjoys wide support, is an earlier standard that was developed for heavier client/server-based connections. Later, mobile device adoption for browsing required lighter-weight identity APIs and the definition of OAuth 2.0 and OpenID Connect. Now, almost everyone can bounce from one web session to the next leveraging authentications associated with existing session cookies. This is among the biggest user benefits enabled by identity and access management solutions.

As SSO continues to evolve, IDC expects a growing adoption of social media platforms to become the identity providers for numerous online activities, as most people will almost always keep one of these platforms open. Organizations should register a certificate with these identity suppliers to reduce the risk of multiple log-ins leading to compromised credentials.

OTPs Come in Many Forms

Most organizations' first venture into adopting MFA technology begins with a one-time password approach. This effort shouldn't be discounted as it is a major step up in securing user identities. The weakest form has been shown to be SMS implementations, and NIST has issued directives against their use, but lots of companies still choose an SMS solution because it's very easy to do and, again, far better than doing nothing. Email and push-based OTP solutions that include things such as QR codes are better still, but many of these solutions also use mobile devices that are capable enough to deliver a far better PKI-based alternative.

In many cases, these more capable solutions also require some level of service registration, and for anything associated with funds transfers and other commercial exchanges, the effort is easily justified. Organizations register their private keys with some number of vendors or service providers and reap the SSO benefits for other sites accepting the validity of our existing identity assertions.

Considering Yubico

Yubico was founded in 2007, a little before online identity security issues were a daily concern for most users. This small Swedish company set out on a lofty mission to make secure log-in easy and available for everyone. In 2011, Yubico moved its headquarters to the United States to better enjoy close collaboration with the leading internet companies and thought leaders. The company's investment focused on developing native security key support for the major online platforms and browsers. In 2012, Yubico signed an agreement with Google to jointly develop a new two-factor authentication standard built upon a one-touch dongle to establish PKI secrets.

Yubico, Google, and NXP Semiconductors then join the existing FIDO Alliance with the intent of productizing a hardware fob implementing the FIDO Universal Authentication Framework (FIDO UAF) and FIDO Universal Second Factor (FIDO U2F). Key usage has been strong within technology companies that best understand its protective value as well as with highly regulated industries as a more convenient upgrade to older n-factor authentication systems that are quickly becoming obsolete.

The partnership was a big win, giving Yubico exposure to internet-scale dynamics as it built a convenient implementation of a developing secure log-in standard. Today, the company supports security keys that can authenticate identities through multiple solution APIs and support industry-standard formats as well as vendor unique identity system interfaces such as OATH-TOTP, OATH-HOTP, SmartCard PIV, OpenPGP, and Yubico OTP. Google has also since defined and developed its own FIDO U2F/FIDO2 key implementation based on a Trusted Platform Module named Titan. Titan is a processor with a built-in PKI certificate that can be embedded into the delivery environment for service providers, helping them maintain trusted connections. Both Yubico and Google are working to influence, define, and execute upon delivering identity authentication technologies.

Yubico has sold more than 7 million YubiKeys in more than 160 countries. The security keys address multiple industry standards (FIDO2, TOTP, SmartCard PIV, OpenPGP, etc.) and are packaged in a wide range of desktop and mobile device formats (USB-A, USB-C, NFC, and iOS Lightning). The technology arguably represents the most broadly accepted, product-level deployment of a hardware-based MFA solution since RSA introduced its proprietary SecureID token back in the early 1980s.

Challenges

Not every Boy Scout achieves Eagle Scout rank despite his best efforts, intentions, and consistent seatbelt usage. Yubico is betting on good intentions perpetuated among educated market participants to capture and apply secure token-based authentication technology. It must simply be the best-of-class solution defined in FIDO terms. First-mover status and limited mistakes will likely carry the company unless some other major alternative emerges. There are now more than 465 FIDO-certified products.

The investment Google has made in its own FIDO-compatible platform (Titan) and the ability of any Samsung G7+ Android or Windows 10 device to be a hardware key pair divide the total market opportunity but strengthen the agreement on a FIDO-influenced future.

Yubico products help secure ubiquitous internet application access while minimizing user certification acquisition and trusted partner service registrations. One potential growth speed bump is that a Yubico enhanced authentication experience is not a complete IAM solution for most organizations. Yubico will be the hardware token validation partner to some broader, identity-focused software/service platform solutions. Those solutions must be in place (investments made) and compatible with YubiKey solutions.

Conclusion

Younger generations should heed the advice of older generations, who have run into similar execution obstacles and learned from their mistakes. "An apple a day...," "A stitch in time..." — the one thing that never really changes with preventive action is that everyone eventually becomes wiser (hopefully sooner than later). We'll more readily do that which makes us more successful than that which someone says we should. MFA is nice, but so is releasing new application functionality that might create more business revenue and employee bonuses. Ah, decisions.

Should your company do MFA, and should the technology do it well enough to include PKI capabilities, you'll lay a foundation upon which value-added, data-analyzing activities can be secured and the results harvested for future outbound sales opportunities. So you'll get to do a social media–like analysis on anyone who visits the site(s). Cool, right?

Whenever IAM vendor selections get complicated and murky, go for strength and choose a leader.

Expect some bumps along the way though because there's still a lot of agreement required to document what needs to be acquired when and stored for how long. But whenever IAM vendor selections get complicated and murky, go for strength and choose a leader — the value of any API rests with how many solutions currently support it. Many smaller, best-in-class technology providers will be acquired, and their technology will be folded into the utility of broader security platform services. Bummer if you've invested a bunch of dollars and cycles on dead-end integrations.

Borrowing a famous hockey-inspired quote, IDC recommends that CISOs, "Skate to where the puck is now, and score before the ice melts." Adding a modern authentication solution such as YubiKey is becoming increasingly easy, and Yubico's latest upgrade of touch proximity technology with a biometric fingerprint scanner makes a passwordless future all the more realistic.

For CISOs, building a secure identity future aligned with FIDO standards is unarguably a smart move. As with other fundamental communications or networking technologies (TCP/IP and NFS), everything works better if we can all agree on one language or data interchange format. These standards can take time, and Yubico has been at this for more than a dozen years. It's simple: Get your organization using keys (actually two each) and just say no to legacy identity attacks.

About the Analyst

Jay Bretzmann, *Program Director, Security Products*

Jay Bretzmann is Program Director for IDC's Security Products responsible for Identity and Digital Trust and Cloud Security. Jay focuses on identity management, privileged access management, identity governance, B2C identity management, and a multitude of other identity and cloud security topics.

MESSAGE FROM THE SPONSOR

About FIDO2/WebAuthn

Imagine a world where users no longer need to set, reset, forget and reset again multiple passwords. Passwords are known as the weakest link for enterprise security and are an obstacle to streamlined customer journeys and internal processes. The world is about to change with passwordless authentication.

The FIDO2/WebAuthn authentication standards offer the opportunity for organizations to solve the problems inherent in password-based security. FIDO2 is an open standard, co-developed by Yubico, Microsoft, and other members of the FIDO Alliance that enables expanded options for strong authentication including the flexibility to now offer passwordless or multi-factor strong authentication to users.

To learn more about passwordless authentication and considerations for enterprise deployment, read the Yubico white paper, ***Going Passwordless with FIDO2 and WebAuthn***.

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The **o**pinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.