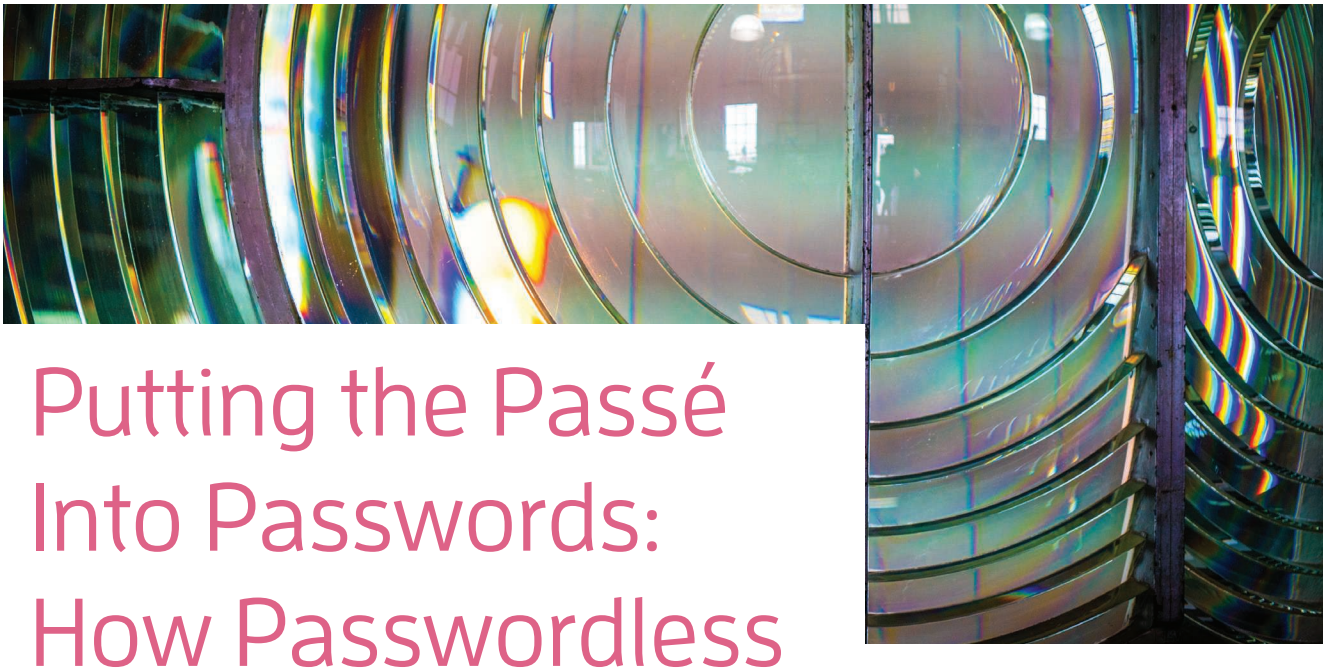
EDITOR **MARK CAMPBELL**
EVOTEK; mark@evotek.com.



Putting the Passé Into Passwords: How Passwordless Technologies Are Reshaping Digital Identity

Mark Campbell, EVOTEK

Despite significant flaws, passwords persist as the predominant method to authenticate digital identity. What are the alternatives, and are we going to move onto something better?

A wise man once said to set your password to "incorrect," so if you forget it, the system will tell you "your password is incorrect." OK, maybe not such a wise man, but many of today's users are not much more sophisticated. Passwords have some very attractive features. They are easy to implement, do not require any special hardware, are compatible across all devices and applications, and are very easy to use. Passwords provide such a frictionless customer experience that more than 300 billion of them are in active use today. However, more than 8 million are also stolen daily.[1]

There are monumental problems with passwords.

- *Passwords are hard to manage*: Good security dictates passwords be long, hard to guess, unique across applications, and changed frequently. However, managing an ever-changing array of cumbersome passwords for an average of 90 accounts[1] can tempt even the most diligent user to take shortcuts. The U.K.'s National Cyber Security Center found "123456" was used over

Digital Object Identifier 10.1109/MC.2020.2997278
Date of current version: 30 July 2020

23 million times in a database of breached passwords.[2]

- *Passwords can be stolen*: Techniques to capture a user's password can range from trivially simple to very complex. Shoulder surfing or even reading from a note stuck to a monitor can discover passwords with little effort. A touch more involvement allows keyloggers to intercept and send key clicks to a bad actor, while network sniffers can capture unencrypted passwords sent over the wire. Phishing attacks all too often trick unwary users into providing their username and password to fake web sites. Credited studies show 29% of breaches in 2019 involved stolen credentials.[3]
- *Passwords can be guessed*: Simple dictionary attacks can reveal common words, phrases, and numbers used as passwords. However, rules-based heuristic and Markov model-based password guessers like HashCat and John the Ripper can find passwords containing combinations of words, numbers, upper and lowercase, and see through obfuscation techniques like "leet speak" (for example, l33t 5p3ak). Artificial intelligence (AI)-based PassGAN, when combined with a heuristic guesser, can guess over a third of the passwords in the RockYou and LinkedIn leaked data sets.[4]
- *Passwords can be bypassed completely*: Various attacks directly target the underlying password management systems. One notable technique, known as *pass the ticket*, uses open source tools like Mimikatz and Rubeus to obtain what they call a *golden ticket* to generate credentials for any account in a targeted Active Directory repository.[5]

PASSWORD WRANGLING

To plug a finger in the leaky password dyke, many systems augment passwords with an additional security picture, phrase, or question, such as the obligatory mother's maiden name. However, security questions must be easy for the user to remember and thus are generally linked to memorable life events or people, which, in the age of deep social media, are increasingly easy for attackers to guess.

> Passwords provide such a frictionless customer experience that more than 300 billion of them are in active use today.

Password managers and single sign-on solutions have become ubiquitous. Products like Dashlane and LogMeIn's LastPass enable frictionless password use in a "one ring to rule them all" scheme, which uses an authenticated identity from one system as an identity proxy for other systems. This so-called federated identity allows the user to sign on once and transfer this identity to other systems behind the scenes through protocols like SAML 2.0, OAuth, and Open ID Connect. However, these underlying protocols have a growing list of vulnerabilities[6] and, worst of all, should the master password be guessed or stolen, an attacker gains full access to all accounts. The one ring now rests on an evil finger.

MULTIFACTOR AUTHENTICATION: THE FACE THAT LAUNCHED 1,000 APPS

Passwords are based on something we know. Since others can learn what we know, multifactor authentication (MFA) verifies identity based on something we are or have.

Biometric solutions measure a unique feature of who we are to verify our identity.

- With an accuracy of over 99%,[6] cheap fingerprint scanners can be built into any device and are now one of the most common MFA techniques in use.
- An iris scan is generally accepted as the most reliable biometric, only misclassifying about one scan in 100,000.[7]
- Facial scans are a common method to gain access into handheld devices, laptops, and vehicles.
- Voice recognition, although easy to deepfake with AI,[8] is increasingly used to authenticate call-in services and digital assistants like Amazon's Alexa.
- Behavioral biometrics dynamically measure patterns in human activities, such as how you walk, type, hold a phone, or drive to provide authentication. Today's mobile devices can track more than 2,000 behavioral patterns to continuously verify a user's identity.[9]

Several biometric methods, like iris, face, voice, and behavioral biometrics, do not require physical touch, making them ideal for use in clean rooms and hospitals or by operators in protective gear. It is easy to foresee an explosion of touchless authentication in a postpandemic world.

Several misconceptions have sprung up around biometrics, however. In the movies, super spies can make wax fingerprints, rubber faces, recorded voices, or contact lenses to trick the scanners. In real life, though, authentication devices also use temperature, infrared, motion, and sophisticated "liveness" detection to prevent spoofs. Another erroneous belief is that biometric scans are stored in a repository somewhere, and if the bad guys break in, they can hijack your scans to get at your goodies. In reality, biometric scans

are converted to mathematical or statistical files called *biometric templates* stored on the device itself and are used as a digital reference against which future scans can be compared. Should a biometric template fall into the wrong hands, it would provide no access advantage, since the attacker would need to generate a biometric scan to compare to the template.

MFA can also authenticate our identity by way of something we physically possess, such as a key, card, or phone. When fingerprints are coupled with a physical security device, like Yubico's YubiKey, they provide a very secure and easy-to-use authentication with no passwords. With the rise of the smartphone, "phone-as-a-token" techniques are developing as another authentication factor.[10] This is Alice's phone, touched by Alice's finger, so it must be Alice.

Despite their many advantages over passwords, biometrics and other MFA techniques have a few drawbacks. Unlike passwords, biometric patterns are generally impossible to replace. It is very tough to replace your voice, face, or gait with a new version should you discover your identity has been compromised. Like passwords, biometrics such as fingerprint, iris, or face scans can be physically extracted by force or incapacitation. There is also an alarming rise in cyberattack tools, like Murean and NecroBrowser, designed to target MFA.[11] Because of these and other concerns, many government regulations, including the National Institute of Standards and Technology Electronic Authentication Guideline, only allow biometrics as a secondary authentication factor in an MFA structure.[12]

FORGING ALLIANCES

Over past decades, several standards and protocols, such as OAuth, Kerberos, OpenID, TLS, JSON Web Tokens, SAML, and WS-Federation, have emerged to standardize, manage, and harden identity authentication. However, several newer standards, regulations, and alliances are expanding passwordless infrastructure.

The Fast Identity Online (FIDO) Alliance is a consortium of hundreds of companies, such as Amazon, Facebook, Google, and Microsoft, that have the express aim to reduce the reliance on passwords to authenticate users. All FIDO specifications are available free online, including

- *WebAuthn*: One of the fastest growing authentication protocols uses platform authenticators (such as phones and laptops) and public key cryptography enabling secure web transactions while protecting the user from advanced phishing attacks, session hacking, man-in-the-middle, and malware attacks—all without the use of passwords. WebAuthn is now built into most leading browsers and used by more than 600 certified applications and devices.[13]
- *Universal second factor (U2F)*: This is an open authentication standard requiring no client-side drivers or plug-ins that gives users access to web services using only one security key. U2F can bind a user's U2F security key to his or her government issued electronic ID as seen in the U.K.'s GOV.UK Verify program.[14]
- *Client to authenticator protocol*: This protocol allows a roaming device, like a smartphone or a security key, to interoperate securely with client platforms such as a laptop.[15]

Governments are working closely with alliances and standards bodies like FIDO to implement national identity programs to secure consumer and citizen services. The European Union's Electronic Identification, Authentication and Trust Service framework was implemented by Germany, Italy, Estonia, Spain, Croatia, and Luxembourg to create their secure electronic identification programs.[16]

THE USER

The end goal of passwordless security solutions is to provide the user with an easy-to-use, yet secure, method to verify their identity. While this is a simple concept, it is exceedingly tricky to balance the tradeoffs between protection and user experience. Security is a greater concern over convenience for 86% of online consumers,[17] and this preference is so strong that many service providers introduce small "positive friction" delays into their authentication process so the user feels the system is "working hard" to verify their identity.

> Security questions must be easy for the user to remember and thus are generally linked to memorable life events or people, which, in the age of deep social media, are increasingly easy for attackers to guess.

Beyond a frictionless (but not too frictionless) customer experience, passwordless authentication must protect the privacy of the user's digital information from the trusted agent on the other end of the transaction. Six in seven employees have reservations about sharing their biometric data with their employer.[13] While many consumers have embraced consumer protection regulations like Europe's General Data Protection Regulation and the California Consumer Privacy Act, there are gray areas between protection of a user's security and surreptitiously figuring out his or her identity. Online service providers, like retailers and banks, use software to track

thousands of biometrics data points to determine if the user is an automated attacker, a human impostor, or the actual real person. In a recent example, the Royal Bank of Scotland spotted an online user interacting by means of a mouse scroll wheel and numeric keypad, behaviors never exhibited by that particular user. The system alerted the antifraud department and prevented a serious theft.[18] In situations like this, biometric capture appears to be an overwhelmingly positive consumer protection method. However, it can also be used to reverse-engineer a user's identity—as soon as you scroll your mouse across a website or type in a query, you could be inadvertently revealing clues as to who you are.

> The end goal of passwordless security solutions is to provide the user with an easy-to-use, yet secure, method to verify their identity.

WHERE TO FROM HERE?

An army of startups, like Nok Labs, Hypr, Yubico, and Secret Double Octopus (my personal nominee for Best Startup Name of the Decade), are developing more advanced features to make passwordless technologies more secure, easier to use, increasingly accurate, and more private. They join standard-bearers like Okta, Ping, and Auth0 on the quest to eradicate passwords altogether. For example,

- Trusona's Driver License Data Verification can securely derive your identity from a picture of your driver's license.
- Pixies extends facial recognition techniques to any object users choose, such as their wristwatch or a vase on their desk.[19]
- IBM and the Sovrin Foundation explore passwordless technologies to build a distributed self-sovereign identity ecosystem in which individuals have sole ownership over their digital identity.[20]
- EOSIO applies blockchain technology to create "passes" that obviate not only passwords but also security keys.[21]
- The zero-trust security movement transforms user access from a one-and-done event into a scenario where identity is re-verified for every service, system, and data source accessed.[22]
- Quantum computers, should they become viable, threaten to unravel asymmetric encryption techniques like those built into public key infrastructure. Passwordless visionaries look to decentralized methods and post-quantum encryption techniques to avoid a potential security meltdown in the future.[23]
- Adaptive authentication uses spatial and temporal techniques to corroborate identity using geolocation and time. By restricting or learning a user's location, time of day usage, or Internet Protocol address, a security system can alert on anomalies that may indicate a compromised identity. One example is Microsoft's Cloud App Security which, among 30 other risk indicators, will alert on what are known as *impossible traveler* scenarios, where two activities are originating from physical locations within a period shorter than it would take to travel between them.[24]
- Techniques like adaptive and risk-based authentication, just-in-time provisioning, best-fit access, and automatic deprovisioning continue to mature and reshape how access is granted and revoked.

While no one debates that passwords are the bane of digital security, developing the perfect passwordless solution has proven elusive. However, recent advancements are turning a passwordless future into a reality. The universal adoption of passwordless solutions and the deletion of the world's last password may still be a way off … but it is coming.

REFERENCES

1. "New report finds 300 billion passwords will be at risk by 2020," *Cybercrime Magazine*, Jan. 31, 2017. [Online]. Available: https://cybersecurityventures.com/300-billion-passwords/
2. "Millions using 123456 as password, security study finds," *BBC News: Technology*, Apr. 21, 2019. [Online]. Available: https://www.bbc.com/news/technology-47974583
3. A. Steel, "Passwords are still a problem according to the 2019 Verizon Data Breach Investigations Report," LastPass, May 21, 2019. [Online]. Available: https://blog.lastpass.com/2019/05/passwords-still-problem-according-2019-verizon-data-breach-investigations-report.html/
4. B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, PassGAN: A deep learning approach for password guessing. 2017. [Online]. Available: arXiv:1709.00440v3
5. "Pass the ticket (ID: T1097)," Mitre ATT&CK, 2017. [Online]. Available: https://attack.mitre.org/techniques/T1097/
6. "NIST study shows computerized fingerprint matching is highly accurate," *NIST News*, July 6, 2004. [Online]. Available: https://www.nist.gov/news-events/news/2004/07/nist-study-shows-computerized

-fingerprint-matching-highly-accurate
7. M. Besley, "Biometrics: A guide," Government Office for Science, London, 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf
8. K. Lyons, "FTC says tech behind audio deepfakes is getting better," *Verge*, Jan. 2020. [Online]. Available: https://www.theverge.com/2020/1/29/21080553/ftc-deepfakes-audio-cloning-joe-rogan-phone-scams
9. A. Turgeman, "Machine learning and behavioral biometrics: A match made in heaven," *Forbes*, Jan. 18, 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/01/18/machine-learning-and-behavioral-biometrics-a-match-made-in-heaven/#23abd2983306
10. G. Omale, "Eliminate centrally managed passwords for better security, fewer breaches, lower support costs and enhanced user experience," Gartner, Stamford, CT, Mar. 6, 2019. [Online]. Available: https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/
11. Z. Doffman, "FBI issues surprise new cyber attack warning: Multi-factor authentication is being defeated," *Forbes*, Oct. 7, 2019. [Online]. Available: https://www.forbes.com/sites/zakdoffman/2019/10/07/fbi-issues-surprise-cyber-attack-warningurges-new-precautions/#4c1351157efb
12. W. E. Burr et al., *Electronic Authentication Guideline (NIST Special Publication 800-63-2)*. Reston, VA: U.S. Dept. of Commerce, 2013.
13. "The passwordless future report," Okta, San Francisco, 2019. [Online]. Available: https://www.okta.com/passwordlessfuture/thank-you/
14. "Guidance: GOV.U.K. Verify," U.K. Government, Mar. 25, 2020. [Online]. Available: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
15. "Client to authenticator protocol (CTAP)," FIDO Alliance, Wakefield, MA, Feb. 27, 2018. [Online]. Available: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html
16. "National eIDs of six countries available for the EU citizens to use cross-border," *Shaping Europe's Digital Future*, Nov. 7, 2019. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/national-eids-six-countries-available-eu-citizens-use-cross-border
17. "Human versus machine: Which provides the highest assurance levels?," Raconteur, London, May 5, 2020. [Online]. Available: https://www.raconteur.net/sponsored/human-versus-machine-which-provides-the-highest-assurance-levels
18. S. Cowley, "Banks and retailers are tracking how you type, swipe and tap," *NY Times*, Aug. 13, 2018. [Online]. Available: https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html
19. M. Samuels, "Photo-based pixie 2FA system takes authentication to a new dimension," *Security Intelligence*, Oct. 31, 2017. [Online]. Available: https://securityintelligence.com/news/photo-based-pixie-2fa-system-takes-authentication-to-a-new-dimension/
20. D. Gisolfi, "Decentralized identity: An alternative to password-based authentication," IBM Blockchain Blog, Oct. 5, 2018. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/10/decentralized-identity-an-alternative-to-password-based-authentication/
21. EOSIO, "A passwordless future: Building towards more secure and usable authentication systems," Medium, Apr. 16, 2019. [Online]. Available: https://medium.com/eosio/a-passwordless-future-building-towards-more-secure-and-usable-authentication-systems-e188f07e4b87
22. L. Columbus, "Passwords are the weakest defense in a zero trust world," *Forbes*, July 14, 2019. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2019/07/14/passwords-are-the-weakest-defense-in-a-zero-trust-world/#63bbca365218
23. S. Dolev, "The quantum meltdown of encryption," TechCrunch, Bay Area, CA, July 22, 2018. [Online]. Available: https://techcrunch.com/2018/07/22/the-quantum-meltdown-of-encryption/
24. "Get instantaneous behavioral analytics and anomaly detection," Microsoft, Corp., Redmond, WA, 2020.
25. R. Lemos, "Single sign-on still open to attack: An inside look," TechBeacon, Aug. 7, 2019. [Online]. Available: https://techbeacon.com/security/single-sign-still-open-attack-inside-look

MARK CAMPBELL is the chief innovation officer for EVOTEK. Contact him at mark@evotek.com.