IDC ANALYST CONNECTION

Sponsored by: Transmit Security

Originally developed as a means for granting access to computing resources, cracking username/password combinations now leads as a cybercriminal attack vector for data breaches and account takeovers due to design weaknesses. It's a total nonstarter for consumer usage.

Why Passwordless Customer Authentication Should Be a Priority for CISOs

March 2022

Questions posed by: Transmit Security

Answers by: Jay Bretzmann, Program Director, Security Products

Q. What is a passwordless approach to customer authentication?

A. The concept has existed for many years, but the computing infrastructure behind eliminating passwords just wasn't there for supporting any true mass-market consumer adoption. Previous identity solutions were developed using chip-based smartcards, hardware dongles, and so forth, but none of them were practical for helping secure connections with consumers due to physical distribution issues and the orders-of-magnitude greater scale of consumer-focused applications and services.

Requiring any sort of password creation activity for a consumer-facing application is just a bad idea. As consumers, we make up passwords on a whim and don't typically remember them past the current session. Most of the industry rhetoric on passwordless seems to completely miss this point. Consumers want, and will soon insist on, registered devices on which they can access web application services with the touch of a finger or a glance at a screen. Consumers also won't tolerate a proprietary solution that works for only one or two situations.

The watershed event here was when one company developed a smart device that included a new cryptographic security engine within its system-on-a-chip (SoC) main device processor offering the ability to generate and store public/private PKI key pairs circa 2013. It would take a half dozen more years to create an industry standard (Fast IDentity Online, or FIDO2) and the necessary platform support to provide the true ability to leverage user finger and facial biometrics and completely eliminate the password-based device registration process. That identity security infrastructure is now in place for devices (e.g., mobile phones, laptops, desktops) and software (e.g., browsers, authenticators), making it possible for companies to hide all the background processing taking place when consumers authenticate to their applications and services.

Q. Why should passwordless authentication be a critical priority for CISOs?

A. As the COVID-19 pandemic has rapidly accelerated many organizations' digital transformation timescales, IDC believes that many CISOs who downplay or overlook the unique requirements of a consumer identity and access management capability will find themselves at a sales and marketing disadvantage. Indeed, consumers today find themselves using

more online services than ever before, which means they have more accounts and passwords to track. This has increased complexity for consumers, which is bad for both user experience and security.

Many enterprises have turned to social log-ins as a consumer-friendly solution. CISOs should be wary of this measure as not all single sign-on (SSO) assertions are created equal, especially those created using shared passwords as is a common practice. Social log-in models provide very little assurance to the relying party, and because they share almost no information about the device, location, or authentication method or other facts about the consumer's identity, they fail to support a risk-based model to thwarting fraud. Many social networks are not focused on delivering a reliable consumer identity and access management solution for other enterprises; they are paid to drive advertising and other revenues and use social log-ins as a benefit for members.

In general, passwords are recognized as an inherently insecure method of authentication. They are a common attack vector for account takeovers, and user bad practices such as using the same password across many services make them especially vulnerable. In response, CISOs have mandated multifactor authentication (MFA) measures, which adds complexity for users. Passwordless solutions based on FIDO2 provide for "one-touch" or "one-look" MFA that relies on both what you have (your device) and what you are (device-based biometrics), without requiring one-time passwords, magic links, or other mechanisms that introduce complexity and potential vulnerabilities.

Consumer identity requirements are typically quite different from the identity requirements of a workplace solution, and few technology suppliers can serve both camps. Up-front log-in friction sends lots of surfers to other links. A recent IDC survey uncovered what we believe to be an accommodation strategy where workplace identity solutions were being stretched to include consumers. We further believe that most of these respondents will replace such band-aid approaches within the next 18–24 months — the upside being that's just about enough time to reexamine priorities and find a better, long-term solution. A poor consumer identity and access management solution is little better than no capability at all and likely much worse because it can lead to degradation of vendor brands.

CISOs should also view supporting an organization's customers as an opportunity for their office to become more of a business enabler rather than an application technology roadblock. Security has often been referred to as the party of "no" as businesses increasingly migrate to the cloud. IDC believes passwordless identity to be a foundational element of a more frictionless identity management approach and a linchpin for consumer applications of the technology.

Q. What are the benefits of adopting a passwordless authentication approach for reaching customers?

A. There are four main benefits to a passwordless approach: user experience, cost, revenue, and security.
First, passwordless authentication contributes to a superior customer experience generating measurably higher user satisfaction levels. Good customers generally appreciate being recognized and presented with opportunities stemming from past interactions, which is made possible when your service authenticates consumers earlier in their interaction. Digital dictates a new and largely unforgiving sales model requiring a fresh approach to identity practices.

Second, any injected friction translates to confused and angry customers. Passwords, in particular, are often forgotten, which then requires resets. Because passwords are less secure, they require additional layers of security. All of this translates to call center costs and customer churn.

Third, friction reduces conversion rates. Digital marketers carefully manage and tune their investments to attract and convert prospects into paying consumers, guests into registered accounts, and repeat visitors into repeat buyers. It's a numbers game. At every step of a consumer's journey, from the consumer's first visit to a web site or first download of an application, there is a risk the consumer will not take the next step. Friction of any kind reduces those conversation rates. In a digital model, even a tiny bit of friction can lead to thousands of lost transactions and revenues.

Finally, passwordless significantly enhances security and reduces the risk of fraud. The use of biometrics for identifying both new and repeat customers is also much more secure than many existing second-factor authentication solutions based on messaging systems where (annoying) codes are sent back and forth via SMS phone lines or email, both of which are susceptible to interception along the way. A FIDO2-based biometric system is unphishable because both clients and servers are cryptographically identified during the authentication process, virtually eliminating credential compromises and account takeover (ATO) fraud situations.

There are additional security benefits of passwordless solutions that truly eliminate passwords from the user store. In particular, there are no centralized vaults of registration and backup passwords that can be discovered by attackers via lateral network movements following a successful credential phishing attack after someone mistakenly clicks on a bad link. Passwords of any type are unnecessary exposures that can do irreparable harm to consumer relationships and company brands when compromised. Furthermore, organizations whose customer credentials are stolen must send out breach notices, often offering to pay for 12 months of identity theft monitoring services.

Q. Why should CISOs trust passwordless authentication?

A. Although CISOs must carefully evaluate any authentication solution they are considering, they should prioritize FIDO2-based passwordless solutions. By choosing solutions that rely on FIDO2, CISOs can rest assured the underlying technology is mature; FIDO2 capabilities have been built into devices produced by Apple, Microsoft, Samsung, Google, and other vendors with a strong focus on security. FIDO2-based authentication has been adopted by technology companies (e.g., Amazon Web Services, Citrix, Dropbox), banks (e.g., Bank of America, BBVA, PNC), payments companies (e.g., PayPal, PlusCard), governments (e.g., Login.gov, UK NHS), and more. The FIDO Alliance, which maintains the FIDO2 standards, has a robust board of directors (including representatives from the U.S. National Institute of Standards and Technology) and a broad community of identity experts, all of which operate openly and transparently.

CISOs should take comfort in knowing that consumers have become very comfortable with biometrics-based log-ins. Most users open their personal/professional device home screens with a quick touch or look and sign into important applications the same way. It's painless and — while not truly addicting — a highly appreciated capability. Evidence abounds that multifactor authentication is highly effective, and FIDO2 removed the final friction-related objections to consumer identity applications.

IDC believes passwordless identity authentication is a foundational step in the process of building more secure identity management systems and a stepping-stone toward what many call zero trust environments. Simple browsing activities should be open to all, but as risk profiles increase, step-up authentications become required when personally identifiable information (PII) is disclosed. Face recognition can be that quick and painless reassurance that the requester hasn't changed after a somewhat extended period of device inactivity. It's a security enhancement that can make the experience much easier for consumers, leading to repeat website visits to "buy it again" in two to three clicks.

Q. Is passwordless identity authentication necessarily separate from workplace identity solutions?

A. Yes and no, but most workplace solutions were built long ago and lack the appropriate schema and data collection/retention capabilities that a consumer-oriented solution includes, especially when paired with customer loyalty program software. Consumer solutions are also compatible with new public-facing access and management modules that privacy standards such as Europe's General Data Protection Regulation (now others too) require, such as the ability to correct inaccuracies and the right to be forgotten.

Passwordless solutions built for consumers also work well with devices that aren't under the control of the service provider (relying party). While workplace identity solutions often depend on mobile device management (MDM) policies and controls, those controls are not feasible in a consumer scenario. Transfer of trust from one device to another is also a challenge that workplace solutions are not designed to handle but is a particular concern in consumer scenarios. Consumers change out their phones, switch from their mobile device to a laptop, use their spouse's device, and exhibit other behaviors that are largely unique to the consumer experience.

Consumer identity sign-on screens are also highly customizable, and vendors will be investing and improving what they offer for many years to come. Sign-on screens are one of the first touch points people encounter when they decide to convert from an application visitor to an application customer. Consumer solutions must work well with marketing automation tools, supporting use cases such as progressive profiling or adaptive authentication that aren't common in the workplace.

Practically speaking, most workplace identity and access management solutions just don't hit the mark.

About the Analyst

Jay Bretzmann, *Program Director, Security Products*

Jay Bretzmann is Program Director for IDC 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 Transmit Security

Transmit Security, the Identity Experience company, is on a mission to revolutionize customer identity and access management and eliminate passwords. BindID™ by Transmit Security is the only customer authentication service that completely eliminates passwords from the entire customer experience. BindID™ offers cross-channel passwordless authentication, enabling customers to seamlessly authenticate on any channel from any trusted device — all without a password. By eradicating passwords, organizations are able to prevent fraud and captivate customers with elegantly simple identity experiences all while effectively reducing all forms of identity attrition and saving enterprises substantial costs.

Go passwordless with BindID. Visit: https://www.transmitsecurity.com/bindid

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com