Beyond The Password: Identity and Access

TECHNOLOGY SOLUTIONS TO A HUMAN PROBLEM

People + Passwords = Pain

- 3 out of 4 people use duplicate passwords
- 60% of users forget a password at least once a month
- 17% of users forget a password 6-10 times per month
- Most people don't change their passwords for 5 or more years

Florencio & Herley

Background

In the past decade, the number of passwords in use by the average American has almost tripled. People are stacking up subscriptions to SaaS products and connecting more with vendors and suppliers through password-secured portals. Ten years ago, the average person only had 6.5 accounts that required logins; today, the average is 27.

All those passwords are intended to keep data safe, but they have the opposite effect— the more passwords a person has to remember, the less secure those passwords become. Call it Post-It Syndrome or the 1234 Enigma, but a person with a lot of passwords is more likely to reuse a few simple ones that are easy to remember (and, therefore, easy to hack) over a number of sites. Most people only have 5 or 6 passwords that they use over their 27 accounts.

Passwords Are Not the Problem

On the surface, the security challenge is password management. However, the real problem is not the strings of characters that make up a password—it is who is using that password to access a secured system, and what services they can access once they're inside.

Attempts to come up with better ways to manage identity and access have mostly been either easy to use and not very secure, or hard to use and very secure. When access is made difficult, people will find workarounds, such as writing down the password on a Post-It or choosing an insecure password. Identity and access management (IAM) is as much a human puzzle as a technological one.

[1] Florencio & Herley

Keeping It Simple with Single Sign-Ons

There are still some organizations that have a mix of web- and legacy-architected, thick Windows client applications that must be supported for a single sign-on (SSO) initiative when the endpoint devices are Windows-based. This requirement set is much less common, because applications have become web-architected, and the need for mobile device support has increased.

However, the requirements are still prevalent in the healthcare provider vertical and some manufacturing floor environments. Enterprise single sign-on (ESSO) tools provide a means to address these requirements. They operate by using Windows endpoint agent technology to intercept sign-on prompts[2] and password change prompts, and transmit IDs and passwords though the application user interface. They also provide a means to rapidly switch user sessions on shared Windows workstations.

Social Sign-ins: Balancing the User Experience with Security Needs

The user experience for SSO took a leap forward when social sign-in was developed. With social sign-in, a user can enter the same credentials he or she has used on a social networking site to access[3] other sites. Users like the option of logging in with a Facebook, LinkedIn, or other social networking account. In fact, as far back as 2013, 77% of users reported that social sign-on "should be offered by any site".

However, security analysts aren't so enthusiastic. Attackers have exploited weaknesses in social sign-on to conduct some high-profile attacks. All they need is a target's email address, which they then use to create a new account on a social networking site where the victim's email address has not already been used. The social networking site will send a verification email to the target, allowing the hacker to create the account and use it as a means to access sites that rely on social sign-ins.

That is called a SpoofedMe attack, and it's not the only way a social sign-on can endanger the security of an enterprise.

If a social network is breached, as happened to LinkedIn in 2012 when 1.7 million of its customers' credentials were stolen, or in 2016 to LinkedIn's learning unit, Lynda.com, when 9.5 million credentials were stolen, any enterprise that allows social sign-on from[4] that social network is at risk as well.

[2] Russell

[3] Francisco

SSO: A Result of Federation

SSO is a practical solution for managing identity within a single network; a user logs in once and is authenticated, and authorization is granted for the duration of the session. But few workers go through their days without venturing outside of their corporate network anymore. To handle authentication and authorization between the networks of trading partners, an overarching architecture was needed.

Business as a Team Sport: Federated Identity

As gaining access to distributed resources becomes increasingly vital, the ability to manage identity effectively becomes a paramount concern. Federated identity is a set of mechanisms through which companies can share identity information between secure networks.

As a result of federation, companies can create identity-based applications -- such as a federated single sign-on -- that enable increased access to cross-company information.[6]

For instance, a large box store may have many vendors who need to access its supply chain management solution; some of the vendors' workers only need to enter data, while others need to edit data.

Federated identity enables these workers to access the services of the box store's supply chain system that they are authorized to access without reauthenticating.

The companies in a federation form a circle of trust.

The companies in a federation form a circle of trust. In a circle of trust, each party may act as an identity provider or a service provider that manages its own workers' identities and the other systems function as service providers that give validated users access to services. Circles of trust are not without risk; if one member of a federation has weak security practices, all members may suffer.

> **Through 2018, federated single sign-on (SSO) will be the predominant SSO technology required by 85% of organizations.**[4]
> *("Take a Pragmatic Approach to Single Sign-On for Quicker Value", Gartner - July 29, 2016)*

4 Take a Pragmatic Approach to Single Sign-On for Quicker Value", Gartner - July 29, 2016

6 Eric Norlin and Darren Platt

Business as a Team Sport: Federated Identity

The companies in a federation form a circle of trust. In a circle of trust, each party may act as an identity provider or a service provider that manages its own workers' identities and the other systems function as service providers that give validated users access to services.

Circles of trust are not without risk; if one member of a federation has weak security practices, all members may suffer.

Authentication vs. Authorization

Who I Am	What I Can Do

The Lingua Franca of Federation

For all the systems in a circle of trust to share information, they need a common language.

Federated identity for enterprises is based on an open-standard data format called Secure Assertion Markup Language (SAML).

SAML uses XML to allow an identity provider and a service provider to exchange authentication and authorization information.

With federated identity, the users' experience is seamless; once they've logged into their employer's system, they are free to move between the domains of its trading partners without having to register a new account or log on with a unique password each time they visit.

Sometimes a user must still be identified and redirected home for authentication and enter credentials – at least the first time, but the user never provides credentials directly to anyone outside of his corporate network, so the corporate network's security remains uncompromised, and the user's attributes—name, title, role, username, password, permission level, or any other information the federation members have selected—are automatically known to service providers in the circle of trust.

More Services, Fewer Risks

Federated identity decouples identity from access. Each company in the federation only needs to manage its own users' identities and accept credentials from other companies in the circle of trust. User attributes are verified by the user's company and there is no need to propagate status changes across the whole federation.

For the businesses in the trading circle, the benefits of federated identity are:

- Reduced costs because no proprietary solutions are required
- Improved productivity due to a smoother user experience.
- Flexibility to authenticate users from partner organizations and provide them with seamless access to protected online resources.

[5] Eric Norlin and Darren Platt

More is Better: Multi-Factor Authentication

Authentication is based on three common factors: something you know, something you have, and something you are. Until a few years ago, single factor authentication was considered adequate, and something you know —a password—was all most networks required.

That is no longer the case. Current enterprise best practice requires that two of the three factors be in play for a person's identity to be validated. This is called multi-factor authentication (MFA), and anyone who has reset their Google or Microsoft password will be familiar with how it works—Google verifies that the reset request is from the legitimate account holder by sending a code via SMS to the phone number associated with the account. In the enterprise, physical tokens can serve as a second factor. The physical token is usually a card or a fob, but the problem with a physical item is that it is easily lost or stolen.

The third factor, something you are, is a biometric factor, like a fingerprint, voice or iris pattern. The concern with biometrics is that the fingerprint or iris pattern may be stored in a database as a piece of encrypted data, and if the database is hacked, that piece of data can be stolen just like a password can be stolen. In fact, fingerprints were one of the types of data stolen in the OPM breach – 5.6 million of them.[4] However, many good biometric technologies extract data from the biometric and convert it into something else that cannot be converted back to the biometric.

Dynamic Credentialing with TOTP

> "When offered as a stand-alone solution, TOTP can be hard to integrate with existing systems"

Today, the gold standard in authentication is time-based one-time password (TOTP). With TOTP, an algorithm generates a one-time password based on a shared secret key and current time stamp. Because the password changes every 30 to 60 seconds, it is resistant to attacks.

Originally, TOTP services sent the password via text; that method, however, has become vulnerable to attack as well. Now there are several ways TOTP services can deliver a password: via SMS to a cell phone previously registered to a network, to a mobile app, through a QR code that is scanned by a smartphone, or to a special physical device with a small screen.

The high level of security offered by TOTP doesn't come cheap. Most providers charge a per user, per device monthly fee which can get expensive fast, especially for enterprises with a lot of virtual offices and mobile devices. When offered as a stand-alone solution, TOTP can be hard to integrate with existing systems and time-consuming to manage.

[4] Peterson

Leveraging PKIs with Push Authentications

There's another type of authentication that's even more secure than TOTP. Push authentication is already in use by major social networking sites, and in May of 2016, NIST updated its guidelines to recommend push authentication as a best practice.[7] In this scenario, when a user tries to access a protected resource, a login request is pushed to the user's mobile device. He then opens an app on the device and chooses to approve or deny the login request. If the user chooses to approve it, he is logged in to the resource.

Dynamic Credentialing with TOTP

A multi-factor authentication solution needs to integrate with remote access and network technologies, as well as the existing directory service, and be flexible enough to provide security in cloud, hosted, and on-prem environments.

A new approach to MFA that provides companies with the cost-savings and staffing benefits of scale is MFA as a Service. MFA as a Service allows developers to use an API to stand up MFA quickly but never have to maintain it. That burden is shifted to the provider, who already has the technology, infrastructure, and expertise to manage the service.

Controlling Identity and Access Requires Expertise and Infrastructure

Users want to login to all of their accounts as easily and rapidly as possible. Enterprises want that as well; the faster staff members can access the services they need, the more productive they can be and the fewer man-hours the IT department has to spend resolving lost-password tickets.

IAM is one of the most fundamental and critical elements of an organization's security strategy, yet few enterprises have the appropriate level of expertise on staff to choose the best technology, integrate it with the rest of the IT environment, and upgrade it to meet emerging threats. IAM is a specialized area in the security landscape—a riddle within a conundrum— so many businesses choose to partner with a managed services provider to control who is doing what inside their walls.

Selecting from among providers can be confusing because so many solutions look alike on the surface—but it's what's behind the username and password fields that makes the difference.

Criteria For Choosing a Provider

Security. You may be more comfortable choosing a provider that offers private servers rather than shared servers in a pooled public cloud. This eliminates added exposure if one server is compromised.

Customizability. Look for a solution that can be customized to meet your unique needs, such as by providing a rules engine that allows your organization to do things like specifying the hours of the day or locations from which an app can be accessed

Scalability. Your solution needs to grow or shrink with you as your needs change. Look for functionalities such as delegated administration, which allows the access controls to be decentralized so businesses can scale easily.

[7] Grassi, Garcia and Fenton

Works Cited

Florencio, Dinei and Cormac Herley. "A Large-Scale Study of Web Password Habits." 2007. *Microsoft Research*. <https://www.microsoft.com/en-us/research/wp-content/uploads/2006/11/www2007.pdf>.

Franciso, Maricris. *Microsoft's LinkedIn Hit By Data Breach: 55,000 Passwords Reset For Subsidiary Lynda.com*. 20 December 2016. http://www.techtimes.com/articles/189475/20161220/microsoft-deal-linkedin-data-breach-yahoo-data-breach-lynda-breach.htm.

Grassi, Paul A., Michael E. Garcia and James L. Fenton. "Special Publication 800-63-3 Digital Identity Guidelines." 2017.

Humphries, Daniel. *Best Practices for Workplace Passwords*. 15 January 2015. <http://www.softwareadvice.com/security/industryview/password-workplace-report-2015/>.

Jones, Brad. *Intel hates passwords, even on World Password Day*. 5 May 2016. <http://www.digitaltrends.com/computing/intel-world-password-day-true-key-app/>.

Okyle, Carly. *Password Statistics: The Bad, the Worse and the Ugly (Infographic)*. 3 June 2015. <https://www.entrepreneur.com/article/246902>.

Peterson, Andrea. *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought*. 23 September 2015. <https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.c56e7c137845>.

Russell, Matt. "Who's Sharing What – The State of Social Sharing in 2013." 21 March 2013. *WebHostingBuzz*. <http://www.webhostingbuzz.com/blog/2013/03/21/whos-sharing-what/>.

TechNewsWorld, *Federated Identity Standards: Confused?* Eric Norlin and Darren Platt http://www.technewsworld.com/story/33197.html