IDPro News

The Member Newsletter of IDPro.org

From The Board

Though this isn't the final month of 2019, with the holiday season imminent we will find ourselves in 2020 sooner than we expect. And as one year winds down and we look toward the start of a new one, it's time for some retrospection, introspection, and – for those insufferable type-A personalities – a little goal setting. As an organization with big goals, we are most definitely counted among those insufferable, improvement-minded types. As such, the Board has begun its 2020 planning.

Although the final product of these efforts will be revealed once fully baked, many of the themes will be familiar. Refining and accelerating the Body of Knowledge will be a focus for years to come. We intend to invest not only in the continuation and acceleration of the growth of the organization, but in new initiatives and support structures so as to provide real, tangible value for individual members. And of course, we want to support the continued development and professionalization of the industry. Suffice to say, there will always be opportunities for membership to get involved and leave their mark on this organization – and we plan to be able to better channel that energy moving forward.

Finally, one more thing that merits highlighting this month. The work going on within the Body of Knowledge committee continues to bear fruit, with two additional original articles now en route to public review since the last newsletter. As always, we express our appreciation to the commitment and hard work of our BoK Principal Editor Heather Flanagan as well as the rotating cast of volunteers who find the time to contribute.

We wish you all a fantastic holiday season.

Jon Lehtinen
Thomson Reuters
Board Member, IDPro

In Brief

Identiverse Call for Presentations

The call for presentations for Identiverse 2020 is officially open for the 11th annual event being held June 8-11, 2020 in Colorado. For information on submitting a presentation, visit the Identiverse website.

Member Presentations

Member presentations from Identiverse 2019 have now been conveniently collated on the IDPro website. To view these presentations, visit the IDPro site at https://idpro.org/member-present. You can aso view the complete collection of presentations from Identiverse 2019 on the Identiverse YouTube Channel at https://www.youtube.com/channel/UCUOo7SSG-a4yk8-11kPDKqg.

Verified Credentials Data Model

The W3C has approved the Verified Credentials Data Model as a Recommendation. For more details, check out the spect at https://www.w3.org/TR/vc-data-model/

Implementer's Draft of OpenID Connect for Identity Assurance Specification Approved

The OpenID Foundation membership has approved the OpenID Connect for Identity Assurance 1.0 specification. More information on this spec can be found here.

Get Involved

We are working on many initiatives such as the Body of Knowledge, collaboration with industry orgs, increased visibility & presence at industry conferences, & we need your help. If you'd like to get involved with IDPro, send a message to IWantToHelp@idpro.org.

Make the most of your membership**!** Don't forget to follow us on Twitter @idpro_org, check our our LinkedIn page, and join the conversation via the email discussion groups or on Slack at https://idprofessionals.slack.com. If you need an invitation, or if you're not receiving the email list messages, drop a message to director@idpro.org.

Get in touch with your ideas and contributions & help us make **your** newsletter even better! The editorial team can now be contacted at editorial@idpro.org. Theoretical or practical, your editorial team wants to hear from you! And if you've never written an article before, don't worry - we're more than happy to help provide whatever guidance or support you need.

From the Membership

My phone is My Password

Everyone has a smartphone (in fact, many have more than one). Nobody wants to remember yet another password. Surely the combination of these two means that the smartphone app is the logical solution to securing authentication and delivering a truly passwordless experience for both employees and customers? Unfortunately, it's not always as simple as that, though. In the ongoing war between convenience and user experience on the one side, and strong security and privacy on the other, we need to ensure that we do not unwittingly create new risks and attack surfaces in our rush to remove passwords.

The Trouble with Passwords

It's probably not all that controversial to say that we, as an industry, are not doing knowledge-based authentication (and passwords in particular) at all well. Knowledge is fallible and unreliable – just because somebody knows a particular random string of characters at one point in time is unfortunately no guarantee that they'll remember that same thing days, months or years later. Bad password hygiene thus abounds, as individuals would rather use weak passwords to eliminate complexity and improve their own user experience. Companies often counter by enforcing impossible password policies that only make the user experience worse.

Smartphones are commonly used today as a secure yet convenient second factor, for a number of good reasons. Phones offer built-in private keystores protected with a biometric and a built-in way to deliver secure authentication challenges via push messaging. Smartphone apps often double as a soft token, and organizations can stay in control of the user experience and branding of the app. They are also cheaper and more convenient than hard-token based solutions

Are we ready, though, to abandon passwords entirely and rely solely on the smartphone as a way to authenticate users? I believe that we certainly can do this now.

The Boy who Logged In using (only) his Phone – with apologies to JK Rowling.

A number of techniques and patterns exist today for enabling authentication using only a smartphone. There are, of course, pros and cons to each of them.

Identifier + Push is one technique that I've seen. This is where the password is dropped entirely, with the user instead only providing a username (which can, of course, be cached in a browser cookie). Once the user has been identified, a push notification is sent to the smartphone app in

order to authenticate the user through the possession factor. In order to implement this model securely (and not reduce security to single-factor, possession only authentication), it is strongly advised to ensure that a biometric login or approval is required on the mobile in order to accept the authentication request.

Claiming an authentication session through scanning a QR code is another popular approach – one that has the added usability bonus of removing the username entirely. In this model, the user opens a trusted app that is strongly linked with her identity, uses a biometric to unlock her private key, and then scans a code that is presented by the website she wishes to access. It's a great and novel approach to the problem but can lead to something of a proliferation of different authentication apps on the phone. Some level of user retraining may well be required, too.

Native app auto-login is a good approach for passwordless authentication when the user's journey starts on the smartphone itself. Once again, the combination of possession (a private key within the app) and inherence through a biometric can be used to enable login without requiring users to type in usernames and passwords each time they launch an app.

Across the industry, we continue to evolve and develop new standards to improve authentication and two newer options for passwordless authentication have emerged from the identity standards community – each aiming to tackle the problem in different ways.

Client-Initiated Back-channel Authentication, or CIBA, is a new standard from the OpenID Foundation that complements the existing redirect-based OpenID Connect flows with a decoupled option that uses a push to a smartphone app as the primary means of user authentication. CIBA is still emerging but offers a solution to a wide variety of use cases, moving beyond authentication towards transaction approval as well.

The new WebAuthN standard developed under the auspices of the W3C provides an end-to-end secure flow for user authentication with a high level of resistance to phishing and man-in-the-middle attacks. Central to the approach is the Client-to-Authenticator Protocol (CTAP) that enables a user agent to communicate with any authenticator device that implements the standard. Google's latest phones incorporate a built-in CTAP authenticator, allowing the native biometric capability of the device to be used as an authentication factor.

With Great Power comes Great Responsibility

I do need to end with a few caveats, though. While the approaches outlined above all offer a far better user experience than anything based on passwords, we do need to take some key points into consideration. It's a pretty small leap from "My Phone is my Password" to "My Phone is my Identity" and it thus becomes very important to include a strong process of identity proofing in any enrollment process that allows enablement of a smartphone app as a primary authentication factor. As the smartphone becomes the primary authenticator, it is equally

important to ensure that possession of the smartphone alone is not sufficient to allow access; a biometric or knowledge step must always be added to the authentication process.

Some of these approaches are reliant on standards that are not yet implemented consistently across mobile operating systems and/or browser ecosystems; others rely on the user installing 'yet another' authentication application on their device, which can mar the user experience. Both of these situations will improve with time, but for now, take care to pick solutions which are appropriate for your target user base.

Finally, we need to be realistic about the risks and vulnerabilities of a smartphone-app-based approach to identity and security and ensure we are implementing the necessary countermeasures to protect our users against the threat of compromise of their mobile keystores. This starts with detection of rooted or jailbroken devices but should also encompass an appropriate level of malware detection and anti-tampering counter measures.

(For additional background, check out Rob's Identiverse presentation on this topic)

Rob Otto
Office of the CTO
Ping Identity

So You Think You Can Two-Factor

If every year is The Year of PKI, then when exactly was The Year of Two-Factor Authentication? Was it 2012, when the epic hacking of Mat Honan highlighted just how vulnerable all of our digital lives are? Was it 2014, when the even higher profile iCloud leaks of celebrity photos pushed various consumer services to hastily make two factor authentication an option available to users? Or did it really arrive in 2018, at least for financial institutions, when PSD2 delivered a regulation with some real teeth?

The Struggle is Real

Two-factor authentication (or 2FA as the cool kids call it) isn't really new. We've all experienced it during the course of our professional lives, but organizations still struggle with rolling out 2FA to customers. Why? The simple reason is that while employees are a captive audience that will submit to whatever painful, inconvenient mechanism you force them to adopt (ok, except for MDM on their personal phones), customers are a whole different ballgame. The customer experience matters, and if you don't do it right then people are either going to not enable it (when you make it optional), work their way around it, or not engage at all.

For any organization starting down the path of implementing 2FA, it can be confusing and challenging. They find a large list of factors spread across the "something you ___" categories, but little guidance on how to put a good 2FA scheme in place. Most organizations simply end up taking the approach of picking an additional factor that they can simply tack on to the end of their password authentication step, and call it a day. Unfortunately, that simplified approach falls far short of successfully addressing the problem.

A Framework for Designing Your 2FA Schema

I first started going down the 2FA rabbit hole when I wrote a blog post analyzing the Mat Honan hack. Since then, I've had the benefit/privilege/misfortune (which one it is depends on the kind of day I'm having) of having worked on strong authentication models quite a few times. More recently in my current role at Uniken, our efforts to create a multifactor authentication model that is focused on the customer experience, and can work across industries for both small and large organizations, user bases and threat models, has yielded some deep insights into what works and what doesn't when it comes to 2FA. The effort to distill these learnings into something that can be explained to our product team and our customers has resulted in a basic framework for how organizations should go about implementing 2FA for their customers, built on 6 pillars.

Viability

The first pillar of that framework is **Viability**. When going through the long list of factors possible, you have to assess which of those factors is viable for your 2FA scheme. Assessing viability has multiple considerations:

- You have to think of the people that make up your user base, and what factors they'd be willing to accept and use.
- You also have to think about the cost of the factor, and whether that is a cost that the business will bear, or the customer will bear. Hardware tokens are great, but

expensive. Is the business buying it for their customers, or are they expecting the customer to buy it themselves?
- You have to carefully consider the threat model associated with the factor. The Yubikey is a really secure authentication factor, where the user has to plug the key into a port on their desktop in order to authenticate. But research studies have shown that people will often leave them plugged into their desktop even when they leave the office, virtually negating its assurance as a possession factor.
- You obviously have to consider the effectiveness of the factor. See: security questions.
- In many cases, regulatory compliance can enter the equation, since regulators are increasingly rendering opinions on which factors are acceptable for your business.

Multimodal

The second pillar of the framework is **Multimodal**. When implementing two-factor authentication, the goal is to have each user employ at least two factors when authenticating (obviously). However, that does not mean that the business is only going to support two factors. Not all factors work for all users, and when you're trying to increase the number of customers turning on 2FA, you have to offer options that work with your vast and diverse user base. The idea that you can find two factors that work for everyone leads you to a least common denominator approach, and that's how we got SMS OTP as the de facto "standard" in 2FA, and a weakening of the security model. Offering choice allows you to address the varying capabilities, preferences and circumstances of your end-users, and avoid a "one size fits all" approach that alienates customers and often weakens your security.

Adoption

I've alluded to the third pillar, which is the one that is the most misunderstood - **Adoption**. The reality is that unlike enterprise environments where you can mandate 2FA, the customer environment requires you to actually convince your end-users to start using 2FA. There's a wonderful research paper called "Why Johnny Doesn't Use Two Factor" that I highly encourage everyone to read. While there are many important takeaways in the paper, one overarching lesson from the paper is that organizations need to make UX research a core element of their IAM program, especially as they design their 2FA scheme. It's a critical and foundational element to creating the right set of messaging, training, and incentive components that you will have to incorporate into your roll out plan to drive adoption.

Omnichannel

An overlooked pillar is **Omnichannel**. Businesses have often failed to recognize that 2FA shouldn't apply just to their web or mobile channels, but must be deployed across all their

customer facing channels. Businesses are engaging with customers and partners across many channels – web, mobile, call center, in-person, chat, smart home assistants, and more - and each channel usually brings a completely different way of authenticating the end-user. That inconsistency frustrates your end-users, creates a headache for your customer-facing staff and IT staff, and delights bad actors. Attackers look for the weakest link across those channels, and go after that one, exploiting not only the weakness of the channel, but also the frustration that your customers and employees feel. The result is rampant account takeover attacks and fraud. Businesses have an imperative to transition away from an inconsistent hodge-podge of varying authentication models, and bring some consistency and equality of security levels across their various channels.

Processes

The fifth pillar of the framework is the one that most organizations don't pay enough attention to – **Processes**. Enabling and maintaining 2FA for individual customers involves many different processes, each of which needs to be properly designed:

- **Enrollment**: If the enrollment process is flawed, the assurance of your 2FA is suspect from the very beginning. Many organizations will allow users to set up their second factor after they've authenticated solely using their first, and that is a massive vulnerability point in your scheme.
- **Backup**: No authentication factor is immune from loss or destruction, so you have to think about ways to not only allow, but proactively encourage, your customers to set up additional authenticators as backups. And those backups better have the same strength as the primary, otherwise you're creating a backdoor for attackers.
- **Escape Paths**: Not all authentication factors are always available for use. Consider what happens to push notification-based authentication for someone working in a part of the building, or on a plane, where they get no signal. Locking them out under those circumstances can be hugely problematic.
- **Recovery**: Consider how you will support an end-user that has lost their authentication factor(s), so that they aren't faced with the dire consequence of being permanently locked out (think of all the horror stories of bitcoin wallets irrecoverably locked up because their owner lost the hardware token containing their private key). Recovery paths must also be designed properly to avoid having them turn into backdoors for bad actors. And for heaven's sake, *never* use an authentication factor as the verification factor for also doing recovery. I'm looking at every service that uses SMS OTP as a second factor of authentication, and also as a way of resetting a forgotten password. You've effectively created a backdoor that turns your two-factor authentication scheme into a one factor authentication scheme.
- **Deprovisioning**: Of course, you have to consider how one can go about invalidating a factor that is no longer available to the customer, or is no longer acceptable to the

business because of vulnerabilities or issues discovered in it (whether it be at an individual level or system wide).

Importantly, escape paths and recovery flows need to be treated as exceptions with higher risks associated with them. That often implies increasing the risk evaluation and security of those flows, which often means adding friction. However, customers are frequently understanding of the increased scrutiny in those paths (provided you're explaining it to them).

Trusted Environment

The sixth and final pillar of the framework is establishing a **Trusted Environment** within which to execute 2FA. It won't really matter how good or strong your factors of authentication are if the environment within which those factors are being accepted, stored, transmitted, and evaluated is compromised, allowing them to be stolen, manipulated or replayed. Keyloggers that capture secrets, malware apps that intercept SMS codes or steal keys, malicious WiFi, reverse proxies, and rogue cell towers that capture and replay credentials or tokens – threats like these reduce the effectiveness of 2FA and degrade organizational trust in those factors. Your two-factor authentication project has to be part of a larger security program that enforces defense-in-depth (or, to use the industry term du jour, zero trust security) to not only leverage the factors of authentication, but also look at the health of the devices and hardware being used and the networks being relied upon, as well as other signals of risk, in order to build trust in (hopefully) the simple act of authenticating your customer.

So, there you have it. A simple framework to apply while designing, building and rolling out your two-factor authentication program. May all your authentications be strong, and all your customers be happy, engaged and protected.

[This article is adapted from my talk at EIC, Identiverse and Identity Week. You can watch the Identiverse talk here.]

Nishant Kaushik
Uniken Inc

2019 IDPro Skills Survey

IDPro is excited to announce the release of the 2019 Skills Survey results. The Skills Survey is located on the members site at https://idpro.org/Skills-Surveys. We appreciate everyone's participation in this survey and hope you find the information useful.

Curated News

To add more value to the monthly IDPro newsletter, we're testing out adding a curated list of recent identity news and articles. These are recent articles from the area of privacy, tech, business, and entertainment, all as they relate to identity. These particular articles were chosen because of their timeliness and relevance to the topics we think the identity community may find interesting. Tell us what you think: editorial@idpro.org.

Risk-based digital identity benefits CIOs, CMOs and customers
Brave 1.0 launches, bringing the privacy-first browser out of beta
Privacy as a basic human right
Blockchain is Dead? Crypto Geeks Debate Merits of Once Dear Tech
A Vision for Collaborative Customer ID Verification in Africa
What is a Digital Identity?

Upcoming Conferences and Seminars

Date	Location	Organizer	Event
November 25-26, 2019	Stockholm, SE	Internet Stiftelsen	PasswordsCon 2019
December 10-12, 2019	Las Vegas, NV | USA	Gartner	Gartner Identity & Access Management Summit 2019
February 17-20, 2020	Vienna, AT	IDnext	Trust and Internet Identity Meeting Europe (TIIME)
February 24-28, 2020	San Francisco, CA | USA	RSA	RSA Conference 2020
March 11-12, 2020	Washington, DC | USA	Terrapinn	connect:ID 2020
March 21-27, 2020	Vancouver, BC | CAN	IETF	IETF 107 Vancouver

For additional details check out the Conferences and Seminars page at https://idpro.org/events/conferences-and-seminars/ and the Webinars listing at https://idpro.org/events/webinars/.

Upcoming User Group Meetings

Date	Location	Event
November 19, 2019	Milwaukee, WI	Q4 Milwaukee/Madison IAM User Group Meeting
November 21, 2019	Nashville, TN	Q4 Save the date (11/21/19)

For additional details and a list of known user groups, check out the User Groups page at https://idpro.org/events/user-groups/.

The IDPro Newsletter is brought to you thanks to the kind support of our corporate members, including: