Designing MFA for Humans

By Nishant Kaushik

Table of Contents

Abstract

This article describes how to deploy a thoughtful, consumer-friendly multi-factor authentication (MFA) program that will allow the IAM practitioner to successfully deliver on both the security and usability needs of their authentication systems. The approach is based on a framework of six pillars: determining the viability of different forms of MFA, allowing a multimodal rollout of MFA options, encouraging adoption, supporting MFA across all services and access channels, designing support processes, and creating a trusted environment where MFA can offer additional security to both the consumer and the company.

Introduction - Designing MFA For Humans

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? [i],[ii],[iii],[iv] Was it 2014, when the even higher profile iCloud leaks of celebrity photos pushed various consumer services to rush offering two-factor authentication an option available to users?[v] Or did it really arrive in 2018, at least for financial institutions, when PSD2 delivered a regulation with some real teeth?[vi],[vii]

Terminology

- Adaptive Authentication - Adaptive authentication aims to determine and enforce the authentication level required at any time during a user session - when the session is commenced, during the session when access requirements force a re-evaluation, or when the session token expires. The factors to be used in achieving that authentication level are determined dynamically based on the access control policy governing the resources being accessed, and a variety of environmental conditions and risk factors in effect at that time for that user.
- Account Takeover - Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials.
- Continuous Authentication - Continuous authentication is a mechanism that uses a variety of signals and measurements to determine during a user session if there is any change in the confidence that it is still the same user that authenticated at the beginning of the session, and trigger an authentication action if there is a drop in confidence.
- PSD2 - PSD2 (the Revised Payment Services Directive, Directive (EU) 2015/2366) is an EU Directive, administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA). It contains many requirements specifically related to Strong Client Authentication.
- Social Engineering - Social engineering is a method of manipulating people so they give up confidential information, such as passwords or bank information, or grant access to their computer to secretly install malicious software.
- Step-Up Authentication - A method to increase the level of assurance (or confidence) the system has regarding a user's authentication by issuing one or more additional authentication challenges, usually using factors different from the one(s) used to establish the initial authenticated session. The need for increasing the level of assurance is typically driven by the risk associated with the sensitive resource the user is attempting to access.
- Threat Modeling - Threat modeling is an analysis technique used to help identify threats, attacks, vulnerabilities, and countermeasures that could impact an application or process.
- Two-Factor Authentication (2FA) - A specific case of Multi-Factor Authentication (see: IDPro's Consolidated Terminology) where two factors must be checked to validate a user's identity.

The Struggle is Real

Two-factor authentication (2FA) is not new. IAM practitioners are certainly familiar with it through their professional lives (remember keychains full of hardware tokens?), but organizations still struggle with rolling out 2FA to customers. Why?

Figure 1: Remember carrying these?

The simple reason is that while employees are a captive audience that will submit to whatever painful, inconvenient mechanism they are forced to adopt (ok, except for mobile device management on their personal phones), customers are a different story. The customer experience matters, and if it is not done well, people are either not going to enable it (when it is optional), will work their way around it, or decide not to engage at all.

For any organization starting down the path of implementing 2FA, it can be confusing and challenging. They find an extensive list of factors spread across the "something you ___" categories, but little guidance on how to put a good 2FA scheme in place. It's like getting all the parts in a model kit, but without the instruction manual.

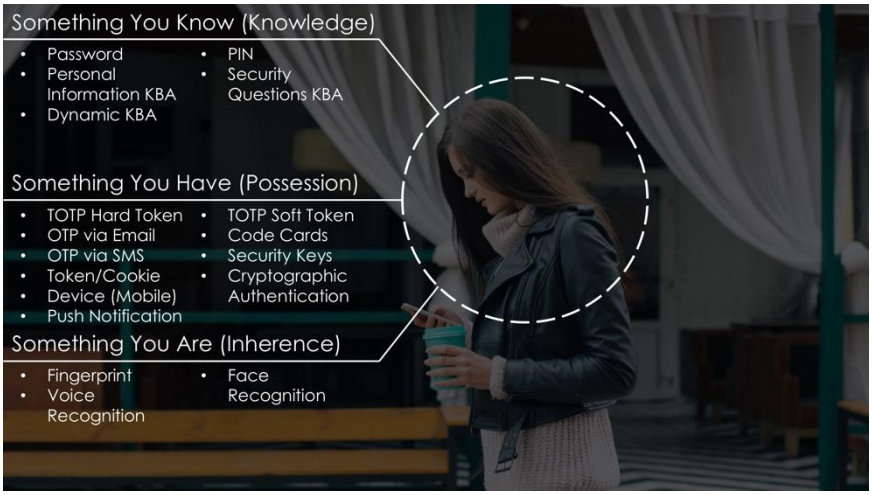

Figure 2: A vast menu to choose from

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 then call it a day. Unfortunately, that simplified approach falls far short of successfully addressing the problem, resulting in continued breach vectors, brittle infrastructure, and unsatisfied customers.

Thinking in Factors

Multi-factor authentication (MFA) aside, the goal of any authentication framework is to validate that the returning person (or thing) is the same one that the system saw last time, *to the required level of assurance*. That last part is what makes authentication difficult to implement well. Measuring the assurance of authentication is subjective, and cannot be normalized across organizations, industries, or end-user communities since a critical element in evaluating the assurance of authentication is trying to determine how easy or likely it is for an adversarial party to get around it. Determining this correctly requires doing threat modeling and risk analysis (more on that later), and then translating this into how to authenticate in different contexts.

This requirement for assurance is where factors of authentication become relevant. Factors make the abstract concrete by giving the authentication framework something tangible to evaluate, invoke, and measure. An important evolution that has happened is the realization that not all factors are created equal. This realization has expanded the kind of factors that can be used, while also creating the understanding that the same level of authentication assurance can be achieved using different sets of factors that are not numerically the same (i.e., one set of 2 factors can achieve the same level of assurance as a different set of 4 factors). The requirements around assurance are helping drive the discussion away from 2FA and towards **MFA**.

One important consideration that overshadows all of this is the nature of the factors and their impact on the user experience. When authentication factors translate into explicit challenges (or "active" factors) that an end-user has to engage with (as opposed to "passive" factors that work silently in the background), then the impact on usability will drive organizations to try and reduce the number of factors used in the authentication process. One way that they can compensate is to invoke additional (active) factors when the risk associated with the access request is elevated (often called **step-up authentication** or **adaptive authentication**). An even more refined approach to evaluating authentication assurance and risk is **continuous authentication**, which recognizes that the assurance level degrades over the life of the user session given how identity or access information may change during the session, and that passive factors can be used to constantly measure any changes or degradation to that assurance level, and determine if step-up authentication is required to bump the assurance level back up.

In all of these approaches, the factors of authentication are the control vector that allows the authentication framework to measure, achieve, and maintain the assurance level of the authenticated session as required by the business.

A Framework for Designing Your MFA Schema

MFA has become an imperative across industries, user bases and threat models, and the challenges and practices described below apply equally to both small and large organizations. It lays out a basic framework to build an MFA program that should prove useful to product teams, employees, and clients. This framework is built on six pillars that address the challenge of balancing security, usability and privacy.

1. Viability

The first pillar of that framework is **Viability**. When going through the long list of factors possible, implementors and decision makers must assess which of those factors is viable for their MFA scheme. Assessing viability has multiple considerations:

- User Acceptance: Think of the people that make up your user base, and what factors they'd be willing to accept and use.
- Cost: 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?
- Threat Model: Consider the threat model associated with the factor. A USB device can be a very 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. Discussing this in detail is out of scope for this article, but do note that there is a need to introduce threat modeling as a core discipline in identity management.
- Effectiveness: Consider the effectiveness of the factor. For example: security questions, a widely deployed form of MFA, are universally acknowledged as being ineffective in this age of public social media profiles and social engineering threats.
- Regulatory Compliance: In many cases, regulatory compliance can enter the equation, since regulators are increasingly rendering opinions on which factors are acceptable for different industries.

2. Multimodal

The second pillar of the framework is **Multimodal**. When implementing 2FA, the goal is to have each user employ at least two factors when authenticating. However, that does not mean that the business should only support two factors. Not all factors work for all users, and when a business is trying to increase the number of customers turning on MFA, they must offer options (i.e., be multimodal) that work with their vast and diverse user base. The idea that they can find two factors that work for everyone leads them to a least common denominator approach, and that's how so many industries have ended up with SMS OTP as the de facto "standard" in MFA, and a weakening of the security model.[viii]

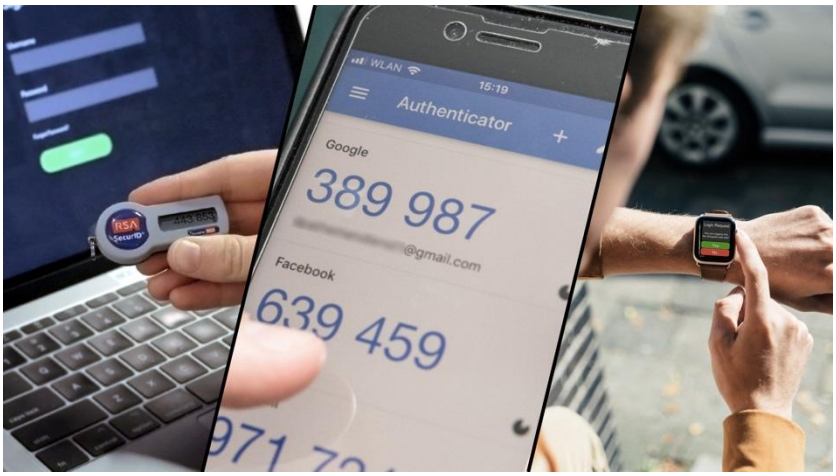

Figure 3: Different strokes for different folks

Offering choice allows a business to address the varying capabilities, preferences, and circumstances of their end-users, and avoid a "one size fits all" approach that alienates customers and often weakens security.

Being multimodal will necessarily require the authentication platform become adaptive, not just to risks, but also to user (cap)abilities. This ability to adapt will require the authentication service/platform/provider to create intelligent user flows – a concept commonly being referred to as orchestration.[ix]

3. Adoption

The third pillar is the one that is the most misunderstood - **Adoption**. The reality is that unlike enterprise environments where the business can mandate MFA, the customer environment requires a business to convince their end-users to start using MFA. While acceptance for this pattern is growing, in general this is easier said than done.[x]

Organizations need to make UX research a core element of their IAM program, especially as they design their MFA scheme. It is a critical and foundational element to creating the right set of messaging, training, and incentive components that the business will have to incorporate into their rollout plan to drive adoption.[xi]

4. Omnichannel

An overlooked pillar when designing MFA is **Omnichannel**. Businesses have often failed to recognize that MFA should not apply just to their web or mobile channels; they must be deployed across all their customer-facing channels. This ties back to the pillar on multimodality. 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.

This inconsistency frustrates end-users, creates a headache for 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 customers and employees feel. The result is rampant account takeover attacks and fraud. Watch this video of a classic social engineering attack that exploits weaknesses in the customer service authentication process to take over an account.

Businesses today have a pressing 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.

5. Processes

The fifth pillar of the framework is the one that most organizations do not pay enough attention to: **Processes**. Enabling and maintaining MFA 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 MFA is suspect from the very beginning. Many organizations will allow users to set up their second factor after they have authenticated solely using their first, and that is a massive vulnerability point in the overall security scheme.
- **Backup / Alternate**: No authentication factor is immune from loss or destruction, so the business has to think about ways to not only allow, but proactively encourage, customers to set up additional authenticators as backups. And those backups must have the same strength as the primary; otherwise, this creates a backdoor for attackers.
- **Escape Paths**: Not all authentication factors are always available for use, and the alternate mechanism may not be available. 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. It is not out of the question that they left their FIDO security key that they use as a backup safely locked in their office drawer. Locking them out under those circumstances can prove to be hugely problematic and result in workarounds that open up exploitation vectors. Escape paths may not be appropriate in all circumstances; consider carefully whether they should be designed into your system.
- **Recovery**: Consider how the business will support an end-user that has lost their authentication factor(s), so that they are not 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. *Never* use an authentication factor as the verification factor for also doing recovery (e.g., every service that uses SMS OTP as a second factor of authentication, and also as a way of resetting a forgotten password). This effectively creates a backdoor that turns a 2FA scheme into a one-factor authentication scheme.
- **Deprovisioning**: Of course, the business must to consider how to invalidate 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 implies increasing the risk evaluation and security of those flows, which often means adding friction. It is important to remember that in these circumstances, customers will frequently be understanding of the increased scrutiny in those paths (provided the business offers adequate explanations). One of the techniques emerging for these exception flows is the use of identity verification tools (e.g., document-based identity proofing) in these scenarios.

6. Trusted Environment

The sixth and final pillar of the framework is establishing a **Trusted Environment** within which to execute MFA. It will not matter how good or strong a business's 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 MFA and degrade organizational trust in those factors. All multi-factor authentication projects must 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.

Conclusion

This framework offers guidance for rolling out a strong and usable MFA service for their users. The considerations of factor viability, multimodal support, adoption rates, omnichannel applicability, and the infrastructure that guarantees a trusted environment, applies to any organization in any sector, and should be considered at every stage -- designing, building, and rollout – of any MFA program.

May all your authentications be strong, and all your customers be happy, engaged, and protected.

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

Author Bio

Nishant Kaushik is the CTO of Uniken, the first security platform that tightly integrates identity, authentication and channel security. He brings over 15 years of experience in the identity management industry architecting and delivering market leading products, with stints at Thor Technologies, Oracle, SCUID and CA Technologies. His current role allows him to focus on his latest passion of solving the user experience problem in delivering exceptional security by leveraging identity. Nishant is a recognized thought leader and notorious photoshopper of the identirati, regularly speaking at conferences and provoking discussion through his blog (blog.talkingidentity.com) and on twitter (@NishantK).

Nishant Kaushik
CTO, Uniken Inc.

---

[i] Berinato, Scott, "Only Mostly Dead," CSO Online, 23 May 2002, https://www.csoonline.com/article/2113027/only-mostly-dead.html.

[ii] Stiennon, Richard, "The new Entrust: is 2011 the year of PKI?" Forbes, 9 May 2011, https://www.forbes.com/sites/richardstiennon/2011/05/09/the-new-entrust-is-2011-the-year-of-pki/#2bdb8f5a171e.

[iii] Hils, Adam, "2015 Network Security Predictions: 8 Things That Won't Happen," blog, Gartner, 29 December 2014, https://blogs.gartner.com/adam-hils/2015-8-network-security-trends-that-wont-gain-t-raction/.

[iv] Honan, Matt, "How Apple and Amazon Security Flas Led to My Epic Hacking," Wired, 6 August 2012, https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

[v] Wikipedia contributors, "ICloud leaks of celebrity photos," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=ICloud_leaks_of_celebrity_photos&oldid=974755004 (accessed September 21, 2020).

[vi] *Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC,* European Commission, 12 January 2016, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en.

[vii] Constantin, Lucian, "What is PSD2? And how will it impact the payments processing industry," CSO Online, 13 September 2019, https://www.csoonline.com/article/3390538/what-is-psd2-and-how-it-will-impact-the-payments-processing-industry.html.
[viii] Suau, Roxanne, "SMS OTP Authentication: Not As Safe As You May Think," blog, Pradeo, 17 February 2020, https://blog.pradeo.com/sms-otp-authentication-not-safe.
[ix] Goldberg, Joel, "Workflow Orchestration: An Introduction," DevOps Blog, BMC, 15 October 2019, https://www.bmc.com/blogs/workflow-orchestration/.
[x] Camp, L. Jean, Sanchari Das, "Studies of 2FA, Why Johnny Can't Use 2FA and How We Can Change That," RSA Conference2019, video session, 12 February 2020, https://www.youtube.com/watch?v=UH9yWvvp4k8.
[xi] Das, Sianchari, Andrew Dingman, L. Jean Camp, "Why Johnny Doesn't Use Two Factor: A Two-Phase Usability Study of the FIDO U2F Security Key,"in *2018 International Conference on Financial Cryptography and Data Security (FC),* 2018, https://fc18.ifca.ai/preproceedings/111.pdf.