Multi-Factor Authentication: Do I Need It, and How Do I Get Started? [And If I Do Need It, Why Aren't Folks Deploying It?]

Joe St Sauver, Ph.D. (joe@internet2.edu)

Internet2 Global Summit, Denver Colorado
Tuesday, April 8thth, 2014 3:00-4:00PM
Governor's Square 10

http://pages.uoregon.edu/joe/global-summit-mfa/

Disclaimer: all opinions expressed are strictly my own.

Everyone Agrees That Passwords Are Insecure

- Passwords are potentially vulnerable to sniffing, brute forcing, phishing, hash cracking, reset attacks, etc.

- We know that we *could* do better, typically by combining a regular password *with* a "second factor" such as a registered mobile phone (or a smart card, or a biometric method, etc.)

- Nonetheless, as far as we can tell, **the higher education community still hasn't broadly embraced multifactor.**

- ***WHY?***

Really, Please Tell Us! We Need to Know!

- No one knows better than you why you're not currently using MFA everywhere on campus. If you could simply tell us, that would be great.

- Unfortunately, we believe that at least in some cases sites that aren't doing MFA may not have thought much about why they're not doing MFA (or at least may not be able to articulate why).

- Therefore, we'd like to suggest a few *potential* reasons, and then see if any of these reasons resonate with you.

- Please speak up if any of these do strike a chord with you....

"MFA's On Our List, We're Just Really Busy"

- This may be the most common reason why at least some sites haven't done MFA yet: they're just really busy with lots of other projects. Is "I'm too busy" the main holdup for MFA at <u>your</u> site?

- Do you want to do MFA, but worry that deploying MFA would take too long or demand too much in the way of staff resources?

- If that's the case for your site, how long (order of magnitude) do you think deploying MFA would actually take? And what's a higher priority on your to-do list? How can we make deployment easier, or a higher priority?

"MFA's Too Expensive" (Or Is It?)

- Another commonly heard (historical) reason for not deploying MFA broadly was that it was "too expensive."

- That may have been true at one point, but these days the out-of-pocket cost MFA for some MFA enterprise solutions is under a dollar per person per year. That's pretty cheap.

- Some of us may even have accounts from 3rd party cloud providers (such as Google) where we can enable use of MFA for **free.**

- And yet, somehow, many sites (and many users) still don't use it. So is money ***really*** the issue?

For Financial Comparison Purposes...

- Universities routinely spend $1/user/year (or more) on antivirus software. Why? Well, most sites worry a LOT about malware (bots, worms, trojan horses, etc.)

- But isn't phishing ***just*** as big a deal? Wouldn't it be worth $1/user/year to make (most) phishing go away, too?

- And how much do we spend **recovering** from plain old password failures? Wouldn't it make more sense to spend a *little money* on MFA to *prevent* breaches rather than a *lot of money recovering* from phishing attacks?

- What do YOU think? Is MFA still too expensive? How much would you and your site be willing to pay for MFA?

"MFA's Too Big A Pain To Use" (Or Is It?)

- If you login many times a day and you needed to copy six or eight secret digits from a hard token each time you did so, I could easily see that quickly becoming a huge pain.

- These days however, MFA has become easier to use (just push "OK" on a smart phone while logging in, for example), and in other cases, use of risk-based approaches means that MFA won't pester you at all unless you're doing something "unusual" (or particularly "significant").

- Thus MFA isn't as painful to use as it once was – is it? What do those of you in the audience think? Is MFA *still* too painful to routinely use? If so, in what way? How could we make it easier for you to use?

"It's Not About Routine Use..."

- Another thing I've heard is that MFA isn't too bad when it comes to *routine* use, its the problems that MFA can cause when things are *unusual* that worry folks:

  -- I forgot my MFA device at home, what do I do now?

  -- I just got a new phone. How do I *update the devices that the MFA system uses for me*?

  -- If I use a cloud-based MFA solution, what happens if our site gets DDoS'd and we can't access the cloud?

- Are exceptions really the roadblock? Do we need to focus on making sure that failure paths resolve painlessly?

"We Don't Have Anything Top Secret"

- This is another commonly heard comment... namely, that from a risk management POV, MFA is "overkill" for regular university users.
- At sites where this is the case, you'll often see "targeted deployments:" "we'll just do MFA for high risk accounts only" (or comments to the effect that "nobody's really interested in just plain old student accounts," etc.)
- In fact, however, we know that even a "mere" student account can still be leveraged to send spam, or it can be used as a stepping stone for attacks against higher value assets. Even "just" student accounts really *can* matter.
- Or consider faculty/staff access that's able to be used to access/change HR records (including things like direct deposit destinations).... ALL employees MAY need MFA.

"We'll Do MFA When Everyone Else Does"

- This is what is sometimes referred to as the "herd phenomenon" or "critical mass problem" in higher ed.

- That is, at least some sites aren't willing to adopt a new technology until it becomes a well accepted practice for higher education as a whole (or at least well accepted for their peer cohort institutions).

- Of course, this has the potential to cause deadlocks unless/until you can get a critical mass of institutions to take a leadership role and set the example for others...

- If MFA is the right thing to do, and important, is your site willing to be an MFA leader rather than an MFA follower?

"We'll Do MFA When Compliance Requires It"

- As we discuss in another session during the Global Summit, there's growing emphasis on governance, risk and compliance these days.

- Some sites may have gone so far as to say that GRC is their top priority, and if a potential project isn't something required by GRC mandates, it isn't going to get done.

- Is it possible that GRC considerations are derailing MFA at your site?

"I Can't Tell What Sort of MFA I Should Do!"

- Are there just too many MFA possibilities?
- Are you confused about what product or technology you should choose?
- Traditional cryptographic hard tokens?
- Personal certs on smart cards or USB-format PKI hard tokens?
- Smart phone-based solutions?
- Biometrics?

"MFA Can't Totally Prevent *All* Authentication Risks, So Why Bother?"

- Sometimes people are profoundly disappointed that MFA isn't a magic bullet that will perfectly protect all users against all possible authentication-related attacks.

- For example, hypothetically, at least some "man-in-the-browser" attacks may continue to work, even if users are using MFA (e.g., the user may *think* they're confirming access to their secured site, but in reality a third party may be intercepting the user's MFA input and using it for their own nefarious purposes)

- Are we really going to let a "quest for the perfect" prevent us from making genuine meaningful progress?

"Using MFA *Doesn't* Eliminate Passwords!"

- Some sites hate passwords and may have hoped that deploying "multifactor auth" would somehow let them completely eliminate passwords.

- Because passwords normally remain half of the MFA process, doing MFA usually **doesn't** mean that you'll be "eliminating passwords."

- Given that, doing MFA means you end up with passwords (which you hate), PLUS potentially something else, too. That's not really what folks would prefer, I suspect.

- Did I capture this one correctly? Is this the "big deal" that's delaying deployment of MFA at your school?

MFA Doesn't *Have* to Include Passwords

- If you wanted to, you could try a password-less multifactor combination.

- One option might be something you have (like your smart phone) plus some sort of biometric factor (perhaps a voice recognition-based method)?

- Or what if you just used a smart card that had a client certificate on it, secured with just a single local password? Would *that* be sufficiently "non-passwordy" from a user's POV?

- Are we really ready to finally kick the "password habit?"

"There Are Too Many Campus Services That Need MFA Protection!

- For example, hypothetically you might want to secure "enable" access to your routers, and "root" access to large shared systems, and faculty access to your VPN, and web access to your ERP system, and...

- If you have to implement MFA support for campus services on a service-by-service basis, that can feel daunting.

- But what if you could secure broad chunks of your infrastructure in one fell swoop?

MFA Done *At Scale* via Federated IdPs

- If we assume that institutional identity management is federated (e.g., Shibboleth), can we deploy MFA for an entire IDP?

- Is so, does that make this service-by-service deployment issue go away, at least for web-based applications?

- I think the multifactor multi-context broker (MCB) will help make this a reality (see https://spaces.internet2.edu/display/InCAssurance/Multi-Context+Broker)

- Is this the key we've been looking for? How can we work to ensure that SPs actually leverage MFA?

What About Assurance As a Potential Driver?

- We know that higher levels of assurance routinely require multifactor security. Is a desire to attain LOA-3 or LOA-4 enough to drive adoption of multifactor auth?

- Maybe, but currently we don't have an LOA-3 or LOA-4 class assurance profile (e.g., nothing like InCommon "Gold" or InCommon "Platinum" yet), in part because the community has been slow to identify use cases where LOA-3 or LOA-4 is needed. If there's no need for LOA-3 or LOA-4, why create those assurance profiles, eh?

- If anything, might ubiquitous deployment of multifactor will help to set the stage for easier deployment of LOA-3 or LOA-4 class assurance?

Might MFA Actually Make Some People Feel Paradoxically *Less* Secure?

- Multifactor authentication is meant to, and generally *does*, eliminate at least some risks. Doing MFA *should* make us feel MORE secure.
- However, human minds are funny things. Is it possible that MFA paradoxically makes us feel LESS secure?
- After all, doing MFA may make users **think** more about the possibility that their accounts may be at risk:
  -- "Why do I need MFA?" Answer: "There must be *really serious* attacks going on against MY accounts! OMG!"
  -- "I feel better knowing that my brokerage account is secured with MFA... but what about my bank account and all my other sensitive accounts??? All my *other* accounts *don't* use MFA! OMG!"

MFA's "Not Really About MFA?"

- Normally we think about MFA being all about **authentication** (heck, "authentication" is even part of the name!)

- However, is the real potential driver for "MFA" something else like end-to-end encryption or digital signatures? Those sort of objectives are facilitated by some types of "multifactor technologies" (such as the client certificates usable for S/MIME), but not by others (such as phone-based 2nd channel methods).

- If the benefits of MFA aren't being seen, is it because we're focusing on the wrong sort of "MFA" technologies and not thinking about these ancillary benefits?