All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

2-factor this into your thinking

I see lots of folks pushing for 2-factor authentication – because they think it will make us more secure. They are sincere, but have they thought it through? Let's look a bit deeper.

A security challenge

The challenge is to make things more "secure" (whatever that is)[1] without unduly increasing (1) costs, (2) load on people. The deeper challenge is to choose from among all the available options for protection, but let's not rush ourselves into boiling that ocean.

2-factor authentication increases both cost and load on people. Worse yet, it has little if any well-defined or demonstrated advantages over … passwords.

> "Yes, passwords... Get your passwords here. They're inexpensive, easy to use, and ..."

I'm not trying to make a sales pitch here, just comparing alternatives. So let's look at the modern password situation for a comparison.

What do you do for your house?

I think it's fair to say that most people have most of their value invested in their primary residence. And most of those who don't probably still want to protect the place they live more than most of their online accounts. So if we are going to spend some money on protection in our lives, most folks acting rationally would probably spend it on their homes rather than on one of their social media accounts. So let's ask...

> Do you have 2-factor authentication on your front door?

Most folks don't. They have a key to a lock that is easily picked and readily breakable windows. But of course that depends on the neighborhood you are in. In some neighborhoods, people have bars on their windows and doors. But few have 2-factor authentication. Some have alarm systems, so that when they enter they use a password as their 2nd factor. Something they have (a key) and something they know (the alarm disable code). One prevents entry (through the door) and the other responds to break-ins.

> Do you have an alarm on your computer accounts and an alarm disable code?

Why not? Because we don't have an industry to support it perhaps? And now that I published it you can't patent it... so we likely won't have an industry. But that's a different issue. If you had an alarm that went off after you logged in and when you started to do something more risky, would that help? Would the alarm company come and arrest the folks who didn't disable it? What would that cost anyway? But I digress...

Passwords – and back to the future

In almost all cases, an 8-symbol password is more than adequate to prevent attack, changed every several years or less often is fine. I say "in most cases", but actually, I should say "in some specific cases" So let's get more specific.

---

1 The reader is encouraged to review "2014-06 - Is it secure?" at http://all.net/

The key to safe computing is staying in safe neighborhoods. For example, your home computer should only be accessible (login should only be feasible) from the keyboard and display - not from the Internet. Yes – I know – you use mobile devices now. Your phone is of little use if you have to keep it at home. And your pad computer has to be with you at all time. And you have to do anything from anywhere any time.

But I need to do anything from anywhere any time!!!

No you don't.

But even if you think you do, how does this make 2-factor authentication a solution for your needs? Are you really going to use 2-factor authentication for all your online accounts? Or for access to your phone or pad computer? How is that going to work? Fingerprint on your pad computer (go Apple) along with a password? Voice authentication perhaps? Or are you going to have another device in your pocket to allow you to use your cell phone?

And when someone steals your fingerprint[2] to access all your accounts, how exactly are you going to change it? And how are they going to verify this securely over the Internet and telephone system? And since you gave hundreds or more providers copies of the fingerprint data, … I know.... let's use some cleaver cryptographic scheme will save us.[3] But in addition to all of the other issues with cryptography, how will we authenticate to the cryptographic system? Another password? Wait... I have it... let's use 2-factor authentication!

What happens when we really try to do this?

Niche solutions often seem to work well when the first mover takes the initiative. Think about automated answering computers that replace people answering phone calls. The first company that does it has a financial advantage over the others – it costs less. And novelty will drive people to it – for a while. But as more and more folks use it, we start to realize it shifts the joint cost in time from the operator and the caller spending a few seconds to get to the right answer into a caller spending far longer and the answering company spending almost nothing. This is to say, we pay a higher price as a society and as individuals so the companies can save money. It is far less efficient in the large, but more efficient for the companies that deploy it, so most companies deploy it and society suffers for their local optimization. At scale, it sucks for society, but saves for those in control of the niches. And by now, too late, we all know it.

Let's talk about what will happen at scale for 2-factor authentication. Suppose every site you went to required 2-factor authentication with their own token...

- The rest of this point is left as an exercise for the audience

Or are we proposing that we rely on a single token for the second factor for all of our access?

- Aren't we aggregating all the risk, now in a 3rd party product that may (will eventually) be broken (if the value is high enough to break it). Think RSA. And doesn't this only lead to larger security problems? Denial of access? Replacement cycles and the ever increasing expense? Supporting infrastructure that creates even more dependencies? Companies going bankrupt leaving us with broken systems? And more such things?

2 Yes they can... More than a decade ago, fingerprints were readily duplicated and bypassed most fingerprint scanners using the same stuff gummy bears are made of. And these days, with 3-d printers, ...

3 You might want to read “2014-07 - Encrypt it all!!!” at http://all.net/

Or are we proposing a diverse set of multi-factor schemes competing in the market place?

- So now we have N different schemes each with their own properties and useful for different purposes with different providers, and we have to have them all with us in order to have all access always anywhere, but there are only a few score of them total, and over time, some survive while other don't, so we have to keep changing, and the ones we have still aggregate risk, but less so individually.

I'm sure there are other schemes. Here's a likely market entrant at some point. They will give you one device, take all the other devices, and act as a trusted intermediary authenticating to everyone else for you. That's back to the one-token for everything solution only adding another trusted 3rd party to the mix so we have to trust even more folks.

Going home again

Just as you might have keys to your safe deposit box, car(s), shed, rental properties, etc. in a lock box or safe in your house, you might reasonably have passwords for Internet sites 'locked up' in your home computer. Thus your online accounts can be accessed from home over the Internet, but not from elsewhere. And of course because remote access is being used, the length of the passwords might reasonably be longer. But since they are in the computer and copy and paste works, they can be very long indeed. Here's an example:

wefj094uts09e4utp08e94up408u5j94f8pj4d9850spd9e48j5pd490ep504s98ej5ps049d8kps

I know... It has less randomness than it appears to have at first glance. I generated it in a few seconds by rippling fingers on the keyboard. It doesn't have special characters, it's all lower case, it doesn't have much diversity in characters, is has recurring sequences like 'ps' and too many 9's. But still, if you have to guess passwords like this by trying one after another over the Internet at a rate of a few per second, I doubt if you will succeed in guessing the next one. Guessing the password is not the issue here.

There is an issue, and that is the security of the vendor holding (the hopefully encrypted version of) the password.

> If the vendor isn"t adequately protecting information to keep folks from getting my password or their password file, a 2nd factor probably won't help me.
>
> That's because they won't likely be able to protect my other content or the mechanisms that use it or the rest of the things they hold/control/manage for me if they can't protect my password.

I have a different password for every online account I care about, most generated in a similar way. I choose the accounts I care about, make them harder, and make the ones I don't care about easier - because I don't care about them.

By having different such passwords for each account, I limit the aggregated risk so that when one is broken it doesn't break the rest. Unless of course I trust some with access to others (e.g., use a twitter login to access facebook, etc.). This I should not do unless I want to aggregate the risks. But if I do this, 2-factor authentication won't help me.

Many of the vendors really use accounts and passwords to favor or protect them and not me. For those accounts, I tend to use really easy to guess passwords. It's because I resent the notion that in order to read your paper on why 2-factor authentication is good, I have to get a

user ID on your site, provide an email address, and use a single factor authentication (password) for access to the account. So if you require a letter, number, special symbol, Upper, and lower, of at least 8 symbols in length, I will likely pick Aa1!Aa1! - or perhaps EZ2Get!! and provide an email address like nobody@nowhere.net.

Returning to the user

There is a key to understanding all these things that many people in the security business don't seem to get most of the time.

It's all about the user.

If you want effective protection, you really can't get it by squeezing the user.

"The more you tighten your grip, the more systems will slip through your fingers"[4]

It's like creating a curfew when protesters are holding peaceful all night vigils. You just create a focus for their anger and wrath, wrecking more havoc, and creating more conflict.

If you want effective authentication, you need a balance between the user's desire for access, low cost, and ease of use, and the effectiveness of protection. Today, 2-factor authentication rarely achieves that balance for the average user and uses. The one exception is the use of stored information on the user's endpoint device as an authenticator. Something they have (the device and it's stored content) and something they know (the password or finger swipe used to enable device use) provide the 2 factors, one used by the user for use of the device and the other used by the device for access to the content.

Time and change

Nothing lasts forever. Protection, regardless of particulars, eventually fails under adequately skilled and resourced attack. The utility of authentication stems not from perfection, but rather from delay and reaction. The idea of an effective authentication scheme is to delay attacks and allow change as and if attacks succeed or are about to succeed. For this reason, the passwords and other similar authenticating information need to be effective at delaying use long enough to disable unauthorized access before the consequences rise to too high a level and at allow change to support ongoing legitimate access and denied illegitimate access.

If someone steals my phone, I will know it before long. If the password delays them long enough, I can disable the utility of the phone for accessing 3rd party sites by changing the passwords it stores before the harm from such grows too high for me to tolerate. If theft of the phone delays them by a day of password guessing, it's easy to win. If it's 5 minutes, it's hard.

Summary

2-factor authentication controlled by the user to allow the user's endpoint devices to facilitate and control access to 3rd party sites works reasonably well, scales well, provides adequate protection in most cases, and is a low cost and burden to the user if done reasonably well. 2-factor authentication controlled by 3rd parties or providers currently works poorly, doesn't scale well, provides questionable protection, and is a high cost and burden to users.

I think it's important to factor this into your thinking.

4 George Lucas, "Star Wars Trilogy" #4, "Force will not keep the empire together. Force has never kept anything together for the very long. The more you tighten your grip, the more systems will slip through your fingers. You're a foolish man Governor. Foolish men often choke to death on their own delusions."

