

Forum:[Hack Forums](#)

Thread: [Consider physical USB key for two-factor authentication](#)

D3xus - May 30, 2020, 4:59 am

At my previous job, I was required to use a physical security key any time I logged into a corporate device or needed privileged access to something/to perform some action. Today, I use a physical security key (Yubico) as an additional layer of security for some of my personal accounts.

For people with a lot of value, importance, or power in their accounts, the ability to use a physical USB security key would provide people with an even more secure option on top of (or as a replacement for) existing two-factor authentication.

<https://developers.yubico.com/>

<https://webauthn.io/>

On Reddit, I've required all moderators on a popular subreddit I managed to have basic 2FA. I'd have required them to have physical security keys if Reddit had that option.

Hero - May 30, 2020, 5:21 am

Where is the difference to authy? Isn't it harder for thieves to unlock my iphone than to just use my key?

webdev77 - May 30, 2020, 7:51 am

(May 30, 2020 05:21 AM)Hero Wrote: [\[CITE\]](#) Where is the difference to authy? Isn't it harder for thieves to unlock my iphone than to just use my key?

Your iPhone can be sent a malicious payload to exploit iMessage without your knowledge or require user interaction. This has been done many times over the past few years and is proven to work well. Someone would have to break into your house and steal a physical key to get a hardware token. So no, they are not of equal security. A non-internet connected device is far safer.

VisualSoft - May 30, 2020, 8:27 am

(May 30, 2020 05:21 AM)Hero Wrote: [\[CITE\]](#) Where is the difference to authy? Isn't it harder for thieves to unlock my iphone than to just use my key?

also we see many users locked out because of crashed Phone or phone reset.
this can be fixed with the USB Hardware.

Hero - May 30, 2020, 8:35 am

(May 30, 2020 08:27 AM)VisualSoft Wrote: [\[CITE\]](#) also we see many users locked out because of crashed Phone or phone reset.

this can be fixed with the USB Hardware.

Okay but what if the usb gets lost? Or do people usually back the key up? Also can malware copy the usb content and copy it to a new key or is it protected against it with for example encryption?

D3xus - May 30, 2020, 8:48 am

(May 30, 2020 08:35 AM)Hero Wrote: [\[CITE\]](#) Okay but what if the usb gets lost? Or do people usually back the key up? Also can malware copy the usb content and copy it to a new key or is it protected against it with for example encryption?

If you lose the key, then you should be able to revoke access to any site that would use the key. It's

similar to if you got a new phone and needed to reconfigure 2FA with an app like Authy/LastPass/Google Authenticator: you remove the ability for your old phone to log you in, and only your new phone can log you in.

I don't think malware can copy the content of a key in the same sense as a traditional USB key works. The method with which a Yubico key communicates with a website, for example, is very different than how a normal USB keys allows you to store files. Yubico keys require you to plug in the key to the computer, and press a physical sensor on the key to authorize the key with the site.

<https://www.yubico.com/why-yubico/for-individuals/>

<https://support.yubico.com/support/solutions/articles/15000010242-can-i-duplicate-or-back-up-a-yubi-key->

D3xus - May 30, 2020, 8:55 am

(May 30, 2020 08:49 AM)xadamxk Wrote: [\[CITE\]](#) If it is easier to reset access to sites that use the key than it is to physically steal a key, wouldn't that be the new attack vector? Whatever that method is would be used to hack accounts.

I don't think it's any easier to reset access to sites that use a Yubikey than it is with 2FA. You still need the physical key, which is an authorization token. That's true for 2FA through an app. I'd argue that getting access to an account that requires a physical key is much harder than getting access to their phone, or to their 2FA account which has all their credentials (Google, LastPass, etc.) Even if you get your hands on a key, it's not immediately obvious what it's for, or for what site a key applies to. In an app, it's all labelled for you and self-documenting.

Eagle 95 - May 31, 2020, 2:14 am

Don't you think that this would be an overkill for a forum account? From my knowledge as a full stack dev, this is usually done in corporate settings where you access highly sensitive data and you need to know every action that has been done that system. I said usually in corporate settings but there are other situation where this would be completely understandable. You can protect your gmail with a physical key and if the emails are important to you, it's a valid step to take.

What is sensitive data here? What do you need to protect that requires that security level? While I'm not necessarily disagreeing it's a bad idea, you didn't convince me why this would be beneficial to have on a forum account of lets say some ub3r member that does CE two times a month and posts in Lounge over a "traditional" 2fa method we have here.

Edit: if you want to mimic the physical usb, you probably have an old android phone laying somewhere around the house. You can install authy on it and use it the same way as an USB device. Don't connect it to the internet after you downloaded the app and you're going to be fine.

Mister Slyther - May 31, 2020, 2:18 am

This is just an online forum...the idea itself is fine.

How can you compare IRL and actual organizations with this? this is certainly applicable in the real world and the crypto/financial industry. But for a forum? I disagree, that's too much. This would be overkill as Eagle 95 said.

Recovery keys exist for a purpose, and the auth is good enough as it is.

Just my .2 cents.

D3xus - May 31, 2020, 4:33 am

(May 31, 2020 02:14 AM)Eagle 95 Wrote: [\[CITE\]](#) Don't you think that this would be an overkill for a forum account? From my knowledge as a full stack dev, this is usually done in corporate settings where you access highly sensitive data and you need to know every action that has been done that system. I said usually in corporate settings but there are other situation where this would be completely understandable. You can protect your gmail with a physical key and if the emails are important to you, it's a valid step to take.

What is sensitive data here? What do you need to protect that requires that security level? While I'm not necessarily disagreeing it's a bad idea, you didn't convince me why this would be beneficial to have on a forum account of lets say some ub3r member that does CE two times a month and posts in Lounge over a "traditional" 2fa method we have here.

Edit: if you want to mimic the physical usb, you probably have an old android phone laying somewhere around the house. You can install authy on it and use it the same way as an USB device. Don't connect it to the internet after you downloaded the app and you're going to be fine. You're right that this is overkill/excessive for most users. I was thinking that this could be more aimed at group leaders, moderators, and other people that can do a lot of different things with their account. It might also be a peace-of-mind measure for people who think they need the extra security.

But is it completely necessary for the general masses? Probably not. Maybe such a feature would only even be enabled for some usergroups, due to the unlikeliness of most people outside of a specific subset of users to even know what it is, let alone enable it.

Omniscient - May 31, 2020, 10:37 am

I've never seen a 2FA account stolen on HF.

Quote:Your iPhone can be sent a malicious payload to exploit iMessage without your knowledge or require user interaction. This has been done many times over the past few years and is proven to work well. Someone would have to break into your house and steal a physical key to get a hardware token. So no, they are not of equal security. A non-internet connected device is far safer.

Yes, pretty much. I still don't trust some of these hardware devices.

Quote:also we see many users locked out because of crashed Phone or phone reset.

Authy has backup. There is also a way to export all your secret keys. Print them out and save them just in case.

Quote:this can be fixed with the USB Hardware.

Just as people lose phones, they can also lose their hardware keys or they can stop working.

Quote:Yubico keys require you to plug in the key to the computer, and press a physical sensor on the key to authorize the key with the site.[quote]

Such a pain in the ass. Especially when I use 2FA dozens of times per day.

[quote]Edit: if you want to mimic the physical usb, you probably have an old android phone laying somewhere around the house. You can install authy on it and use it the same way as an USB device. Don't connect it to the internet after you downloaded the app and you're going to be fine.

LOL, I was about to suggest exactly that.

Basically stolen accounts under our current 2FA structure is non-existent. We don't need hardware key support. We hold no private or financial data that would place members into a high-risk category.

D3xus - May 31, 2020, 11:21 am

(May 31, 2020 10:37 AM)Omniscient Wrote: [\[CITE\]](#) I've never seen a 2FA account stolen on HF.

Yes, pretty much. I still don't trust some of these hardware devices.

Authy has backup. There is also a way to export all your secret keys. Print them out and save them just in case.

Just as people lose phones, they can also lose their hardware keys or they can stop working.

LOL, I was about to suggest exactly that.

Basically stolen accounts under our current 2FA structure is non-existent. We don't need hardware key support. We hold no private or financial data that would place members into a high-risk category.

If there aren't any cases of lost/stolen accounts with the existing 2FA solution, then my original idea is probably overkill. I feel much better that it's never been an issue for accounts. Thank you for clarifying that point! And thank you to all the other posters who offered alternative ideas/critique.

Gonna close this thread now, given everyone's input. Take care!