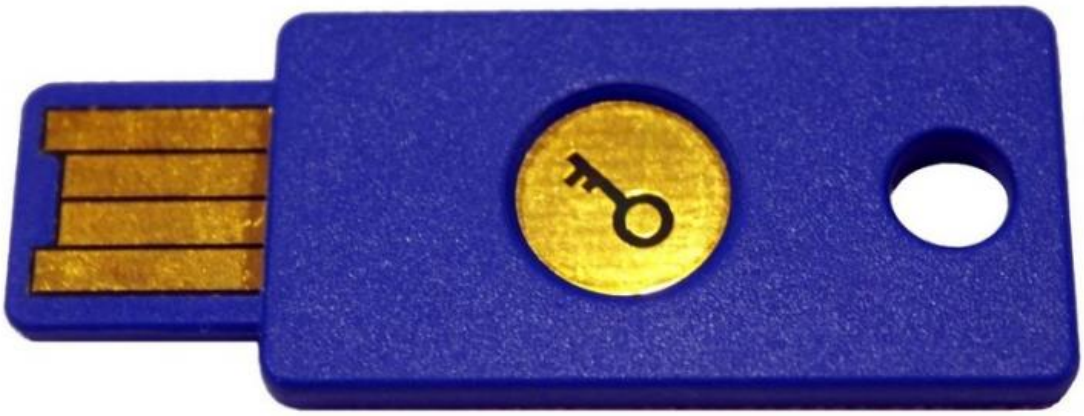
The age of hacking brings a return to the physical key

March 23 2017, by Jungwoo Ryoo



Have hackers driven us back to the age of the physical key? Credit: Bautsch

With all the news about Yahoo accounts being hacked and other breaches of digital security, it's easy to wonder if there's any real way to keep unauthorized users out of our email and social media accounts.

Everyone knows not to use the same username and password combination for every account – though many people still do. But if they follow that advice, people end up with another problem: way too many passwords to remember – 27 on average, according to a recent survey. That can lead to stress about password security, and even cause people to

give up secure passwords altogether. It's an ominous feeling, and a dangerous situation.

But there is hope, through what is called "two-factor authentication," in which a user needs not only a login name and password but also another way to validate her identity, before being allowed to connect to, say, Gmail or Snapchat. That way, even an attacker who gets a user's login name and password still can't access the account.

When it happens, this usually involves the user either receiving a text message on her phone with a six-digit code, or opening an app on her phone that will give her the code, which changes every 30 seconds. As a cybersecurity researcher, I know that even as this method is just starting to become common, a newer method, a return to the era of the physical key, is nipping at its heels.

Proving identity

In the security industry, we typically refer to three broad ways to prove identity:

- Who you are, usually expressed through biometrics, like a fingerprint, facial recognition or a retinal scan.
- Something you know, like a password or PIN.
- Something you have, such as a conventional key that unlocks a door, or even a smartphone with a particular app installed.

User authentication is strongest when a person proves her identity in multiple ways. This is called two-factor, or sometimes multi-factor, authentication.

Despite its potential to improve security, companies and government agencies alike have been slow to adopt two-factor authentication. For

many years, there were no common standards, so authentication methods often worked only for a single system or program or company.

An early standard is today's most common method: getting a numeric code by text message. But that is on its way out. While initially thought to be a convenient way to verify that someone had a particular phone, it turns out to be vulnerable to attack.

A phone number can be "cloned" onto an attacker's phone, allowing him to intercept text messages. In addition, many people use internet-based phone systems, such as Google Voice, that allow them to receive text messages without actually needing physical access to a specific device – subverting the very purpose of sending a text message in the first place.

Toward improved security

A new, even more secure method is gaining popularity, and it's a lot like an old-fashioned metal key. It's a computer chip in a small portable physical form that makes it easy to carry around. (It even typically has a hole to fit on a keychain.) The chip itself contains a method of authenticating itself – to prove that it is the real "thing you have" that's required to connect to a particular online service. And it has USB or wireless connections so it can either plug into any computer easily or communicate wirelessly with a mobile device.

How a login works with a physical key. Credit: FIDO Alliance

Backing this effort are technology industry giants, including Google and Microsoft. They and other companies recently formed the Faster Identification Online (FIDO) Alliance to create a new standard that is both shared among providers – so users can have one physical key that gives them access to many services – and useful with mobile devices as well as desktop and laptop computers.

They're calling their standard "Universal Second Factor (U2F)," and it's based on public-key encryption. Also known as asymmetric key encryption, public-key encryption uses a pair of keys, one public and one private. Either key can be used to encrypt a message, but that coded message can be decrypted only by someone who has the other key in the pair.

One of the paired keys is shared with others – this becomes the public key. The other, the private key, must be protected. Because just one person should have access to the private key, a login process that requires it can ensure the authorized user is the only one who can

connect to an online service.

How it works

When adding a physical key to her account's security credentials, a user first logs in to her account as normal, perhaps even using a text-message method of two-factor authentication. When she follows the site's instructions for adding her U2F key to the account's security settings, that process creates a new public-private key pair. The private key is encrypted and stored on the physical U2F key. The matching public key is stored on the site's authentication server.

Thereafter, when logging in, the user types her user name and password as usual. Then, the site provides an alert asking her to plug the physical security key into her computer. (Some keys can also connect wirelessly via Near Field Communication, or NFC.)

What happens next requires minimal action by the user; the computer, the website and the physical key handle everything nearly instantaneously. The website sends a message to the computer, requesting a reply. The computer reads the private key from the physical U2F device and uses that to encrypt its response. The server uses the account's public key to test the reply; if it was encrypted by the corresponding private key, the server knows the person trying to log in has the physical device, and is therefore the authorized user. At that point, the server logs the user in.

The best option we have

Although U2F strengthens the current practice of password-based authentication, it doesn't solve every problem. Of course, if a person loses the key and doesn't have a backup copy, logging in can be

impossible. But most sites that use U2F also, in the initial U2F setup process, give an authorized user a limited number of single-use login codes she can type in if she loses her key.

In addition, passwords are inherently challenging because we have to memorize them. Forcing people to make them longer and more complex, involving numbers and capital letters and punctuation, makes them even harder to remember. And with so many passwords needed regularly, it's terribly difficult to memorize that many long, complex unique sequences.

Password management programs can help. These services, including LastPass and 1Password, securely store your username and password combinations in the cloud or locally on your computer, requiring users to memorize just one long – but often relatively easy to remember – "master password" that decrypts the others when they're needed.

Those services can even work in tandem with U2F. For example, a user can create one master password for LastPass and set it up to only decrypt the stored passwords when the physical security key is plugged in.

When paired together, a service like that can give you very strong passwords that you don't need to memorize, bolstered by the security of a physical key. It's not perfect, but it's our current technology's best defense against hackers and account thieves.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation