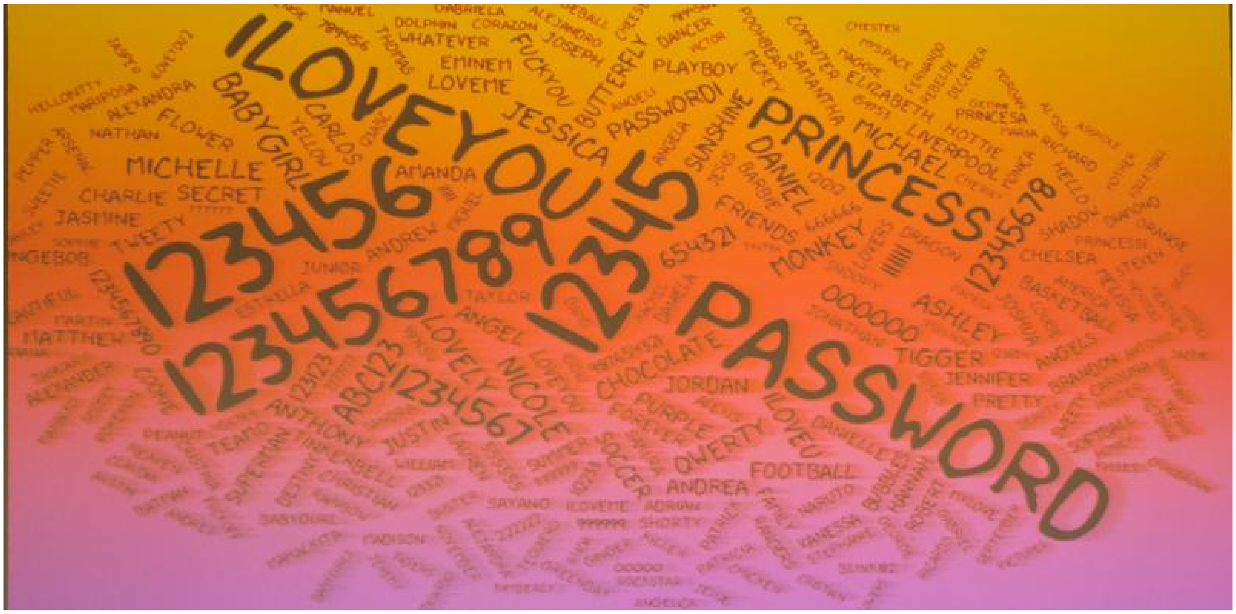
PHYS.ORG

There must be smarter security than a ban on 'dumb' passwords

June 2 2016, by Mike Johnstone, Edith Cowan University



Believe it or not but ‘123456’ and ‘password’ are still used by people today as passwords. Credit: Flickr/alexljackson, CC BY-NC

In cyberspace we are facing password fatigue, caused by having to recall (seemingly) endless streams of (apparently) unrelated numbers and letters at odd times.

One answer is to make those passwords longer and more incomprehensible. The logic here is that people have an unlimited capacity to remember such things, or perhaps they have an unquenchable desire to write passwords on yellow post-it notes.

Why do we want or need passwords at all? We want to be assured that only the right people (ourselves) have access to the information contained in the systems we use. Witness the after-effects of the Ashley Madison hack.

So many passwords

Privacy is a basic human right and one that many people take seriously. Authenticating to many systems is something most of us do without thinking every day. Unfortunately, those systems often have different rules about what is considered a good or acceptable password.

The need to remember competes with the requirement for security leading people to devise memorable (to them) schemes for passwords that they think are unique and unguessable.

For example, if I have to access 12 systems, I might use the months of the year, coupled with my birth date and rotate combinations around. At face value, this appears a clever scheme because no-one else knows my birth date.

Except of course for several government agencies, health service providers, an insurance company or three, some social media systems (which might have been hacked recently) and anyone else with whom those bodies share information. Of course, then there are my family and friends with whom I like to celebrate my birthday each year.

I could use the dog's name instead. No one is aware of that. Except of course for the local vet, anyone who hears me yelling at the dog down the local street, my legions of Facebook friends and so on.

Coming up with so many different and apparently secure passwords that you can remember can be tricky, despite the many tips and guides, hence the password fatigue.

One potential solution is a single sign-on for many systems (into one, into all) – an idea which is interesting, but also has its own issues.

A different approach

To quote from Led Zeppelin's Stairway to Heaven: "Yes, there are two paths you can go by, but in the long run, there's still time to change the road you're on."

One path is systematic, based on the idea that if small passwords are bad, the answer is larger, more complex passwords. For example, Microsoft now says it wants to compile a list of what it calls dumb passwords that will not be allowed on its system.

That dumb passwords are a problem is undeniable, as the online security company SplashData gleefully publishes its annual list of the most common passwords, where "password" and "123456" are, ahem, quite high in the list. This shows people choose convenience over security when it comes to setting a password (but they still want privacy).

The systematic response is that users are constantly being asked to set more complex passwords with upper, lower case, numbers, symbols etc., to the point we get password fatigue. Asking us to keep changing passwords just encourages minor or incremental changes to the same supposedly unguessable passwords, something even Britain's intelligence agency GCHQ recognises is a problem.

This mode of thinking works well for some problems, but the whole idea is rendered moot when anyone can easily download a lists of millions of the most common passwords.

Yes, "123456" can be cracked in a fraction of a second, but a random 15 character password could be cracked in less than a week using relatively inexpensive hardware. It all depends on the time value of information. Your bank account will still be there in seven days (the funds remaining therein are a different matter).

Think again

Do we need to re-think the whole system? The other path is a systemic approach. This uses the concept that components of systems are connected in ways that are not immediately obvious.

An example of a systemic effect, that could not have been predicted directly, is where Cornell University's associate professor Garrick Blalock and his colleagues found that driving fatalities in the United States increased significantly after the September 11, 2001 terrorist attacks. The reason? People chose to travel by car in place of aircraft, the former being much more dangerous.

So what might a systemic solution to password fatigue look like? If longer passwords are not the answer, but we still need to authenticate ourselves, why not dispense with passwords altogether?

When we provide a credential, it is one (or more) of something we know (a password), something we have (a card) or something we are (some physical property of ourselves).

It is this latter idea that is most attractive. A biometric signature – such as your iris, retina, thumbprint or voice print – means not needing to remember anything, not having to bring an access card. You just be yourself and some property of you will identify you. Such a system would be very hard for any cyber criminal to replicate or hack.

At present, biometric solutions are expensive (compared to other technology) and imperfect (they get it wrong more than we would like), but the future would be nicer if you could phone your bank account and be authenticated by your voice print.

You could then simply ask to transfer 'X dollars' to the travel agent for a holiday and book a rental car, all at the same time, without having to remember three separate passwords (or you could just talk to a real person).

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: There must be smarter security than a ban on 'dumb' passwords (2016, June 2) retrieved 26 April 2024 from https://phys.org/news/2016-06-smarter-dumb-passwords.html