Passwords: How to choose one and why we need them

May 7 2013, by Philip Branch

Having trouble remembering all your passwords? Don’t expect respite any time soon. Credit: Jonno Witts

I just did a count of the systems I use that require a password and gave up at 40. I know I'm not alone; for many of us, it often seems we have too many passwords to manage.

They are, however, required to access most of the systems we interact with for work, entertainment, and everyday living.

Perhaps it is because they are so ubiquitous that we take them for granted without ever really understanding how they work.

Passwords are an example using of something you know to prove your identity. In security circles it is often said the way we prove our identity falls into three categories:

- something you have, such as a bank card
- something you are, such as some form of biometric such as a photograph of the user, fingerprint or iris scan
- something you know, with passwords being the most common example

What are passwords really made of?

Well-designed password systems never store passwords directly. What's stored instead is

- the hash – a cryptographic function that takes a sequence of characters or numbers and generates a sequence based on it
- the salt – some additional characters which do not form part of the password, but are added during encryption to make it harder for hackers to hack password files

The output of a hash function tells you very little about its input so is very difficult to reverse.

It takes vastly more computation to reverse a hash value than it takes to calculate it.

When a password is entered into a system, the hash of the password and any salt value is calculated and compared with the stored value.

If it matches then the user knows the password and identity is assumed to be proved.

"Assumed to be proved" is an important point. Because we have so many passwords, people tend to reuse them or choose passwords that are easily remembered but also, unfortunately, easily guessed.

As a result, passwords by themselves are often regarded as inadequate proof of identity.

Certainly when we get cash from an ATM or pay for goods via EFTPOS the password (the PIN) is not sufficient proof or identity.

In those cases a second form of identity proof (the bank card) is also required.

Of course, PINs are not particularly good passwords, being so short and restricted to the digits 0 to 9, but in general, where reasonably strong level of proof of identity is needed passwords alone are usually regarded as insufficient.

Credit: B. Rosen

Using rainbows to generate a storm

One of the reasons passwords are less trusted than they once were is the availability on the internet of rainbow tables, which are precomputed tables that enable the hash of passwords to be reversed.

For example, rainbow tables are used in dictionary attacks, where real words found in the dictionary are used for passwords.

Rainbow tables also exist for passwords that are all lower case and fewer than eight characters long.

What's the big deal?

Often it is not understood why cracking of any password is a serious matter. What does it matter if passwords to the office footy tipping competition are compromised?

Unfortunately, it matters a great deal because of the way people use passwords.

Most of us have many passwords; far too many to be able to remember. As a result, we tend to reuse them.

The password used for low risk systems such as the office footy tipping competition will often be reused in high risk systems such as internet banking, email systems, and the like.

In this way, compromising one low risk system may compromise a much higher risk system. Consequently, it is important to use different passwords for different systems.

Or, if this is too difficult, at the very least use unique passwords for high risk systems.

This gets us to the vexed question of whether systems should force regular password changes. As always in security system design the answer is "it depends".

In some cases the importance of the information protected is such that it warrants a regular change of password.

But often forcing regular changes of password is counterproductive. We have so many passwords as it is, and forcing us to change them regularly may cause us to choose passwords that are easy to remember but also easy to crack.

What makes a good password?

A good password should be easy to remember but almost impossible for others to guess.

It should either include characters from a large character set (such as upper and lower case, numeric and non-numeric characters) or be very long.

Some approaches are to make use of information that only you can possibly know, such as the phone number of a girlfriend or boyfriend from a few decades ago, the street you lived on when at high school, or something similar.

Of course, in these days of social media, such information is not always as unknowable as it once was.

You might blend multiple sources of such information and include some non-numeric characters in a way only you know and perhaps include the name of the site.

Another suggestion is to choose long random sequences for passwords and write them down on a list which you store in your wallet, or use a password manager such as those available as an app on most mobile phones these days.

Such advice is controversial (particularly writing passwords down) but the counterargument is that most of us are quite good at securing our wallets, and the rainbow table based systems for cracking passwords are so sophisticated that anything other than a random sequence is vulnerable to a dictionary attack.

This advice does beg the question: what happens if you lose your mobile phone or your wallet, or forget the password to your password manager application?

So, are there alternatives to passwords?

Not really. Of course if the system being protected warrants it, there are alternatives such as security token systems, retina and iris scans, fingerprint systems, and face recognition, to name but a few.

But there is nothing as cheap and as well understood as passwords.

So keep your memory sharp – passwords are likely to be around a while yet.