ID and password or PKI for your security?

Overview

Most web sites at the moment give their 'registered users' an ID and a password to provide for security of data. PKI provides 'digital identities'. This paper reviews the arguments for and against each mechanism. It concludes that digital identities offers a better long term result but questions how this will be achieved.

Introduction to ID/password

The use of ID (identity) and password has been the mainstay of computer security for quite a while now. For most modern users its development is lost in the mists of antiquity. More seasoned campaigners remember Timeshare, George 2 and Maximop, PDP-5 or any of the higher IBM mainframe operating systems with RACF, TopSecret or ACF2.

Basically, this was the early approach to identity and authentication. Experts refer to this as two-factor, because it is something that you are (the identity – issued by someone who was confident that they knew you) and something that you know (a secret, namely the password).

(If you wanted to know, authentication factors include something that you are, something that you know, something that you have. The something that you are can be split down quite a lot because of biometrics such as voice, fingerprint, handprint, face, retina and so on.)

For reasons lost in the mists of time the ID was never considered to be a secret. Your public identity as a user was always known to everyone. It was much easier to administer the system that way. Of course if they had made the ID a secret and linked it to a pseudonym then systems could have been made significantly more secure, but that's history.

So there you have it. Systems to date have used a visible, almost public identity and a 'secret' password to allow people entry into a computer system.

Is this secure?

Well, that's rather a piece of string question. In most original implementations certainly not. Any systems programmer (or anyone who knew the right places to look) could find the file with the passwords in it, read them and then log in as anyone they felt like.

Surely things have improved?

Yes. On the technical side things have improved significantly. We now try to avoid storing passwords in a form that you can read them, or even in a form where you can figure out what they are even when they are hidden by encryption.

So are there any problems still?

Yes, unfortunately. It appears that every programmer implementing a password control system thinks they can do better than anyone (or, even more grandly, everyone) else. If you think about it, this is nonsense since you only need one implementation that really works providing you can manage to copy it correctly. (This is one of the ideas behind the open source movement – get it right once and implement it everywhere.)

Even if there were perfection in the implementation, that ignores the weakest point in the whole system – the user.

For a password system to be strong, it is stated that passwords must be un-guessable. More than that – they should be changed regularly so that an attacker, even if they manage to learn one password by watching a user type it in, can only use it for a limited time. That's because it will change soon and they will have to try and watch out for another one.

That's great for security theorists, but not so good for normal people like users. They have a hard time with the whole thing. They are not touch typists so they don't want to type in huge long passwords that go wrong frequently. They like passwords they can remember (especially since they have been told not to write any of them down). They can't cope with un-guessable passwords precisely because they are somewhere between difficult and impossible to remember. They also hate change, and therefore have significant problems every time a password changes. (The average help desk spends most of its time sorting out forgotten passwords.)

So what do normal human beings do when confronted with the password problem? They pick something that's short and nice and easy for them to remember, and they make sure that's the password they use for every system they use.

So the weakness is password systems is that they tend to be open to what are called dictionary attacks (hackers have dictionaries of all the common words that people use as passwords) – it takes so much less time than having to try every possible combination to find the right one.

PKI Digital Identities

Unlike ID/password these are rather new and we have not had much time to settle down with them. They don't work in quite the same way. With ID/password you had to type both of them into an input screen, press send, and off they went to whatever was checking them. They may have gone just as they are (just because you see asterisks on the screen doesn't mean that anyone watching on the connection couldn't read everything, although the more modern systems do use some form of encryption, including SSL but see a separate paper for issues with that approach).

PKI is rather different in that it is possible for everything to be fully encrypted right from the user to the program using the data. That's much stronger than ID/password. Even if the password is encrypted the data is not, unless some other mechanism is also used.

A great advantage of the digital identity is that it is impossible to guess and impractical to reproduce. So it does not have any of the vulnerabilities of the password to normal attack.

So from a security perspective the digital identity mechanism is significantly stronger than ID/password. But what are the downsides?

Well, for one thing, the digital identity has to be protected from being used by someone else by – a password. After all, something has to stop just anyone borrowing your digital identity just like borrowing your password. So we are back to that problem. However, it is a smaller problem, because nothing to do with this password is ever sent anywhere.

Another disadvantage for the digital identity is that it has to be stored on (or available to) the user's computer, whereas the password is stored with the system that is going to use it. That means that mobility might be more constrained unless the user is willing to carry round however many digital identities they require on a floppy disk or a smart card or something similar. Mobility might be improved if you allowed the user to download their digital identity, but you would have to control that through a mechanism – like ID/password. Sometimes you feel you are going backwards to go forwards.

Analysis – a balance of forces

One thing not considered often enough in security analyses is the effect of administration. Both systems require administration.

Where we are considering internal administration for an internal system it's hard to say if there's much to choose. Someone has to administer identities either way round.

Looking at an external system you have slightly different choices. With ID/password you have to provide password change capabilities as well as coping with the fact that people in the external world forget passwords. With digital identities, people will lose them and will also forget the passwords. (This assumes that the organization issues the identity. If it does not, but accepts the identity offered, either from another organization or from the person themselves, then the administration ceases to be their problem.)

Let us consider attacks against the security of the methods

ID/password is open to attack in transmission unless the information is encrypted within the client. Digital identity does not have this problem.

ID/password is open to being sniffed if the attacker can gain any access to the client desktop. This is also true if many versions of Microsoft Windows are being used to cache passwords since these are open to known and published attacks. Digital identity is open to having the password giving access sniffed and to having the file containing the identity copied, assuming that the attacker can gain access to the desktop.

For an attacker to make use of the compromise of either system they would need to know the sites that either system is used to connect to. This may or may not be obvious. The extent of a compromise would be a factor of the amount of observation material the attacker could collect in order to know what systems were in use. ID/password methods tend to allow the attacker to be able to see what is being connected to, and it is technically more difficult to avoid this compromise. Digital identities allow secure connections, which if implemented properly, effectively prevent the attacker from knowing what actual system can be connected to.

The extent of compromise of a single password where multiple passwords are in use is low. Thus, ID/password systems that have different passwords for each system are difficult to compromise, whereas a single digital identity may be used for multiple systems, and compromise of it may be worse. However, as we note from practical experience, outside military systems people tend to use the same password for all systems whenever possible. On balance, therefore, it seems unlikely that a password compromise creates more weaknesses with either system.

Conclusions

Whilst the greatest experience to date is with ID/password systems, they appear to suffer from greater overall weaknesses than digital identities. However, they have the advantage that nothing has to be put on a desktop, and that centralized administration can be imposed.

Digital identities are currently more complicated in that something (whether you call it an identity or a cookie it doesn't matter) has to be put on the desktop, together with some software in order to be able to process all the cryptography that is needed to make it work (naturally there is never anything really useful on the desktop when you want it). They also have central administration, but with a bit of luck it might not be at a cost to every site, unless every site really wants to continue to do all the administration on all its users. (That's probably true for systems internal to an organization and probably not true where the general public are involved.)

But the administration of them should not be any harder than the systems we use today. After all, if we are willing to use ID/password because it is 'good enough' there's no reason to put a load more administration into digital identities.

Digital identities offers the best secure route forwards providing that administrators can get their minds around the idea that you can agree to accept an identity created by someone else, providing the user of that identity agrees. The linking of that digital identity to a real identity is something we already handle with the ID/password system, so there is no reason why we should not use the same methods with digital identities.

So it's a balance. You can get much better security using digital identities, but you need to alter some thinking about administration and the means of getting a real identity linked to a digital one. You could waste huge amounts of time (and some people already have) agonizing over needing to have some external mechanism – such as the Trusted Third Party so excessively loved by the PKI communities. From a security standpoint there are many advantages to not making the true identity of your customers obvious to the observer, particularly if you can be sure that when the user reveals things like credit card details through what is the most secure information protection mechanism available today, only you know – and you can be sure if the credit card works that you have the real identity, without any of these other confusions.