

## Authentication – Who are you?

Identity fraud is rising. It is increasingly simple, with more ways of doing it than ever before. As more and more applications become available to us over the Internet, there is a growing need to prove our identity, in order to prevent criminals from taking advantage of us. To achieve this protection we use the same techniques we have used since the very beginning of computer security: usernames and passwords. These just aren't enough any more – they are neither secure enough, nor easy enough to manage in the current web 2.0 environment.

Let's start with the problems of usernames. A username varies from site to site. It might be the user's email address, or their first name and surname initial, or their first name initial with surname, or just initials, or first name on it's own, or something else entirely. The variety at this stage is pretty large and we haven't even got to passwords yet.

So let's look at passwords. Received wisdom tells us:

1. Have a different password for every account
2. Don't use anything personal
3. It must be complex
4. It must be changed regularly
5. It must not be written down
6. Don't ever tell anybody your password

You may have passwords for eBay, Facebook, your banks, your credit cards, online subscriptions, email accounts, ecommerce sites... the list goes on. The average person has in excess of [25 usernames and passwords](#) to remember. The result is that in a desperate attempt to remember a password, many people simply use the same one for all their online accounts. Thankfully, not even this is foolproof: some sites insist the passwords are more than a certain number of characters, others limit the number of characters, some require two or more numbers and symbols, others don't recognise symbols at all. It is very difficult now to have a single password that covers all possibilities (which obviously is a good thing). But we're human, with the limitations of human (not computer) memories. Most people will write their passwords down in the front of their diaries, or on post-it notes on their monitors, or resort to using very basic passwords that can be easily guessed by anybody. There is no consistency and this exacerbates the problem, resulting in ever poorer security.

Recently, Dr Jakob Nielsen (<http://www.useit.com/alertbox/passwords.html>) suggested that dropping the masking of passwords might encourage people to use more complex passwords because they would be easier to enter. He argues that masking means users cannot see a typing error, and so opt for easy passwords to ensure quick access to their accounts. He has a point, but of course any improvement in password complexity is counteracted immediately by a system that displays a password on your screen to anyone who happens to pass by. In these days of mobile workforces, wi-fi and remote access, that could be very dangerous. I think there's another aspect to this, too. Masking a password is a continual reminder to the user that a password is about secrecy and security, to be kept safe and not shared.

Another study by Dinei Florencio, Comac Herley and Baris Coskun ([http://www.usenix.org/event/hotsec07/tech/full\\_papers/florencio/florencio.pdf](http://www.usenix.org/event/hotsec07/tech/full_papers/florencio/florencio.pdf)) has reported that the most common attack on passwords is done not by brute force (which is the reason for a complex password), but by phishing and keyloggers. This means that the complexity of the password is largely irrelevant. In fact, they argue, complex passwords are actually detrimental: because they are so difficult to remember, they are used across multiple

accounts and not changed regularly. So if a hacker successfully phishes for a password to one account they will get access to all account. A sort of 'hack one, get the rest free' deal.

So people continue to forget their username and their passwords. This results in procedures for resetting passwords – which often are, themselves, inherently insecure. A good example of this was the case of Republican Vice-presidential candidate, Sarah Palin. Hackers were able to access her email account and reset her password, simply by knowing her birth date, her zip code and the answer to a 'secret' question (where she met her husband). All information that is publicly available for a person in the national spotlight. So our human vulnerability – the fact that we forget information – has created a security vulnerability which is being exploited.

With card-not-present (CNP) being one of the most popular form of identity fraud, Visa moved to provide extra security in the form of a password. This initiative was given the name "Verified by Visa". This provided a basic form of two-factor authentication with the customer needing both the credit card details and a password. So, we're back to the now familiar issue of relying on the user remembering another password for every credit card under the scheme. The irony is that this 'verification' is arguably easier to reset even than Sarah Palin's password. With credit card details now so widely available on the Internet, a thief only needs the user's date of birth to reset the password. This is also likely to be widely available on the internet, so the improvement in security is next to insignificant.

To improve website security, some banks have introduced two-factor authentication where users still have a password ('something they know') but now also now need to carry a token ('something they have'). This has entailed the distribution of key fobs that generate random numbers or, in the case of Barclays and NatWest, calculator sized devices that need credit cards to be inserted to generate the required random number. This obviously increases the security by ensuring that hackers need access to that physical device which makes the task of fraudulently accessing accounts much more difficult. The trouble is that each bank and each account needs a key fob or device which reduces the practicality of using these devices. How many can customers carry in their pockets?

This mess is emphasised by contradictions in the system. Some banks use encrypted email to communicate with their customers. When they want to send a communication, it emails the customer telling them that they have an encrypted email and asking them to log on to an account that they have to create specifically for this purpose. The temptation for the customer is, of course, to use the same password as they do for their main account. The problem is that this account does not have two-factor authentication and is frequently not hosted by the bank. The chances of passwords being compromised are obviously increased along with the sensitive information that is being sent in these emails.

In the end, all the user is trying to do is to identify him- or herself in order to access an account. The user is just a single discrete entity. They need a clear easy way of proving who they are, so that every person or organisation they deal with can identify them. This is being referred to as 'Identity 2.0'.

The idea behind the Identity 2.0 approach is that rather than using multiple usernames and passwords to register onto different websites, users can have a single identity that is recognised by many (or even all) entities with which that user interacts. Identity 2.0 treats the *user* as the 'object', rather than the website or account. Implementing this approach requires identifiable transactions between users and the entities they deal with, using verifiable data that can trace transactions and cut down on fraud and theft.



There are, of course, some related issues to having a single identity. For instance, an open identity might be compromised through phishing attacks or malware. This means that having more than a single factor of authentication is critical to making attacks more difficult and tracking attacks more achievable. There is also the question of privacy - a strength of the internet is that people can find out what might be embarrassing or financially sensitive information without being identified. A single identity mechanism would have to allow for users to be logged out, and therefore unidentifiable, if they wished. Finally, it would be very tempting for companies to track users and use identifiable information for marketing purposes. It is possible that in more oppressive societies this could be used to control or track an individual's use of the Internet. It would require a powerful independent regulatory body to ensure the privacy of personal data.

There are currently a number of initiatives attempting to provide this Identify 2.0 functionality: OpenID, Higgins, WS-Federation, Shibboleth, and Windows Live ID to name a few. But, to date, there is no single system that can show a clear advantage to users or suppliers. The result is that they are not yet widely used. But the issues surrounding authentication are such that all parties involved in securing transactions of all kinds must move to provide some uniformity and consistency in this field so that better security becomes the norm.