NETWORKWORLD

This story appeared on Network World at
http:// www.networkworld.com/columnists/2008/041108-jericho.html

Why does a person need so many electronic identities?

Or better stated, "How can we kill off passwords!"
The Jericho Forum Outlook By Adrian Seccombe , Network World , 04/11/2008

What is the solution to the growing number and risks of the identities that are now connected with us all? Will a simple identity trust framework be part of such a solution? How will users be able to reduce the number of passwords they have to handle? This article will attempt to explore these questions.

Problem

One of the growing frustrations of the Internet is the number of password-based identities that we, its users, are required to accept. This is leading to a new kind of identity risk. The average Internet user is likely to have upwards of 50 identities. Because we are not very good at remembering that many different unique/strong passwords, we are likely to re-use passwords across different sites. Furthermore, these sites are not all capable of protecting our passwords to the same degree. Worse, we do not regularly keep changing passwords, which serves to exacerbate the problem. How can we effectively manage the security and currency of so many passwords for so many identities? Simply put, we cannot; at least not securely!

Why should I care?

Different Web site suppliers ask us to share different personal details. This enables someone with a criminal intent to harvest our identities by cracking a weak site and then using the identities and passwords obtained to visit different sites and extract further personal details. Often, as a treat for the hacker, we have allowed the Web sites to store our credit card details. Some sites even openly display the credit card numbers to the accredited user. Sites that don't display numbers often allow products and services to be obtained and sent to alternate locations. It won't be long before we see automatic harvesting using this approach – if it isn't already being used.

Short-term fix

Accepting that pass-phrases are more secure than passwords, we can immediately start reducing our risk by introducing simple methods that enable us to use different pass-phrases on each site, rather than passwords. It is, however, important that such approaches are not obvious. For example if a hacker finds that your pass-phrase on the Google site is: "mycorepassword?google!", it will not take him long to work out your password for the PayPal site, despite it looking like a strong password.

Components of the solution

Open ID is showing one approach, but unfortunately the strength of OpenID's security model is not sufficient to be used for high-value information. This is not to say that Open ID is not a useful solution for low-risk activities. It is simply not robust enough for transactions or activities that require high degrees of confidentiality or integrity. Open ID is not designed to withstand targeted attacks, such as "man in the middle attacks" because there is too much reliance on the Open ID provider's capability and trustworthiness.

Identity selectors like Microsoft's Card Space are likely to play a part in the final solution. One-time passwords (paper and electronic) are also interesting components, as are one-time credit card numbers. A trusted device that allows for a simple verification step for high-value or high-risk information would be valuable. The long-term solution will require cooperation from providers (the site owners) and a new breed called identity management service providers (IMSP). Many effective security protocols have already been developed.

There are some key innovations still needed in this space, especially around secure persona management. This is the ability for users to be able to present different personas. Happily some new innovations are in development. The next step is to mold these components into a useable service.

Recommended solution/response

The issue is not the number of identities but the ease of managing them securely. One key first step is a more effective means of identifying the trustworthiness of the participants in any new electronic relationship. The primary issue on the Internet is not "Who is the user?" The primary issue is more often exemplified by the question, "Am I connecting to a trustworthy partner in this transaction?" Another step will be to provide a simple means of allowing the user to create a unique user/provider identity using a specific persona for the provider. This identity would be easily identifiable to the user and would be created during the initial user/provider registration process. Turning the process on its head and using a simple, yet robust means of exchanging public keys, assisted by a trusted third party, could be designed to improve the user experience, as well as reduce the overall system risk.

Example Personas:
I am an anonymous human being.
I am an anonymous human being over 18 years old.
I am USERNAME, a human being, over 18 year old.
I am FULLNAME, a human being, over 18 year old.
I am FULLNAME, a human being, over 18 year old, my Full Address is…

A financial transaction could be initiated by any of the above personas.

Conclusion

The current approach is not satisfactory to any of those involved, because its risks are too high and there are not sufficient numbers of different trust levels provided in the alternatives, beyond the "low trust" service currently being provided by the Open ID model. High-risk identity activities, especially those involving financial transactions, continue to be provided around the globe using a model that operates on the principle that assumes that the losses incurred can be borne by the users of the systems. This is fast becoming a false assumption, and these losses must be reduced. Banks might consider themselves to be potential IMSPs especially because they currently have the most to gain from the improvement in security.

(For a more detailed analysis of the broader aspects of identity assurance, refer to Sir James Crosby's "Challenges and Opportunities in Identity Assurance." Note: this report does not focus on the electronic identity issue.)

The way forward

A new approach is required that involves recognizing the user as central to the process. Rather than having the provider at the center, an "identity switch" would change the model to be user centric, with the aim of introducing lower-risk and easier-to-use processes.

The ceremony that creates a user/provider identity – one that is easily recognizable by the user who created it – would also develop a trusted link between the user and provider with various means of initiating, affirming and maintaining this trusted link. The preferred process would avoid third parties as the repository of the user/provider identities. In the future, IMSPs will more than likely refine this approach and provide additional services – for example, allowing each user to have a unique e-mail address for each supplier.

For this to work four fundamental components are needed:

• Demand from service providers and users alike.

• The development of an easy to use infrastructure that is based on open standards.

• A broadly understood trust framework that enables simple persona choices to be made.

• A secure means of tracking the trustworthiness of both parties (this last being fraught with privacy implications).

If we work together, we can achieve this goal.

All contents copyright 1995-2008 Network World, Inc. http://www.networkworld.com