Time for Authentication Shake-out

The time is right for the banking industry to take the lead and standardise approaches to authentication

BY STEPHEN WILSON

On May 2 at *Online Banking Review*'s seminar Combating Cybercrime, news broke of plans for an exciting new shared authentication utility. The project, initiated by Westpac and subsequently discussed at a meeting of the ABA in April, is said to be taking a major step beyond marketing and education, towards a true shared utility.

Internet security as a utility is an idea that's time has surely come. Why shouldn't our Internet services be as clean, reliable and available as our water or electricity? With a few exceptions, we don't ordinarily ask consumers to treat their own water or install power filters.

Yet the standard advice to Internet users often treats them like technical specialists. A major US bank for instance advises its customers to make sure their browsers use "the strongest encryption available" and to be aware of the "encryption levels of the sites and applications you use". How is the average user supposed to determine the encryption levels of their applications?

The reasonableness of technical instructions given to users is a fine legal question and notoriously difficult to judge when technologies are new. Banks are well advised to generally avoid novelty in their products. Customer behaviour should be consistent and predictable; from the customer's point of view, the Internet banking experience must be made as familiar as possible.

The long term answers lie with new Internet protocols, software engineering practices, software product designs and service models – developments which will become commoditised and incorporated as a matter of course into Internet banking platforms. But in the meantime, banks and e-businesses wrestle with the slippery notion of security "best practice".

Happily, banks appear not to believe that Internet security is a competitive differentiator, and are all the more willing to look at sharing authentication infrastructure, as they do with cheque processing and a number of other cost centres. On the other hand, product vendors understandably *do* see security competitively. And so, inevitably, there is a huge array of authentication options vying for market share.

Yet, as I've discussed in previous *OBR* columns, not all authenticators are created equal. If the bottom line is security and trust, then we should expect a shake-out in identity technologies to be just around the corner.

Perhaps the shared trust centre initiative will create a vehicle for rationalisation, facilitating a critical review of the large scale efficacy of different authentication methods.

The Combating Cybercrime panel discussion provided an ideal opportunity to examine some of the many nuances in authentication today. The issues are complex and subtle, and they benefited greatly from experts spending quality time discussing them.

There was broad agreement that two-factor authentication solutions do vary markedly in their inherent security; in particular, not all of them resist "man-in-the-middle" attacks. One speaker felt that PKI technology was the "ultimate" in this regard but it had yet to be embedded into commercial solutions with sufficient transparency and ease of use.

Meanwhile, because something has to be done, many banks are putting their toe in the water with one new identity technology or another. SMS messaging, one-time password generators, USB tokens and TAN cards are all under evaluation, and seem to be viewed (correctly in my view) as stop-gap measures.

Most of today's authentication gadgets are very novel to the average user. If we really think about it, even the most basic Internet operations are actually a mystery to many customers. Otherwise phishing, pharming and Nigerian e-mail scams simply wouldn't enjoy such embarrassingly high success rates! People tend to put a disproportionate level of trust in the Internet medium while being horribly unable to tell at a glance what is real and what is not.

Making customers more active participants in Internet transactions through two-factor gadgets may go a little way towards grounding their Internet experience. But fumbling around with a "necklace of tokens" brings new risks, because the required user behaviours are becoming even more novel and inconsistent, drifting further away from what people are used to. We need to be careful that the illusion of active involvement created by scratching off TAN cards for one website or re-keying security codes received by SMS or OTP for another, doesn't make customers even more complacent and therefore vulnerable to online fraud.

In my view, the authentication debate till now has been complicated by a handful of possible red herrings. The advent of a shared infrastructure approach is the ideal opportunity to re-visit a range of industry-wide issues and to seek some consistent answers.

A critical question is customer choice. It may seem politically incorrect, but it's worth asking gently, do consumers really need a choice of security technologies? What do lay users really know about security threats, and can they ever be equipped to make risk management decisions?

Choice of infrastructure technologies is usually moot. Consumers can choose between banks and between banking products, but they are not offered options when it comes to the design of vaults or ATM networks or plastic cards. Instead, the industry makes careful, collaborative and transparent decisions in technically complex areas, setting standards which in effect narrow the options for the good of all stakeholders.

As the trust centre team points out, the need for reliable authentication has become an all-of-community issue, spanning all business sectors. It may take some determination to review today's interim measures, but the time is right for the banking industry to again take the lead and standardise approaches to authentication.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au