Smartcard fears unfounded

The community deserves real safety when accessing the Internet and only smartcards can enhance both security and privacy online

BY STEPHEN WILSON

What is holding back smartcards in Australia? Almost everyone in Britain, Malaysia and Taiwan uses them daily in banking, and EMV rollout worldwide has topped half a billion cards.

While the technical arguments are beyond dispute, businesses in Australia and New Zealand still find it hard to justify capital investments in technology. Compounding the challenge is a range of misconceptions among the public.

In recent issues of *Online Banking Review*, several writers have exposed the issues of phishing, pharming, DNS cache poisoning and the man-in-the-middle attacks. There is increasing recognition that most of today's two-factor authentication devices are already obsolete.

Many believe that smartcards are the only way forward. The head of cryptography at the US National Institute of Standards and Technology says, that in respect of Man-in-the-Middle attacks, "the only practical solution today uses PKI" in hard tokens like smartcards.

But smartcards sure inspire fear. A *Sydney Morning Herald* editorial earlier this year was blithely unaware of even the possibility that smartcards could enhance privacy, when it said: "Technological change means such a card would now pose far greater challenges to liberty and privacy than the Australia Card suggested by the Hawke government in the mid-'80s". In fact, properly applied, smartcards could bring the most significant improvements to online privacy we have ever seen, by tackling phishing, pharming and spam.

There is also an almost universal default view that privacy can be traded off in the interests of "security". Yet the truth is that smartcards can dramatically enhance both security and privacy. It isn't just that smartcards resist card fraud by skimming; they can also return far greater degrees of control to consumers, reversing the trend for their personal information to be centralised and copied across countless unseen backend systems.

So perhaps we need a new "manifesto" to lay the foundations for up-to-date and optimistic technological responses to the challenges of security and privacy.

First of all, we should not even think about having a debate about privacy! Privacy should not be readily negotiable. The public have a right to enjoy privacy and security at the same time.

Secondly, consumers should have enhanced abilities to deal anonymously. National Privacy Principle No. 8 is in fact all about anonymity, but most businesses have come to view it as impractical. Moreover, for banks, the new regulatory mandates of AML and Basel II appear to cancel out any possibility of anonymity or pseudonymity. However, new technologies like zero-knowledge methods and smartcards shed fresh light on these challenges. Surely competitive advantages await for those institutions that safeguard the identity of their customers from prying eyes while being able to meet their legislated obligations.

Thirdly, we should all do more to resist the ever increasing centralisation and aggregation of personal data. One of the more obvious and worrying outcomes of data centralisation has been the sale of massed personal information to criminals by corrupt call centre workers. Theft, or accidental leakage of personal information from government agencies, financial institutions and data processing bureaus is becoming more common. So why have we allowed huge stockpiles of our personal details to be amassed by third parties? As identity crime soars, large stores of personal information are increasingly valuable to sophisticated and highly organised attackers. E-commerce providers struggle to manage their legal liabilities to lockdown these repositories without expending huge funds and resources on security.

And finally, the community deserves real safety when accessing the Internet. The government has the laudable goal of moving more and more of its services and transaction traffic online. Human Services agencies in particular send out hundreds of thousands of pieces of mail every day, and they envisage moving as much correspondence as possible to email.

But the paradox of course is that at the same time, banks and other institutions gripped by phishing, are busily telling consumers to distrust email! So if it expects citizens to use email, government must surely take active steps to guarantee the safety of the channel in regards to phishing, pharming, spam and website spoofing. There is huge potential for the new Human Services Access Card to be applied in the war on phishing and spam.

There is a clear strategic opportunity for the banking sector to take a lead in these national developments. If we take a shared infrastructure view of smartcards, then a number of critical projects could usefully be merged. For example, impending health and welfare smartcards and smart drivers licenses could be made available as secure carriers for other agencies' identifiers, enabling true anonymity of government service delivery. And banks' EMV rollout could be joined to Internet banking services, to deliver mutual authentication and real protection against web fraud.

Australians have long proved to be early and enthusiastic adopters of new technologies, so long as the value proposition is clear and true. The experience of smartcards here could be hugely positive if the full spread of capabilities was communicated and delivered to consumers.

A new smartcard manifesto

- **There should be no privacy debate**
- We have the right to deal anonymously
- **We should resist the centralisation of data**
- The community deserves safe means to access the Internet

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