Improving your smartcard ROI

Could the move to chip cards see smartcard infrastructure applied to online banking?

BY STEPHEN WILSON

In the latest skirmish in the cyber-crime arms race, the UK's Barclays Bank has announced it will deploy half a million special-purpose smartcard readers to transform its EMV cards into personal security tokens for Internet banking.

This is an important development, though not so much for security per se, as this approach remains vulnerable to certain attacks. Rather, it shows how institutions can improve their smartcard ROI and create useful security upgrade paths along which their customers' experience can steadily improve. It is one of the first strong signs of convergence of banking products onto a uniform, user-friendly electronic key.

The stand-alone readers – branded "PINsentry" – resemble simple calculators with a slot to insert the smartcard. The readers are used to create one-time passwords (OTPs) to login to the bank's website. The devices use cryptographic codes and firmware embedded in the card.

The generic vulnerability of all one-time password generators has been known for a long time. In the February 2005 edition of *Online Banking Review*, I wrote, "most two-factor authentication solutions don't protect against all forms of identity fraud. There are new ways to undermine SSL website security – chiefly through man-in-the middle attacks – and only smartcards and USB keys have the power to prevent them".

The past 18 months has seen a steady succession of attacks on OTP authentication in all its various guises. Public examples of successful man-in-the middle attacks include on Nordea Bank's Transaction Authentication Number (TAN) scratchy cards, Citibank's event-based OTP key fobs, and ABN Amro's time-based OTP key fobs.

Sadly, PINsentry and similar cableless smartcard readers are as vulnerable to man-in-the-middle attacks as any other one-way authenticator. Simply put, these approaches are not smart enough to know the difference between a spoofed website and the real thing. They cannot actively challenge the veracity of websites on behalf of the customer before allowing a connection. We therefore should expect them to be subjected to the same types of attacks in coming months.

Nevertheless, I am enthusiastic about PINsentry and the like, as they represent a progressive intermediate step towards a long-term robust solution for mutual authentication. These products show clearly how banks can improve their ROI on smartcards.

Australian institutions have understandably resisted the migration of credit and debit cards to chip: we enjoy some of the lowest plastic-card fraud rates in the world, and very slow rates of fraud growth. But inevitably the time has come for us to join the new global standard for all plastic-card products. Part of the push comes from the increasing difficulty Australian bank customers have using their credit cards in overseas markets where EMV is now in place.

While card fraud indeed is low, phishing and pharming remain almost completely out of control. Late last year, the UK payments association, APACS, provided figures to a British House of Lords inquiry that showed an 80-fold increase in phishing over the past two years. And APACS admitted there was no sign of phishing decreasing in the short term.

The latest monthly report of the Anti-Phishing Working Group in April 2007 shows the usual ups and downs typical of the arms race. But over the medium to long term, the trend mirrors the APACS experience. The overall rate of appearance of new phishing sites, on my conservative estimates, more than tripled in the 12 months to February 2007.

Phishing is most commonly classed as a form of social-engineering attack, since it relies on unwitting users falling for dodgy emails or clicking on unverified links. But the inexorable rise in phishing attacks must be seen as mainly a technological phenomenon, as it is driven by the industrialisation of cyber-criminal methods. With spoofing techniques becoming ever more sophisticated, it is high time we recognised the limits of our ability to educate customers to beware of phishing and pharming. It is simply not practical anymore, even for expert users, to discriminate between suspect websites and dangerous content and safe sites.

Sooner or later serious e-business services will have to adopt true mutual authentication, using active authentication devices like smartcards and USB keys, or integrated mobile transaction solutions that can leverage intelligent SIMs. EMV smartcards can fit the bill, but they have to be connected directly to the PC, so they can interact automatically and seamlessly with the browser or other software. With integrated card readers increasingly available as standard options in laptops and PCs, and a wide range of native drivers shipping in Windows Vista, my guess is that, within two years or so, smartcards will become accessible to the majority of banking customers.

Meanwhile, devices like PINsentry serve two important strategic purposes. Firstly, they help normalise the use of smartcards across multiple channels, taking them from EFTPOS and ATM settings into Internet banking. Secondly, they radically improve the issuer's return on investment, by applying the smartcard infrastructure to a greater range of banking services.

And in this regard, PINsentry is only one amongst a whole wave of innovative new applications that enhance the utility and value of smartcards. Other examples include the use of spare slots in digital TV set-top boxes in the UK to accept chip-and-PIN cards for online shopping, and bluetooth-enabled identity badge carriers that connect US government employee smartcards to their Blackberrys to support digitally signed email.

Of course, for an enhanced ROI to be calculable, it requires profit and loss for smartcard investments to be syndicated across more than just the bank's cards group. And that might be another story!

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