Understanding the Man-In-The-Middle

Two-factor authentication could soon be obsolete thanks to a new generation of security attacks

BY STEPHEN WILSON

In the last edition of *Online Banking Review*, I observed that "most two-factor authentication solutions don't protect against all forms of identity fraud. There are new ways to undermine SSL web site security – chiefly through 'man-in-the middle' attacks – and only smartcards and USB keys have the power to prevent them."

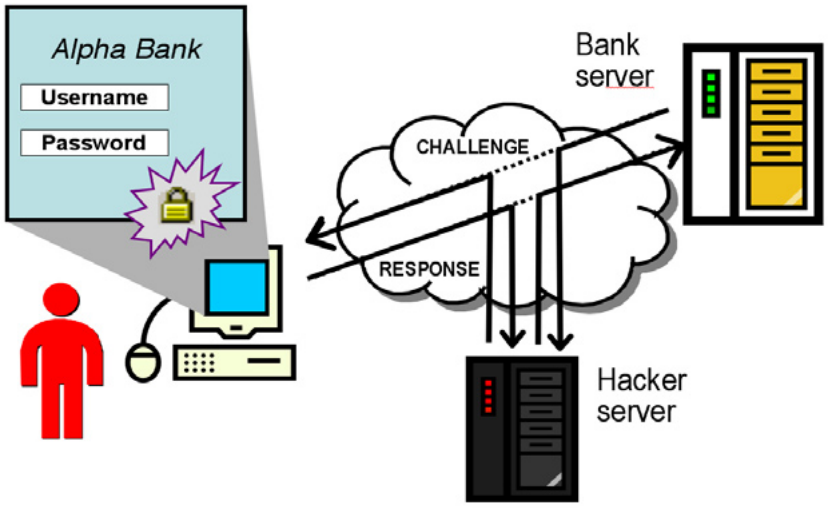
Since then, renowned security expert Bruce Schneier has published an article that is reverberating through banking circles. In "The Failure of Two-Factor Authentication", Schneier says "two-factor authentication won't work for remote authentication over the Internet" because of the man-in-the-middle problem.

Some security managers downplay the real world threat of man-in-the-middle attacks, arguing that two-factor authentication is a whole lot better than static passwords alone. But we cannot afford to be complacent, not when organised crime is being squeezed out of Europe and parts of Asia, where smartcards have been introduced.

And it's not just purists like Bruce Schneier who are worried. The US Government is rolling out new Federal employee identification standards. Bill Burr, the head of computer security at the National Institute of Standards and Technology, told last month's Asia PKI Forum conference in Tokyo that to resist man-in-the-middle attacks and account hijacking, the "only practical solution today" uses smartcards or USB keys with public key infrastructure.

It's easy to see how most two-factor authentication methods are vulnerable to man-in-the-middle attacks, whether they be random password generators, lookup tables, text messaging or even biometrics. As ingenious as these tools may be for safeguarding the identity of customers, none of them protect the online identity of the issuer. Put simply, these technologies do nothing to prevent Internet users from "knocking on the wrong door". In the cybercrime arms race, hackers grow unrelentingly clever at building fake front doors or "ghost" websites. Most successful phishing scams work by tricking customers into clicking through to a ghost site.

The man-in-the-middle attack works like this. A ghost site – complete with counterfeit SSL padlock – is set up. The ghost site intercepts authentication messages exchanged by the customer and the bank, both of whom remain oblivious to the interloper. It doesn't matter what these messages are, nor how they are created; the hacker's server simply passes them back and forth until the user authentication is done. From that point on, the "man-in-the-middle" ignores the user and instead issues its own fraudulent requests to the bank's server, such as funds transfers to the hacker's account.



Unlike phishing scams, which mostly depend on unwitting users making some sort of mistake, a man-in-the-middle attack can have a 100 per cent hit rate. Until the hacker's server is detected, all connections from all customers can be hijacked.

The best defence against the man-in-the-middle is *bilateral authentication*. Not only must the bank know for sure which customer it's talking to, the customer has to actively challenge and verify the identity of the bank. Alone among two-factor identity solutions on the market today, smartcard technology has the ability to perform bilateral authentication. For instance, smartcards (or equivalently, USB dongles) can safeguard copies of the bank's SSL "master codes". This ensures that each SSL session is properly encrypted from each end, and resistant to hijacking.

From the customer's perspective, a unified and consistent approach to identity fraud is called for, preferably one that preserves traditional ways of interacting with banks, merchants and other services. If smartcards can protect not only customers from identity theft, but institutions as well, while preserving the longstanding plastic card experience with ATMs and Eftpos, then perhaps the time for this technology has come.

Banks have been careful and measured in their response to cyber crime. The true seriousness of the threat has of course lagged behind the public imagination. But with mounting pressure now to act, it is important that banks be seen to act decisively. Customer confidence is thought to now be really suffering as a reaction to phishing. To allay peoples' anxieties (and their natural scepticism), the next security solution must be a lasting one. Some major change in customer behaviour is going to be inevitable, no matter what authentication method we choose to introduce next. It is important that we don't make customers change yet again, if ordinary two-factor authentication is going to be obsolete just around the corner.

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