Smartcards offer best protection

BY STEPHEN WILSON

Everybody's talking about identity theft. And many banks are doing something about it, through a plethora of new customer ID technologies.

But banks have identities too. The twin scourges of phishing and website ghosting in effect steal a bank's online identity. And, unfortunately, very few of the new technologies can secure the identity of the institution which issues them.

So this column examines identity at both ends of an Internet transaction. We will see that only by putting certain active devices in the hands of customers can banks combat phishing and ghosting, while safeguarding their customers against identity theft.

Internet transactions require the parties at both ends to identify each another, through a communications "handshake". Several steps are involved, most of which are carried out automatically by web browser software.

The customer's browser first "knocks on the door" of an e-business site, and is answered by the web server, which asks "who goes there?". A special message called a *challenge* is issued by the server, which the browser must meet with another message, the *response*. If the response is satisfactory to the server, then the user is taken to be authenticated and an encrypted web session follows.

A lot depends on the challenge-response method. The simplest systems don't have any challenge, and make do just with a passive user password. Far better is two-factor authentication where a personal hardware device generates a one-time password, or calculates a dynamic response code, which is entered into the browser, proving to the server the identity of the device holder.

A new variation on two-factor authentication uses text messaging to send a random number to the customer's mobile phone. All they need to do is type the code back into their browser, to prove that the proper person is online.

But none of these technologies are any good to users if they happen to be knocking on the wrong door. In the cyber-crime arms race, hackers grow unrelentingly more clever at building fake front doors.

It is not hard to tamper with the Internet's domain name servers, so that, at least for a while, a legitimate URL is made to point to a rogue server, or "ghost site", dressed up to look like the real thing. Most successful phishing scams work by tricking customers into clicking through to what turns out to be a ghost site.

The well known "SSL" security protocol with its trademark padlock icon is supposed to prevent ghosting. For years, users have been taught to look out for the padlock at the bottom of the browser as proof they are at a secure site. SSL works by loading unique security codes onto certified web servers, and checking them against "master codes" that come pre-installed in browsers. But there the codes are vulnerable.

One of the most serious security developments to date is the discovery by hackers of ways to substitute the SSL "master codes". As a result, the SSL padlock itself is no longer trustworthy.

It's tempting to think that two-factor authentication can save us from phishing and website ghosting, because banking servers won't transact unless the user is fully verified. Unfortunately this line of reasoning overlooks the so-called "Man-in-the-Middle" attack.

A ghost site is set up between the customer and the real bank server. The ghost site poses as the front door, and passes handshake messages to and from the customer and the bank, both of whom remain oblivious to the interloper. Once the challenge-response is done, the Man-in-the-Middle ignores the user and instead issues its own fraudulent requests to the server, such as funds transfers to the hacker's account.

So, who is winning the arms race? SSL itself is still secure but better care must be taken of the "master codes". Instead of storing the codes in browser software, they should be kept in active hardware devices. Crucially, none of today's common two-factor authenticators have the necessary active capability.

But it turns out that smartcards do. On the one hand, smartcards have been controversial. Credit card companies urge them as the preferred solution for skimming, yet banks have spent years looking at smartcards, and except for niche areas, have not been able to make the business case. But on the other hand, if smartcards (or equivalently, USB keys) can address phishing and ghosting at the same time as skimming, then the cost-benefit becomes much more positive.

Smartcards and the leading identity alternatives are compared in the table.

A uniform approach to the problem of identity theft is called for, preferably one that preserves customers' long standing ways of dealing with their banks. If smartcards can protect not only customers from identity theft but institutions as well, then perhaps the time for this technology has come.

■ **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.

Weighing up the security options

TECHNOLOGY	STRENGTHS	WEAKNESSES	
SSL alone	Very low cost No hardware	Security codes vulnerable to attack	
PIN token	Requires no reader	Poor fit for wallet/purse	Do not protect security "master codes" Cannot prevent ghosting and phishing
SMS confirm	Works with any mobile phone	May need new phone number if hacked Variable performance	
Biometrics	Convenient Cannot be lost	Expensive, burdensome Variable performance	
Smartcard (or USB key)	Directly safeguards security "master codes" Familiar user experience	In the interim, requires a smartcard reader or alternatively, a USB key	