Lockstep Technologies
www.lockstep.com.au

Towards a uniform solution to identity theft

November 2006 (V2.1)

Everybody's talking about identity theft. And many banks and other institutions are doing something about it, through a plethora of new security technologies. But identity is critical at both ends of most Internet transactions. Organisations as well as customers have identities; the scourges of phishing, pharming and website ghosting in effect compromise an organisation's identity. Unfortunately, very few of the new authentication technologies can secure the identity of the organisation which issues them. This paper examines authentication solutions, and shows that only certain active devices combat phishing, pharming and web fraud, while also safeguarding customers against identity theft.

The need for *Mutual Authentication*

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 in effect 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 identified and an encrypted web session follows.

A great deal depends on the challenge-response method. The simplest systems have a passive response, namely a static password or PIN. These are vulnerable to straightforward "replay" attacks, where a fraudster obtains the victim's password and then replays it against the Internet service, which has no other way to detect if the user is genuine. Far better is a dynamic challenge-response which is varied for each session. The response is most often generated by a portable hardware device – either as a unique code calculated from a challenge number keyed in by the user, or as a one-time random number – and is typed back into the browser to prove the identity of the holder. These gadgets are the most common examples of *Two Factor Authentication*, whereby the holder is identified not only by what they know – a password – but also by what they have in their possession. It is far harder for an attacker to steal both what you know and what you have (at least without being detected).

Two factor authentication comes in many guises. The one-time PIN generator and challenge-response calculator have been used in computer network security for several years and are now being offered to some Internet banking customers. Lower cost variations include:

— the use of text messaging to send a random number to the customer's mobile phone, which is typed back into their browser
— *Transaction Authentication Number* ("TAN") scratchy cards, printed with a series of one time PINs to be used in sequence
— randomised look-up tables, known as *Matrix Cards*, specific to each customer, which furnish pseudo-random codes to be entered into the browser in response to row and column prompts
— a variation on the look-up table, where a card with a randomly printed series of characters along one edge is held against a browser's screen and matched against another series of numbers generated by the website, to provide different logon codes[1]

However, as ingenious as these tools may be for safeguarding the identity of customers, *none of them safeguard the online identity of the issuer*. Put simply, these technologies do nothing to prevent users from knocking on the wrong website door. And in the cyber-crime arms race, attackers grow unrelentingly cleverer at building fake front doors. Most successful phishing scams work by tricking customers into clicking through to what turns out to be a ghost site. More complex attacks tamper with the Internet's domain name servers with a technique called DNS cache poisoning, so that at least for a while, a legitimate URL is made to point to a rogue server made to look like the real thing.

New threats to SSL

The ubiquitous SSL security protocol, with its widely recognised padlock icon, is supposed to prevent website fraud. 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 installing unique security codes (embodied in digital certificates) on certified web servers, and checking them against 'master codes' that come pre-installed in browsers. But in browser software the codes are vulnerable to

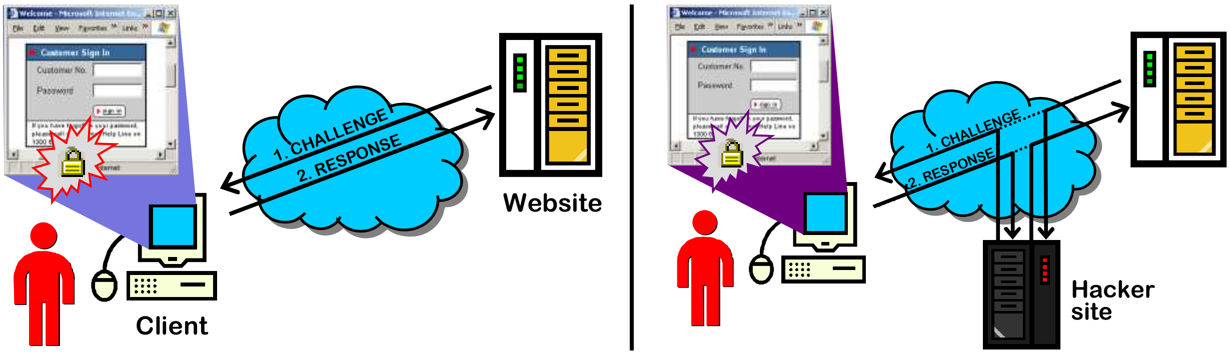
[1] Note that unlike the other two factor authenticators, look-up tables can be duplicated by a thief while not relieving the owner of the original, for example by photocopying the user's card. It might therefore be more fitting to describe look-up tables as "one and a half factors", not two.

attack. One of the most serious security developments to date is the discovery by hackers of ways to tamper with the SSL 'master codes' or to inject additional fake codes to fool the verification software.[2] As a result, the SSL padlock itself is no longer trustworthy.

Now, it is tempting to believe 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 "Man-in-the-Middle" attack.

The Man-in-the-Middle Attack

In the classical Man-in-the-Middle attack, a hidden server is set up between the customer and the real web site. The hidden server passes handshake messages to and from the customer and the e-business, both of whom remain oblivious to the interloper. Once the challenge-response is done, the Man-in-the-Middle machine cuts the user off and then issues its own fraudulent requests to the server, such as funds transfers from the customer's bank to the attacker's account.



Through 2006 we saw increasingly sophisticated Man-in-the-Middle attacks mounted on Internet banking systems, including Nordea Bank's TAN cards, and Citibank's One Time Password.[3]

So who's winning the arms race? The SSL protocol 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.

[2] See www.thoughtcrime.org/ie-ssl-chain.txt.

[3] See www.f-secure.com/weblog/archives/archive-102005.html#00000668 and blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html.

Crucially, very few of today's two factor authenticators have the necessary functionality which would allow them to issue their own challenges to the web server at the very start of a transaction.

Comparing authentication options

Alone amongst two factor authentication options on the market today, smartcard technology has the ability to safeguard copies of the SSL 'master codes' and to thus reliably challenge the identity of e-business web servers.

Admittedly, smartcards have been controversial. Credit card companies urge them as the preferred solution to prevent magnetic stripe card skimming. Yet banks have spent years looking at smartcards, and except for niche areas, have not been able to make a positive business case. But on the other hand, if smartcards can deliver a unified solution to all forms of electronic identity theft – phishing, pharming and web fraud as well as card skimming – then the cost-benefit equation may become much more attractive.

Smartcards and the leading authentication alternatives are compared below.

	Technology	Strengths	Weaknesses	
One way authentication	Password	– Very cheap – Needs no hardware	– Easily stolen; widely regarded as entirely outmoded for significant transactions.	
	OTP token	– Requires no peripherals	– Expensive – Poor fit for wallet, purse – Proven vulnerable to Man-in-the-Middle attack	**No one-way solution safeguards issuer's security codes;** **All are vulnerable to Man-in-the-Middle attack;** **None prevent web fraud & phishing;** **Divergent and novel for users.**
	Lookup table or "matrix cards"	– Require no peripherals – Can be printed onto regular cards	– Can be photocopied – Not truly two factor	
	TAN cards	– Cheap	– Proven vulnerable to Man-in-the-Middle attack	
	SMS text messages	– Works with any mobile phone	– Requires a phone – Must keep phone no. secret – Variable performance	
	Biometrics	– Convenient – Cannot be lost	– Expensive, burdensome – Variable performance	
Mutual Auth.	**Smartcards**	**Can safeguard all the issuer's security codes;** **Familiar user experience;** **Convergent solution for all channels: Internet, ATM and retail.**	– In the interim, requires smartcard reader or alternatively, a USB key	

Conclusion

A unified approach to the problem of identity theft is called for, preferably one that preserves customers' traditional ways of interacting with banks, merchants and other services. The form factor and user experience of the plastic card is universal. It will dominate not only ATM and merchant encounters for decades to come, but most other forms of identification and eligibility as well – drivers licences, government ids, membership cards, public transport and so on. The e-commerce industry should be careful not to depart from this norm unnecessarily; a proliferation of non-standard authentication devices held on key rings, mobile phones, PDAs and paper cards will not be welcomed by consumers, especially if they provide only incomplete solutions to identity fraud. However, if smartcards can not only protect customers from identity theft but safeguard institutions against phishing, pharming and web fraud as well, while preserving the longstanding plastic card experience, then perhaps the time for this technology has come.

About the author

Stephen Wilson is a leading international authority on authentication and identity management. In early 2004 Stephen established Lockstep to provide independent analysis and advice in cyber security, and to develop new smartcard-based solutions to address identity theft and online anonymity. Contact swilson@lockstep.com.au.