Lockstep Consulting
ABN 59 593 754 482
Contact: swilson@lockstep.com.au

Two factor authentication and second class citizens

Stephen Wilson
Online Banking Review column No. 9
January 2005

An unfortunate side-effect of user-pays security could be the creation of two classes of Internet banking customer.

The new year is shaping as a watershed in online banking security. In the last few months of 2004, banking security was of course dominated by the scourges of identity theft and account hijacking. It seems we all know what the problem is. The challenge through 2005 will be to make sure we don't bamboozle customers with too many solutions.

Let's recap the important recent developments.

- In June 2004, the Hong Kong Monetary Authority issued a circular recommending that local banks "conduct a detailed risk assessment to identify high-risk internet banking transactions that need to be subject to two-factor authentication. In general, high-risk internet banking transactions should at least include unregistered third-party fund transfers and payments, and change requests concerning customers' sensitive information".[1] So far the HKMA has stopped short of mandating two factor, but it does require banks to document their risk assessments, and submit them for review.

- In August, APRA wrote to all Authorised Deposit-Taking Institutions: "Over the past year or so there has been a marked increase in the number of Internet-based fraudulent attempts to gain access to ADI customers' accounts. A number of Australian ADIs have been targeted. APRA strongly recommends that all [institutions] offering services over the

[1] http://www.info.gov.hk/hkma/eng/guide/circu_date/20040623e1.htm.

Internet … implement strong authentication and control mechanisms to provide reliable safeguards against identity theft".[2] APRA does not take a firm position on two factor, but tellingly, it did highlight that "a number of banks have recently announced their intention to introduce two-factor authentication as a means of overcoming some of the recent threats".

- In September, Graham Ingram, General Manager of the Australian Computer Emergency Response Team, told the APEC eSecurity Task Group that "single factor, replayable authentication is no longer viable to prevent unauthorised access to valued or sensitive online accounts".[3]

- In October, possibly for the first time, the problem of identity theft was acknowledged by a bank in simple economic terms. One of Australia's majors stated in its 2004 annual report that "non-lending losses also increased [in the second half] with higher levels of internet phishing and cheque fraud."

- In December 2004, the major American banking regulator, the Federal Deposits Insurance Corporation (FDIC), published a report *Putting an End to Account-Hijacking Identity Theft*.[4] It recommended that "financial institutions and government should consider a number of steps to reduce online fraud, including upgrading existing password-based single-factor customer authentication systems to two-factor authentication …". The FDIC's evaluations to date appear to rank the available options in the following order: USB tokens, smartcards, and password-generating tokens. Interestingly, the FDIC has implemented its own internal smartcard and PKI system.

- In January 2005, the British Chip and PIN program reported it had met its milestones for the UK smartcard rollout. There are 77 million smartcards on issue, and eight out of every ten merchants have upgraded their terminals (for a total of 636,000 smartcard enabled tills). At present, four million smartcard transactions are processed daily in Britain; throughput is doubling every eight weeks.

So two factor authentication is emerging as a 'gold standard'. Several local initiatives have been widely publicised already, including the use of password-generating tokens by Bendigo Bank and Westpac, and a trial of text messaging by the NAB. Overseas, password generators have been rolled out to Internet

[2] http://tinyurl.com/3o6m2
[3] http://tinyurl.com/6au47
[4] http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf

customers in South Africa, New Zealand and Europe. And smartcards are used for business banking over the web by the ANZ, as well as HSBC Singapore, Barclays, and the Bank of Scotland. In Europe, it won't be long before the huge installed base of Chip and PIN smartcards is leveraged into secure Internet banking and e-commerce.

At this stage, none of these technologies come cheap. And while the true cost of identity fraud remains controversial, Australian banks don't see it as being large enough yet to justify the economics of switching to two factor across-the-board. So for now, the user-pays principle tends to apply. Institutions typically levy a small fee for the privilege of password generating tokens, the use of which remains optional.

One problem with this approach is that it places the customer in the position of having to make their own technical risk assessment, in weighing the cost-benefit of upgrading to better security. It is unusual in everyday life for lay people to have to make such decisions about safety. An unfortunate side-effect of user-pays security could be the creation of two classes of Internet banking customer.

Another problem is that most two factor authentication solutions don't protect against all forms of identity fraud. As I discussed in the Oct-Nov 2004 edition of *Online Banking Review*, there are new ways to undermine SSL web site security – chiefly through "Man In The Middle" attacks – and only smartcards and USB tokens have the power to prevent them. Genuine solutions to phishing and web site ghosting require active bilateral authentication, which is beyond the ability of one time PIN generators, password translation cards, SMS messaging, and even biometrics.

In the long term, most commentators agree that smartcards will be the standard solution, supporting ATM, EFTPOS, over-the-counter, Internet banking and e-commerce transactions, all with the single, familiar, plastic card format. In the interim, the challenge will be to balance security, cost and ease of use, while minimising the number of times customers will be forced to switch technologies.

About the author

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. Contact swilson@lockstep.com.au.