

Authentication moves beyond tokens

More and more Australian companies are offering alternative solutions to traditional one-time password tokens

BY CHARIS PALMER

After championing tokens as the panacea to online banking fraud and phishing, the security industry is finally acknowledging two-factor authentication is only one component in a range of defensive measures required to address the problem.

Case in point is RSA Security's finance and banking specialist Geoff Noble who rejoined the security giant in August last year after deciding it now had a better proposition to offer. Noble admits prior to the acquisitions of Cyota and Passmark Security that the firm didn't have a solution that represented end-to-end value for the banks. "If you've got a hammer everything starts to look like a nail and the token was starting to look like a hammer."

Noble says tokens today are largely a defensive mechanism.

"If you build a better mousetrap then the mice are going to go somewhere else" and in future there will be less and less front-door authentication and an increasing reliance on behind the scenes transaction monitoring.

Already Australian banks share fraud data and monitor online banking transactions in order to keep fraud levels down. However, in higher risk transaction environments two-factor authentication still has a role to play.

Noble is not ready to write off tokens just yet, arguing rather than becoming redundant they will morph and change. "Something will happen whereby tokens won't be standalone keychain tokens, they'll be embedded in smartcard readers or EMV."

In the mean time, more and more Australian companies are putting up their hand to offer alternative solutions to traditional one-time password tokens.

Start-up TrustDefender points to successful man-in-the-middle attacks on tokens to make the case for its endpoint security solution. The solution scans the users PC for known safe software and allows the bank to defer transactions if any unknown or potentially malicious software is found. Director Andreas Baumhof says: "People should use antivirus but we can provide protection even if they don't use it."

Baumhof says he is a supporter of two-factor authentication, whether it be with a token or via a mobile phone "but the biggest problem is it changes the user experience". And, he says, such solutions become problematic as soon as the user is required to carry more than one device.

But while security experts love the idea of endpoint security, marketers hate the idea of expecting customers to use only one PC for online banking and

Something will happen whereby tokens won't be standalone keychain tokens, they'll be embedded in smartcard readers or EMV

explaining after months of telling them not to download files that they should now install a new solution to their PC.

Baumhof says ultimately the solution provides enough information to banks to allow them to update their risk engines, and for as little as \$1 per user per year is a much more cost effective solution than tokens.

Branko Ninkovic, director of Australian start-up Dragonfly Technologies, says it's unrealistic for banks to expect customers to pay for tokens given they expect the bank to

protect their money whether it be cash or electronic.

Ninkovic says the industry is still some time away from being able to rely purely on behavioural monitoring and, in the mean time, institutions are looking for low-cost stop-gap measures. "Tokens have their place in terms of internal, corporate and staff deployments or if you have a user base doing high value transactions, but when you're talking about 10,000 plus users then you have to start addressing it from a different level."

Ninkovic says those institutions that have already deployed tokens will at some point review the deployment and in some cases come unstuck due to the cost. He says this could mean over a period of two to three years tokens could start to decline.

At the end of the day, Ninkovic says, "Collectively, across the board, banks need to make the decision to start raising the bar on security and look at how they can do that without impacting their customer base."

Adrian Tatham, chief executive officer of m-commerce technology company Alacrity, says thanks to widespread use of credit card transaction monitoring and ANZ's advertising of its Falcon security system, the mindset of consumers has changed. Consumers have become used to being queried by their financial institution if a credit card transaction seems suspicious. "Consumers therefore feel 'if the bank can make this easy for me then it's ok'."

Alacrity is working with three major banks in the UK to deploy its Closed Loop Environment for Wireless (CLEW) technology to both card and account transactions. The system alerts customers via mobile phones, PDAs and PCs of account transactions as they happen, enabling card or online banking users to accept or reject transactions in real-time before they proceed.

Tatham says the company has taken good technology and applied it in a common sense manner.

"We all know the banks have some sort of diagnostic tool, but instead of suspect transactions flagging a call centre, we allow a direct interaction with the customer."

Key Points

- **One-time password tokens are no longer seen as the cure-all to phishing and online banking fraud**
- Institutions are deploying a range of solutions that protect customers with the minimum cost and impact on the user experience
- **More and more Australian start-ups are entering the market as the problem grows and institutions look beyond traditional solutions**