

## Hacked security firm leaves Aussies vulnerable

Ben Grubb

March 21, 2011 - 10:48AM



RSA SecurID tokens. *Photo: [Flickr/Bruno Cordioli](#)*

Hundreds of thousands of cryptographic tokens used by Australians who bank online, the Defence Force and other large corporations are vulnerable to a potential hack attack after a supplier revealed secret data it held had been stolen.

Customers of [RSA](#), a security division of the data storage giant [EMC](#), were on Friday told that the company had been the victim of “[an extremely sophisticated cyber attack](#)”.

Federal government customers of RSA's affected [SecurID service](#) include the Department of Defence, Department of the Prime Minister and Cabinet, Australian Electoral Commission, Family Court of Australia, Department of Parliamentary Services, Department of Veterans' Affairs, Geoscience Australia, AusAid, Department of the Treasury and Crimtrac, according to closed tender documents listed on the [AusTender](#) website.

Known Australian companies that use the RSA token service include Westpac, Telstra and Virgin Blue.

A prominent security expert, Steve Gibson, [said](#) RSA customers should consider their RSA SecurID tokens "completely compromised" and insist upon their immediate replacement. Though RSA may not want to do this, Mr Gibson described it as "the responsible thing" to do, even if it was a "very expensive" exercise to undertake.

An RSA SecurID [cryptographic token](#) is a small, portable device which generates a dynamic digital security code that changes every 60 seconds. It is most commonly used together with a static PIN or password to access a computer system.

The idea behind it is that with two factors of authentication - a PIN (something you know) and the dynamically generated digital number (something you have) - the system is more secure. Many companies give the tokens to their employees as well as outside contractors and partner companies to give them secure access to internal computer systems.

To carry out a successful attack against a company, an attacker "would need to obtain its target device's public serial number as well as one or more current output samples, at a known time, to determine the current state of the device's 22-bit realtime clock," Mr Gibson speculated. "From that point on, an attacker could reliably determine the device's output at any time in the future."

RSA therefore needed to "step up to the plate and take responsibility for what has happened", Gibson said. "That means recalling every single SecurID device and replacing them all. No company can consider RSA's existing deployed SecurID devices to be secure."

In an [open letter to customers](#) on Friday, RSA said an investigation into the attack revealed that it had "resulted in certain information being extracted from RSA's systems".

It said data stolen was "specifically related to RSA's SecurID two-factor authentication products" and that the attack "could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack".

In a brief telephone conversation on Friday afternoon, Telstra's public key infrastructure specialist of perimeter security, Paul Lexa, said Telstra had "been in contact" with RSA. "I can say that but I can't say anymore," he added. Fairfax understands that Telstra is one of RSA's largest Australian customers, with it administering about 45,000 authentication tokens. It's also understood that about 7000 Westpac staff use them.

Airline Virgin Blue uses 1500 hardware-based RSA cryptographic tokens, according to a case study [posted](#) on the RSA website. As of 2004, Westpac had [issued 15,000 RSA tokens](#), mostly to business customers. It planned to issue an additional 60,000 over the 18 months following September 2004. As to what exact information was stolen from RSA remains unclear as the company hasn't exactly been very forthcoming about it - and understandably so.

Other than the open letter posted on the RSA website, the only other piece of information given to clients on Friday was two PDF documents with best practises a company should take to ensure it is secure. Seen by Fairfax, one was labelled "RSA SecurID security best practices summary" and the other "RSA SecurID authentication engine security best practices guide".

The documents provided steps companies should already be taking to ensure that their tokens are secure. The documents do not spell out what data was stolen.

"There's probably one key piece of information in the [documents provided to clients] which would protect against whatever vulnerability now exists due to the RSA security breach," said one Australian IT manager who wished to remain anonymous. "But RSA wouldn't want to tell us which one because that would be telling the world exactly what was stolen."

The IT manager said it would "be much nicer if [RSA] just explained exactly what happened and which key steps you should take to make sure you were protected".

**Do you know more? [bgrubb@smh.com.au](mailto:bgrubb@smh.com.au)**



**This reporter is on Twitter: [@bengrubb](#)**

Source: <http://www.smh.com.au/technology/security/hacked-security-firm-leaves-aussies-vulnerable-20110321-1c2i4.html>