DigitalIDNews
ONLINE AND DIGITAL IDENTIFICATION, SECURING WEB 2.0, PKI AND DIGITAL CERTIFICATES

September 8, 2011

# RSA Breach Threatens Trust in One-time Passcodes

## Experts affirm technology's security, viability

**By Zack Martin**

While there are many one-time passcode devices on the market, RSA's football-shaped key fobs are most often associated with the technology. In March a well-publicized hack of RSA's seed code for its SecurID solutions sent shockwaves through the ID community. It led to attacks on the company's end users, including military contractor Lockheed Martin.

RSA has responded to the incidents by expanding its security remediation program. This program offers best practices and further expands two separate options to help assure customers' confidence:

- replace SecurID tokens for customers with concentrated user bases typically focused on protecting intellectual property and corporate networks.

- implement risk-based authentication strategies for consumer-focused customers with a large, dispersed user base, typically focused on protecting Web-based financial transactions.

While RSA has taken steps to ease the burden of the hack, some say it should never have ever happened. This is the position of Kenneth Weiss, developer of the token-based authentication technology that became SecurID 25-years-ago.

"When I was running RSA, every few years a well-intentioned member of the executive team would suggest that the secret seeds, which are programmed into every token, be stored on a corporate computer," he says. "I would have to explain that that was grossly unnecessary and would put us at great risk."

At the time of the March hack, RSA had indeed put the seeds on a network computer and it was breached. "What they've done is stupid, arrogant, greedy … those words are really appropriate to the circumstance," he says.

"There was no necessity, ever, to put the secret seeds on a computer that is online," he adds. "They did it for internal convenience and put everybody at risk."

The seed is a random binary pattern that is unique to each token, Weiss says. The seed is tied to an algorithm that is used to create a random number that changes every minute. "If you have that seed, you can create a SecurID token," he says. "You may also need to capture a password, but in a major espionage situation which I think this breach was triggered by, you'll have the password as well."

Weiss is now the founder of Universal Secure Registry and is developing a solution that combines voice biometrics with one-time passcodes on mobile devices for three factor-authentication. While he says the breach of RSA is unforgivable, it doesn't affect the security of one-time passcodes. "The SecurID technology has never been breached in 25 years," he says. "There have been contests where large sums of money were offered for any hacker to break it, and there's never been any success.

The fault lies with the management of the information, not the technology, Weiss says. He compares it to a bank vault manufacturer who stored the combinations online. “If the combinations were stolen, you wouldn’t say there’s something wrong with the vault. You’d say there’s something wrong with the management of the company that would allow that type of information to be online and not in a secure computer that’s independent of online access,” he says. “That’s what happened with RSA.”

RSA is going to have some damage control to undertake and 40 million tokens to replace, says Mark Diodati, a research vice president at Gartner. But, he says, “the death of RSA has been greatly exaggerated.”

The underlying technology behind one-time passcodes remains unaffected, he says, noting this is the case for technology from other vendors and RSA tokens issued post-breach. “Tokens are secure as they ever had been,” he says.

Diodati does foresee a switch to other form factors though. In the future employees or customers won’t be issued a token, but instead will download an application to their mobile phone to perform the function that the token did, he says.

“OTPs are one solution for the enterprise, smart cards are the other,” Diodati says. “Smart cards are good for organizations that want convergence (a single credential for physical and logical access).”

It all depends on what the end user is looking for, Diodati says. For strong authentication on the desktop smart cards may be a better option than one-time passcodes. But for other applications, like remote access or logging into a virtual private network the tokens work just as well. Gartner is working on a roadmap that will walk organizations through whether smart cards or one-time passcodes are a better option.

Gemalto has found that there are two distinct groups of users after the RSA breach, says Ray Wizbowski, global senior director of marketing for the Security Business Unit at Gemalto. There are those who already wanted to move away from RSA and are using the breach as an excuse and those who say it as a wake up call and are considering a move to stronger authentication.

“Some are looking at one-time passcodes with new technology and in the case of companies that have already done OTP they are seeing what’s one step forward,” he says.

Gemalto offers the Ezio line of tokens, but organizations are considering smart cards and PIV-I as well, Wizbowski says.

“One-time passcodes will still be valid for (a certain) level of risk,” he says. “But when you start getting to more personal and private information we’ll see a move to stronger authentication be it hardware-based, software-based or the mobile handset.”

###

http://www.digitalidnews.com/2011/09/08/rsa-breach-threatens-trust-in-one-time-passcodes