NETWORKWORLD

June 29, 2011

Inventor of SecurID token has new authentication system

Kenneth Weiss says technology designed for mobile phones, payments and the cloud

by Ellen Messmer

The inventor of the two-factor authentication SecurID token says the latest technology he's come up with is better because it can be used with a voiceprint biometric, plus it can be deployed for purposes of secure authentication in mobile phones, payments and cloud computing.

"This is much more appropriate for emerging cloud technology and financial payments," says Kenneth Weiss, founder of Newton, Mass.-based Universal Secure Registry, says of his company's electronic wallet. The core technology hasn't been deployed in products or services yet, but Weiss says the various elements, which also entail a server component to authenticate the user's identity, is stronger than SecurID because it not only provides a one-time password but can verify identity based on the user's voice biometric for three-factor authentication.

"You enter a PIN and voice, and only then does the unique seed inside the phone produce a random number," says Weiss, who hopes to license the technology.

Part of the core technology in the Universal Secure Registry strong-authentication system relies on the SecurID token technology patents that are now in the public domain, Weiss says.

SecurID has been much in the news since RSA acknowledged earlier this year that it had suffered a stealthy attack into the RSA network in which the attacker managed to steal undisclosed sensitive information related to SecurID. That information was later used by the attackers to try and break into Lockheed Martin. Weiss says the sensitive information at stake is the seed values for the two-factor authentication system associated with SecurID customers.

"The seed is the logical equivalent to a combination to a vault," Weiss says. "Their secret seeds were compromised." Basing an attack on stealing this kind of information would not necessarily be easy because the determined attacker would be trying to emulate a SecurID token, and they'd have to steal a password as well, he said, but it could be done.

Weiss contends that his USR design is better because seed values can be updated at periodic intervals, and "it's a stronger algorithm" than the RSA SecurID, and the password-digit combination is 16 digits long rather than just eight. He believes that despite the infiltration into the RSA corporate network, SecurID remains fundamentally sound "but there are many things it cannot do."

Weiss adds he and RSA, now part of EMC, aren't on particularly congenial terms because of a dispute over certain business practices he objected to vehemently in the 1990s when he was founder of Security Dynamics, which acquired RSA Data Security. The security industry has gone through many permutations since then, and Weiss is out to prove his latest technology feat will outdo his first.

###

http://www.networkworld.com/news/2011/062911-kenneth-weiss-securid.html?hpg1=bn