

June 30, 2011

## **L'inventeur du token SecurID crée un nouveau système d'authentification**

**Kenneth Weiss, l'inventeur du système de token à deux niveaux SecurID dit avoir mis au point une nouvelle technologie d'authentification, meilleure que la précédente.**

**by Jean Elyan (via Ellen Messmer)**

La nouvelle technologie d'authentification de Kenneth Weiss, qui utilise en plus la biométrie vocale, pourrait être déployée pour sécuriser les paiements mobiles, les transactions bancaires et le cloud computing. « C'est beaucoup plus approprié pour la technologie cloud émergente et les transactions financières, » a déclaré l'ancien fondateur de Security Dynamics Technologies, devenue RSA. Pour l'instant, cette technologie n'a pas encore été déployée dans des produits ou des services, mais l'inventeur explique que les différents éléments de cette technologie, parmi lesquels on trouve aussi un composant serveur pour authentifier l'identité de l'utilisateur, sont plus puissants que le système SecurID précédent, car elle ne se contente pas seulement de livrer un mot de passe à usage unique.

Elle vérifie l'identité de l'utilisateur en réalisant une analyse biométrique vocale, ce qui en fait un système d'authentification à trois niveaux. « Vous entrez un code PIN, vous parlez, et ensuite, la séquence de code unique à l'intérieur du téléphone produit un nombre aléatoire, » explique Kenneth Weiss, qui espère bien vendre sa technologie sous licence via son entreprise nouvellement créée Universal Secure Registry (USR). « Une partie de la technologie au coeur de ce système d'authentification repose sur des brevets de token SecurID désormais dans le domaine public, » a expliqué l'inventeur.

### **Une sécurité compromise chez RSA**

SecurID a beaucoup attiré l'attention ces derniers temps, depuis que RSA a reconnu que ses réseaux avaient été piratés et que les attaquants fussent parvenus à dérober des informations sensibles relatives à la technologie SecurID. Ces éléments ont été ensuite utilisés par les pirates pour essayer de s'introduire dans les systèmes de Lockheed Martin. Selon Kenneth Weiss, les informations confidentielles en question concernent les

générateurs de code du système d'authentification à deux facteurs, chacun étant associé à un client SecurID unique. « Ces séquences sont comme des combinaisons de coffre-fort, » explique le CEO de RSA. « Ces générateurs de séquences secrètes ont été compromis ».

Cependant, monter une attaque avec ces informations ne serait pas forcément facile, parce que même un attaquant déterminé, qui tenterait d'imiter un jeton SecurID, a également besoin d'un mot de passe. « Mais ce serait possible ». Kenneth Weiss affirme que la conception de l'USR est meilleure parce que les valeurs des semences peuvent être mises à jour à intervalles réguliers, et « son algorithme est aussi plus puissant » que celui de SecurID. La combinaison qui sert de mot de passe comporte 16 chiffres au lieu de 8. Cependant, celui-ci reste convaincu que, malgré l'intrusion dans le réseau de RSA, SecurID reste fondamentalement fiable, même si « il y a beaucoup de choses qu'il ne peut pas faire ».

### **Repartir sur d'autres bases**

Le CEO ajoute qu'entre lui et RSA, devenue une division sécurité au sein d'EMC, les relations n'étaient pas très bonnes, à cause d'un différend sur certaines pratiques commerciales : dans les années 90, au moment où il a créé Security Dynamics, qui a ensuite acheté RSA Data Security, il rappelle qu'il s'était vivement opposé à ces pratiques. Depuis, l'industrie de la sécurité a subi de nombreux changements, et Kenneth Weiss est là pour prouver que sa dernière technologie va dépasser la précédente.

*Illustration principale: Kenneth Weiss, CEO d'Universal Secure Registry (USR)*

---

### **TRANSLATION:**

#### **Inventor of SecurID token has new authentication system**

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

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.lemondeinformatique.fr/actualites/lire-l-inventeur-du-token-securid-cree-un-nouveau-systeme-d-authentification-34101.html>