THE WALL STREET JOURNAL.

December 16, 2013

Inventor of RSA's SecurID Wins Patent on New Cybersecurity System

by Steve Rosenbush

Kenneth P. Weiss, the entrepreneur who invented the computer password devices that millions of people carry with them daily, told CIO Journal that he has received a patent on a next-generation cybersecurity system.

Dr. Weiss said the new system combines three layers of security, making it almost impossible to defeat. It employs aspects of the SecurID password system, now owned by EMC Corp. EMC +1.69%'s RSA Security, with unique identifying characteristics that are part of each person's body, as well as unique codes found in their smartphones. The patent has been awarded and will be published on Dec. 17, according to Dr. Weiss.

The new system will be much more secure than SecurID, according to Dr. Weiss. The new system may have applications beyond computer passwords. Other possible uses might include vehicle access, payments and building security. The U.S. Patent and Trademark Office is expected to officially award the patent to Dr. Weiss on Dec. 17. He plans to bring the product to market during the first or second quarter of next year, through Universal Secure Registry LLC, of which he is the founder and CEO.

The strategy is to introduce the product, known as USRID, as an inexpensive app on the Apple Inc. and Google Inc. app stores. "I think that in the next 10 years, you will use one technology, one device, to identify yourself. You won't need to carry around all kinds of devices, or keys, and a wallet with credit cards," Dr. Weiss said. "I hope it will be my technology."

Over the years, the security devices known as "fobs" have become standard issue in many corporations. Each user is assigned a permanent personal identification number, usually four digits or longer. But that code is only part of the numerical password. The second, variable, part of the password is generated at regular intervals by an algorithm inside the fob. Only the combination of the two numbers can unlock the computer.

That might seem like a secure system, but in an age of increasingly powerful code-cracking capabilities, even stronger protections are necessary, according to Dr. Weiss.

In 2011, the New York Times reported that an intruder stole digital information from RSA that "related to RSA's SecurID two-factor authentication products." In September 2013, there were concerns RSA Security cryptography components had been weakened by the NSA, although RSA later issued a statement saying "under no circumstances does RSA design or enable any backdoors in our products."

His new system adds layers of security. And while it is more complex, a higher degree of automation could make it easier to use.

In this system, the fob disappears and is replaced by the smartphone. The idea is that the user will wake up in the morning, and enter a fingerprint and a password into the phone to authenticate him or herself, and then boot up the USRID app. The system assumes that all phones used in this way will have biometric capability.

As soon as the user is in range of his or her computer, the phone will transmit a 16-digit code that unlocks the computer. The code is updated every 30 seconds. If the user steps away from the computer, the computer will be locked after a moment or two, and unlocked as soon as the user is once again in range. The system requires that the user carry a smartphone at all times. The smartphone also has a unique code that is necessary to authenticate the identity of the user, who is turn must use a biometric measure to log into the phone.

How secure is the system?

Dr. Weiss said that the odds of defeating the 16-character code—never mind the biometric security or the mobile phone password—are three in 180 billion.

###

http://blogs.wsj.com/cio/2013/12/16/inventor-of-rsas-secureid-wins-patent-on-new-cybersecurity-system/