AMERICAN BANKER
On Focus and In Depth

Breach at RSA Security May Threaten Bank Systems

American Banker | Friday, March 18, 2011

By Jeremy Quittner

A severe security breach at EMC Corp.'s RSA Security may threaten the thousands of banks that use its technology.

Most banks secure online banking access and other systems with RSA's technology. The company is best known for its one-time passcode generating tokens, though many banks also use its software to invisibly protect their websites.

Without disclosing the exact scope of the breach, RSA indicated that it is a serious and far-reaching threat. Experts said the break-in demonstrates a weakness of passcode tokens, and advised banks to begin migrating to a multi-layered approach to protect their systems.

"This is an enormous deal, and you have to assume the worst case," said Avivah Litan, a vice president and distinguished analyst at the research firm Gartner Inc., in Stamford, Conn.

"If the criminals got the master key, they could use it to create unauthorized cards or counterfeit tokens and then steal passwords and create their own one-time passwords," Litan said.

RSA disclosed the breach to customers in a letter it posted to its website Thursday.

"Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA," Art Coviello, chief executive of RSA, said in the letter. "Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products."

Coviello went on to say that the information could "reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack." He said RSA is actively communicating with customers, providing them with immediate steps to strengthen their implementations of SecurID.

EMC, of Hopkinton, Mass., said it would not comment further on the break-in.

RSA. located in Bedford, Mass., is one of the largest security vendors in the world. Upwards of 90% of U.S. banks use RSA's technology in some part of their business, according to Aite Group LLC in Boston.

RSA's one-time passcode tokens lets users authenticate their online banking transactions with a string of numbers code generated roughly every 60 seconds. It is primarily used with employees or with corporate banking customers, though some banks offer it to consumers.

Coviello described the attack as an Advanced Persistent Threat. Researchers said that means the threat was likely a combination of hacking and some form of malware that would have burrowed deep into RSA's corporate computer systems, and which is extremely difficult to root out once it has been discovered. Researchers also speculated that this type of attack was an inside job conducted by a current or former knowledgeable employee, or that hackers had exploited a previously unknown software vulnerability.

The New York Times reported in a story March 17 that it is possible criminals might have stolen an internal "master key," from which it might be possible to gain access to the corporate networks and computer systems of banks.

With that knowledge, George Tubin, a senior research director with TowerGroup, Needham, Mass., said it might be possible for criminals to know the randomly generated passwords of corporate clients. Criminals could then "go in and impersonate you logging into your system because [they'll] have that one-time password," Tubin said.

Experts said the breach demonstrated the need for banks to have a multi-layered approach to security, as will almost certainly be mandated when Federal Financial Institutions Examination Council issues its guidance later this year on what banks must do to protect the security of online transactions.

Many of the banks that use RSA's technology today with consumer online banking do so because of a 2005 mandate from the FFIEC that they require stronger authentication than a simple username and password. Most banks that chose passcode tokens offered them only to wealthy consumers or business clients, due to the cost of deploying them and the potential they had to disrupt the online experience by adding a step during every login.

For most consumers, banks chose to use software to identify whether a user is connecting from a trusted computer or a low-risk location. This method is largely invisible to the end user.

"Banks should be doing now what they should have been doing a long time ago, which is looking at deploying multiple layers of protection based on the levels of risk of the transaction," said Julie Conroy McNelley, a senior risk and fraud analyst for Aite.

McNelley said that in addition to passwords and device identification, corporate clients should consider using specialized keys, hardened browsers, behind-the-scenes analysis of transaction behavior and setting dual controls.

Other observers said the attack on RSA demonstrated the ineffectiveness of tokens.

"Banks should already be aware the token is pretty much rendered useless as second factor of authentication," said Jacob Jegher, a senior analyst at the research firm Celent. "This is yet another nail in the coffin for the token."

Litan added that tokens are susceptible to the same kind of intermediary attacks leveraged by the Zeus Trojan, which hijacks browser sessions during the legitimate user's online banking activity.

"One-time tokens can be compromised," Litan said.

Besides ramping up security procedures, experts said banks using SecurID should definitely consider contacting their clients about the potential threat to their accounts.

"Knowledge is power, and the more their customers know they are not bullet-proof with a token, the more measures they can take," McNelley said.

In addition to Coviello's letter to customers online, RSA also included in an 8-K filing Thursday with the Securities and Exchange Commission a note that said it did not think the breach would have a financial impact on the company.

Andrew Johnson contributed to this story.
