SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

March 20, 2011

RSA Breach: Reactions Pour in, Many Questions Remain Unanswered Following SecurID Attack

by Mike Lennon

After notifying customers on Thursday that it had been breached after hackers mounted a highly sophisticated cyber attack that put its **SecurID** product at risk, **RSA** has yet to expand on the details and potential impact of the attack, leaving customers concerned and with many questions.

Since disclosing the event, information coming from RSA been extremely limited and vague, and despite attempts to get further information from RSA on the incident, the company has remained quiet while it continues its investigation and works with authorities.

In the meantime, reactions are pouring in from customers and the information security community in general, some saying to prepare for the worst, and some brushing it off as not-so-serious incident. Based on what RSA has shared so far, it’s a tough call, and until the company shares more, it’s really tough to tell what customers should expect and what measures will need to be taken.

Stephen Northcutt, CEO of the SANS Institute, doesn’t believe the incident is a game changer. “It's serious news that RSA's SecurID solution has been the target of an advanced persistent threat. But It's not a game-changer. Anybody who says it is [a game-changer] is an alarmist,” Northcutt told Bankinfosecurity.

Steve Gibson of Gibson Research thinks otherwise, and in a blog post writes, “If ‘the keys to the kingdom’—the public serial number to secret key mapping database—had **NOT** been compromised, there would be **zero** danger to users of RSA’s SecurIDs. But we know at least that the danger is not zero. **Therefore, the most reasonable conclusion to reach is that RSA believes that at least some of ”the keys to the kingdom**” have been compromised. (Because that’s their system’s only real vulnerability.)”

I reached out to **Kenneth Weiss**, the original inventor of the SecurID technology for comment. Here’s what Weiss had to say: "The SecurID technology I designed and patented has never been breached in 25 years of use. This unfortunate breach of security at RSA speaks to the quality of their internal security not the security of the SecurID token. The possession of 40,000,000 random SecurID seeds is meaningless unless a subset can be associated with a particular one of 30,000 worldwide clients and then in turn directly associated with a particular client user. Even if such identification were possible, an attacker would also have to know the particular user's PIN. This information is not stored on RSA computers." Weiss is now CEO of Universal Secure Registry, a company that recently emerged from stealth mode.

RSA's Art Coviello, in his "Open Letter to RSA Customers," on Thursday, wrote that "While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack."

“Attackers are exploiting rapidly multiplying network access points, that represent very real targets and often provide the powerful access that leads to damaging data breaches,” Adam Bosnian, EVP of Americas and Corporate Development at Cyber-Ark told *SecurityWeek*. “We need to wait and see what emerges from this latest attack to see what vector was used – but we support and re-emphasize the response by RSA to its customers as it provides some valuable, current and real-world lessons every organizations need to follow.”

A briefing from **NSS Labs** suggests this was a direct attack to steal the virtual keys used to power the SecurID tokens. “This was a strategic move to grab the virtual keys to RSA’s customers – who are the most security conscious in the world,” the briefing notes. “One or several RSA clients are likely the ultimate target of this attack. Military, financial, governmental, and other organizations with critical intellectual property, plans and finances are at risk.” NSS Labs, in its briefing, also said that it expects a string of breaches stemming from this event. “The locksmith’s secrets may have been stolen, and the integrity of RSA’s 2-factor authentication compromised.” What is especially concerning, the NSS briefing notes, is that if this is the case, attackers could be authenticated as a trusted user. “As such, existing security technologies, which look for 'intrusions', will not be able to detect this kind of attack. New detection and mitigation strategies will need to be formulated and implemented.”

In the Midst of Silence, What should Customers do?

Cyber-Ark’s Adam Bosnian emphasized the importance of enforcing the rule of least privilege for end-users and security administrators– the idea being to provide only that amount of privilege necessary for a given activity. “When applied to privileged accounts, those used by administrators or applications to access and manage key systems, applications and databases, it becomes a bit harder to do, since these powerful accounts often provide full, unfettered access to enterprise systems and applications. However, what’s often overlooked is how these accounts can provide unwanted ‘escalation of privileges’ for APT attacks These access points, often in the form of embedded or hardcoded passwords, exist in almost every networked system, application, database etc… We saw this recently with the Stuxnet virus – entering in through an embedded credential in a SCADA system, as well as in the Operation Aurora attacks on several companies source code management systems.”

Bosnian also adds, “While malicious outsiders and insiders have focused often on the administrative credentials on typical systems like servers, databases and the like, in reality, IT organizations need to identify every asset that has a microprocessor, memory or an application/process. From copiers to scanners, these devices all have similar embedded credentials that represent significant organizational vulnerabilities.”

“At the end of the day, the use of privileged access to exploit vulnerabilities such as hardcoded password is a very real threat that provides malicious hackers with new ways into the enterprise. It’s not just about ensuring that your system administrators are equipped with least privileged access, it’s something that ever company—security vendors and enterprises alike—needs to recognize and proactively guard against,” Bosnian tells *SecurityWeek*.

Dell SecureWorks notes that with the potential impacts from the RSA Breach, response efforts should focus on a few key areas, including:

• Direct attacks against an ACE server.

o Confirm current patch levels and general server hardening

o Monitor IPS/IDS logs

o Monitor server logs

• Brute-Force attacks attempting to determine the specific seed used for a given account's SecurID token, as well as attacks aimed at compromising other authentication factors.

o Monitor for repeat authentication failures, both on the ACE server and on intermediate appliances and systems

o Monitor for authentication failures not followed by success both on the ACE server and on intermediate appliances and systems

• Changes in source of authentication attempts.

• Multiple concurrent logins for a single account.

Dell SecureWorks also suggests that caution is also warranted surrounding the integrity of communication channels over which OTPs and tokencodes are submitted. Even under a conservative scenario where seeds were disclosed, but specific customer ownership was not, it may be possible to determine which seed is in use by observing a small number of submitted tokencodes. PINs can also be exposed through such observation. Considering these factors yields the following recommendations:

• Ensure OTPs are only submitted over encrypted channels.

• Be vigilant for phishing or impersonation schemes that may seek to capture OTPs.

• Educate users' expectations as to which systems prompt for OTPs to protect against phishing and social engineering attempts.

RSA Sent the following email to customers via its SecureCare program as well as a filing with the SEC.

Dear RSA SecurCare Online Customer,

Summary:

We have determined that a recent attack on RSA's systems has resulted in certain information being extracted from RSA's systems that relates to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. RSA urges immediate action.

Description:

Recently EMC's security systems identified an extremely sophisticated cyber attack in progress, targeting our RSA business unit. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is related to RSA's SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We strongly urge immediate customer attention to this advisory, and we are providing immediate remediation steps for customers to take to strengthen their RSA SecurID implementations.

Affected Products:

The affected products are RSA SecurID implementations. Overall Recommendations:

RSA strongly urges customers to follow both these overall recommendations and the recommendations available in the best practices guides linked to this note.

• We recommend customers increase their focus on security for social media applications and the use of those applications and websites by anyone with access to their critical networks.

• We recommend customers enforce strong password and pin policies.

• We recommend customers follow the rule of least privilege when assigning roles and responsibilities to security administrators.

• We recommend customers re-educate employees on the importance of avoiding suspicious emails, and remind them not to provide user names or other credentials to anyone without verifying that person's identity and authority. Employees should not comply with email or phone-based requests for credentials and should report any such attempts.

• We recommend customers pay special attention to security around their active directories, making full use of their SIEM products and also implementing two-factor authentication to control access to active directories.

• We recommend customers watch closely for changes in user privilege levels and access rights using security monitoring technologies such as SIEM, and consider adding more levels of manual approval for those changes.

• We recommend customers harden, closely monitor, and limit remote and physical access to infrastructure that is hosting critical security software.

• We recommend customers examine their help desk practices for information leakage that could help an attacker perform a social engineering attack.

• We recommend customers update their security products and the operating systems hosting them with the latest patches.

Steve Shillingford, President and CEO of **Solera Networks**, suggests that Network Forensics is key when incidents like this occur. "Breaches do occur and will continue," said Shillingford. "Next generation threats--APTs--are being specifically architected to subvert installed security defenses. Knowing the full extent of a breach is key to appropriately dealing with it."

Until RSA provides more information, the impact and required response will be difficult to predict. But we'll be keeping a close watch on yet another eye opening event in the industry.

###

http://www.securityweek.com/rsa-breach-reactions-pour-many-questions-remain-following-securid-attack