RSA confirms its tokens used in Lockheed hack

By William Jackson

Published: 2011-06-07 · Archived: 2026-04-06 00:43:53 UTC

By William Jackson,
GCN

| June 7, 2011

The complicated attack might have used log-in data obtained via a phishing attack along with algorithm seed numbers taken from RSA to generate new passcodes.

- Authentication

RSA Security has confirmed that stolen data about the company's SecurID authentication token was used in the recent attack against defense contractor Lockheed Martin. RSA has offered to replace the compromised tokens for high-risk customers.

The RSA breach, reported March 17, was the result of what the company called an "extremely sophisticated" attack. The company said that it believed the likely motive was to take data that could be used against defense contractors rather than against financial institutions or to steal personal information.

Art Coviello, executive chairman of RSA, the Security Division of EMC, wrote in **a letter** posted after close of business June 6 that other victims in a recent "unprecedented wave" of cyberattacks, including Epsilon, Sony, Google, PBS and Nintendo, were not related to the RSA breach.

Related stories:

After hack, security of RSA SecurID tokens in the hands of customers

Another major defense contractor hacked; RSA tokens likely involved

---

"It is important for customers to understand that the attack on Lockheed Martin does not reflect a new threat or vulnerability in RSA SecurID technology," Coviello said in the statement. "Indeed, the fact that the only confirmed use to date of the extracted RSA product information involved a major U.S. defense contractor only reinforces our view on the motive of this attacker."

There was no mention in the statement of the recent and similar attack against L-3 Communications, another major defense contractor, which is believed to have leveraged the same kind of data as that used against Lockheed Martin.

“Whoever attacked Lockheed Martin was the same as attacked RSA or had access to information from the RSA breach,” said Harry Sverdlove, chief technology officer of Bit9, an end-point security company.

The initial RSA breach was described by the company as an Advanced Persistent Threat that targeted information related to the SecurID two-factor authentication product.

Although details of that attack still have not been released, it is believed that information about the seed numbers used by an algorithm to generate one-time passcodes on the token was taken. The passcode is used together with a user’s log-in ID and personal identification code. Because the system generates a new one-time passcode every 60 seconds, they cannot be reused. The algorithm used to generate the codes is publicly available, but without the seed number it is not possible to duplicate the passcode sequence.

“Whoever attacked RSA has certain information” about the product, “but not enough to complete a successful attack without obtaining additional information that is only held by our customers,” the company said at the time the breach was reported.

But if a hacker with access to a list of seed numbers could obtain several passcodes from a token, they could be used to determine which seed number was being used, which could allow a hacker to spoof a legitimate new passcode. This, together with other stolen log-in data, could be used to obtain access.

This apparently is what happened with Lockheed Martin and L-3. Researchers believe that a keystroke logger was placed on a computer used for remote log-in, possibly through a spear-phishing attack, and was able to steal a user ID, PIN and several one-time passcodes.

Coviello said the company remains confident in SecurID and that remediation advice offered to customers is adequate.

“However, we recognize that the increasing frequency and sophistication of cyber attacks generally, and the recent announcements by Lockheed Martin, may reduce some customers' overall risk tolerance,” Coviello said in the statement. “As a result, we are expanding our security remediation program to reinforce customers' trust in RSA SecurID tokens and in their overall security posture.”

The company will replace SecurID tokens for customers “with concentrated user bases typically focused on protecting intellectual property and corporate networks.” For consumer-focused customers with larger, more dispersed user base RSA is offering to implement risk-based authentication strategies to protect Web-based financial transactions.
