US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Technical Information Paper-TIP-11-075-01
System Integrity Best Practices

The two key components of system integrity are **software authenticity** and **the assurance of user identity**. US-CERT recommends that organizations routinely evaluate how to integrate the following best practices into their current environments to achieve these objectives.

- Enable strong logging.
  - Enable logging for all centralized authentication services and collect the IP address of the system accessing the service, the username, the resource accessed, and whether the attempt was successful or not.
  - Limit the number of authentication attempts and lockout the user if the limit is reached. Security professionals should conduct a manual review before unlocking the account and prohibit automatic unlocks after a specified time period.
  - Conduct near real-time log review for failed attempts per user and per unit of time independent of successful logins; abnormal successful logins; and lockouts. Correlate this data to identify anomalous activity.
- Limit remote access.
  - Restrict access by IP address wherever possible.
  - Limit concurrent logins to one per user.
- Apply additional defense-in-depth techniques.
  - Maximize complexity of passwords, passphrases, and personal identification numbers (PINs) whenever possible.
  - Enable defenses against key logging such as forced frequent credential changing and updated anti-virus (AV) signatures.
- Validate software.
  - Require validation of vendor-provided hash values or digital signatures prior of installation. If information is not customarily provided, request validation guidance from the vendor.
  - Exercise additional caution when receiving unsolicited or unexpected software media.
  - Establish installation baseline (e.g., file names, versions, hash values) and periodically revalidate this information.
  - Enable revocation checking to include Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) checking.

Contact US-CERT

For any questions related to this paper, please contact US-CERT at:

E-mail: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/

Document FAQ

What is a TIP? A Technical Information Paper (TIP) is issued for a topic that is more informational in nature, describing an analysis technique, case study, or general cybersecurity issue. Depending on the topic, this product may be published to the public website.

If this document is labeled as UNCLASSIFIED, can I distribute it to other people? Yes, this document is intended for broad distribution to individuals and organizations interested in increasing their overall cybersecurity posture.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.

Open Letter to RSA Customers

Arthur W. Coviello, Jr.

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. 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 led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). 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. 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 are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

We have no evidence that customer security related to other RSA products has been similarly impacted. We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident.

Our first priority is to ensure the security of our customers and their trust. We are committed to applying all necessary resources to give our SecurID customers the tools, processes and support they require to strengthen the security of their IT systems in the face of this incident. Our full support will include a range of RSA and EMC internal resources as well as close engagement with our partner ecosystems and our customers' relevant partners.

We regret any inconvenience or concern that this attack on RSA may cause for customers, and we strongly urge you to follow the steps we've outlined in our SecurCare Online Note. APT threats are becoming a significant challenge for all large corporations, and it's a topic I have discussed publicly many times. As appropriate, we will share our experiences from these attacks with our customers, partners and the rest of the security vendor ecosystem and work in concert with these organizations to develop means to better protect all of us from these growing and ever more sophisticated forms of cyber security threat.

Sincerely,

Art Coviello
Executive Chairman, RSA

Security Firm Is Vague on Its Compromised Devices

By JOHN MARKOFF
Published: March 18, 2011

SAN FRANCISCO — More than a day after RSA security posted an "urgent" alert warning that a sophisticated intruder might have initiated a "broad attack" on a password device used by millions of customers, the announcement and its meaning remain shrouded in mystery.

RECOMMEND
TWITTER
SIGN IN TO E-MAIL
PRINT
REPRINTS
SHARE

Enlarge This Image

The New York Times
RSA didn't say how its SecurID tokens, carried on key chains and in wallets, were compromised.

RSA, a division of the data management company EMC Corporation, will not say how its system was compromised and what specific kinds of threats its customers are facing. But from its extremely limited disclosure on Thursday afternoon about what might have been taken, customers and computer security specialists are scratching their heads about what the risks may actually be.

There was wide bewilderment about the company's claim that the intruder was "extremely sophisticated," as it suggested that one of the nation's premier security firms had no better security than dozens of companies that have fallen victim to a computer break-in that deceives employees and exploits unknown software vulnerabilities.

On Friday, a spokesman for RSA said it was briefing its customers individually but added that its executives were declining to speak publicly about the breach.

The announcement touched off intense speculation about

Subscribe to Technology RSS Feeds

Technology News
Internet | Start-Ups | Business Computing | Companies

Bits Blog
Personal Tech
Pogue's Posts

MOST E-MAILED | RECOMMENDED FOR YO

We don't have any personalized recommendations for you at this time. Please try again later.

Log in to discover more articles based on what you've read.

PRESENTED BY

Log In | Register Now | Log In | What's This? | Don't Show

whether RSA's popular SecurID tokens, which are carried on key chains and in wallets of millions of corporate and government users, have been significantly compromised.

"It's a weird situation," said Dan Kaminsky, an independent Internet security specialist. Referring to the Tokyo Electric Power Company, he said, "It's like the Tepco situation in Japan, but here everyone is freaking out" and "nobody has Geiger counters."

The system is intended to provide additional security beyond a simple user name and password by requiring users to append a unique number generated by the token each time they connect to their corporate or government network.

A potential weakness that could be exploited involves a factory-installed key called a seed. Typically 16 characters, it is different for each token and is stored on a corresponding computer server program, which authenticates the session each time a user connects to a secure network.

If the database containing customers seeds was taken, the intruder might still not know which user had which seed, but cryptographers said it would be possible to use a reverse-engineered version of the RSA algorithm to determine that information by simply capturing a single log-in session. That would be a potentially serious vulnerability that could be exploited by a sophisticated attacker.

A technical expert in New York whose financial services firm uses the SecurID system said that even after listening to a telephone briefing on Thursday evening, he was uncertain about which potential threats he should be concerned about.

The company offered only extremely general "belt and suspenders" advice, the expert said. A copy of the company's terse "RSA Securcare Online Note" posted on the Securities and Exchange Commission Web site on Thursday offers such advice as "Focus on security for social media applications" and "We recommend customers re-educate employees on the importance of avoiding suspicious e-mails."

RSA notified the federal government, whose agencies widely use the tokens to guard access to its networks, some time before the public announcement was made. On Wednesday, the Computer Emergency Readiness Team in the Department of Homeland

Security posted a “Technical Information Paper” on its Web site describing a set of security practices meant to limit vulnerability to attacks based on the stolen information, according to a person close to the organization.

“We have notified all of the federal agency chief information officers to take remediation steps,” said a government official who declined to be identified because he had not been authorized to speak about the breach.

What the actual risk is and what precautions a user of the key fobs and wallet-size cards depends on what was taken in the theft.

“I’m speculating, but I’m pretty confident that somebody has the root seed file,” said a former RSA employee, referring to the master file at the company, which is based in Bedford, Mass. He asked not to be identified because he still has a business relationship with the firm.

The worst case, many security consultants say, is that the vulnerability created by the theft might require companies to replace the secure tokens, which, according to analysts, cost $15 a year or more to maintain. The vulnerability might also force RSA to rethink the design of its SecurID system.

“They may have to change their security model to one where a third party does not hold the keys to your devices,” said Paul Kocher, president of Cryptography Inc., a San Francisco computer security consulting firm.

A version of this article appeared in print on March 19, 2011, on page B3 of the New York edition.