



*4600 Montgomery Road, Suite 400*

*Cincinnati, OH 45212*

*Phone 513.841.5000*

*Fax 513.841.5072*

## **The RSA SecurID Compromise: Analysis & Response**

*Justin Hall, CBTS Information Security*

*Originally published on March 24, 2011*

*Last updated June 7, 2011*

# Executive Summary

## What happened?

RSA Security announced an intrusion into their systems, where information about their SecurID product was stolen by sophisticated attackers. The company proceeded to warn their customers to monitor for suspicious activity and take extra precautions to protect their critical systems and data.

## What was stolen?

In an open letter to customers, RSA confirmed that “certain information” about SecurID tokens was stolen. Based on an analysis of recent attacks involving duplicated tokens, it can be concluded that serial numbers of tokens, and seed records that are used to calculate tokencodes, were stolen.

## What steps should we take?

Contact RSA to discuss replacement of compromised tokens. Customers should identify the systems and data that are protected by RSA SecurID and Authentication Manager, and begin to monitor both the Authentication Manager logged events, as well as the protected systems, for suspicious activity. Users of the SecurID product, as well as any individual with the ability to view or change credentials used by SecurID, should be made aware of modern phishing and social engineering techniques employed by attackers to steal credentials. Controls that protect the Authentication Manager database, as well as other enterprise authentication systems that may tie into Authentication Manager, should be reviewed to ensure that unauthorized access is restricted, and authorized access is constantly monitored.

## Should we switch to another two-factor authentication system?

Token-based systems from other vendors could be safer, while continuing to offer the combination of increased credential strength and flexibility of deployment that has made it the primary choice for enterprise two-factor authentication systems. The cost of migration, as opposed to continued operation of SecurID, could be extensive depending on the number and complexity of systems currently protected by SecurID.

Other two-factor authentication systems, such as those that employ certificates, biometrics, or smart cards, may appear appealing if trusting a vendor to protect token records no longer seems viable. However, an organization must consider not only the technical cost of replacing the backend two-factor authentication product, but also the cost per client, as well as user adoption challenges.

# Detailed Analysis

## Initial Disclosure by RSA

On Thursday, March 17, in an open letter to its customers, RSA Security announced that they were the victim of “cyber attack”. Specifically, they indicated that the attackers obtained access to information that was “specifically related to RSA's SecurID two-factor authentication products” and that the information “could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack”.

Notes posted to RSA's SecurCare Online support portal offered no further disclosure on the nature of the stolen data. The notes did offer recommendations to their customers on increased security measures that should be taken in light of the attack. Most of these revolved around monitoring and response – identifying suspicious activity and investigating, with particular focus on enterprise authentication systems.

## Possible Scenarios

Widespread speculation about the nature of the data that was stolen began almost immediately among members of the information security community. In their open letter, RSA claimed that “the attack is in the category of an Advanced Persistent Threat (APT)”. We will assume RSA is adhering to the original definition of this class of threat actors – as coined by the Air Force in 2006 – and not the definition adopted by security vendors in 2010, which uses the term to any sophisticated human intruder that employs modern malware as an attack vector.

APT refers to a specific set of threat actors – professional hackers, most likely state-sponsored, whose goal is the theft of intellectual property. Richard Bejtlich's article *Understanding the Advanced Persistent Threat* is recommended reading to learn more about these actors. If APT is truly responsible for this attack, it furthers certain conclusions we can draw about the target of the intrusion and, as a result, how an RSA customer should respond.

APT traditionally seeks methods to bypass security controls that stand as obstacles to their target data. In this case, RSA's SecurID product is a widely deployed two-factor authentication system that is often used to protect access to critical systems and data. To successfully authenticate to this system and access the protected systems or data, one must possess not only a user-specific password, but a physical or virtual token that generates a temporal code. This tokencode changes frequently – normally every 30 to 60 seconds – and is generated using a hashing algorithm that uses the current time, the token's serial number, and a secret key (known as a “seed record”) that is unique to the token. This makes guessing the tokencode extremely difficult.

If an attacker wanted to authenticate as an authorized user, they would need a valid user ID, password, and the ability to guess the tokencode. As RSA does not store user ID's or passwords for their customers, this data would not be targeted by attackers when conducting operations against RSA. The only data possessed by RSA would be the serial numbers and seed records that are used in conjunction with the publicly available algorithm to calculate the tokencode.

## Attacks Lead To Further Disclosure

On May 21, 2011, defense contractor Lockheed Martin was targeted by unspecified attackers in an intrusion attempt. Press reports, and later an open letter from RSA to their customers, confirmed that the attackers were able to duplicate Lockheed's SecurID tokens using the data stolen from RSA. These duplicate tokens were used, along with information about user ID's and passwords obtained in auxiliary phishing and malware campaigns (which were disclosed in a Reuters news article about the attack), in an attempt to obtain unauthorized access to Lockheed's network.

On June 6, 2011, RSA published another open letter, confirming the Lockheed attack and the use of stolen data by the attackers. In the letter, RSA offered to replace SecurID tokens for "customers with concentrated user bases" and to "implement risk-based authentication strategies for consumer-focused customers with a large, dispersed user base".

The use of duplicate tokens in an actual intrusion attempt, along with RSA's offer to replace tokens, leads us to conclude that existing RSA SecurID tokens, deployed in production by RSA customers, can no longer be relied upon to provide unique authentication capability to their users. While no direct confirmation that token serial numbers and their seed records were stolen has come from RSA, the theft of this data can be inferred from an analysis of the Lockheed intrusion attempt.

If the attackers already possessed the token serial numbers and seed records, the only remaining information they would need to successfully authenticate would be:

- A valid user ID and password
- Knowledge of which token was in use by that user, i.e. the token's serial number

The attacker tricks the user into disclosing at least the user ID and their token's serial number. At this point the attacker can calculate the tokencode that shows up on the user's token without actually possessing the token. They only need to guess the user's password to successfully authenticate. A further attempt to trick the user into disclosing their password as well would provide the remaining information necessary to authenticate.

As RSA has broadly offered to replace tokens, and not limited this offer to specific customers, it can be assumed that serial numbers and seed records for the entire set of customer tokens were stolen. SecurID customers should take immediate action to ensure their users' tokens have not been duplicated.

## Mitigation Strategy

Based on bulletins published by RSA, and our research into the attack, we recommend customers that operate SecurID deployments take the following steps to mitigate the risk introduced by this incident:

**Replace existing SecurID tokens.** Contact your local RSA sales team, or RSA Security directly, to begin the replacement process. Assess the cost of replacement and map a replacement strategy.

**Protect the SecurID Authentication Manager application and backend database.** The database used by Authentication Manager stores credential information that, if available to an attacker that possessed the ability to generate tokencodes, would allow that attacker to access resources protected by SecurID two-factor authentication.

? Which users are authorized to perform maintenance and administration of the Authentication Manager system – including accessing the system with elevated privileges, perform database backups, or create entries in the database?

! Monitor the Authentication Manager system's audit logs and investigate any suspicious activity, especially by users with elevated privileges. Disable the use of any administrative privileges that are unnecessary.

? How is access to the database controlled? What credentials allow querying of the database? Who has physical or remote access to the server on which this database is stored?

! Monitor access to the database service, raw files, backups, and the server on which they are stored. Investigate any suspicious activity. Disable the use of any administrative privileges that are unnecessary.

**Review resources – systems and data – that are protected by SecurID.** This may include remote access systems, wireless network access, critical servers, or network infrastructure. Attackers with capability to bypass SecurID controls may attempt to target these resources.

? What resources do users need a tokencode to access? What would happen if an unauthorized user was able to access those resources? What data would be of interest to an attacker interested in gaining competitive economic or political advantage?

! Monitor resources for unauthorized or suspicious access. This could include user accounts attempting to exceed permitted access, or elevated activity from users with elevated privileges.

! Monitor critical systems for suspicious activity. This could include applications or services stopping and starting unexpectedly, installation or removal of services, changes to system files, or creation of local user accounts.

! Monitor the network perimeter for unusual activity. This could include tunneled traffic, sessions with unexpected remote hosts, unusual protocols or high volumes of traffic, or sessions occurring at unusual times of day.

! Audit successful and failed attempts to access critical data – files, databases, and content management systems, for example. Limit access to this data to only those that absolutely require it.

! Monitor SecurID authentication logs for failed authentication attempts and “next tokencode” events, which suggest that the user supplied the correct user ID and password with an invalid tokencode. This could indicate an attacker attempting to guess a valid tokencode.

! Enforce strong PIN/password policies in SecurID. Strong PIN length, strength, age, and history requirements, along with a low lockout threshold, should be enforced.

**Review authentication systems that are used in conjunction with SecurID**, such as Active Directory or RADIUS services. If an attacker is able to obtain valid credentials from these systems without the knowledge of the user, they could use the credentials along with the tokencodes to impersonate an authenticated user.

? What authentication systems tie into the SecurID deployment? What controls protect the stored credentials of those systems? Are they vulnerable to attack? Have they been patched or updated recently?

! Ensure authentication systems are running the most recent code release and are patched in a timely fashion. Monitor administrative access to these systems for suspicious activity – this could include frequent authentication failures or an unusual pattern of successful authentication, frequent password resets, or activity from unexpected hosts.

! Enforce strong password policies on authentication systems. Strong password length, strength, age, and history requirements, along with a low lockout threshold, should be enforced.

**Review the state of user awareness** concerning modern techniques employed by attackers to deceive users into disclosing their credentials. If an attacker is able to obtain valid credentials from a user, they could use the credentials along with the tokencodes to impersonate the user.

? Are users, as well as technical staff with access to create or change credentials, aware of recent trends in phishing and social engineering, including email, phone, and social networking attack vectors? Are controls in place to restrict access to known or suspected phishing websites, and to filter suspicious email content?

! Conduct user awareness campaigns to educate employees on phishing and social engineering attacks. Warn users against any disclosure of credentials or information about their token, such as the serial number or tokencode. Encourage users to report any suspicious activity, including emails, phone calls, IM communication, and social networking communication, where an individual attempts to coerce this information.

# Alternative Solutions

## Other Token-based Two-factor Authentication Systems

This incident may significantly impact RSA customers' confidence in the organization to provide a secure token-based two-factor authentication solution. While the lack of detail provided to customers up to this point has resulted in frustration and disillusionment with RSA, it also means that customers may not have sufficient information to properly weigh the cost of migrating to a different vendor.

RSA has offered to replace tokens for customers with "concentrated user bases", which can be interpreted as "small numbers of tokens". Depending on the number of tokens an organization has in use, RSA may not offer to replace them all. Instead they may offer to assist the organization with authentication system redesign and improved monitoring, in an effort to assure the customer that the tokens in use are still trustworthy.

If these assurances are insufficient to restore the customer's trust, they may still investigate migrating to another vendor. Note that any migration will almost certainly require replacement of tokens, and as a result the customer will not avoid the cost of that replacement activity. A review of the replacement vendor's internal security practices should also be considered, to ensure that a vendor with a weaker security posture than RSA is not selected.

A full review of the existing SecurID deployment should ensue, identifying all systems that rely on or interact with SecurID products. Compatibility with these systems should be reviewed with the replacement vendor. A cost analysis should be performed by IT staff, encompassing the new product itself, operational time and effort for replacement, hardware cost, productivity impact, training, professional services, and ongoing maintenance and administration workload change.

If a decision is made to begin migration, a deployment plan should be developed and phases of evaluation and testing should be considered before production systems are addressed.

## Other Two-factor Authentication Systems

Due to the necessity of the token manufacturer retaining token records that could cause exposure if compromised, customers may no longer trust the technology to provide reliable controls for their organization. Other two-factor systems have unique strengths and weaknesses that contribute to their relative popularity in comparison to token-based systems.

### Certificates

Possession of an electronic certificate, acting as the "something you have" piece of two-factor authentication, is used in many cases where the cost and complexity of using tokens is not viable. Certificates present many of the same risks of theft as software-based tokens, namely, if an endpoint

holding a certificate is compromised by an attacker, it is possible that the certificate can be stolen and used for future authentication. A physically separate certificate would help mitigate this risk – stored on removable media or on a smart card.

## **Smart Cards**

A smart card, distributed to individual users, usually contains a secret key embedded in a chip that is passed along with a set of credentials for authentication. Unlike a token code, this key does not change, making interception of the key by a third-party a risk. Physical separation from the client is beneficial, but introduces the possibility of theft or loss, and the cards are often expensive to replace. Card readers also add to the per-client expense of deployment, and may multiply if smart cards will be used in more than one location – for example, from a desktop in an office, as well as a home PC.

## **Biometrics**

Biometric keys – normally based on a user's fingerprint, retina, or facial recognition – offer benefits over hard tokens or smart cards. As they rely on the user's physical person, they are extremely difficult to 'lose'. The cost of implementing the biometric reader hardware was a significant adoption barrier at one point, although many modern laptops and desktops now include readers. Occasional reports of slow performance of scanning and verifying the fingerprints has caused hesitation and has likely contributed to a lack of widespread use. This mechanism is also vulnerable to replay attacks, where the key is recorded (i.e. a user's fingerprint is copied) and re-used without the user's knowledge.

# **Final Thoughts**

It is regrettable that RSA was unable to protect its data properly, and as a result its customers are facing, at a minimum, replacement of some or all of its tokens. We do not believe sufficient information is available about the compromise at RSA to warrant a customer's migration to a new product. Customers should continue to communicate with RSA, and use the output of those discussions to develop a strategy to mitigate the risk introduced by the compromise.

The security controls and monitoring recommended as a response should, in some form, already be a part of any organization's information security practices. Customers may want to seek outside assistance from a third-party security consultant to meet these recommendations, as well as to assess the state of the controls that protect their critical systems and data. The most important control to remember is the end-user – they must understand that disclosure of credentials or token information will present significant risk to the organization and must be guarded against constantly.

SecurID customers are still able to protect themselves. This incident may encourage security practitioners to strengthen elements of their organization's security program that haven't received adequate attention in the past.

## For More Information

Bejtlich, Richard. "Understanding the advanced persistent threat."

[http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14\\_gci1516312,00.html](http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1516312,00.html)

Bellovin, Steve. "The RSA SecurID problem." <http://www.cs.columbia.edu/~smb/blog/2011-03/2011-03-18.html>

Coviello, Art. "Open Letter to RSA customers." <http://www.rsa.com/node.aspx?id=3891>

Markoff, John. "Security Firm Is Vague On Its Compromised Devices."

<http://www.nytimes.com/2011/03/19/technology/19secure.html>

Finkle, Jim and Andrea Shalal-Esa. "Hackers breached US defense contractors."

<http://www.reuters.com/article/2011/05/27/us-usa-defense-hackers-idUSTRE74Q6VY20110527>

Bright, Peter. "RSA finally comes clean: SecurID is compromised."

<http://arstechnica.com/security/news/2011/06/rsa-finally-comes-clean-securid-is-compromised.ars>

**Disclaimer:** This publication is © 2011 CBTS. All rights reserved. CBTS is a registered trademark of Cincinnati Bell, Inc. The information contained in this publication has been obtained from sources believed to be reliable. CBTS disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of CBTS's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.