FREQUENTLY ASKED QUESTIONS ABOUT RSA SECURID®

Information for RSA Customers

INCIDENT OVERVIEW

1. What happened?
In March 2011, our 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 customers and our business including further hardening our IT infrastructure and working closely with appropriate authorities.

2. What specifically was taken during the attack on RSA in March?
As we said on March 17, 2011, the attack resulted in certain information being extracted from RSA's systems that is related to RSA SecurID multi-factor authentication products. While we believe the information extracted does not enable a successful direct attack on any of RSA's customers, it may be used to reduce the effectiveness of a current multi-factor authentication implementation against a broader attack.

3. Why can’t you give more detail about the information that was compromised?
Our customers’ security is our number one priority. We continue to provide our customers with all the information they need to assess their risk and ensure they are protected. Providing additional specific information about the nature of the attack on RSA or about certain elements of RSA SecurID design could enable others to try to compromise our customers’ RSA SecurID implementations.

4. What constitutes a direct attack on an RSA SecurID customer?
To compromise any RSA SecurID deployment, an attacker needs to possess multiple pieces of information about the RSA SecurID solution. Some of this information is never held by RSA and is controlled only by the customer. In order to mount a successful direct attack, someone would need to have possession of all this information.

5. What constitutes a broader attack on an RSA SecurID customer?
The broader attack most likely would be an indirect one that uses a combination of technical-and social-engineering techniques to attempt to compromise all pieces of information about the RSA SecurID solution. Social engineering attacks typically target customers’ end users and help desks. Technical attacks typically target customers’ back end servers, networks and end user machines. Our prioritized remediation steps in the RSA SecurID Best Practices Guides are focused on strengthening your security against these potential broader attacks.

6. What has RSA done to change it manufacturing process and security practices?
RSA started manufacturing new RSA SecurID hardware authenticators on March 23, 2011 in response to the cyber attack. In the enhanced manufacturing process, RSA generates new token records at the time we program the hardware authenticators. RSA developed
this process after consulting with several third-party experts. It includes keeping key processes offline, adding multiple layers of security, and putting additional physical security measures in place. The new process also adds greater security and control for end-user interactions.

7. Are any other RSA or EMC products affected?

We have no evidence that customer security related to other RSA products has been similarly impacted by this attack. We also are 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 has been compromised.

8. RSA is a security company. How did you get attacked and why can’t you say more?

Cyber attacks are a fact of life for any major organization, and we are no exception. EMC and RSA invest heavily in information security. The attack on RSA was very sophisticated and targeted. Our teams detected the attack in-process and immediately began very aggressive defense and remediation efforts to protect our business and our customers.

LOCKHEED MARTIN INCIDENT

9. What has changed since March when you first announced the breach?

While there has been significant news coverage, there has been no additional breach of information at RSA and there is no new threat to customers related to this situation. Everything we said in March remains true. What has changed is that one customer, Lockheed Martin, has confirmed that information taken from RSA has been used as part of a broader attack against it; an attack that the customer successfully thwarted. Lockheed Martin continues to use RSA SecurID authentication as part of their layered approach to security.

10. Did Lockheed Martin implement all of the best practices that you recommended in March?

We continue to work with Lockheed Martin, but we are not able to speak specifically about the remediation steps that they have taken.

11. Did you withhold information from your customers and leave them exposed to risk?

A. No we did not. We provided customers with all the best practices for remediation we believe are needed to ensure their continued security, and everything we said in March remains true. As Art Coviello stated in his open letter on March 17, 2011 the information stolen from RSA could be used to reduce the effectiveness of a customer’s RSA SecurID implementation as an element of a broader attack. We now have confirmation that it has been used in this way, but this does not reflect any change in our position or any new threat or vulnerability in RSA SecurID technology. Since March 17th, we have worked with thousands of customers to help them implement our best practices.

12. Who do you believe is responsible for the attack?

We are not going to comment on the party who may be responsible for the attack on RSA. However, we believe a likely objective of the attack was to obtain an element of security information that could be used to target defense secrets and related IP.
13. How can you determine the motive without knowing the exact identity of the attacker?

Based on certain characteristics of the attack, such as particular techniques and tools. We have worked with relevant government and security industry experts to review these characteristics. We have published a few useful “indicators” from the attack on RSA, and these and others were released by the U.S. Department of Homeland Security.

REMEDICATION PROGRAM

14. Are you replacing tokens for your customers?

We continue to work with all of our customers to understand and address their unique business characteristics and implement best practices for remediation based on their risk profiles. Based on our belief that the motive of the attacker on RSA was centered on defense-related secrets and related intellectual property, we have been actively working with the defense industry and governments in several countries, helping them implement our entire set of remediations as outlined in March, including refreshing their tokens at an accelerated rate in some limited cases.

We now are expanding our security remediation program to reinforce customers’ trust in RSA SecurID tokens and in their overall security posture. This program will continue to include the best practices we first detailed to customers in March, and will also include two new options based on our typical customer profiles:

– An offer to replace hardware tokens, for customers with concentrated user bases typically focused on protecting intellectual property and corporate networks.

– An offer to implement risk-based authentication strategies for consumer-focused customers with a large, dispersed user base, typically focused on protecting web-based financial transactions.

15. Is there an option to replace hardware tokens with software tokens? What are the benefits of transitioning to software tokens?

Yes, customers have the option to replace hardware tokens with software tokens as part of the remediation options. Software tokens can provide several advantages including immediate availability, increased end-user convenience, and lower Total Cost of Ownership (TCO).

16. Are you replacing tokens at no cost to customers?

We are working with our customers to meet their unique security requirements. We will work directly with customers to replace their hardware tokens in a manner that’s fair and equitable to them and to RSA. As always, we intend to keep the specifics of our business relationships confidential.

17. Do customers have to return the tokens that are being replaced?

No, customers are required to stop using tokens that have been replaced, but we do not require customers to return tokens to RSA. If tokens are returned to RSA, they will be disposed of in a green fashion. RSA contracts with environmentally friendly waste management companies around the world to ensure that expired tokens are disposed of in such a way as to limit and minimize as much as possible their impact on the environment.
Customers who wish to return expired tokens to RSA can rest assured that all expired tokens received back at any of RSA’s worldwide manufacturing facilities will be dismantled, and that all reusable and recyclable parts will be appropriately reclaimed. Parts that are no longer usable will be disposed of in such a way as to produce minimal impact on the environment. For more information, visit:

18. When can a customer expect to receive new hardware tokens?

RSA is fully able to handle potential demand from those customers that would like to take the additional remediation step of replacing their hardware tokens. Customers can expect to receive specific information regarding anticipated timing of availability once an order is in process. The total demand for replacement tokens will determine delivery dates. We expect the entire process of delivery and deployment to be largely completed this fall.

For more information, see the PIN Management section in the RSA Authentication Manager Security Best Practices Guide.