White Paper

F5 and RSA SecurID: Supporting NSA Guidance

A 2011 breach of RSA networks resulted in a loss of data that could pose a threat to RSA SecurID two-factor authentication. F5 BIG-IP Application Security Manager (ASM) and BIG-IP Access Policy Manager (APM) support the implementation of NSA recommendations for mitigating potential threats.

by Lori MacVittie
Sr. Technical Marketing Manager

Contents

Introduction

In March 2011, the National Security Agency (NSA) issued an Information Assurance Alert (IAR-001-2011: Mitigations for the RSA Cyber Intrusion) that included information about how to mitigate potential threats related to a loss of data from RSA's network. RSA had concluded the data lost could potentially reduce the effectiveness of its SecurID two-factor authentication system, which requires two forms of evidence to prove identity.

As a result, NSA issued guidance detailing the steps organizations should take to further harden systems that rely on SecurID authentication.

This guidance specifically discusses:

- Hard and soft token use.
- Fortifying security related to SecurID's authentication factors.
- Hardening RSA Authentication Manager.

F5® BIG-IP® Application Security Manager™ (ASM) and BIG-IP® Access Policy Manager™ (APM) enable organizations to implement recommendations published by NSA to minimize the impact of the RSA SecurID cyber intrusion.

Hard and Soft Token Use

RSA SecurID supports both hard and soft tokens as part of the authentication process. In its advisory, NSA provides recommendations for further securing both token types. In the case of hard tokens, the threat of compromise may seem minimal based on the exposure of the system to external networks, and therefore no additional mitigations may be required. However, NSA still recommends further securing authentication-related SecurID components.

In the case of soft tokens, NSA recommends using one-time password generation and/or non-networked, external devices such as a PDA or smartphone to manage soft token–based authentication. These devices carry with them their own set of potential threats, so use of external devices should be carefully governed.

While F5 supports both hard- and soft token–based SecurID systems, it recommends replacing hard tokens with certificates or CAC cards. BIG-IP APM easily supports both certificate- and CAC card–based authentication. For soft tokens, via advanced customization, BIG-IP APM can automatically generate one-time passwords,

where the token is pulled and pre-filled on the BIG-IP APM login page. (This capability is also natively supported by F5 FirePass® SSL VPN.)

If hard-token authentication is preferred, F5 recommends augmenting hard token access policies to include checks for location- and device-specific settings such as MAC address, as well as using whitelists and blacklists where possible to redress potential risks.

Fortifying Authentication

Many systems, including SecurID, use multiple authentication factors to protect against intrusion by illegitimate users. SecurID has long been a primary example of two-factor authentication, one factor of which must be token-based. In securing critical applications, NSA recommends against using SecurID as the sole means of authentication. The NSA advisory offers guidance around how to augment existing SecurID systems with additional authentication measures.

- **Augmentation with user names and passwords.** BIG-IP APM supports a combination of user name, password, and SecurID, as well as SecurID and client certificate (soft token). BIG-IP APM can support these combinations across a wide variety of client device types, including emerging mobile devices such as tablets and smartphones, even when the device is limited to HTTP form-based authentication.

  With the ability to create customized policies for authentication and authorization in BIG-IP APM, organizations can layer on n-factors by integrating AD, LDAP, and/RADIUS-based authentication. Adding a form that prompts for a PIN and traditional credentials to be verified against any number of corporate identity stores can be easily accomplished using the BIG-IP APM Visual Policy Editor.

  - **Enable account login restrictions.** BIG-IP APM can enforce restrictions on remote access based on time periods as well as geolocation. These restrictions can be obtained from an Active Directory policy or can be configured directly within the BIG-IP APM access policy itself.

    Because BIG-IP APM is contextually aware, it has access to a broad set of variables specific to the client such as device type, operating system, location, and network-specific data. Administrators can therefore define very granular access policies using any combination of these variables.

Additionally, BIG-IP ASM can aid in detecting and preventing unauthorized attempts at accessing the authentication system or attempts to bypass the system. Such attempts can then be correlated back to user names stored in BIG-IP APM to better enable forensic analysis of the attacks. BIG-IP ASM can also enforce layer 4 and layer 7 (application) access control lists (ACLs) to prevent attempts to circumvent access policies as well as brute force attacks. These additional restrictions further mitigate risk associated with the SecurID breach.

- **Phone-in before use.** NSA suggests using a phone-in request prior to authorization to log in for a period of time. The suggested process requires remote logins be disabled by default and then manually enabled by an administrator after receiving a phone call. This can certainly be accomplished in BIG-IP APM, but the overall process of using a partially manual authentication system may be too time-consuming and financially prohibitive. Phone-in requests can be implemented using more automated systems integrated with identity stores, such as PhoneFactor and Active Directory, LDAP, and RADIUS.

  Assuming integration is possible with the phone-in system, a phone call can set a flag in the appropriate identity store. This will subsequently enable login for the user through BIG-IP APM for a specified period of time, after which the flag is reset to its default disabled setting.

- **Augmentation with Department of Defense (DoD) Common Access Card (CAC).** BIG-IP APM also natively supports using CACs as an authentication factor, described more fully in the F5 paper, "Kerberos Constrained Delegation and Protocol Transition in Smart Card PKI Architectures." Furthermore, BIG-IP APM version 11 can support seamless single sign-on (SSO) capabilities while providing the enhanced security of CAC, reducing the potential for negative effects related to integrating CAC into existing architectures as noted by RSA in its recommendation. This support includes the ability to provide SSO across multiple domains and Kerberos ticketing (see the F5 paper, "Simplifying Single Sign-On with F5 BIG-IP APM and Active Directory," for more information). BIG-IP APM also enables additional forms of authentication such as PIV (Personal Identity Verification) cards, which are mandated for federal employees and contractors by Homeland Security Presidential Directive 12 (HSPD 12).

- **Perform regular audits of remote login activity.** NSA suggests regularly auditing log files with attention to unusual IP addresses and failed login

attempts. It also recommends verifying remote logins for each user on a daily or weekly basis, and notifying users of last logins with every login. These audits can be accomplished via BIG-IP APM Reports and Dashboard. BIG-IP APM v11 now generates customized, granular reports including detailed session reports by:

- Access failures
- Users
- Resources accessed
- Group usage
- Geolocation

Additionally, BIG-IP APM integrates with third-party Security Event and Incident Management (SEIM) vendors to provide a variety of options for performing audits and analysis of login data as well as detecting outliers and unusual access patterns. Some advanced integrations, for example with Oracle Access Manager (OAM), allow not only the detection and logging of suspicious activity but immediate, automated triggering of policy enforcement. For example, if OAM detects suspicious or malicious activity, it can inform BIG-IP ASM which in turn can enable policies designed to thwart any attempted illicit activity.

RSA Authentication Manager Hardening

NSA also recommends hardening RSA Authentication Manager (AM), the management component of the RSA SecurID system. AM verifies authentication requests and provides centralized administration of corporate access policies. NSA offers a lengthy list of potential ways in which AM can be made more secure. The options focus on system and network isolation combined with restricted access to the system, most of which fall under industry best practices for securing sensitive systems from unauthorized access.

Deploying AM topologically behind BIG-IP APM provides an additional layer of protection against intrusion. Layered authentication, endpoint security verification, and access controls offered by BIG-IP APM enhance the overall security posture of AM by filtering out users and traffic that may be a threat. As with restricting access to secure remote access systems, BIG-IP supports using layer 4 and layer 7 access

control lists to further restrict access to systems, which limits risks considerably. BIG-IP APM can enforce tight, context-based policies to govern access to AM, providing an exterior hardened perimeter around AM to prevent unauthorized access and tampering.

BIG-IP APM can help organizations implement NSA recommendations for hardening AM, including:

- Restricting Internet access from AM.
- Limiting user access to AM.
- Establishing firewall rules to restrict network access to AM.
- Limiting user access to only a specific IP address or range of IP addresses.
- Restricting remote access to AM.

The full-proxy architecture of the core TMOS® operating system, on which BIG-IP APM and BIG-IP ASM are deployed, also provides a full stack of protections against a variety of potential threats such as distributed denial of service (DDoS) attacks and emerging upper-layer DoS attacks designed to slip through traditional security systems.

Conclusion

Because of the sensitive nature of applications and resources often protected by complex two-factor authentication systems such as SecurID, the recent breach of RSA networks and subsequent data loss is troubling to many organizations. The unquantifiable possibility of a vulnerability based on the stolen data leaves many organizations with higher risk than is tolerable for their business. The NSA recommendations offered in IAR-001-2011: Mitigations for the RSA Cyber Intrusion provide a foundation for further securing sensitive systems and data from theft to minimize that risk.

Many of the recommendations are based on best practices that should be considered for all Internet-connected and remotely accessible corporate resources. BIG-IP APM and BIG-IP ASM, in conjunction with F5's core technology platform TMOS, provide a broad spectrum of control and policy enforcement options that enable organizations to implement NSA recommendations.

BIG-IP APM gives organizations the added benefits of supporting more granular and sophisticated, context-aware controls over access to secured resources.

Integration with SEIM solutions and with BIG-IP ASM empowers organizations with both the data necessary to detect potential intrusions or abuse and the ability to rapidly provision or enable policies to thwart the potential exploitation of the SecurID system.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com