Virtual RSA SecurID Authentication Agent

Challenge:

Implementing RSA SecurID authentication and authorization on non-compliant devices and applications without installing individual RSA SecurID Authentication Agents.

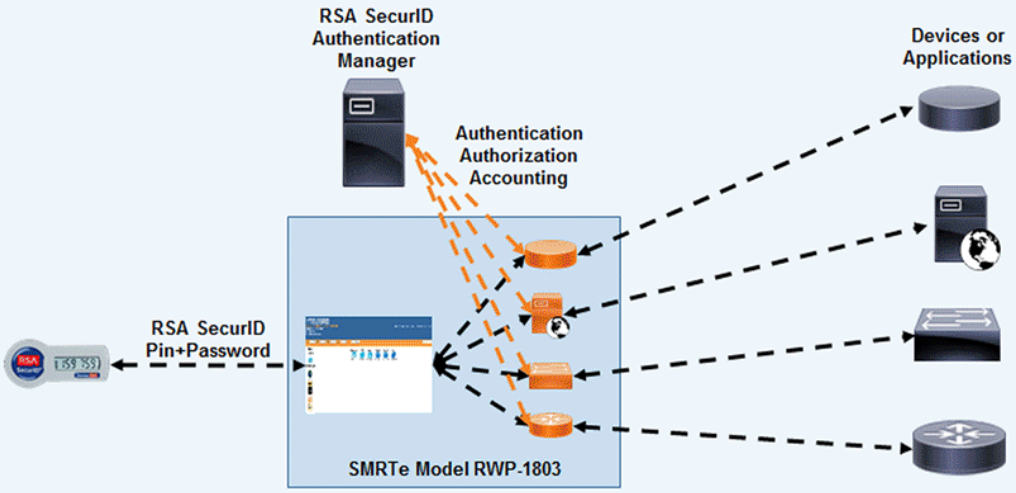
Solution:

Simply deploy the SMRTe™ with an existing RSA SecurID infrastructure and create Virtual RSA SecurID Authentication Agents for all non-compliant devices and applications. The SMRTe promotes network-wide MFA, allows granular user-specific logging, and controls device and application access.

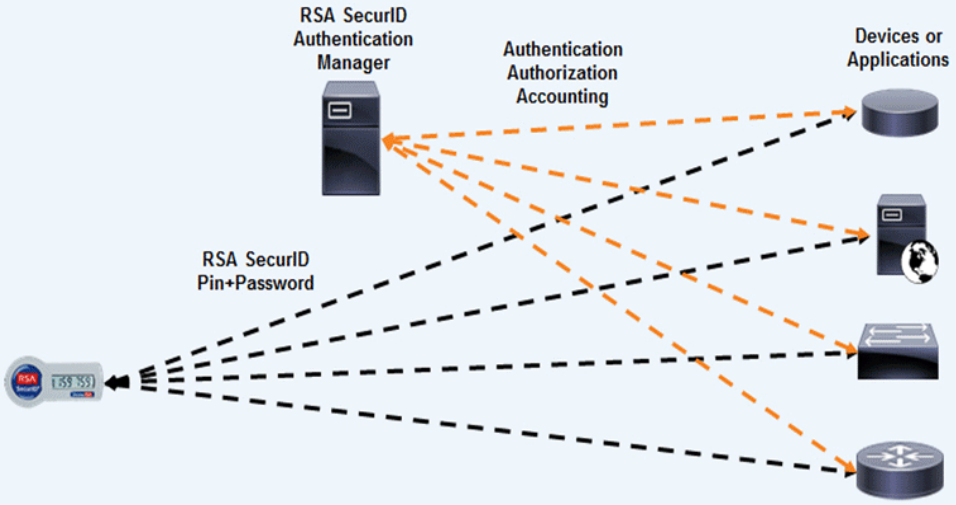
According to a 2015 study by IBM, 63% of data breaches were caused by weak usernames and passwords, making Multi-Factor Authentication (MFA) the front line of cybersecurity. RSA SecurID is the market leader in MFA with a market share of over 50%. TELEGRID's Secure Multi-web Remoting Tool – Enterprise (SMRTe) Model RWP-1803 lets organizations broaden the protection provided by their existing RSA SecurID infrastructure by allowing MFA to devices and applications without the installation of RSA SecurID Authentication Agents.

The core of the RSA SecurID infrastructure is its Authentication Manager which provides user Authentication, Authorization, and Accounting (AAA). When a user logs into a device or application their password and one-time pin is sent to the Authentication Manager which then authenticates the user and grants them access to the device or application. What facilitates communication between the Authentication Manager and the device or application is a RSA SecurID Authentication Agent, which is currently pre-installed on over 400 devices. For devices that do not currently include an Authentication Agent, RSA SecurID provides software for multiple platforms that can be installed and configured to allow MFA and Single Sign-On (SSO).

Installation of a RSA SecurID Authentication Agent on an existing device or application, that has already been tested and certified, is problematic. Organizations are often unwilling to undertake software changes on critical devices and applications for fear of affecting uptime. Additionally many organizations' devices and applications were developed by third parties and



RSA SecurID Infrastructure with Virtual RSA SecurID Authentication Agents



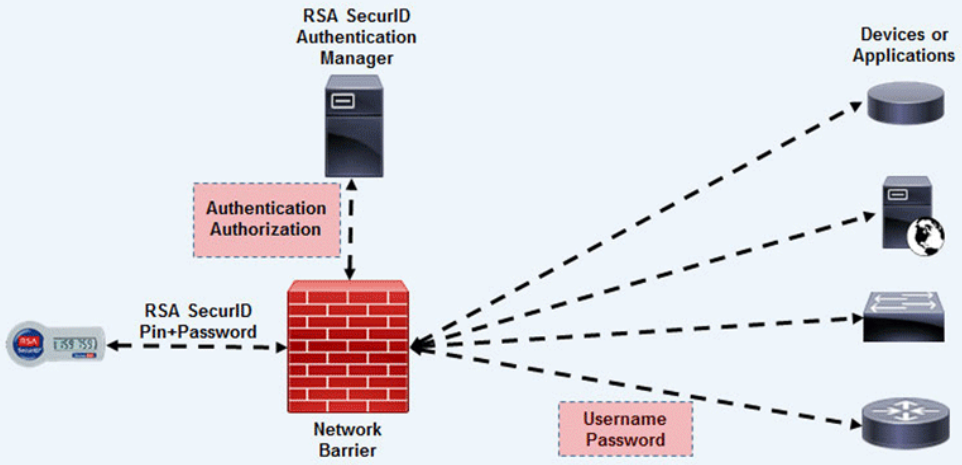
RSA SecurID Infrastructure with Embedded RSA SecurID Authentication Agents

therefore cannot be easily or inexpensively changed. Therefore, in order to implement RSA SecurID, most organizations choose to deploy a network barrier (e.g., firewalls, gateways or jump servers) and re-architect the network so the unsecure devices and applications sit behind the network barrier. While using a network barrier secures the device or application it also creates network visibility issues relating to accounting, as shown below.

RSA SecurID's power lies not only in it authentication and authorization capabilities, but also in its accounting (i.e., AAA). RSA SecurID provides granular user-specific accounting for after-action reporting. When an organization uses a network barrier the only information they will receive from RSA SecurID is that a user logged into the network barrier, anything that happens after that point will be hidden. While it may be possible to obtain logging information from the device or application, that information is not automatically stored with the logging information provided by the RSA SecurID Authentication Manager creating a potential logistical nightmare for network managers. Another issue is that, if an administrator wants to restrict access to a specific device or application beyond the network barrier, the only way to do so is with an unsecure username and password, as shown below. This perpetuates the "hard on the outside/ soft on the inside" problem and greatly increases the probability of an insider attack.

TELEGRID's SMRTe expands the protection provided by existing RSA SecurID infrastructures. It creates a Virtual RSA SecurID Authentication Agent for each device and application. When a user logs into the SMRTe, with their RSA SecurID credentials, and requests access to a device or application, they are re-prompted for their RSA SecurID credentials. This allows the RSA SecurID Authentication Manager to provide granular user-specific logging. This also allows an administrator to restrict access to a specific device or application.

Organizations have been spending time, money, and effort deploying RSA SecurID infrastructures. While we have seen organizations expand RSA SecurID usage among their user base, we have not seen organizations expand RSA SecurID to protect non-compliant device and application due to cost and the fear of unintended consequences. The SMRTe provides organizations with a simple solution to include devices and application in RSA SecurID infrastructures and increase overall network security.



RSA SecurID Infrastructure with a Network Barrier

TELEGRID Technologies, Inc.
973-994-4440
sales@telegrid.com
www.telegrid.com

TELEGRID