INTERLINK
NETWORKS

Interlink Networks RAD-Series AAA Server and RSA Security Two-Factor Authentication

As the world increasingly depends on computers to do business, the need for safeguarding computer resources also increases. Unfortunately, some individuals endeavor to attack computer networks, steal information, and spread malicious viruses. These attackers often seek to compromise, damage, or destroy valuable information resources. It should be little surprise that these attackers will break into unprotected or poorly protected computer systems and networks. This paper describes how RSA Security's two-factor authentication can be used with Interlink Networks RAD-Series AAA Servers to fortify network access security.

© 2002 Interlink Networks, Inc.

All Rights Reserved.

This document is copyrighted by Interlink Networks Incorporated (Interlink Networks). The information contained within this document is subject to change without notice. Interlink Networks does not guarantee the accuracy of the information.

Trademark Information

Brand or product names may be registered trademarks of their respective owners.

Interlink Networks, Inc.

775 Technology Drive, Suite 200
Ann Arbor, MI 48108 USA
Phone: 734-821-1200
Sales: 734-821-1228
Fax: 734-821-1235
info@interlinknetworks.com
sales@interlinknetworks.com
www.interlinknetworks.com

BACKGROUND

The typical means of protecting computer resources is to require users to identify themselves by providing a user name and password. Once these credentials are verified, the user can access the computer resources. This type of password authentication could be vulnerable to attack. Two-factor authentication provides a way of improving the login process to make it far more secure. The Interlink Networks RAD-Series of AAA Servers is an enabling technology that combines the security of two-factor authentication with the authorization and accounting features of AAA.

WHAT IS WRONG WITH PASSWORD AUTHENTICATION?

The main problem with passwords is that there are many ways in which the passwords can become compromised. Consider the possibilities below:

- A user writes down a password on a sheet of paper that is seen by someone else.
- While a user types a password, someone watches over his shoulder and sees what is entered for a password.
- Someone installs a program on a user's computer that records every keystroke the user enters.
- A user mentions a password to somebody, and the conversation is overheard.
- A user selects a password that is easy to predict, like the name of a family member.
- A user has the same password for all accounts, and an administrator of one account doesn't protect passwords.
- An attacker can eavesdrop on the conversation between the user's computer and the authenticating computer using a network traffic-monitoring program.

These are not far-fetched scenarios. Many organizations have concluded that password authentication by itself is not sufficiently secure. Many have turned to two-factor authentication methods to protect their computer resources.

WHAT IS TWO-FACTOR AUTHENTICATION?

With two-factor authentication, the user login requires two things:

- Something the user has (a token)
- Something the user knows (a password or PIN)

Bank ATM machines perform two-factor authentication. In order to perform bank transactions using an automatic teller machine (ATM), a customer must have an ATM card (a token) and must know the correct PIN to use with the card. If a user's PIN becomes compromised, the user's bank account cannot be accessed without the user's ATM card. If the user's ATM card is stolen, it is useless without the associated PIN. Requiring two factors for authentication, as in the ATM example, is far more secure than password authentication alone.

TWO TYPES OF TOKEN

Hardware Tokens

A hardware token is a physical device or card that may be used for two-factor user authentication—an ATM card, for example.

RSA Security, Inc. is an industry-leading supplier of hardware tokens. RSA Security tokens are referred to as SecurID tokens. Most SecurID tokens are small, handheld devices containing microprocessors that calculate and display unpredictable codes. These codes change at a specified interval, typically 60 seconds.

The user combines his secret PIN (something the user knows) with the code displayed on his hardware token (something the user has). The result is a one-time-use PASSCODE that can be used to log in.

Software Tokens

A software token can be installed as an application on a computer. When the application is run, a token card is displayed to the user that looks much like a hardware token card. This "soft" token card is used in the same manner as a hardware token card. The user combines his secret PIN with the code displayed on his soft token to get a one-time-use PASSCODE.

While software tokens provide more security than simple password authentication, they're not as secure as hardware tokens. Hardware tokens cannot be easily replicated, but computer disk contents can more easily be copied without the owner's knowledge. If the contents of a user's disk are copied to a second computer, an attacker need only acquire the user's PIN to log in.

USING RAD-SERIES AAA AND RSA SECURITY TWO-FACTOR AUTHENTICATION

Many organizations use two factor methods for user Authentication. Using RSA two-factor authentication with the Interlink Networks RAD-Series AAA server combines secure two-factor authentication with powerful authorization and accounting features.

Authentication

Network administrators can use RSA two-factor authentication to increase security during user authentication. Interlink Networks RAD-Series AAA Servers can authenticate using RSA SecurID and ACE/Server.

In addition, Integrating SecurID with the RAD-Series Server allows different authentication methods to be used for different types of users. For example, dial-in users might be authenticated using the SecurID two-factor authentication while local users might be authenticated using an LDAP server.

Authorization

Network administrators need to discriminate among users, specifying which users can access what resources. An organization's data is a valuable asset and is typically shared on a need-to-know basis. Only those users that require the use of a resource, such as a database or a network application, should be allowed to use it. Also, network administrators need to be able to limit how much a user can use a resource. This helps to limit the cost of using the resource or to ensure that the resource is available for others to use. Authorization services are required to support these needs. The sophisticated policy features of the Interlink Networks RAD-Series AAA Servers provide tremendous flexibility in specifying and enforcing network access policy.

Accounting

Network administrators need to track when users are logged in and what resources they consume for billing purposes, to justify network maintenance expenses, or to track down network problems. Logging user access also plays a crucial role in network security. The Interlink Networks RAD-Series AAA Server provides the Accounting services that are required to support these needs.

RADIUS is the de-facto standard protocol for providing AAA services. Network access servers (NAS), such as dial-in routers, use the RADIUS protocol to obtain AAA services from an Interlink Networks RAD-Series AAA server. When a NAS performs RADIUS-style AAA, well-established procedures can be used for accessing powerful AAA features.

PUTTING IT ALL TOGETHER

The Interlink Networks RAD-Series of AAA Servers is an enabling technology that helps combine AAA services with two-factor authentication. The flexible architecture of the RAD-Series servers allows the use of plug-ins that can interface to a wide variety of authentication systems, such as the RSA SecurID ACE/Server. A network administrator can implement two-factor user authentication with a RAD-Series AAA Server to provide a secure authentication mechanism that leverages the RAD-Series RADIUS authorization and accounting features.

With this scenario, a dial-up user login requires the following components:

- A user that dials into a network access server (NAS).
- A NAS that communicates with a RAD-Series server providing AAA services.
- A RAD-Series server that uses a two-factor authentication service to provide authentication services.

- A two-factor authentication service that verifies user credentials.

Figure 1 below shows how the pieces fit together.

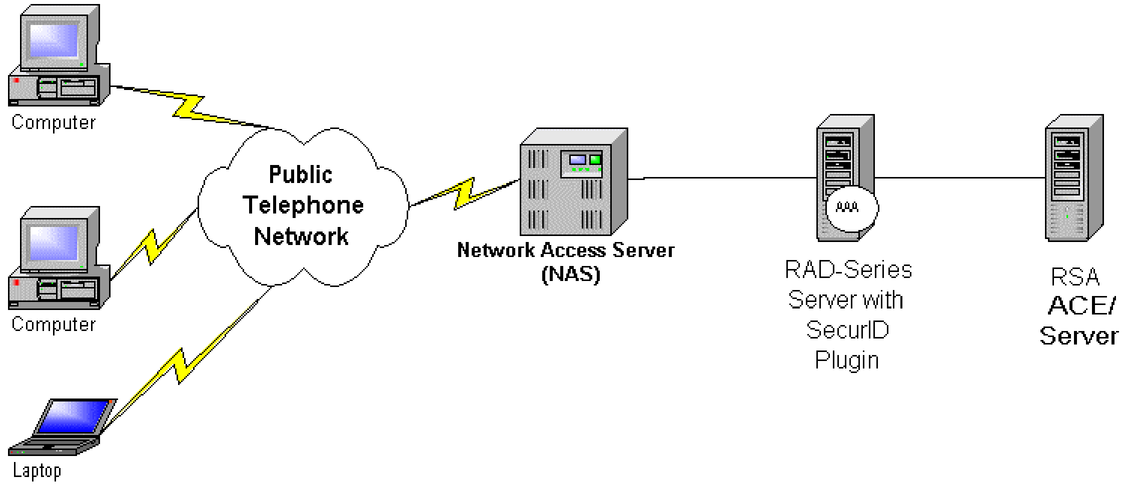
Computer
Computer
Laptop
Public Telephone Network
Network Access Server (NAS)
AAA
RAD-Series Server with SecurID Plugin
RSA ACE/ Server

Figure 1 - Authentication using SecurID. Remote users can connect via modems to a Network Access Server (NAS). The NAS authenticates the user through the RAD-Series Service which acts as a client to the RSA ACE/Server.

The RAD-Series server acts as a client to the two-factor authentication service. When the server receives an Access-Request (login request) from a network access device, it can forward the request to the two-factor authentication service. The network access device does not need to know that a two-factor authentication service is being used.

When a NAS uses RADIUS, standard procedures can be used for managing RAD-Series RADIUS log and accounting files. Accounting and billing systems can use these log files to track usage and bill remote users for access. RADIUS authorization features, such as setting the maximum user idle time before automatic log out, and setting users' maximum connect time are also available.

RAD-SERIES SECURID AUTHENTICATION PROCESS

The steps below show how Interlink Networks' RAD-Series server uses the RSA ACE/Server to authenticate remote users.

1. Users dial into a Network Access Server (NAS) over the public telephone network. The user provides a username along with a PIN combined with the number generated by the SecurID token.
2. The NAS sends a RADIUS Access-Request message with username and PIN+CODE combination as RADIUS password.
3. The SecurID Plug-In within the RAD-Series architecture communicates the authentication credentials to the RSA ACE/Server.
4. If the credentials are accepted, the RAD-Series server sends an Access-Accept message that informs the NAS to allow the remote user access to the network.

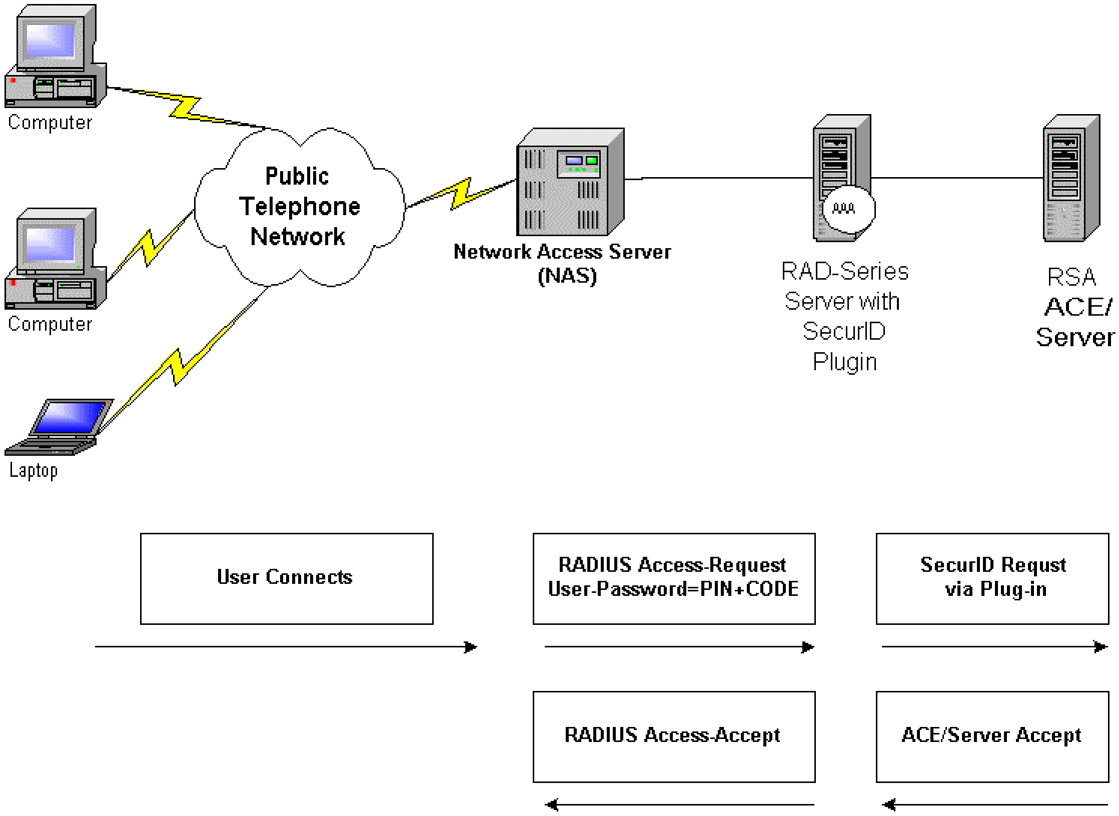
Computer
Public Telephone Network
Computer
Laptop
Network Access Server (NAS)
AAA
RAD-Series Server with SecurID Plugin
RSA ACE/ Server
User Connects
RADIUS Access-Request User-Password=PIN+CODE
SecurID Requst via Plug-in
RADIUS Access-Accept
ACE/Server Accept

Figure. 2- The user connects to the NAS over telephone network. The NAS sends a RADIUS authentication request which is passed to the ACE/Server. When the ACE/Server authenticates the user, a RADIUS Access-Accept message is sent back to the NAS.

CONFIGURING RAD-SERIES TO AUTHENTICATE USING SECURID

In order to configure the RAD-Series AAA Server to authenticate SecurID users, several steps must be accomplished.

1. Edit the users (/etc/opt/aaa/aaa.users) OR realms (/etc/opt/aaa/authfile) file to specify authentication method as 'SecurID'. Each entry that will use SecurID authentication must be configured this way.

2. Copy /opt/ace/data/sdconf.rec from the ACE/Server into /etc/opt/aaa/. This points the RAD-Series server to the IP address and UDP port of the ACE/Server.

For more information on configuring the RAD-Series server, see the document: *Interlink Networks AAA Server: Administrators Guide for the Advanced Server*

SECURID TOKEN MODES

When a SecurID user authenticates, the user is prompted to enter a password (PIN) and the token code currently displayed on his or her token card. Sometimes, during the authentication process the user may be prompted to provide additional information. Exactly what a user is prompted for depends upon the mode of his or her token card as tracked by the ACE/Server.

New PIN Mode

When a SecurID token is first assigned to a user, a PIN is not yet associated with it. The token is in the New PIN mode. If a user attempts to authenticate with a token in the New PIN mode, the user may be prompted during the authentication process to enter a new PIN or to accept a new PIN assigned by the ACE/Server. Note that only the ACE/Server knows the mode of a token and that no mode information is stored in the token itself.

Next Tokencode Mode

When a token is in Next Tokencode mode, and it is used in a login attempt, the user is required to input a second successive tokencode from the SecurID token. The ACE/Server puts a token into Next Tokencode mode if the token has drifted out of synchronization with the server system's clock or if it seems that the token's PIN has been compromised and an unauthorized user is attempting to guess a valid tokencode. Requiring two consecutive tokencodes ensures that the user actually has the SecurID token associated with the PIN that was entered.

The Interlink Networks RAD-Series RADIUS servers will handle the dialog necessary to support these modes. The operation of these modes will depend on the Network Access Server and client software used by the remote user.

USAGE SCENARIOS

Below are some examples of how a user may be set up to use SecurID authentication with the RAD-Series RADIUS Server.

Scenario 1: Remote User Authenticates Using a Terminal Window

A Windows user configures Dial-Up Networking to “Bring up terminal window after dialing.” The user connects to a NAS and a terminal window is launched. The user then uses the terminal window to be authenticated using SecurID credentials. Support for this approach varies among NASs. Consult your NAS documentation to see what terminal window support is available. Some NAS vendors offer alternatives to the terminal window program by providing client software that can be installed on client workstations.

Scenario 2: Remote User Authenticates Using PPP PAP

A Windows user configures Dial-Up networking. The user connects specifying the user's name as it appears in the SecurID user database and using a PASSCODE as the user's password. The user must use PPP PAP; PPP CHAP and PPP MS-CHAP are not supported with this scenario. RADIUS Access-Challenges cannot be sent to the user. The New PIN mode and Next Tokencode mode are not supported. It is up to the administrator to use ACE/Server administration tools to get tokens out of these modes.

Scenario 3: User goes to a Web Page to Log In

A user may be forced to log in at a web page before being allowed privileges such as VPN access. A web page login utility can use RAD-Series RADIUS to provide AAA services for SecurID users.

SUMMARY

RSA SecurID offers increased security through two-factor user authentication. The Interlink Networks RAD-Series server makes two-factor authentication possible with all RADIUS compliant network access servers. By combining these technologies, network administrators can utilize the security advantages of the SecurID system while leveraging the Interlink Networks RAD-Series advanced AAA capabilities.

ABOUT INTERLINK NETWORKS

THE COMPANY

Interlink Networks is a leader in securing access to public and private networks. Our products manage user access to dial-in, broadband, mobile, and wireless LAN networks. Interlink Networks' RADIUS-based access control software provides the authentication, authorization, and accounting infrastructure that enables secure and reliable network access for thousands of enterprise and service provider networks worldwide.

Interlink Networks is headquartered in Ann Arbor, Michigan. We have a worldwide network of resellers and distributors.

OUR MISSION

Interlink Networks' mission is to be a worldwide leader in providing solutions for securing access to public and private networks. By securing access to the network, we provide network operators the first line of defense against unauthorized access to an organization's computing resources.

OUR HISTORY

In July 2000, Interlink Networks was formed by a spin out of technology and developers from Merit Network, Inc., a world-renowned designer, developer, and implementer of Internet technology, hosted at the University of Michigan.

The founders of Interlink Networks spent over a decade defining and developing the world's best carrier-class RADIUS (Remote Access Dial-In User Services) server. Mr. John Vollbrecht, Interlink Networks' Founder and CTO, issued the first RFP for centralized AAA ten years ago, and championed the resulting RADIUS standards through the IETF Standards Groups. Mr. Vollbrecht's name is on many of the RFCs that define RADIUS and AAA.

The charter of Interlink Networks is to expand upon its vision of providing the most advanced authentication products, and to expand its solution set beyond remote access into other network access mechanisms that require authentication and authorization. As networks become more complex, and the means to access networks expands, Interlink will continue to assure that the "interlinks" between users and their networks are protected and secure.