Remote Access Network Security

This document is intended for MIS, telecommunications or security managers with network security responsibilities. The material is organized into three sections:

- *Introduction to Remote Access Security*
  provides an overview of network security considerations.
- *Remote Access Security Options*
  describes various techniques available.
- *Ascend's Security Solution*
  outlines features implemented in Ascend's product line.



Ascend Communications
1275 Harbor Bay Parkway
Alameda, CA 94502
800-621-9578
510-769-6001

Introduction to Remote Access Security

Remote access means that networks are becoming more "open." Corporations have a growing number of telecommuters that are working at home. Mobile employees are staying in touch while traveling, customers are calling into corporate bulletin boards, vendors are coordinating deliveries with master production schedules and, of course, users are accessing the wide-open Internet. But "open" does not mean a remote access network needs to be vulnerable to a security breach.

Most companies reap substantial benefits from their "open" remote access networks. However, along with these benefits comes an increased security risk. The measures most companies use currently to guard against security breaches at the corporate worksite (host passwords, LAN firewalls, locked doors, etc.) serve as a solid foundation for the additional precautions recommended for "open" networks. With remote access, users are not under local LAN administrative control. Equipment that is located in unsecured home offices or hotel rooms, and public communications links are vulnerable to tapping or snooping. Remote access security, therefore, begins in the network itself, before someone even has a chance to gain access to a mainframe, midrange system or server. When the remote access network equipment provides a solid frontline of defense, a potential saboteur is forced to come on-site where existing security mechanisms should come into play (e.g., physical security).

Remote access security provisions should meet the following three objectives:

Provide adequate security - A 0security system should validate users with passwords to protect network-attached resources from unauthorized access. Added security measures can grant users access only to certain resources and protect the network communications link itself from eavesdropping. The more levels of security provided, the more secure the network resources and information become.

Provide ease of administration - The security systems chosen should be easy to both set up initially and maintain over time. The security system's administrative functions must also be secure from tampering by users.

Be transparent to users - Users may attempt to circumvent security methods that are difficult to use, so the security system should, to the extent possible, make logging on from a home office as easy as logging on from a workstation attached to the corporate LAN.

The next section highlights some of the remote access security options available. The final section outlines specific security features supported by Ascend Communications.

Remote Access Security Options

There are numerous options available for securing remote access networks. What follows is a brief description of the most commonly used security options segmented into four different categories: basic security methods; security standards; third-party offerings; and security administration systems. Advantages and disadvantages are given for each option.

Basic Security Methods

There are three basic methods to prevent unauthorized access: restricted address, caller ID and callback. Use of passwords is assumed with each method.

Restricted Address Every node on a network has an address (IP, IPX or other LAN protocol address). Restricted address is a frontline defense that prevents unknown or unauthorized users from being granted access to the network. Only incoming calls from addresses on the approved list are accepted. Restricted address also works with multi-user links, such as incoming links from the Internet. Unknown IP users with legitimate reasons to call can be granted quite limited access (to a single Web server, for example) with the use of a firewall which then precludes access to all other network-attached resources (see Firewall Protection).

Advantages: *Protects sensitive resources against unauthorized use while permitting general access to "public" resources.*

Disadvantages: *Authenticates the equipment, not the user, so stolen equipment or forged addresses can be used to gain broader network access.*

Firewall Protection As a firewall in an office building is used to stop the spreading of a fire from room to room, a firewall is used within a network to limit access from an untrusted network (e.g., a public switched network) to a secure network. One of the most popular ways of implementing a firewall today is based on packet filters. Packet filters use a set of defined rules to examine each packet received and determines if it meets the pre-established criteria to be routed to the requested destination. As an example, an authorized user may dial into the network but can be restricted to a server or service by filtering the packet for certain addresses or packet types. Most commercially available routers have implemented some form of packet filtering. Packet filtering should be used in conjunction with other security measures described above and below.

Advantages: *Packet filtering can check each packet's type, protocol, source and destination address for unauthorized access.*

Disadvantages: *Writing the packet filtering rules can be very difficult. It is also difficult to write filters that identify or segment out certain users; and one can never be sure that all possibilites are covered.*

Caller ID - This security method checks each caller's telephone number (provided by the telephone company whenever an incoming call is received) against an approved list. If the numbers match, the user is granted access to the network.

Advantages: *Very secure, because defeating it requires calling from an employee's home or tampering with the phone company's central office switch.*

Disadvantages: *Caller ID service is not available in all areas, will not protect against unauthorized use from an authorized location, and does not work for mobile or traveling users or users gaining access via the Internet.*

Callback - With callback, users dialing into a remote access server must identify themselves with passwords or identification numbers. The server then automatically terminates the connection and calls the user back at a predetermined telephone number.

Advantages: *Reliable for verifying a call from a particular site, such as a telecommuter's home or a branch office.*

Disadvantages: *Does not address mobile workers calling in from locations such as client sites or hotel rooms, adds a delay to establishing a network connection, can be bypassed using call forwarding, and may not protect against unauthorized use from authorized locations.*

Security Standards

There are two popular standards for password-based authorization: PAP and CHAP.

PAP (Password Authorization Protocol) - PAP is a simple, standards-based password protocol. A user's ID and password are transmitted at the beginning of an incoming call, then validated by the receiving equipment using a central PAP database. The PAP password database is encrypted, but PAP does not encrypt the user ID or password on the transmission line.

Advantages: *A standards-based solution that provides interoperability in a multivendor network, inexpensive to install and operate, and the database is encrypted to prevent password snooping.*

Disadvantages: *The password is transmitted in the clear, making it easy to snoop by tapping the line.*

CHAP (Challenge Handshake Authorization Protocol) - CHAP is a standards-based authentication service for periodically validating users with a sophisticated challenge-handshake protocol. The initial CHAP authentication is performed during the logon attempt; the network administrator can specify the rate of subsequent authentications. The use of repeated challenges is intended to limit the time of exposure to any single attack. CHAP transmissions are encrypted to afford greater protection.

Advantages: *Also an inexpensive, standards-based solution that provides greater security while maintaining multivendor interoperability, inexpensive to install and operate, and is secure against eavesdropping because CHAP encrypts the password during transmission in the WAN.*

Disadvantages: *Because CHAP's standard password database is in plain text form, it is vulnerable to snooping.*

Third Party Offerings

To address the shortcomings of the above security methods, 3rd-party vendors have designed complimentary security offerings based on dynamic, rather than static passwords.

Dynamic Password Authentication Servers - Third-party products for creating dynamic passwords can substantially enhance security. Password generators employ software-based or hardware-based "tokens" the size of credit cards (security cards) that users carry with them. These password generators use two-factor authentication, a method that requires the user to provide something they know (a password or personal identification number) and something they have (the software- or token-generated password). This is analogous to using a bank ATM machine: both a personal ATM card and a PIN# are required to effect a transaction. There are two types of these authentication systems: time-based and challenge-response. A time-based authentication system generates a password every 60 seconds that is valid for only a minute. A user must send the password over the network within that time period in order to gain access to the system. Challenge-response systems generate a Data Encryption Standard (DES) password valid for only a single use.

Advantages:	*Harder to defeat than other security methods because passwords are dynamic; good for traveling workers who call from different locations and may use different equipment. The same token generator from third parties can also provide enterprise-wide security for computers, networks, and physical access security.*
Disadvantages:	*Can be expensive and the third-party nature may cause compatibility problems in multivendor environments, though this can be made easier by the use of a centralized security database such as RADIUS.*

Security Administration Systems

With very large remote access networks, it becomes impractical to store all relevant security and access parameters in individual pieces of equipment, each potentially with its own conventions. Standards-based centralized security databases simplify maintaining user lists, passwords and user profiles. The central security database can be utilized by all remote access equipment when users attempt to establish connections. Thus, one database can serve many systems and locations, while security management can be more efficiently audited and controlled. There are two dominant security administration systems that are used to manage enterprise-wide remote access security: TACACS and RADIUS.

TACACS (Terminal Access Concentrator Access Control Server)

TACACS is a query response protocol standard (RFC 1492) that allows an authentication server to validate a user's password based on security requests from remote access servers. Extended TACACS (XTACACS) is based on the TACACS protocol with additional extensions to support multiple TACACS servers, and provide accounting information to a UNIX syslog file. It also supports multiple protocols such as SLIP, PPP and ARA.

Advantages:	*Standards-based solution that simplifies administration of security systems in multivendor environments.*
Disadvantages:	*Only works with basic password exchanges used in PAP authentication servers, and does not permit configuration options.*

TACACS+ (Terminal Access Concentrator Access Control Server PLUS)

TACACS+ is Cisco's proprietary protocol used exclusively with their hardware solutions. TACACS+ is an upgrade to the TACACS protocol, providing authentication, authorization and accounting for their access servers on the network.

Advantages: *Designed to be more flexible than TACACS*
Disadvantages: *Not an industry standard, not compatible in a multi-vendor environment.*

RADIUS (Remote Authentication Dial-In User Service) RADIUS is a more robust industry standard that simplifies security administration by providing central management services to the authentication servers. RADIUS functions as an information clearinghouse that stores authentication information about all network users in individual profiles. The profiles include access restrictions, destination-specific routing, packet filtering and billing information. Used in conjunction with CHAP or third-party authentication servers, a single RADIUS database server can administer multiple security systems across complex networks, maintaining security profiles for thousands of users. RADIUS, a defacto industry standard, is currently being submitted to the IETF (Internet Engineering Task Force) with the intent of making RADIUS a formal standard.

When a user attempts access to a RADIUS-managed network, the remote access server answering the call requests the user's profile from the RADIUS server. The RADIUS server looks up the user by using the log-on ID and passes the request to the authentication server for that user. The RADIUS server receives the authentication response and passes the information, along with user profile information contained in its database, back to the remote access server. The remote access server then uses this information to either grant or deny access to the network according to the parameters contained in the RADIUS profile.

Advantages: *Robust yet inexpensive solution for simplifying security administration while maintaining multivendor interoperability.*
Disadvantages: *As a relatively new standard, vendor support is currently limited.*

Summary

There are many security alternatives, the more you implement the greater the level of security that can be attained. But each additional security provision also increases the level of complexity and administration. Each company needs to migrate their security at a pace to satisfy the needs of the corporation, information systems and the end users.

Ascend's Security Solution

Ascend's MAX and Pipeline product families provide full remote access security. The MAX is a family of WAN access switch products for the central site that integrates routing, terminal server, bandwidth multiplexing, and remote access server functions. The Pipeline products are remote access bridge/routers for homes and offices. Ascend's comprehensive security is achieved through a combination of security standards and Ascend security extensions. Ascend supports both server-based authentication security standards, PAP and CHAP, along with both centralized security administration system standards, XTACACS and RADIUS. The MAX/Pipeline products support all of the methods described earlier, except the proprietary TACACS+. Ascend also supports multi-level password access, restricted address, callback, caller ID, and third-party dynamic password authentication products, including security cards.

Ascend's comprehensive security offering is embodied in four elements:

- *Access Control* that provides callback, caller ID, routing and packet filtering protections. Packet filtering is a very thorough security measure that will check each packet's type, protocol, source and destination address, for unauthorized access.
- *User Authentication* provides support for PAP, CHAP and third-party authentication server protocols.
- *Security Administration Systems* include support for TACACS, XTACACS and RADIUS, in addition to Ascend's own security management extensions.
- *Management* provisions facilitate customization of Ascend's security facilities through system-wide and individual user profiles (with tight security measures to control read/write access). Extensive event files are available to record attempted security breaches and other useful information.

Authentication Server Protocols Supported

Ascend supports both PAP and CHAP for single channel sessions, as well as for multilink sessions. The Multilink Protocol Plus (MP+) automatically and transparently handles security matters when channels are added during a multilink session. MP+ is a defacto standard for dynamically inverse multiplexing multiple channels together. MP+ is being openly licensed to other vendors, is supported by the majority of Internet Service Providers, and will be submitted to the IETF in late 1995 for formal standardization.

PAP (Password Authentication Protocol): PAP provides basic password validation using a simple two-way handshake. PAP is not a robust authentication method, but does provide for baseline security when interoperating with non-Ascend equipment.

CHAP (Challenge-Handshake Authentication Protocol): CHAP validates access throughout a session with periodic challenges. The MAX, as configured by the security administrator, controls both the frequency and timing of the challenges.

Security Administration Systems Supported

Ascend has its own built-in security administration provisions, and also supports both popular standards for centralized security administration: TACACS and RADIUS.

TACACS (Terminal Access Concentrator Access Control Server) and XTACACS (Extended TACACS): TACACS is a simple query/response protocol that allows MAX or Pipeline remote access switches to obtain centrally-maintained security information.

RADIUS (Remote Access Dial In User Server): RADIUS is a more robust system which allows MAX or Pipeline products to control remote access based on complete user profiles that include routing, packet filtering, destination-specific static routes, and usage restrictions. In addition to providing routes for incoming calls, the MAX can use the RADIUS database data to create and advertise static routes, and to place outbound calls.

Additional Ascend Security Features

The following Ascend security extensions operate in a stand-alone mode in the MAX/Pipeline or in conjunction with a RADIUS security server.

Multi-level Access Password Security: The Ascend MAX/Pipeline provides multi-level password-based security to permit different levels of access for different users. Access permissions are defined in security profiles maintained on the MAX/Pipeline. With multi-level security, fairly open access can be granted to "public" resources, using a firewall to secure all other non-public, network-attached resources.

Restricted Address: A MAX/Pipeline may be configured with a list of IP network addresses that are permitted dial-in access. The MAX/Pipeline rejects incoming calls from any unrecognized network address. Destinations and routes can also be restricted on a per-user basis. Restricting network access at the MAX/Pipeline provides high level, frontline security.

Packet Filtering: The MAX/Pipeline can be configured to check each packet's type, protocol, source and destination address, and port number for unauthorized access. Using the RADIUS user profiles, the filter profiles can be triggered on a call-by-call basis.

Callback: The MAX/Pipeline can be configured to force a callback for any dial-in session. Each authorized user's callback number is registered in the MAX/Pipeline. The remote Pipeline system cooperates with the MAX/Pipeline transparently to the user (except for a small time delay). Callback provides a very high level of security.

Caller ID: Caller ID validates the user's phone number, which is provided by the telephone company when the call is placed to the MAX/Pipeline. Caller ID works with both digital (ISDN or Switched 56) and analog WAN services.

Security Cards and Dynamic Password Authentication Servers: Ascend's MAX/Pipeline products support security card and/or Dynamic Password Authentication Server solutions from the following vendors:

CryptoCARD, Inc. / Buffalo Grove, IL
Digital Pathways Inc. / Mountain View, CA
Enigma Logic Inc. / Concord, CA
Lee Mah DataCom Security Corporation / Hayward, CA
Security Dynamics Inc. / Cambridge, MA
SmartDISK Security Corporation / Naples, FL

Summary

Ascend is committed to leadership in every aspect of remote access, including security. Here is a summary of Ascend's security solution:

- Security is an integral part of the entire Ascend product line, including Ascend's overall system management architecture (at no additional cost).
- The security mechanisms are intuitive and straightforward for users.
- Ascend fully supports industry standards for security.
- Ascend is interoperable with advanced third-party security systems.
- Ascend can be customized easily to meet customer-specific needs.
- Ascend provides the most comprehensive multi-level security features available.

Notes

Notes