INTRODUCTION

In the 1970s, remote access computing meant dumb terminals, 300 baud modems, and host mainframe computers. Today, however, remote access computing means high-performance workstations, high-speed modems, Integrated Services Digital Networks (ISDN) terminal adapters, and sophisticated servers. This article attempts to give an overview of today’s remote access computing and highlight the issues surrounding this technology.

OVERVIEW

Remote access is the ability to connect and gain access to internal network resources that are physically disbursed. Typically, this means that a workstation equipped with remote access software will give authorized users at the remote site access to dial in over a phone or ISDN line to read E-mail, troubleshoot problems, run applications, and transfer files to and from the corporate computers. There are many things that the security professional should be aware of relative to remote access solutions. The following sections examine them.

WHO USES REMOTE ACCESS?

The current number-one user of remote access is the telecommuter. The
newest in a number of traditional users. The mainstay of the remote access usage has always been the traveling workforce, either sales and marketing personnel or field technicians and service representatives. For many years, the applications development support personnel and systems support employees have had remote access to the systems to solve problems that may occur during off-shift operations.

WHY ORGANIZATIONS NEED REMOTE ACCESS
Remote access computing helps businesses comply with the Clean Air Act by reducing travel to work. It also helps businesses comply with other legislation like the Family Leave Act, which allows employees to spend time away from the office to be with a newborn child or for family medical emergencies. Service technicians who are on the road need office connectivity to get assignments, order parts, and send billing information.

Small branch offices need access to the information from the corporate systems and may not need their own processor. For many organizations, remote access is a cost-effective replacement for additional hardware. Busy executives need connectivity to work from home or on the road.

Successful telecommuting programs require reliable connectivity to the corporate network. Coupled with reliable access is the ability to remotely troubleshoot and fix applications and system problems. An effective telecommuting program incorporates all elements found in the workplace and moves them out to the remote access user.

BENEFITS OF REMOTE ACCESS
Telecommuting pilots show the productivity of employees working at any hour of the day or night actually increased by 10% to 30%. To test this statistic, when working on a specific item, log the number of interruptions received every hour. Count the telephone calls, the visitors to the office and the times stopped for other matters and conversation. Employees working at home are less likely to take time off if they are sick or have a cold or minor aches and pains. They can also adjust their work schedules to meet necessary appointments.

Telecommuting can reduce the stress of commuting, eliminate interruptions and frustrations at the office, and give workers more time with their families. It can help businesses cut costs by reducing office space requirements. A number of companies, including many of the Big 6 accounting firms, have introduced the concept of “Hoteling.” Employees are not assigned specific office space, but are registered daily and given available space.

Employees who have instant access to information from anywhere at anytime can provide customers with the best possible service. The technical staff is no longer required to travel to the office to troubleshoot an
application problem. These benefits can give a business a decisive advantage in its ability to hire and keep employees as well as improve customer satisfaction.

Remote users need the applications they have become accustomed to using in the office, including checking and exchanging E-mail, accessing host computers, uploading and downloading files, and accessing corporate databases and corporate applications. Remote users can either dial in to their Internet service provider or connect to their corporate networks to gain access to all Internet services.

CONNECTIVITY OPTIONS

Analog connections are provided through dial-up phone lines and are the most common connections for remote access to LANs, WANs, and the Internet. Analog lines can carry digital data traffic at speeds up to 56K bps. On the positive, this kind of connection is inexpensive and easy to set up. On the negative side, it is relatively slow.

The ISDN supports video, audio, voice, and data over a single connection. It comes in various sizes; the single size portion is called Basic Rate Interface (BRI), and has two 64K bps B (Bearer) channels and one 16K bps D (Data or Delta) channel. Some access equipment allows users to combine the two B channels to achieve 128K bps throughput. This form of connection is normally used to connect homes, schools, and small businesses. It is high speed and relatively low cost, but it is not available everywhere.

Switched 56 allows digital calls to be placed on demand between various locations and provides connections at 56K bps rate. This form of connection is usually available where ISDN is not; however, the big negative to switched 56 is its cost.

Leased services are permanent high-speed connections that provide various bandwidths: 56K bps; Fractional T-1: 64K bps; T-1: 1.544M bps; T-3: 45M bps. Leased services are commonly used to connect various enterprise network sites and small branch offices to large regional offices.

Frame relay, a method for sending packets over private and public networks, provides bandwidths of 64K bps to 512K bps. Frame relay is used to connect branch offices and remote facilities to the enterprise network.

Asymmetric Digital Subscriber Line (ADSL) is a technology that was driven by the telephone companies to compete with the cable industry to provide video services. It offers downstream speed of up to 6M bps and upstream rate of up to 640K bps. Experts believe that this technology has great potential for remote access computing.

HARDWARE REQUIREMENTS

Three key components are required to provide remote access to a corporate network:
1. Transmission devices are required on the client side for dial-in capability and at a central site for receiving dial-in sessions. These can be:
   • Modems for analog connections
   • ISDN terminal adapters for ISDN connections
   • Channel Service/Data Service Units (these are the equivalent of a modem in the digital world) and possibly routers for switch 56 and dedicated connections
2. Remote access servers are required to aggregate dial-in user connections onto the corporate network. These can be dedicated PCs in the case of remote control method, communication servers in the case of remote node method, or a specialized application like Lotus cc:Mail.
3. Communication software needs to be installed on the remote user's workstation as well as the remote access server to provide the intelligence necessary for establishing the remote link.

Some operating systems like Windows 95 have made it easier to utilize remote communications to office environments and to the Internet. The plug-and-play technology has made installation and setup of dial-up networking a snap. In most instances, the only information needed to make dial-up connections is the telephone number, a user ID, and a password.

REMOTE ACCESS METHODS
Several remote access methods are available today. The predominant methods are Terminal Servers, Application Specific, Remote Control, Remote Node, and a combination of several of these methods. Each of these methods differs significantly from the others and offers certain advantages that lend themselves to certain applications.

Using E-mail no longer constitutes complete access for the remote user. Today's typical remote user may be in a hotel room across the continent and needs to update a spreadsheet that is stored on a file server or needs to extract some sales figures from a corporate database. Which of the remote access methods would help accomplish these goals? The following subsections examine these access methods and discuss the pros and cons of each.

Terminal Servers
Terminal servers provide remote network connections for remote users who need to access multi-user systems like UNIX, DEC VAX, and mainframes (see Exhibit 1). A terminal server is a device that connects to a network and has one or more RS232 serial ports. Users connected to one of the serial ports become a terminal on the network. A modem pool can front end the terminal server to allow many users to access the terminal server and, therefore, the network at the same time. Terminal servers support a limited suite of protocols, namely Telnet. Remote users
require a dumb terminal, like VT100, or workstations with Terminal Emulation software.

Strong authentication means more than just the traditional user ID and password. If these techniques are used, it is recommended that they be supplemented with another layer of security such as callback or some form of token ID.

Although this method does not support a multitude of protocols, it still represents a gateway to the corporate network. A hacker with a dumb terminal, who breaks in through the Terminal server security, will most likely be able to break into one of the corporate computer systems and possibly gain Superuser privileges.

Pros:
• Easy to manage
• Inexpensive — emulation software is available on most desktops

Cons:
• Does not support GUI
• No access to LAN resources

Security issues:
• Requires strong authentication

Dedicated Application
With this method of remote access, the user connects to an application running on a server on the network (see Exhibit 2). The remote workstation is equipped with the application communication software that al-
allows users to dial into the application server and gain access to the application. Most E-mail systems and database management products come equipped with dedicated dial-in capabilities.

The problem with dedicated application access is precisely that it is dedicated. Users do not gain access to any network resources other than those provided by the specific application. If users want to do anything else on the network, they will have to hang up and dial in again. Security is dependent on the application, and not all applications implement security equally well.

Pros:
• Generally easy to set up

Cons:
• Allows access to one application only
• Requires a dedicated server
• Requires a separate client on remote workstation

Security issues:
• Difficult to integrate with site security

Remote Control
This technology allows a user to connect to a workstation on the corporate network and control the workstation from a remote location, such as home or a hotel (see Exhibit 3). The office workstation is typically called the host and the off-site machine the remote. Applications are executed on the host workstation; only keyboard, mouse, and screen information are transferred between the remote and host workstation. The remote communication is accomplished through two software components: a
Remote control access provides remote users with access to the network resources in exactly the same way they access the resources at the office. In this environment, each workstation is set up with its own dial-in port, making it difficult to manage in a centralized way.

This method of access poses several security challenges. Without special precautions, anyone at the office can view the screens on the host computer or interfere with the running of the application if the screen is not blanked out and the keyboard is not disabled. One of the major drawbacks of this method is that the modem that is attached to the host system must be left in auto-answer mode. This will represent an additional gateway to the network, which can be targeted and exploited by hackers.

Because the software is installed and managed (most likely by the user) on the host machine, it is impossible to enforce security policies in a consistent manner. Additionally, if the user disconnects without logging out of the system, the next dial-in user can effectively appropriate the previous user log-in status.

Pros:
- Good when executables cannot reside on remote workstations
- Provides transparency of access

Cons:
- Inefficient; requires dedicated workstation, modem, and phone line for each user
• Difficult to manage
• Not suited for graphic-intensive applications

Security issues:
• Sensitive information may be displayed on host screen
• Anyone can interfere with host keyboard
• Modem on host must be left in auto-answer mode
• Impossible to enforce policies

Remote Node
With this method, the remote user dials in from a workstation or laptop and accesses the network through a remote access server, as if the remote computer was a local workstation on the network (see Exhibit 4). Users can communicate with the network using protocols such as TCP/IP, IPC, AppleTalk, etc., and have access to the network resources such as file servers, hosts, and printers.

Remote node access is the most natural form of all remote access methods and is the preferred technique for a wide variety of applications. Client/server applications can be a good fit for remote node, especially if the traffic generated across the link is minimal.

When using remote node, application clients must be installed, maintained, and run on the remote workstation. All network traffic is passed through the link to the remote workstation. The link is usually a phone line or ISDN line at best. Because communication over these remote links is slower than when physically connected to the network, performance of applications generating high-volume traffic suffers greatly.
Pros:
- Can support access to many platforms
- Provide true extension of the network
- Good for remote users that do not have office workstations
- Provide access to all network resources

Cons:
- Clients must be installed and maintained on remote workstations
- Not well-suited for data-intensive applications

Security issues:
- Requires strong authentication

Remote Control over Remote Access

In the remote control over remote node method, the remote user first establishes a remote node connection to the network through a remote access server as described previously (see Exhibit 5). Once connected, the remote user initiates the remote control program to take over a machine on the network that is running the remote control host software.

With this method, remote access administrators only have to manage one centralized gateway rather than multiple distributed workstations. By consolidating modems and phone lines into a single gateway, these resources become shared. Network integrity can be maintained by providing an appropriate level of security on the remote access server. Most remote access servers provide several levels of security and can work in
conjunction with third-party security and authentication devices. All accesses through the remote access server are centrally logged.

Pros:
• Manageable; centralized management
• Efficient; shared resources (modems and phone lines)
• Can be integrated with third-party authentication

Cons:
• Not suitable for graphic-intensive applications

Security issues:
• Host screen should be blanked out
• Host keyboard should be disabled

Integrated Solution
This method incorporates a combination of the previous methods such as remote node, remote control, and terminal servers, in one box (see Exhibit 6). The remote user makes a single phone call and can then access a wide variety of client/server, conventional, and legacy applications. Administrators can configure applications to run locally on the network or remotely on the client. Remote users can transparently launch multiple applications, running both locally and remotely. They can also switch between methods without having to worry about where and how the applications run.

With this approach, remote access users operation is easy; once the user is set up as a remote user, he or she should be able to dial in and

EXHIBIT 6 — Remote Access Methods: Integrated Solution
select and launch the applications without having to worry about what method (remote control, remote node, or terminal server) is being used.

Pros:
• One interface to access all network resources
• Well-suited for environments requiring host, file servers, and corporate applications access
• Centralized management

Cons:
• Difficult to set up

Security issues:
• Requires a strong authentication

INTERNET-BASED REMOTE ACCESS
Currently, most corporate remote access is done by dialing directly into a corporate remote access server (see Exhibit 7). This creates a huge long-distance expense, particularly for a high number of users. Some organizations, however, are taking advantage of their existing connection to the Internet and allowing remote users and branch offices to remotely access the corporate network over the Internet. The remote users simply dial into their local Internet Service Provider (ISP) and initiate a connection to their corporate network.

Internet-Based Remote Access Issues/Solutions
Organizations planning to allow their users to access the network over the Internet must be prepared to deal with several challenges before allowing this type of access (see Exhibit 8). The two major challenges are:

EXHIBIT 7 — Internet-Based Remote Access
1. Protecting the network against unauthorized or unwanted access. Firewalls are commonly used to authenticate legitimate Internet users. A strong authentication mechanism should be used in this case. Traditional passwords can be easily sniffed off the Internet and used to penetrate the corporate network. Address filtering is not effective, because most ISP assign dynamic addresses to their subscribers. Even with static IP addresses, IP spoofing is a scheme that is commonly used by hackers to attack and penetrate networks protected by a packet filtering routers or firewalls.

2. Guaranteeing the integrity and confidentiality of the information being sent over the Internet. Encryption is the only means available today that enables information to be securely transmitted from one computer to another over a public network. Encryption of data over public networks is implemented through a mechanism called tunneling. Tunneling works as follows: packets are encrypted, wrapped with another IP header, and then sent over the Internet. The receiving end unwraps and decrypts the packets to yield the original IP packet and sends it to its final destination. Many firewall vendors are offering firewall-to-firewall or a client-to-firewall encryption (or tunneling) solution. Most firewall vendors are using encryption methods that are Internet Protocol Security (IPSec) compliant, which enables their firewall to communicate with any other firewall that is IPSec compliant.

There are other tunneling solutions that use tunnel end-point servers (sometimes referred to as crypto servers), which create Virtual Private Tunnels between remote location and the enterprise network, protecting data transmitted across the public Internet (see Exhibit 9). These solutions also offer clients that can be installed on home workstations or a laptop and allow users to securely access the corporate network from remote locations.
REMOTE ACCESS SECURITY: GOALS
When developing a security strategy for the enterprise remote access, it is important to remember that remote access security must be stronger than the general network security. Remote access provides a gateway to hackers and uninvited guests to probe and attack the network and poses special risks to an organization. Although security needs are different for every organization, remote access security should at least meet the following objectives:

- Allow access to legitimate users only
- Be easy to administer and flexible to meet the needs of all users
- Be largely transparent to the user. Users go to great lengths to circumvent security methods that are difficult to use.

REMOTE ACCESS SECURITY: BASIC APPROACHES
There are three areas that need to be secured when implementing a remote access security: 1) positively authenticate the users to ensure that only authorized users get access to the network; 2) protect communication links from eavesdroppers to preserve the integrity and confidentiality of transmitted data; and 3) protect the network resources from unauthorized access by restricting users to access the resources that they are authorized to access.

Each of these three areas must be individually protected to secure the entire process, and each requires different techniques.

User Authentication

Passwords. Typically, a user is prompted for a username and a password to get connected to the network. However, password protection is very easy to defeat:
• Users choose obvious passwords  
• Passwords can sometimes be discovered through social engineering  
• Passwords are sometimes sent in the clear over communication link

**Point to Point Protocol (PPP)-based remote access has two password authentication techniques.**

1. **Password Authentication Protocol (PAP)** — the user's name and password are simply transmitted in the clear to the server, and the server verifies the information stored in its database. The password on the database is stored in encrypted format.

2. **Challenge Handshake Authentication Protocol (CHAP)** — the server sends the client a random key (the challenge). The client uses the challenge to encrypt the password supplied by the user and returns the encrypted password to the server. The server looks up the user name in the database to extract the corresponding password, encrypts it using the same key, and compares the results to the user's response. The password is stored in plain text on the database.

To provide a comfortable level of security, traditional passwords should only be used to authenticate users when complemented with other security methods like callback or caller ID.

**Callback.** In this process, the users will dial into the remote access server and authenticate with traditional username and password. The server automatically terminates the connection and calls the authenticated user back at a predetermined phone number. This method is reliable but does not address the needs of the mobile user.

**Caller ID.** When an incoming call is received, the remote access server checks the phone number against an approved list. If the numbers match, the user gets connected to the network. This method is secure, but again does not address the mobile user's needs.

**Dynamic Passwords.** Here, the user carries and uses a password generator (smart card) along with a Personal Identification Number (PIN) that is known only to the user and can be used to gain access to the network. This method enhances the user authentication possibility substantially and it is difficult to defeat; however, it does require a third-party product and can be expensive.

**Biometrics.** Biometric authentication systems use physical characteristics of an individual to authenticate the individual. This method is less mature than smart cards, but gained acceptance during the past few years.
Protecting Transmitted Data

There has been a dramatic increase of new products designed to provide secure communications over public and private networks. These products let security administrators control access of remote users to the corporate network and allow users to secure the transfer of vital information over public networks.

These products are based on end-to-end encryption between two firewalls, two crypto servers, a remote user and firewall, or a remote user and crypto server. Because firewall vendors have their own standard for firewall-to-firewall tunnels, implementations from different vendors were usually not interoperable. Today, however, firewall vendors are supporting IPSec, a common standard that allows interoperation of firewall-to-firewall tunnels from different vendors. By definition, tunnels are established between trusted end systems, and packets are authenticated (initiated from a trusted system).

Tunnel end-point servers or crypto servers allow organizations to create secure, virtual private networks that link their headquarters with regional and branch offices. They can also be used to link their customers and vendors, thus permitting sensitive data to flow between trusted parties in total confidentiality. Crypto servers can be used in conjunction with any firewall. They usually come with packet filtering and are able to perform both user-based and address-based authentication.

Firewall and crypto server vendors offer clients that run on remote laptops or workstations and allow users to create secure tunnels between the desktop and the corporate network over open networks like the Internet. Microsoft has developed Point-to-Point-Tunneling Protocol (PPTP), a new technology that supports Virtual Private Network (VPN) and enables remote users to access the corporate network securely across the Internet. Another product, Layer Two Forwarding (L2F), created by Cisco Systems, is designed to tunnel protocols like PPP and SLIP over the Internet.

Protecting Network Resources

Every node on a network has an address (IP address). These addresses can be used to implement security measures to prevent unauthorized users from gaining access to the network and control access of authorized users to the various network resources. It works by programming into the central site access equipment or an attached router a list of remote node addresses that can connect to the network. For each node, access restrictions such as services that can be used and the destination addresses that can be accessed from the node can be included. Application-level firewalls provide enhanced packet filtering and better access control mechanism to servers and applications.
ADMINISTRATION SYSTEMS
Managing remote access users in large organizations with multiple remote access systems requires a centralized administration system to store and maintain all relevant security and access parameters in one central location. There are two standards-based security administration systems that can be used to manage remote access security:

1. Terminal Access Concentrator Access Control Server (TACACS) — this is a simple query/response protocol that allows servers to obtain centrally maintained security information.
2. Remote Authentication Dial-In User Service (RADIUS) — this is a more robust system that allows remote access servers to obtain user profiles that include authentication and access restriction information.

SERVER FEATURES
When evaluating remote access security server features, it is important to ensure that the server has the ability to provide audit trails or some reporting facility. After performing a risk analysis to ensure that the established controls meet an organization’s needs, it may be a smart idea to implement call back or caller-ID. Most organizations have found it effective to institute an account lockout after a specified number of failed login attempts. Just as in the mainframe environment, there should be a logout or locking of the system after a period of inactivity. For some employees or contract personnel, it may be advantageous to restrict access to certain periods of time or days of the week. Finally, it may be important to ensure that the server that is selected can support third-party authentication and standards-based administration systems.

REMOTE ACCESS POLICY
After a risk analysis, the starting point for any set of controls, is the implementation of a remote access security policy. There are a number of concerns that must be addressed when developing a security policy. The first objective to be considered in the implementation of remote access controls is who should have such an access. Once the business reasons for access have been outlined, it will be necessary to establish a method for requesting such access and what the approval process is to be. If the employee needs dual access — from the office and from home — then who will pay for the additional hardware and software required for this access? Consideration should also be given to how the hardware and software is to be installed and maintained.

Other issues to consider when reviewing the issues revolving around the remote access issue include how training will be provided and by whom. If there are problems, how will support be provided? Will there be a need for 7X24 support? What services will be made available for the
remote access users and what sites will be considered to be off limits? For the organization-provided Internet user, it may be necessary to establish ground rules regarding what types of sites are forbidden and if monitoring of users’ activities will be done. It is strongly recommended that the monitoring of users’ activities be reviewed in the risk analysis process and controls should be implemented if required. Another issue to consider is the installation of virus scanning capabilities at remote sites.

CONCLUSION
Remote access for users is a fact of life as the next millennium approaches. Although enabling tools are still evolving, there is still a need to move forward in processing on all organizations. By understanding the issues and the current hardware, software, and policies available today, every organization can venture into the remote access environment in a controlled and monitored manner.

Tom Peitler is a senior security consultant with CyberSafe, Inc.
Naaman Mustafa is a principal analyst with DTE Energy.