

Glen Doss

Towson University

Center for Applied Information Technology

Remote Access Security

I. Introduction

Providing remote access to a network over the Internet has added an entirely new dimension to keeping business critical information and resources secure. *“The U.S. mobile and remote working population will increase 9 percent, from 39 million in 2000 to 55 million in 2004. Telecommuting will skyrocket as more users adopt handheld devices, as wireless and broadband technologies for remote workers improve, and as technologies to deliver mission critical applications to home workers are enhanced.”* - 2000 IDC (www.idc.com). This is why it is imperative that companies develop and implement solutions to ensure the reliability and security of their remote systems.

Obviously the primary concern of remote access security is ensuring that no unauthorized users gain access to the network and internal resources. However, it is also critical to authenticate legitimate remote users and distribute them according to their resource needs and permission levels. Organizations need to assess the level of security needed, and define and implement a security system that is appropriate for their operational needs. The extent of remote access security needed in an organization varies from simple to complex depending on the associated business risks and costs.

II. System vs. User Threats

There are two main pieces to remote access security, the hardware/network and the telecommuter. Many of the security concerns associated with telecommuting can be addressed and hopefully eradicated by proper user training. Most IT departments focus more attention on the mobile devices and remote access systems, and often neglect the human factor in the equation. 80% of those surveyed by the FISC (Financial Information Security Consortium) have implemented training for telecommuters, and the other 20% are simply opening themselves up for future problems. Not only does internal training enhance security but it also improves the reliability of the remote service for the end user. No matter how successful the remote access security system in place is, if the users do not adhere to it, it is useless.

III. Remote Access System Threats

Remote access threats include data intrusion, system damage, and data destruction. Hackers or employees can gain unauthorized access to trade secrets, company data, and classified information, as well as damage stored information. Remote access obviously relies on the use of an open system, the Internet. This is one of the reasons there are so many significant security threats associated with remote access. A recent survey conducted by Cisco, CMGI, and Verio found that as many as three quarters of businesses on the Web have at least one of 20 widely known security holes. The increasing complexities surrounding new remote access systems and technologies, have resulted in a wide range of security vulnerabilities for administrators to combat.

Some of the significant risks and vulnerabilities are:

- **Weak Passwords:**

Uncontrolled (does not require user to provide any authentication information) or weakly authenticated (a guest account where default password was never changed) dial-ins. Default passwords on terminal servers or RAS (Remote Access Servers) devices; Default passwords can be particularly dangerous, one brand of terminal server even shipped with its IP address as the default password.

- **Multiple passwords:**

Different resources or applications may require different passwords. In this situation a user is required to remember multiple passwords and may be tempted to write down their passwords, nullifying any existing security systems and precautions. The need for multiple passwords, may also lead the telecommuter to using similar or repeat passwords. Requiring different passwords for multiple levels of telecommuting security can actually have the unintended affect of compromising security.

- **Authentication data observation and replay:**

This results in a significant remote access threat via the Internet. Hackers may use publicly available packet sniffing tools to capture information. Remote users using telnet, over the Internet, to connect to their office are transmitting their username and password in the clear. Those with access to the physical wire or router can easily record the data. All sensitive data, in this case username and password, should be encrypted when traveling across the Internet.

- **Dial-back spoofing:**

In dial back spoofing the attacker tricks a dial-back system into calling the

incorrect number, or calling none at all. Call forwarding has been used to automatically redirect the dial-back to the desired number. Another approach involves dialing into the outbound modem port. However, recent dial-back systems have made this type of attack obsolete.

- **IP spoofing and DNS attacks:**

IP spoofing and DNS attacks involve a perpetrator lying about or masking their IP address, in order to gain the trust of the system configuration.

- **Session hijacking:**

Session hijacking is another Internet enabled attack, in which an attacker listens to an existing authenticated session. They then attempt to use IP spoofing and sequence number guessing to take over the current connection. The transition will be transparent to the system, and the user will most likely suspect a typical failed connection. The best defenses for this type of attack rely on strong cryptography such as SSL- enabled tools. For applications or systems with high security concerns, authentication should be performed continuously throughout the session, to reduce the risk of hijacking. Methods such as applying a digital signature to every packet will also help to eliminate these concerns.

IV. Remote Access Security Policy

A robust and user friendly remote access policy, can help to eliminate many of the threats that exist. Remote access policies in most organizations tend to supplement the standard security policy already established. Many organizations today require remote users to sign policy agreements, which can also serve as receipts for the hand-held

authentication tokens or other equipment that may be issued. Maximum connection times for remote users should be established to prevent idle users from staying connected. Idle sessions could provide easy targets for physical hardware access and session hijacking. Remote access security policies should meet the following objectives;

- **Provide adequate security:**

It goes without saying, but a system should use significant authentication methods (strong passwords, etc.) to protect the network from unauthorized remote access.

- **Provide ease of administration:**

The security systems used should be somewhat easy to implement and maintain over time. If the process of administering the security features becomes too much of a burden, administrators may opt to take costly shortcuts or provide lackluster monitoring.

- **The security system should be transparent to users:**

To the extent possible, logging on remotely should be as easy as logging on at the office. This may not always be entirely possible, but if the remote system is too difficult, users may attempt to circumvent established security procedures.

V. Remote Access Security Solutions

The first step in combating the remote access security threats described earlier, is the authentication of the user's identity. Not only should robust authentication be required to remotely enter a network, but it should also be used to route telecommuters to specific computer systems. Authentication can be implemented at three different stages

or locations for remote access, at the remote access server, at the network, or at the application.

Firewall Protection

A firewall is a secure gateway that is used within a network to limit access from un-trusted network. Most firewalls implemented today are based on packet filters. The filters use predefined rules to examine the incoming traffic and determine if the packet meets the established security criteria for the destination requested. Firewalls are used to authenticate remote users and distribute them according to their resources needed and permission levels. In another situation, an unauthorized packet may be turned away by the firewall entirely.

Firewalls can employ sophisticated IP filtering to limit access to resources for authorized users as well as outside attackers. Restricted address protection is a frontline defense that prevents unknown users from gaining access to the network. This type of security must be used in conjunction with other methods, because alone it does not prevent entry from stolen equipment.

Firewalls can reduce the need for routers and provide relatively good security. For most firms, the primary function of a secure gateway or firewall is to provide robust user authentication, but they can also perform auditing and session monitoring functions.

However, setting up all encompassing security permissions and regulations for complex firewall systems can be an extremely challenging task.

In situations where remote users only need access to non-critical or non sensitive

data and resources, this information can be placed outside the firewall. However, in situations where internal databases or other resources are required (which is often the case), this type of configuration would not be possible.

Hand-Held Tokens

Many of today's popular remote access security systems operate on the principle of "security by obscurity" in which users must possess a specific object to access the network. Using a token is one of the most popular ways of promoting "security by obscurity". A token is simply a credit card with a small built-in computer. Even if this token is confiscated or lost, it provides an attacker no use without a confidential password or PIN. Tokens help to reduce the need for remembering multiple passwords.

Whether using usernames and passwords or PIN's and tokens, the user should be validated by the secure system. The user can be required to possess a token in addition to a PIN (personal identification number) or password – "something you know and something you have". In most situations, tokens provide a higher level of security than passwords. A would-be attacker would have to have both a valid token and corresponding PIN. This is much harder for an attacker to obtain than a user ID and password combination, especially because passwords are often proper words or common knowledge phrases.

One-time passwords and smart tokens

Robust authentication can also use one-time passwords. This greatly reduces the threat of password hacking via electronic monitoring (eavesdropping or sniffing). If the one time password was exposed to an unauthorized person, it would be of no value to

them. Many of today's advanced authentication systems employ the use of smart tokens. In this type of configuration the user provides a PIN which unlocks a token, which in turn generates a one time password.

Location validation and call level security:

CLI (Caller Line ID), verifies a remote users call number against a database of acceptable numbers. Fixed dial-back numbers, in which the system dials a pre-assigned number for verification, is another method of location authorization. However, fixed numbers aren't usually an acceptable solution for mobile workers who don't have a dedicated or predefined number. This type of authentication is also susceptible to the dial back spoofing and call forwarding threats described earlier.

PPP (Point to Point Protocol) Security Authentication:

Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP) are the most common of the PPP methods. PAP provides a simple, although not very secure, method for a peer to establish its identity via link establishment. PAP sends passwords over the circuit unencrypted leaving them open for interpretation. CHAP uses a three way handshake for authentication. First comes the link establishment phase, followed by the authenticator sending a challenge message to the peer. This type of authentication relies on a secret known only by the peer and authenticator, and uses it to encrypt the transmission. CHAP protects against playback by using an incrementally changing variable challenge value and identifier. Using repeated challenges limits the time of exposure to a single attack.

Centralized Password/Profile Databases:

The use of third-party password services allows a single database to be used to store privileges and profiles on the local network. These databases can contain access rights for local users on the network, as well remote users. This eliminates the need for constructing, maintaining, and securing multiple databases for network authentication.

RADIUS (Remote Authentication Dial In User Service) has emerged as a common open IETF standard for centralized security implementations. RADIUS offers robust functionality, flexibility and compatibility between vendors. A RADIUS client is the remote access server that requests authorization from a RADIUS server. RADIUS provides a single point of authentication and configuration. When used in a stand-alone setup remote users are authenticated by the RADIUS server, which also stores user privileges, and has the capability to record session statistics. TACACS (Terminal Access Controller Access Control System), although outdated, and TACACS+ are two other open standards that provide similar functionality to RADIUS. TACACS is a query based response protocol that allows the authentication to verify passwords based on the remote servers request. TACACS lacks many of the features that TACACS+ and RADIUS offer, and should no longer be deployed in new installations.

Virtual Private Networks (VPNs)

VPNs were designed to support telecommuting, remote offices, and on-the-road mobile applications by providing end to end security between remote users and private networks. VPNs employ the PPP (point to point tunneling protocol) transport protocol to establish as secure connection, or tunnel, through the company firewall. This method

may employ the use of PKI (public key infrastructure) digital certificate technology to authenticate remote users, which helps to add access control security.

The use of digital certificates in a VPN environment allows administrators to keep a close eye on what people are doing on the network. However, many IT managers have declined using digital certificates because of the difficulty of administering these systems. It has also been difficult to find employees with a sufficient amount of digital certificate experience. An InternetWeek survey (summer 2000) found that only about 1/3 of the 200 IT managers surveyed used digital certificates, mainly because of the lack of in-house expertise.

These private networks support a wide range of protocol options, such as PAP, CHAP, MS-CHAP, L2TP (Layer 2 Tunneling Protocol), IPSec (IP Security), and also support RADIUS and token-based authentication. VPNs are increasingly being used as a solution to provide dedicated and secure remote access.

VI. Logging and Monitoring

Monitoring (Accounting) involves tracking, auditing, and reporting remote access activity. This is important to determine usage patterns, identify unusual network activity, and help to measure the effectiveness of your remote access system. Logging user sessions should be a mandatory process for all remote access systems.

Ease of log file administration should be considering, in order to ensure that it is performed. It is somewhat uncommon for companies to outsource the administration and monitoring of the remote access system, because of the critical business strategy and security issues that accompany the system. Logging can be done at the remote access

server, authentication server, or firewall.

Logging at the remote access server:

In this situation the server can log session initiation and termination, as well as management functions such as the addition or deletion of any remote users.

Logging at the authentication server:

In certain situations significant logging at the remote server is inconvenient or impossible. These type of situations require the use of an authentication server that can log every transaction. In most instances organizations will control the use and administration of the authentication server. This usually makes it an easier process than using the remote server, which the organization may or may not control.

Logging at the firewall:

Firewalls can offer significant control and logging for all remote user sessions. Logging at this layer can provide extensive information about successful sessions and failed intrusions. In most cases using a firewall generates much better log reports and monitoring than remote access servers. However, using a firewall for logging purposes introduces another whole level of complexity to the remote access equation, which many are unwilling to conquer.

This paper has provided a brief introduction into the world of remote access security. Obviously there are many topics beyond the scope of this paper that should be addressed to fully understand the complexities involved with provided reliable and secure remote access. The increasing need for remote access by employees will continue to fuel the necessity for advanced security systems. As remote access technologies begin to

offer more advanced applications, such as high-speed wireless, administrators will have to tailor their security systems and access policies to these new applications.