White Paper

Securing Cisco Secure Access Control Server Running on Microsoft Windows Platforms

Abstract

This paper describes how the Cisco Secure Access Control Server for Windows (Cisco Secure ACS) can be protected against the vulnerabilities of the Windows NT and Windows 2000 operating systems and explains how to improve security on the server host. It discusses making the system dedicated to ACS, removing all unnecessary services, and other measures. It also discusses how to improve administrative security for ACS through such methods as stronger passwords and controlled administrative access. This paper concludes with considerations of physical security for Cisco Secure ACS and its host.

Introduction

Recent attacks on servers running the Microsoft Windows NT and Windows 2000 operating systems have caused serious problems for systems administrators and network security personnel. As a result, many believe that applications running on the Windows NT and Windows 2000 operating systems are not as secure from virus and worm attacks as those running on other operating systems, such as UNIX.

Various methods—from removing unnecessary Windows functionality to devising network protection schemes—are available to protect these systems. With a properly secured server, ACS itself is relatively safe from direct attack. ACS does not rely on many of the peripheral Windows services that are vulnerable to virus and worm attacks.

Windows Operating System Vulnerabilities

Two of the most infamous recent attacks on Microsoft-based systems were the Code Red worm and the Nimda virus. As with other attacks on Microsoft servers and clients, these programs exploited vulnerabilities in Windows services.

The Code Red worm was a self-replicating malicious code that exploited a vulnerability of indexing services on servers running Microsoft's Internet Information Server (IIS).

The Nimda virus was a malicious virus that modified Web documents (.htm, .html, and .asp files) and certain executable files found on the systems that it infected. It also created numerous copies of itself under various file names. Nimda could propagate itself by the following methods:

- Client-to-client through e-mail
- Client-to-client through open network shares
- Web server-to-client through the browsing of compromised Web sites
- Client-to-Web server through active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities
- Client-to-Web server through scanning for the back doors left behind by the Code Red II and sadmind/IIS worms

Other recent viruses include:

- W32.Gibe@mm—A mass-mailing worm that uses Microsoft Outlook and its own Simple Mail Transfer Protocol (SMTP) engine to spread
- W32.hllp.sharpei@mm.html—A mass mailing virus that targets Windows applications if the .NET Framework is installed
- JS/Exploit-Messenger—A virus that uses a Document.Open vulnerability to send a message with a URL that hosts a nonmalicious script that simply replicates the virus using a Messenger buddy list

More details about these and other viruses are available at www.microsoft.com/.

More details about Code Red are available a www.cert.org/advisories/CA-2001-19.html.

More details about Nimda are available at www.cert.org/advisories/CA-2001-26.html.

Microsoft has produced patches to counteract the above issues. Details are available at www.microsoft.com/.

Note: The prime access of these attacks is not on the Windows kernel but on the associated services provided with the operating system.

As shown in the previous section, the primary means of these attacks is not on the Windows kernel but on the associated services provided with the operating system. Because ACS is guardian of the gateway to the outside world, Cisco recommends that you secure this machine from both internal and external exposure.

Cisco Secure ACS as a Dedicated System

The more applications that run on a system, the more users and applications are likely to need access to the system. As a result, security is proportionally decreased as access is increased. If security is a priority, the best solution is to allow access to as few users as possible. The best way to achieve this is to devote a server (or servers) to the task of running the access control service. In other words, do not run any other applications on this system. Although this might seem extravagant because of the hardware costs, the alternative is to reduce the security of the access service. ACS controls access to the network from external and internal sources. Compromising security on the ACS in any way is risky. Moreover, because hardware has become relatively inexpensive, the cost of dedicating a system to this task is not great. This measure should be considered carefully before any other approach is taken.

With any security-sensitive host, it is worth taking the time to reduce the number of applications running on the system to an absolute minimum. While no "extra" applications might have been installed on the ACS host, Windows can and does run a number of operating-system-based services and applications as part of the default installation. As described previously, these offer potential opportunities for a hacker to exploit. It is prudent, therefore, to disable these services and applications.

The following services should be stopped or removed from the ACS host server:

- MS Internet Information Server (IIS) and related servers—Windows NT Version 4.0 and Windows 2000 servers install IIS as part of the standard setup. This includes File Transfer Protocol (FTP) and Gopher. Unless there is a good reason to have these installed, these should be disabled using the Windows "Services" Control Panel applet because ACS does not depend on them.
- The "Server" service—This service provides all disk- and file-sharing support for incoming network connections. For maximum security, disable this service so that no external machines can access the files on the ACS system. Of course, do not do this if any other applications depend on mapping network drives.
- Simple TCP/IP services—Windows NT and Windows 2000 provide a small number of TCP/IP utilities as options for the convenience of the user. If installed, disable this service to prevent these from being used for unauthorized access, at least on the adapter that is connected to the Internet. Unbind the client and server services from TCP/IP on that same adapter. Disable as many services on the server as you can. Services to consider include Alerter, ClipBook Server, Dynamic Host Configuration Protocol (DHCP) Client, Directory Replicator, FTP Publishing Service, License Logging Service, Messenger, Netlogon, Network DDE, Network DDE DDM, Network Monitor, Remote Access Server, Remote Procedure Call Locator, Schedule Server, Simple Services, Spooler, TCP/IP NetBIOS Helper, and Telephone Service.
- Network protocols other than TCP/IP—During installation, Windows NT will install NetBEUI and Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) if the user selects them. On a Cisco Secure ACS machine, it is worth confirming these are not installed while installing the Cisco Secure ACS application. Only TCP/IP is required, and therefore it is best to run only that.

- Windows NT Registry—A Windows NT system relies heavily upon Windows NT Registry for storing configuration data relating to its operation, and a lot of security information is contained therein. Using the Regedt32 utility supplied with Windows NT, it is possible to limit access to a system's Windows NT Registry. Limit access to the minimum set of users possible, perhaps only selected members of the administrator's group who absolutely need access to it. If only TCP/IP is selected for networking, block ports 137 through 139 on the system using the advanced TCP/IP filtering options in the Control Panel network settings section. All remote NT Registry editors supplied with Windows NT use NetBIOS, and this uses the above port range. By blocking these ports, the chances of unauthorized remote editing of the system's NT Registry can be minimized.
- Miscellaneous Services/Applications—ACS does not require email applications, such as Outlook or Eudora. These should not be installed on the Windows server installation.

Other Options

Exercise good user administration by using policies to enforce strong passwords, removing unused accounts such as Guest, and getting control over permissions granted to everyone.

Delete the Administrator account (or remove it from all group membership) and create a new administrator account with an odd name.

Use an Encrypted File System (EFS) for all Web content. (This prevents attackers from changing content, even if they can still take the server down.)

Securing ACS

As with any application running in a security environment, ACS needs to be secured as well. The authentication, authorization, and accounting (AAA) processes themselves are fairly secure, as will be described below. This leaves Cisco Secure ACS administrator control, which is configurable for access control.

AAA Protocols

This interaction between an AAA client and an AAA server is controlled by strictly defined protocols that both the client and server must conform to. Two AAA protocols are widely deployed: Terminal Access Controller Access Control System Plus (TACACS+) and Remote Access Dial-In User Service (RADIUS). They provide similar levels of security. The only really potentially significant difference is that the entire TACACS+ packet is encrypted whereas the RADIUS is plain text (with the important exception of the user's password information). This means that TACACS+ is slightly more secure than RADIUS when it might be possible for a hacker to gain access to the network segment where the AAA communications are taking place between the network access server and the AAA server. If appropriate precautions are taken to protect this traffic, however, this issue can be largely resolved for either protocol.

Both TACACS+ and RADIUS use a "shared secret" or "key" mechanism to encrypt communications. Cisco Secure ACS will respond to requests from any network device that has an address configured within the ACS database and uses the correct shared secret to encrypt its communications. Because they are specified in the relevant RFCs, the encryption algorithms used are well known and in the public domain. The implications of this are important. If a hacker can obtain the shared secret in some way and "spoof" a network–access server address, they would have the ability to spoof a network access server. Although this might or might not be useful, it is definitely a security risk. It

is therefore important to protect the shared secret in the same way as any other important password: Keep the number of people who know it to a minimum, use hard-to-guess alphanumeric combinations, and change it frequently.

RADIUS Vulnerability

Computer Emergency Response Team (CERT) Advisory CA-2002-06, "Vulnerabilities in Various Implementations of the RADIUS Protocol," describes two vulnerabilities that can affect RADIUS servers: VU#589523 (buffer overflow issues) and VU#936683 (failure to check vendor-specific attribute length).

Both of the vulnerabilities allow an attacker to cause denial of service to the RADIUS server. On some systems, VU#589523 may allow the execution of code if the attacker knows the shared secret.

ACS is not vulnerable for the following reasons:

- VU#589523—The length of the buffer question is 1024 bytes longer than required. The maximum key length stored is 32 characters, so 1024 bytes is enough. Keys are held encrypted. This applies to network access servers, AAA servers, proxy targets, and external authentication RADIUS servers.
- VU#936683—Cisco Secure ACS checks for minimum length on vendor-specific attributes.

Administrator Access

Most security breaches involve individuals known to the organization. It is therefore important to protect all aspects of security relating to an ACS. The Cisco Secure ACS graphical user interface (GUI) is proprietary and allows access only to the functions that it controls. It will not permit any access to the system other than that required to configure Cisco Secure ACS.

Remote administrative access—Cisco Secure ACS for Windows supports remote access for configuration using a Web browser. To maintain security, ACS has encryption built in to protect against network snooping of sensitive information relating to the ACS (user passwords, for example). Nevertheless, the risk still exists that a hacker could record an administration session as it traverses the network. The hacker could then try to decrypt this later offline and, if successful, could gain remote access through the account whose details were snooped.

You can protect against such attacks three ways:

1. Ensure that all client browser access to ACS administrative communications runs over network segments that are secured by a reliable firewall.
2. Access the ACS GUI locally only so that no network sessions are ever generated.
3. Configure Source IP Address access to a restricted number of trusted workstations.

Note: Options 2 and 3 can be configured in the Administration Control area under Access Policy Setup.

Option 2 imposes fairly onerous physical restrictions and may well be too inconvenient in many setups. It is, however, the most secure arrangement that can be deployed.

- Restricting physical and logon access to the ACS host—With any security-sensitive server, a wise precaution is to limit access to that machine to as few users as possible. First, configure only the minimum number of Windows-based accounts on the server. With these accounts, ensure that the passwords are particularly hard to guess. Second, if possible, limit physical access by having the ACS in the most secure environment available (in a locked equipment rack, for example).

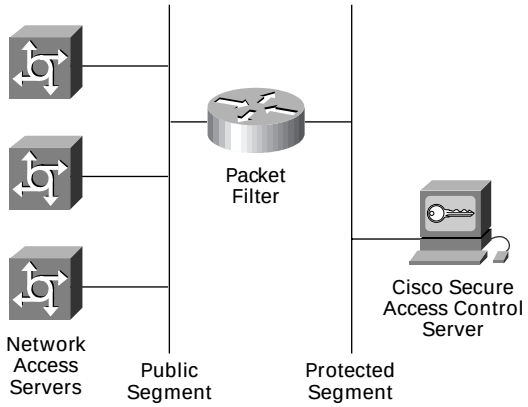
  Restricting physical access is particularly important for the use of the command line interface utility CSUtils. This utility permits full access to the ACS database from the command line (DOS prompt) and does not have any authentication method directly associated with it. Access control is accomplished via the Windows administrative logon. As previously discussed, allow as few system administrators as possible, and make their passwords difficult to guess.
- Use hard-to-guess passwords for the ACS administrator database—Take particular care when assigning passwords for ACS administrators. The usual rules apply.

Physical Security

Firewall employment and placement—Packet-filtering routers or firewalls can and should be used to provide protection to the AAA server. Such a precaution is highly recommended because the AAA server provides the critical network-access-control function. A compromised ACS effectively equates to a compromised network. By definition, a network access server is in a publicly accessible part of the network. The Cisco Secure ACS absolutely should not be.

The easiest way to provide this protection is to put a packet filter between the network-access-server clients and the ACS. The only traffic that should be allowed through from the public side of the network (where the network access servers are located) should be the AAA protocol traffic (TACACS+ or RADIUS), as illustrated in Figure 1.

Figure 1 Placement of Packet Filter to Block Traffic



As noted above, TACACS+ uses TCP port 49, and RADIUS uses User Diagram Protocol (UDP) ports 1812 and 1813 (older 1645 and 1646). The packet filter should block all traffic from the public segment to the ACS on any other ports. In addition, only traffic originating from a recognized network-access-server address should be allowed through the filter. This setup has the following advantages:

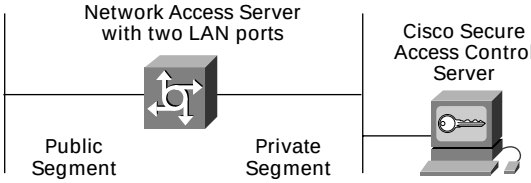
- A hacker trying to interact with the system hosting the ACS can do so only by using the AAA protocol. This greatly reduces the vulnerability of the Cisco Secure ACS host because it can be compromised only if security weaknesses exist in the AAA server software itself.
- Potential "packet flooding" denial-of-service attacks using bogus authentication requests would be stopped by the filter (as long as a valid originating client address were not used).

Without a filter, the ACS is only as secure as the operating system upon which it runs. It is widely accepted that even the most mature and secure operating systems have weaknesses that can be exploited.

With all firewall implementations, logging failed attempts is important. Most packet filters can be configured to provide log output to a variety of logging mechanisms, the most common of which is the syslog daemon. Logs from the packet filter should be collected and analyzed regularly to see whether attacks are occurring. Several good syslog daemons are now available, including some for Windows NT. The best have automated notification utilities that can be programmed to alert an administrator of specified events. Cisco highly recommends this type of setup. If the filter logs a large number of packets addressed to the ACS from "illegal" client addresses or using other protocol ports, someone is probably trying to gain unauthorized access to the ACS. In these circumstances, it is valuable to know about the attack while it is occurring.

For sites that require maximum security, use an entirely private segment or segments for AAA work, as Figure 2 illustrates.

Figure 2 Using a Private Segment for AAA Security



In this scheme, the network access server itself doubles as the packet filter. All dialup traffic is routed through the public segment, and the private segment is used exclusively for AAA protocol through a single static route. Although the illustration shows only a single network access server, this scheme can be applied to any number of servers. In this scheme, unless a hacker can compromise the network access server itself, he has no opportunity as a dialup user to snoop the AAA traffic. The only real drawbacks to this scheme are that it costs more in network equipment (hubs) and that two LAN connectors are required on the network access server used (a Cisco AS5300, for example). As with the packet-filtering approach, illegal attempts to access the ACS should be logged and acted upon.

Another potential avenue that a hacker could employ to try to compromise AAA security is to launch a “brute force” attack on the shared secret. In this scenario, the hacker would send a stream of authentication-request packets to the ACS. Once he got a valid response, even a rejection, he would know the shared secret employed by the ACS for that network access server. This presumes, however, that the requests originate from a valid client address that is recognized by the ACS and that the hacker can intercept the responses in some way. Although this is not particularly likely, it is possible. The logs produced by the ACS will provide a good indication if this kind of attack has been perpetrated. The clue for both protocols will be an abnormally large number of rejections in the failed-attempts log. In the TACACS+ case, it will record that an incorrect secret has been used to encrypt the packet. The danger with this scenario is that the packet filter will not filter out the bogus packet stream as it comes through on the right port from a valid address. Most likely such an attack would be a denial-of-service attempt because, in this case, the hacker does not need to get the responses in order to gain his objective. The private segment solution suggested earlier is a better defense against this type of attack.

Intrusion Detection Systems

Intrusion detection systems (IDS) can be deployed on the network or on the ACS host server itself to detect and react to various forms of attacks. Here are some examples:

- Host-based intrusion detection system (HIDS)—HIDS is a host-based real-time intrusion-prevention and security-enforcement system for LANs designed to protect system resources and applications. HIDS operates by detecting attacks occurring on the host on which it is installed. It works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious-activity modification. Systems running HIDS during recent attacks were protected from infections such as Code Red and Nimda.
- Network-based intrusion detection system (NIDS)—NIDS is used to monitor activity on a specific network segment. Whereas a host-based IDS resides on a workstation and shares the CPU with other user applications, a network-based solution is a dedicated platform. A network-based IDS performs a rule-based or expert system analysis of traffic using parameters set up by the security manager, and the signatures, that flags suspicious activity. The system analyzes network packet headers to make security decisions based on source, destination, and packet type. It also analyzes packet data to make decisions based on the actual data being transmitted. When unauthorized activity is detected, sensors can send alarms to a management console with details of the activity and can control other systems, such as routers, to terminate unauthorized sessions.
- Virus scanning—Virus scanning software is available on the market today and can be easily implemented on the Cisco Secure ACS host sensor. Installing virus-scanning software is not recommended because performance suffers when it performs its scanning process. Virus scanning can consume a significant portion of CPU availability and cause a serious reduction in ACS performance.

Summary

Recent attacks on systems running the Windows server operating systems (Windows NT and Windows 2000), have caused many system, network, and security administrators to question the security of servers running these operating systems. Even though Microsoft has provided quick corrections to the issues as they have arisen, administrators are still concerned about the "next" attack. The problems are not an issue with the Windows kernel but with the peripheral services provided with Windows. Using ACS on a Windows host server does not have to pose a security risk for that system. ACS does not require the use of most of these services, and so, using some common security measures, the ACS can be made secure from intrusion. This paper has discussed the following topics for securing the host:

Securing the ACS host server

- ACS as a dedicated system
- Removing, stopping, or limiting access to unnecessary service and applications:
  - Microsoft Internet Information Server (IIS) and related servers
  - "Server" services (disk- and file-sharing support for incoming network connections, and so on)
  - Simple TCP/IP services such as Directory Replicator, FTP Publishing Service, License Logging Service, Messenger, Netlogon
  - Network protocols other than TCP/IP such as NetBEUI and IPX/SPX
  - Windows NT Registry
  - Miscellaneous services and applications such as mail applications

Securing ACS

- Administrator access should be limited
  - Remote administrative access should be turned off or limited to trusted networks
  - Restrict physical and logon access to the ACS host
  - Use hard-to-guess passwords for the ACS administrator database
  - Physical security
  - Use firewalls
  - Use intrusion detection systems (IDS), both host-based and network-based
  - Do not use virus scanners because of heavy system usage when operating

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

05/02 BW8257