Global Information Assurance Certification Paper

Secure configuration of Widows 2000 IAS
Kris Wicks
March 10, 2002

Summary

This paper provides an overview of Windows 2000 Internet Authentication Service (IAS), Microsoft's implementation of the RADIUS protocol, and guidelines for secure implementation of the product. IAS allows VPN and RAS remote users to access a network by acting as a central authenticator for user accounts requesting access. IAS integrates well with Microsoft's Active Directory (AD) and Routing and Remote Access Service (RRAS). The focus of this paper is secure configuration of IAS for dial-in and VPN remote access.

IAS is a solid implementation of RADIUS, with many extra features not found in the RADIUS specification (RFC 2865). This paper focuses on several vulnerabilities either known specifically to IAS or to the RADIUS specification in general and provides methods to mitigate the risks of those vulnerabilities.

How IAS works: A brief overview

IAS is the Microsoft implementation of RADIUS, and follows the RFC 2865 specifications, but it expands upon Remote Access Policies. These steps are inherent to all RADIUS implementations:

1. A user attempts a connection to a NAS using an authentication protocol such as CHAP or EAP. The connection attempt contains the username and password of the user attempting access.

2. The NAS forwards this information to the IAS server in an Access-Request packet. The packet contains a NAS-Identifier field, which is created by the NAS for the identification of the specific request. This is a simple counter, which is incremented at each new request.
The packet also contains an attribute called a request authenticator. This is a 16 octet random value which is used in conjunction with the shared secret and an MD5 hash to encrypt the username and password.

3. The IAS server already knows the shared secret, and gets the request authenticator from the Access-Request packet. IAS uses this information to decrypt the username and password in the Access-Request packet.

4. If the password is valid, the IAS server sends the NAS an Access-Accept packet. If the password is invalid, IAS sends an Access-Reject packet back to the NAS. Both packets use the NAS-Identifier from the Access-Request packet, and must include a Response Authenticator attribute, which is an MD5 hash of the original Access-Request packet. If the Access-Accept or Access-Reject packet has an incorrect Response Authenticator, the

NAS will silently drop the packet. Silently dropping the packet does not mean that an error code is not generated, but that the IAS server does not spend any more time processing the packet.

Centralized management

Regardless of NAS type, central management is as simple as setting policy on the IAS server and configuring all NAS for RADIUS authentication. After a Windows 2000 RRAS server has been configured to use IAS authentication, the option to set access policy disappears from the management console of the RRAS server.

Logging IAS access

The IAS server can be configured to log all authentication requests from the NAS servers in either DB format or in IAS format. The formatting type denotes a difference in log *entry* format only. Both log types are flat text files. IAS format contains more information on the connection, but more is not always better, and as confusing as IAS logs can be, less is definitely more.

The following is a sample entry (access-request) from an IAS-formatted log file.

10.10.10.10,client,06/04/1999,14:42:19,IAS,CLIENTCOMP,6,2,7,1,5,9,61,5,64,1,65,1,31,1

The format of this record, and of each record in your log file, includes a header followed by the attribute-value pairs for all attributes contained in the packet being recorded.

The first seven positions of the record are the header, which includes:

Value shown in example	Attribute	ID	Data type	Represents
10.10.10.10	NAS-IP-Address	IAS Header	Text	The IP address of the NAS sending the request
client	User-Name	IAS Header	Text	The user name requesting access.
06/04/1999	Record-Date	IAS Header	Time	The date that the log is written
14:42:19	Record-Time	IAS Header	Time	The time that the log is written
IAS	Service-Name	IAS Header	Text	The name of the service running on the RADIUS server
CLIENTCOMP	Computer-	IAS	Text	The name of the RADIUS

Name Header server

("Interpreting IAS-formatted log files", P1)

The RADIUS attributes User-Name and User-Password are considered sensitive, and as such are not logged. It is interesting to note that in practice, the IAS header User-Name attribute will almost always be the same as the RADIUS User-Name attribute.
After the header, the entries are listed by a numerical value indicating an attribute type, followed by an attribute value, usually but not always represented numerically. In other words;
<First_Attribute>,<First_Attribute_Value>,<Second_Attribute>,<Second_Attribute_Value>,…
For example, the first attribute pair after the IAS header is 6,2. 6 is the RADIUS Service-Type attribute. The value 2 corresponds to the Framed Service-Type.
Whereas the DB-Export log file uses a fixed sequence of attributes, the IAS-Formatted log entries are dependent upon the format defined by the NAS. With more than one type of NAS, such as a RAS solution and a VPN concentrator – to say nothing of routers – the IAS-Formatted logs can become very hard to read. Thankfully, the Windows 2000 Server Resource Kit contains a tool to parse this information and make it a little more readable. Iasparse.exe interprets attribute pairs as Attribute name and Verbal attribute value. Iasparse can be very useful for troubleshooting, but not so much for auditing purposes, as it can turn one line in a log into a page of data. Nor can it interpret Vendor Specific Attributes (VSA) that are not built in to IAS.
The IAS-Formatted log type was created first, in the NT4.0 version of IAS, but the DB-Export version, having a static sequence is more suitable for export using ODBC, is easier to read, and contains all the information likely to be needed.

Shared Secrets

A shared secret is a password shared by a NAS and the IAS server for mutual authentication. A shared secret can be up to 128 bytes long, is case sensitive and can include all characters found on a standard US keyboard. IAS allows shared secrets up to 64 characters long, and best practice is to set the shared secret to at least 22 characters long (Davies, 6), with a random mix of upper and lower case, as well as numbers and special characters. Use the most complex password possible. Remember, the shared secret only needs to be entered twice; once on the NAS, and once on the IAS server. If the NAS must be rebuilt or replaced, creating a new shared secret and setting it for the connection is a trivial task.
All RADIUS implementations, including IAS allow using the same shared secret for all NAS, but this is not a good idea. While certainly no one reading this article has ever written down a shared password or kept one in a file anywhere, many administrators who do not understand security do. Also, if shared secrets are the same for all NAS on the network, any vulnerability exploited to obtain the shared secret for one NAS would give away the password for all NAS. Since the shared secret is encrypted with the username and password of the user requesting access in an Access-Request packet, discovery of the shared secret would help an attacker greatly in the discovery of user passwords.

Fault tolerance

IAS does not support network load-balancing of RADIUS servers, but backup servers can be created and set up as forwarders, should the primary IAS server go down. Which machine to be used as primary and which to be used as a backup can be configured on the NAS ahead of time.

Profile management

Simple user-level access permissions can be assigned for remote access by modifying individual user accounts from Active Directory Users and Computers, but this can be difficult to manage and control in a large environment. IAS includes group based Remote Access policies to enable administrators to more tightly control remote access to the network.

Remote Access policies can be used to control remote access based on the following conditions:

Called-StationID	Phone number dialed by user
Calling-Station-ID	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client (NAS)
Client-IP-Address	IP address of RADIUS client (NAS)
Client-Vendor	Manufacturer of RADIUS proxy or NAS
Day-And-Time-Restrictions	Time periods and days of the week during which user is allowed to connect
Framed-Protocol	The protocol to be used (PAP, CHAP, MS-CHAP, EAP)
NAS-Identifier	String identifying the NAS originating the request
NAS-IP-Address	IP address of physical port used by the NAS originating the request
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used (PPTP or L2TP)
Windows-Groups	Windows groups the user belongs to

Once the profile has been created, Remote Access policies can be applied to further control access. The policies which will be focused on in this paper are:

- Permitting the use of only specific authentication protocols.
- Setting maximum idle time
- Setting encryption level.

- Setting packet filters to control host and protocol access while the user is connected.

Packet encryption is especially important in light of recent findings that the User-Password encryption technique is flawed (Hill, 4). It is a good idea to set this to Strongest on all profiles. Strongest encryption uses MPPE with a 128-bit key for Dial-in or PPTP and 3DES-128 for L2TP connections. This setting requires the Windows 2000 strong encryption pack to be installed. If strongest encryption is not an option, strong is supported by win9x clients and provides MPPE with a 56 bit key for Dial-in or PPTP and 56-bit DES for L2TP.

Remote Access policies are restrictive, meaning that a connection attempt which doesn't match a policy is automatically dropped. The first policy that matches the user's settings is applied. If all the requirements of the first policy are not met, the next policy in the list is tried.

The order policies should be assigned is as follows:

Admins – This remote access group will probably only access the network remotely when there is a problem with the network that the administrator can fix from home. Since this group will have the largest amount of access, they should have the most restrictive protocol and policy requirements. Only allow EAP authentication, and set the "Disconnect if idle for" time to 15 minutes. Depending on the security of the facility, you may choose to restrict dial-in to the admin's home number, but this requires a separate Remote Access Policy for each admin.

Contractors or other external users – Each contractor may have its own requirements, which means each contractor may need its own group. A good policy for contractors is to require MS-CHAP v2 for VPN, and MS-CHAP for dial-in, allow access from 6am to 6pm, and allow an idle time of 30 minutes.

Management – This group can be the Achilles heel of an organization's IAS group management strategy, not because they are careless, but because often managers will demand a high amount of access with low protocol requirements, and won't understand the security implications. Win9x clients can be supported by requiring that MS-CHAP v2 be used for VPN connections, and MS-CHAP v1 is used for RAS connections. 24hr access will probably be required. Set the idle disconnect time to 30 minutes.

Remote Access users – If the user has access, but is not listed in any of the other groups, this is the catch-all. Allow MS-CHAP v1 for dial-in, MS-CHAP v2 for VPN, allow access for evenings and weekends only.

Protocol filters should also be set up for these groups. Protocol filters for IAS can be set as permissive (Allow all protocols except), or restrictive (Deny all protocols except). They can also be set to filter incoming or outgoing traffic to the network. It is a good idea to filter incoming traffic to the network. Unfortunately, IAS does not include a pre-configured list of protocols and Multiple protocol entries can't be made in the same filter, so Each entry must be entered manually, and a group of ports which are all used by one protocol can't be grouped together. Including this functionality would have simplified construction of restrictive filters greatly.

Since it will probably not be known what an admin may need access to on the network, the filters for this group should remain un-configured. All other users should be configured with a restrictive filter. Although this can be time consuming, it is by far the more secure filter implementation.
For contractors, only email (TCP 1260 and 1263 if the company uses Exchange), web (TCP 80 and 443), and such other services as are required for them to perform their work should be allowed. If possible, allowing NetBIOS file sharing (UDP 137 and 138, TCP 139) through the contractors filter should be avoided. If this is not possible, the filter should be configured to allow NetBIOS traffic only to the specific servers housing the shares the contractors need access to, and all data should be kepr to a minimum of servers.
For managers and Remote Access users, allow email, web, telnet, FTP, and any other commonly used services at the site.

Disable LAN Manager Authentication for MS-CHAP v1. NTLM contains a vulnerability in the hashing function which allows an attacker to obtain a user password more easily. To disable is, change the DWORD registry value AllowLMAuthentication to 0 in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RAS\Policy on the IAS server.

Secure protocol configuration

The last – but one of the most important – options to configure will be the authentication protocol used. IAS allows five different protocols to be used for authentication. During a connection request, it attempts first to use the most secure of the protocols allowed, followed by the less secure types. Let's take a look at the types, from least to most secure:

PAP (Password Authentication Protocol) – Passes all data clear text, including passwords. Not recommended, but some proprietary token card and one-time password solutions require it.

CHAP (Challenge Handshake Authentication Protocol) – Designed to address the concern of sending plaintext passwords. The encryption algorithm for calculating CHAP responses is well known, and passwords can be cracked with dictionary attacks or brute force with relative ease. Although it's still one of the most highly used authentication protocols, it is not recommended.

MS-CHAP– MS-CHAP is a variant of CHAP which allows passwords to be saved in encrypted form on the authenticating server. The challenge response is calculated with an MD4 hash of the password and NAS challenge. This allows the remote client to authenticate to a Windows 2000 domain. This protocol has the same vulnerability to attacks as CHAP, but it is the most secure authentication available for Win9x dial-in clients.

MS-CHAP v2– Microsoft's second try at a proprietary authentication protocol. It provides stronger initial encryption and mutual authentication. Supported for dial-in or VPN connection using Windows 2000 or XP, but only supported for VPN connections on Win9x and NT4.0 clients.

EAP – Not exactly an authentication protocol in-and-of-itself, but more of an authentication framework for highly secure plug-ins. EAP is designed to support any current authentication scheme such as smart cards, generic token cards and certificate authentication, as well as any future authentication mechanisms. EAP-TLS is built in to Windows 2000 as a smart card or digital certificate reader, but is not present in previous versions of Windows.

Ideally, EAP would be used exclusively for authentication. But unless staff is only allowed to use RAS or VPN services from company laptops, it will be difficult to require that all dial-in users use Windows 2000 or better, and win9x does not support EAP. MS-CHAP v2 at least will be required for standard users, but administrators should be required to use Win2k or XP and EAP made requirement in the remote access policies for the Administrators template.
XP Home Edition does not allow domain authentication from a network connection, but does allow it through a dial-in or VPN connection. Unfortunately, it only allows one-step authentication, so if token cards or one-time passwords are used for remote access, domain authentication will not be possible.

Putting it all together

Now that all the pieces have been put together, let's implement a secure IAS server. One advantage to IAS is that it comes with all Windows 2000 Server platforms (Server, Advanced Server, Datacenter Server), and does not require any extra licensing over the cost of the server license.
These instructions only configure the IAS server; a sample NAS configuration will not be shown. It is possible to place a NAS on the same server as the IAS server, but this is a very bad idea, since the NAS by its nature is more susceptible to direct attack from outside sources, and thus more vulnerable than an IAS server should be.

Installing IAS
IAS should be installed on a Windows 2000 server on the Active Directory domain.
-Go to Start-> Settings -> Control Panel
-Open the Add/Remove programs, select Add/Remove Windows Components.
-Highlight Networking Services, click the Details button. Put a check mark in the Internet Authentication Service box. Click OK.
-Click Next on the Windows Application window, and IAS will be installed and the service started. Click Finish on the Windows Components Wizard. There is no requirement to reboot.

-Open up the Internet Authentication Service administrative console from the Administrative tools. You will do all your administration of IAS from here.

In order to use Windows group-management with IAS, the server must first be authorized in active directory. All this really does is to add the server to the IAS & RAS Computers global group. To do this from the IAS admin console, right click the IAS top level node and left click "Authorize this Server". A domain admin account or an account with permission to modify groups in the default domain must be used to authorize an IAS server.

Add an access client

- To create a new connection to a NAS client, Right click the Clients folder and select New Client.
- Type in a Friendly name, which will be the client's display name. The protocol will always be RADIUS. Click Next.
-Type in the IP Address of the NAS (Do not use the server name), select the Client-Vendor type or leave this set to the default Radius Standard value. Enter the shared secret unique to this NAS.
-Put a check mark in the "Client must always send the signature attribute in the request" box. This tells the IAS server to automatically drop the access request if it does not contain the Message-Authenticator attribute. The Message-Authenticator attribute is an MD5 hash of the entire access-request with the shared secret as the key. In order for this to work you must configure the NAS to always send the message-authenticator attribute.

Set logging

- Click Remote Access Logging, right click the Local File entry in the right hand pane.
- On the Settings tab, put a check mark in the Log Accounting Requests and Log Authentication Requests boxes.
- On the Local File tab, set the log file format to Database Compatible File Format. Although the default is to set no size limit on the log file, the log file can only be cleared by deleting the Iaslog.log file itself, so a functional limit should be set of 10MB.
IAS is also configured by default to log successful and rejected authentication to the Windows 2000 System Event log. This can be changed if so desired by right clicking on Internet Authentication Service, go to Properties, and on the Service tab uncheck Log rejected or discarded authentication requests and Log successful authentication requests.

Set Remote Access Policy

If Remote Access policies are currently in place on an NT4.0 IAS server or a RRAS server, these policies can be copied over using the NETSH command. On the server with policy applied, run:
NETSH AAAA SHOW CONFIG > a:\policies.ext
From a command prompt to copy the files to a floppy. Transfer the floppy to the server the policies are to be copied to, then run
NETSH exec a:\policies.ext

If there are no policies in place on any other servers,
-Right click Remote Access Policy, select New Remote Access Policy.
-Type in a descriptive name for the policy. Click Next.

-Click add to select the conditions to apply to this policy. Refer to the Secure Group Management section above for information on how to set this.
-On the next screen, select Grant Access or Deny Access, depending on the policy. Generally no Deny policy is necessary, since access is denied by default if the connection request is not authorized
-The Edit Profile option allows the new Remote Access Policy to be more finely edited.
-In the Authentication tab, select the authentication profiles appropriate to the current profile. MS-CHAP v2 and MS-CHAP are selected by default.
-In the Encryption tab, the level of communication encryption supported by the connection can be set. This option is only valid if the connection is made through a RRAS server.
-The Dial-in Constraints tab is a slight misnomer. This tab allows access restraints to be set for any access type, as well as maximum session length and idle disconnect time.
-The IP tab allows IP packet filters for this profile to be defined. It also allows an option to specify whether an incoming connection will be allowed to specify its own IP address, or if one will be set for it by the server. The server should always set incoming connections' IP addresses to mitigate the risk of IP spoofing.

And that's it. Once the NAS is configured to point to the IAS server for authentication, this server will be ready for business.

Recent Concerns

There have been several reports issued recently on vulnerabilities in the RADIUS protocol. Most notably, Joshua Hill wrote "An Analysis of the RADIUS Authentication Protocol", exposing some major flaws in the protocol. While some of these vulnerabilities may depend on the implementation of the standard, some of the issues are based on flaws in the standard itself. This is a serious issue, considering the almost ubiquitous nature of the RADIUS protocol in network Access environments. Microsoft seems to have implemented RADIUS fairly solidly as IAS, since most multiple-vendor advisories I found on RADIUS at Security Focus listed IAS as unaffected by the particular vulnerability. It has been attempted here to address all reported vulnerabilities which are particular to IAS or which are flaws in the RADIUS protocol.

References:

"Internet Authentication Services for Windows 2000". June 1, 2000 URL: http://www.microsoft.com/windows2000/techinfo/administration/radius.asp (Feb. 3, 2002)

Hill, Joshua. "An Analysis of the RADIUS Authentication Protocol". November 24, 2001 URL: http://www.untruth.org/~josh/security/radius/radius-auth.html (Feb. 2, 2002)

Davies, Joseph. "RADIUS Protocol Security and Best Practices". January 17, 2002. URL: http://www.microsoft.com/windows2000/techinfo/administration/radius.asp (Feb. 2, 2002)

Rigney, Carl, et al. "Remote Authentication Dial In User Service". RFC 2865. June, 2000. URL: ftp://ftp.isi.edu/in-notes/rfc2865.txt (Feb. 3, 2002)

Rigney, Carl, et al. "RADIUS Extensions". RFC 2869. June, 2000. URL: ftp://ftp.isi.edu/in-notes/rfc2869.txt (Feb. 3, 2002)

"Interpreting IAS-formatted log files". February 28, 2000. URL: http://www.microsoft.com/windows2000/en/server/help/sag_ias_log1a.htm

Zorn, Glen, et al. "Microsoft Vendor-specific RADIUS Attributes". March, 1999. URL: ftp://ftp.isi.edu/in-notes/rfc2548.txt (Feb. 3, 2002)

Deupree, Robert Jr, et al. Designing a Secure Microsoft Windows 2000 Network. Redmond: Microsoft Corporation, 2000.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor