Global Information Assurance Certification Paper

RADIUS – A Protocol for Centralized Authentication

William F. Evans, FAIC

October 27, 2000

Introduction

One of the more daunting challenges facing network administrators and security personnel over the past few years has been the increasing need to provide remote users with network access without compromising required security. The need for network access now extends beyond the company employee working remotely to encompass access by clients, trading partners, and in some cases "cooperative competitors" (i.e., the "co-opetition"). Clearly, the amount of remote access being requested and the nature of the desired access have both changed.

Maintaining control over security for the large number of network access points used by large corporations and Internet Service Providers (ISPs) is a necessary but difficult requirement that may be further complicated by hardware and/or software differences across the enterprise. In many cases, this task can be made less onerous through centralization of security functions associated with remote access. RADIUS (***R***emote ***A***uthentication ***D***ial-***I***n ***U***ser ***S***ervice) represents one mechanism for achieving this objective. This paper will describe and summarize what RADIUS is, it's underlying technology, and it's operation.

History

RADIUS is the name given to a UDP-based protocol used in the authentication and authorization of users attaching to a network via remote access through Network Access Servers (NAS) or other devices. It provides a standardized mechanism for communications between the NAS and one or more centralized security servers responsible for authentication and authorization.

Originally introduced by Livingston Enterprises (now part of Lucent Technologies), an Internet Engineering Task Force (IETF) Working Group for RADIUS was formed in 1996 to standardize the protocol as defined in RFC 2058 (January 1997). This has resulted in IETF recognition of RADIUS as a dial-in security solution as defined in RFC 2138 in April 1997 (with RFC 2138 obsoleting the original RFC 2058).

Partially as a result of this standardization, RADIUS is now a widely accepted protocol that has been adopted by a number of hardware and software vendors. The term RADIUS was originally applied to the Livingston "NAS helper" protocol only, but has been expanded over time to reference authentication and authorization systems using the base protocol. RADIUS technology has likewise been extended to include a number of other functions in the "AAA services" (Authentication, Authorization, and Accounting) category.

Operation

A basic RADIUS system consists of a centralized server responsible for authenticating users requesting network connection via a remote access device. When the user connects to the remote access device (typically a Network Access Server, NAS), an authentication request is sent to the central authentication server (the RADIUS server).

This authentication request message contains the user-supplied name and password, as well as the identity of the access device sending the request and the port being used for the remote connection. Since communication with the RADIUS server occurs across the network, the user-supplied password is typically encrypted by the NAS before the authentication request is sent to minimize the chance for compromise.

The authentication request can be sent to either a "local" RADIUS server via the local area network or to a "remote" server over a wide area network. This provides flexibility in designing the overall network architecture by allowing placement of the RADIUS server at the most appropriate location, not necessarily at the physical point of remote access. This is an important feature in cases where a "host" organization must maintain control of the authentication process but wishes to outsource most or all

other elements of the remote access infrastructure. The RADIUS protocol also facilitates authentication redundancy by allowing the client devices to route requests to alternative servers if the primary RADIUS server cannot be reached.

When the RADIUS server receives the authentication request, it validates the request (to ensure it originated from a valid client device) and then decrypts the data packet to expose the user name and password. These credentials are then passed to the system being used to conduct the authentication process. The information used to authenticate the user logon request can be contained in a password file, centralized authentication database, or a custom (or proprietary) system. Other commercial security systems (e.g., Kerberos) that support the RADIUS protocol can also be interfaced with to provide authentication.

If the credentials (name and password) of the user requesting access are properly matched against the stored information, the RADIUS server returns an authentication acknowledgement message to the NAS. This message contains the connection information (network type and services) necessary for attaching the authenticated user to the network. Hence, the type of connection (TCP/IP, PPP, SLIP, etc.) and access restrictions are applied to the user's login in accordance with pre-established policies. In the opposite case, if the credentials received from the RADIUS client do not match information in the authentication information store, the server returns an authentication reject message to the NAS. This message causes the NAS to deny access to the user requesting it.

In addition to the encryption of the user password during communications between the NAS and the authentication server, the RADIUS protocol also provides for additional security to avoid compromise of authentication via tampering with the message transfer process. As mentioned above, the messages passed between RADIUS clients and servers are validated to prevent "spoofing" of these requests. The RADIUS server accomplishes this by sending an authentication key to the RADIUS client devices. This message acts as a digital signature to ensure that the proper authentication server is truly originating authentication messages.

Technology

RADIUS is a distributed client-server system comprised of an authentication server and client devices communicating via the RADIUS protocol(s). The devices through which remote network connections are attempted act as RADIUS clients and communicate with the RADIUS server to approve or deny access requests. The RADIUS server component is installed on centralized hardware and contains the information necessary to evaluate connection attempts for authorized access (including network connection parameters and access restrictions). This information can be maintained in a password file, a separate database, or other repository determined by the particular requirements of the implementation.

Message traffic (between RADIUS server and clients) is UDP-based. The initial IETF documentation (RFC 2058) specified that the RADIUS server listen for message traffic on UDP port 1645. However, this was changed to UDP port 1812 in the later specification (RFC 2138) to avoid conflict with the datametrics service also assigned to port 1645.

UDP was used for the RADIUS protocol for technical reasons associated with its intended use of authenticating access requests. As described earlier, a login attempt generates an authentication request message directed at the RADIUS (authentication) server. Since the RADIUS protocol supports message routing to alternate available authentication servers in the event of a failure of the primary server, a copy of the message must be retained above the transport layer to allow retransmission. UDP provides this capability. Furthermore, the timing and nature of authentication processes associated with a login attempt do not typically require the level of automatic retransmission, the slower guaranteed delivery mechanism, or the overhead associated with TCP. Finally, the stateless nature of UDP allows elimination of code required to handle maintaining stateful connections – in the RADIUS protocol, the server and client(s) establish a UDP connection and simply leave it open despite any network failure events that may occur.

Several methods of authentication are supported by the RADIUS protocol, including Unix, Kerberos, or domain. In each case, the authentication process is handled in a slightly different fashion. For example, Unix authentication compares supplied credentials (user name/password) to information in a local Unix password file, while Kerberos "mode" determines authentication by passing the credentials to a specified Kerberos server. For the so-called domain authentication mode, the RADIUS server evaluates the user

name/password credentials against information contained in a local "authfile". The entries in the authfile determine the source (type and host) to be used for authorization. If a specific entry does not exist in the authfile, a default entry is typically present to define authentication processing. This architecture provides the network administrator or security officer with the ability to determine and direct authentication methods from a central source.

Although multiple methods of authentication are supported by the RADIUS protocol, there should be only a single method associated with each name existing in the user information data store. The association of multiple authentication methods with a single user name exposes a vulnerability to attacks that are capable of gaining access via the least secure of the listed methods.

Regardless of the authentication method used, the user-supplied password or the user-supplied challenge response is encrypted prior to transmission across the network. The secret key shared between the RADIUS server and its clients is encrypted via a one-way hash algorithm (RSA MD5), the result of which is then mathematically combined with the user-supplied password via an exclusive-or logical operation. The derivative of this manipulation is the value that is passed to the server in the authentication request message. Passwords longer than 16 characters are processed in 16-bit groups via subsequent hash operations in a specified pattern until the password (up to the maximum length of 128 characters) has been encrypted.

Information used for the authentication process includes attributes that can be configured on the RADIUS server on a per-user basis. The mode of storage of this information varies by implementation, but typically the server accesses this information via three files – the USERS file (information required to authenticate users), the CLIENTS file (information required to authenticate RADIUS clients), and a DICTIONARY file (instructions on reading USERS file attributes).

In addition to basic credentials, the authorization request message sent from the RADIUS client (typically the NAS) to the RADIUS server includes information such as client ID, client port, user service, and specialized connection information (e.g. framed-protocol if SLIP or PPP is being requested). As with the basic credentials (user name/password), any other items passed to the server in the authentication request are evaluated against the recorded user information store. Satisfaction of all criteria associated with the authentication request generates an authorization approval by the RADIUS server, and an authentication acknowledgement is sent to the client that initiated the authorization request.

Advantages

The RADIUS client-server architecture provides an open and scalable solution that is broadly supported by a large vendor base and can be readily modified to meet a variety of situations. RADIUS-based authentication servers can be modified for use with a large number of security systems on the market and will work with any communications device that supports the RADIUS client protocol.

Any component of the overall security system that supports the RADIUS protocols can derive authentication and authorization from the central RADIUS server, or the central server can integrate with a separate authentication mechanism. The RADIUS server has modifiable "stubs" which enable customers to customize it to run with any type of security technology. This flexibility in authentication mechanisms facilitates integration with existing and/or legacy systems when necessary, thus allowing an organization to maintain its investment in any existing security technology it may have.

The distributive nature of RADIUS effectively separates the security processes (carried out on the authentication server) from the communications processes (implemented by the modem pool or NAS) and supports a single centralized information store for authorization and authentication information. This can significantly lessen the administrative burden of providing appropriate access control for a large number of remote users. If redundancy is not required to ensure high availability, this centralization can be maximized since all RADIUS-compatible hardware on a LAN can derive authentication services from a single server.

The RADIUS protocol’s utility extends beyond systems using network access devices and terminal servers for network access. RADIUS has been widely accepted by Internet Service Providers (ISPs) in providing virtual private network (VPN) services. In this context, RADIUS technology allows an organization to utilize an ISP’s infrastructure for communications while simultaneously securely

maintaining and controlling its authentication servers in-house. Once an authenticated network connection is established, subsequent communications can be conducted through a secure PPTP ("Point-to-Point Tunneling Protocol") channel.

Since RADIUS is an IETF standard and open protocol, there are a large number of tools, support lists, and archives available. The protocol continues to be expanded and enhanced by the continuing activities of standards organizations such as the IETF and its NASREQ (Network Access Server Requirements) working group. Extensions to the RADIUS protocol have been proposed or approved for areas such as implementation of Point-to-Point Tunneling Protocol/Layer Two Tunneling Protocol (PPTP/L2TP) Compulsory Tunneling, Attributes for Challenge Handshake Authentication Protocol (CHAP) Support, IP Security Extensions, Salt-Encryption of RADIUS Attributes, and a number of Management Information Bases (MIBs) for Simple Network Management Protocol (SNMP) use. The RADIUS protocol also serves as the basis for the emerging IETF next-generation AAA (Authentication, Authorization, and Accounting) protocol called "DIAMETER".

Disadvantages

In its fundamental implementation, the RADIUS protocol combines the processes of authentication and authorization, and the very nature of the protocol makes separation these functions difficult. As a result of this, RADIUS is well suited for situations, such as found in service provider networks, where authentication and authorization processes are relatively simple and typically consist of a single step or at most a few steps. However, RADIUS may not be appropriate for complicated networks requiring frequent and complex authorization dialogs following the initial user authentication. In these cases, alternative protocols that more effectively segregate the authentication and authorization functions (e.g., Cisco TACACS+) will likely be more effective.

Although RADIUS is an accepted standard protocol, not all vendor products (clients and servers) that claim to be RADIUS-based are fully standard-compliant. Hence, interoperability issues can arise in RADIUS implementations.

RADIUS implementations encrypt only the user-supplied password (or challenge response) passed from the client to the server. Other information contained in the messages passed between the RADIUS clients and servers is left unencrypted. Since this includes items such as user name and service authorization information, RADIUS implementations may be more vulnerable to session capture and replay attacks. Other protocols providing authentication functions encrypt all information contained in the authentication request message and may be less susceptible to this type of attack.

Summary

RADIUS is an open, IETF-based remote access security protocol (RFC 2138) that has been widely accepted by a number of security product vendors and Internet Service Providers (ISPs). It provides a relatively simple, flexible and extensible mechanism for enabling client-server based authentication and authorization services. The basic protocol specification is somewhat dated but continues to be extended to provide for enhanced services. Although not applicable for all scenarios, RADIUS does provide a valuable service in today’s security efforts.

References

Aboba, Bernard (Editor), "Network Access Server Requirements (nasreq)",

IETF Nasreq Charter, 9 August 2000,
URL: http://www.ietf.cnri.reston.va.us/html.charters/nasreq-charter.html, (10/2000)

Cisco Systems, "How Does RADIUS Work?", Tech Notes,
URL: http://www.cisco.com/warp/public/707/32.html, (10/2000)

Cisco Systems, "RADIUS Attributes", Security Configuration Guide, 30 August 2000,
URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt6/scradatb.htm,
(10/2000)

Digital Tool, "Your Routers are Probably Not Secure", Networking and Network Security,
URL: http://www.dtool.com/rsec.html, (10/2000)

Funk Software, "Radius Resources",
URL: http://www.funk.com/Radius/, (10/2000)

Karimi, Hamid and Jain, Vipin, "New spec will help secure LANs", Network World/ NetworkWorldFusion, 30 August 1999,
URL: http://www.nwfusion.com/news/tech/0830tech.html, (10/2000)

Klingler, Steven, "Server Speak: RADIUS gets servers talking", Standards Update,

InternetWeek with LANTimes Online, January 1998,
URL: http://www.lantimes.com/98/98jan/801b034b.html, (10/2000)

Lucent Technologies, "R*emote Network Access Security in an Open Systems Environment",* **RADIUS Remote Authentication Dial-In User Service** *white paper,*
URL: http://www.livingston.com/marketing/whitepapers/radius_paper.html, (10/2000)

McLellan, Vin, "Re: Tacacs plus ver Radius", GNAC.NET Mail Archive – Firewalls,
URL: http://www.mail-archive.com/firewalls@lists.gnac.net/msg01219.html, (10/2000)

"Note – radius-desc.txt", Paha Online - Index of /doc/radius, 16 February 1998,
URL: http://www.rest.ru/doc/radius/radius-desc.txt, (10/2000)

Rigney, Carl, Rubens, Allan C., Simpson, William Allen, Willens, Stephen, "Remote Authentication Dial In User Service (RADIUS)", RADIUS Working Group Internet Draft (File: draft-ietf-radius-radius-05.txt), July 1996,
URL: http://www.rest.ru/doc/radius/draft-ietf-radius-radius-05.txt, (10/2000)

Shiva Corporation, "RADIUS Security", 1997,
URL: http://www.shiva.com/prod/docs/lras457/netcon/re0133.htm, (10/2000)

Shiva Corporation, "The RADIUS Protocol - Overview", 1997,
URL: http://athena.shiva.com/prod/docs/archive/sam/samunix/backinf/amre0004.html, (10/2000)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event