

RADIUS Whitepaper

(Remote Authentication Dial-In User Service)

Remote Network Access Security in an Open Systems Environment

Introduction

Every time a modem is added to a computer or communications server on a corporate network, that network becomes more vulnerable to security breaches. Network Administrators are left with few tools to guard against break-ins. State of the art security systems generally require special hardware or are only compatible with a small number of products. This problem is multiplied several times in large networks with many points of access.

Lucent Technologies InterNetworking Systems has developed a distributed security solution called Remote Authentication Dial-In User Service, or RADIUS, that solves the problems associated with meeting the security requirements of remote computing. This solution eliminates the need for special hardware and provides access to a variety of state of the art security solutions. Distributed security separates user authentication and authorization from the communications process and creates a single, central location for user authentication data.

Based on a model of distributed security previously defined by the Internet Engineering Task Force (IETF), RADIUS provides an open and scalable client/server security system. The RADIUS server can be easily adapted to work with third-party security products or proprietary security systems. Any communications server or network hardware that supports the RADIUS client protocols can communicate with a RADIUS server. Lucent offers the RADIUS server free of charge to its customers and supports the RADIUS client protocols in its PortMaster family of communications servers and routers. Lucent is assisting the IETF's Network Access Server Requirements Working Group to allow other vendors to utilize this technology.

RADIUS Client/Server Architecture

RADIUS is a system of distributed security that secures InterNetworking Systems to networks and network services against unauthorized access. RADIUS includes two pieces: an authentication server and client protocols. The server is installed on a central computer at the customer's site. RADIUS is designed to simplify the security process by separating security technology from communications technology.

All user authentication and network service access information is located on the authentication, or RADIUS, server. This information is contained in a variety of formats suitable to the customer's requirements. RADIUS in its generic form will authenticate users against a UNIX password file, Network Information Service (NIS), as well as a separately maintained RADIUS database. Communications servers working with modems-such as the PortMaster-operate as RADIUS clients. The RADIUS client sends authentication requests to the RADIUS server and acts on responses sent back by the server.

How it Works: User Authentication with RADIUS

- RADIUS authenticates users through a series of communications between the client and the server. Once a user is authenticated, the client provides that user with access to the appropriate network services. The following is a description of the authentication process using a PortMaster Communications Server and RADIUS.
- Using a modem, the user dials-in to a modem connected to a PortMaster Communications Server. Once the modem connection is completed, the PortMaster prompts the user for a name and password.

RADIUS Whitepaper

(Remote Authentication Dial-In User Service)

Remote Network Access Security in an Open Systems Environment

- The PortMaster creates a data packet from this information called the authentication request. This packet includes information identifying the specific PortMaster sending the authentication request, the port that is being used for the modem connection, and the user name and password. For protection from eavesdropping hackers, the PortMaster, acting as a RADIUS client, encrypts the password before it is sent on its journey to the RADIUS server.
- The Authentication Request is sent over the network from the RADIUS client to the RADIUS server. This communication can be done over a local- or wide-area network, allowing network managers to locate RADIUS clients remotely from the RADIUS server. If the RADIUS server cannot be reached, the RADIUS client can route the request to an alternate server.
- When an Authentication Request is received, the Authentication Server validates the request and then decrypts the data packet to access the user name and password information. This information is passed on to the appropriate security system being supported. This could be UNIX password files, Kerberos, a commercially available security system or even a custom developed security system.
- If the user name and password are correct, the server sends an Authentication Acknowledgment that includes information on the user's network system and service requirements. For example, the RADIUS server will tell the PortMaster that a user needs TCP/IP and/or NetWare using PPP (Point-to-Point Protocol) or that the user needs SLIP (Serial Line Internet Protocol) to connect to the network. The acknowledgment can even contain filtering information to limit a user's access to specific resources on the network.
- If at any point in this log-in process conditions are not met, the RADIUS server sends an Authentication Reject to the PortMaster and the user is denied access to the network.
- To ensure that requests are not responded to by unauthorized hackers on the network, the RADIUS server sends an authentication key, or signature, identifying itself to the RADIUS client. Once this information is received by the PortMaster, it enables the necessary configuration to deliver the right network services to the user.

Benefits of Distributed Security

The distributed approach to network security provides a number of benefits for Lucent Technologies customers. They include the following:

Greater Security

The RADIUS client/server architecture allows all security information to be located in a single, central database, instead of scattered around a network in several different devices. This approach increases security. A single UNIX system running RADIUS is much easier to secure than several communications servers located throughout a network.

Scalable Architecture

RADIUS creates a single, centrally located database of users and available services, a feature particularly important for networks that include large modem banks and more than one remote

RADIUS Whitepaper

(Remote Authentication Dial-In User Service)

Remote Network Access Security in an Open Systems Environment

communications server. With RADIUS the user information is kept in one location-the RADIUS server-which manages the authentication of the user and access to services from one location. Because any device that supports RADIUS can be a RADIUS client, a remote user will gain access to the same services from any communications server communicating with the RADIUS server.

Open Protocols

RADIUS is fully open, is distributed in source code format, and can be easily adapted to work with systems and protocols already in use. This feature saves tremendous amounts of time by allowing users to modify the RADIUS server to fit their network rather than rework their network to incorporate the PortMaster Communications Server.

RADIUS can be modified for use with any security system on the market and will work with any communications device that supports the RADIUS client protocol. The RADIUS server has modifiable "stubs" which enable customers to customize it to run with any type of security technology.

Future Enhancements

As new security technology becomes available the customer can take advantage of that security without waiting for Lucent to add support to the PortMaster. The new technology need only be added to the RADIUS server by the customer or outside resources. RADIUS also uses an extensible architecture which means that as the type and complexity of service the PortMaster must deliver increases RADIUS can be easily expanded to provide those services.

Current Users of RADIUS

Any company with a centralized MIS department managing a large corporate network is concerned with security issues. Many of these customers have already installed RADIUS and others are in the planning stages. All those customers that are using RADIUS have customized it in some way to work with their network systems. For example, one computer manufacturer has adapted its RADIUS server to work with Enigma's security cards. In this network, the RADIUS server manages the communications with the Enigma security technology to validate the user and allow access to the network. In this way, the customer was able to install PortMaster Communications Servers and also maintain its investment in Enigma's security technology.

RADIUS is being used to secure several university networks that provide dial-in IP connectivity to students and faculty. To provide distributed security, the RADIUS server has been customized to work with the Kerberos security system for authenticating user names and passwords.

Several Internet service providers use RADIUS to provide security to users accessing their networks from multiple POPs (Points Of Presence). UNIX security systems are typically used in these environments.

A utility company has customized the RADIUS server in a similar manner, storing names and passwords from over 1000 UNIX password tables.

RADIUS as a Standard: Current Status

An IETF Working Group for RADIUS was formed in January 1996 to address the standardization of RADIUS protocol. RADIUS is now an IETF-recognized dial-in security solution (RFC #2058).

RADIUS Whitepaper
(Remote Authentication Dial-In User Service)
Remote Network Access Security in an Open Systems Environment

Commonly Asked Questions About Computer Network Security

What is network security?

The term network security covers a number of technologies that protect InterNetworking Systems to a network, whether over telephone lines or between networks. These technologies include passwords, encryption and call-back. Each of these technologies work in different ways, and network managers often combine them to create secure network environments.

Why has network security become such an important issue?

Network security is not new to computing, though it is relatively new to personal computing. Mainframe computers have always used high-level security technology to protect sensitive business data. In the early days of personal computing, most CPUs were stand-alone units that could be protected by locking an office door.

Today, new users of technology have made security a critical issue for any type of computing. Growing use of local-area and wide-area networks, laptops and remote computing has increased access to critical business data. Hackers thrive on breaking into vulnerable networks, and security breaches can wreak havoc on a network. Not only is confidential information stolen, but "crackers" have been known to bring down a network through "worms," computer viruses and other hazards to network traffic.

What type of security does Lucent Technologies PortMaster product family support?

Lucent Technologies PortMaster products use a number of advanced security features, including call-back, access filters for hosts and networks, packet filters and RADIUS.

What is RADIUS?

RADIUS, or Remote Authentication Dial-In User service, is a freely available distributed security system developed by Lucent Technologies InterNetworking Systems. Lucent has worked with the Internet Engineering Task Force (IETF) to define RADIUS as an interoperable method for distributed security on the Internet. RADIUS was designed based on a previous recommendation from the IETF's Network Access Server Working Requirements Group. RADIUS is now an IETF-recognized dial-in security solution (RFC #2058).

What is distributed security?

Distributed security is a client/server approach that allows a number of communications servers, or clients, to authenticate a dial-in user's identity through a single, central database, or Authentication Server, which stores all information about users, their passwords and access privileges.

Is distributed security better than other types of security?

Distributed security provides a central location for authentication data that is more secure than scattering that information on different devices throughout a network. It is also more scalable and much easier to manage.

How many users can one Authentication Server support?

A single Authentication Server can support hundreds of communications servers, serving up to tens of thousand of users.

Do Authentication Servers need to be located on the same network as the communications server?

RADIUS Whitepaper

(Remote Authentication Dial-In User Service)

Remote Network Access Security in an Open Systems Environment

Communications servers can access an Authentication Server locally or remotely over WAN connections.

How do Authentication Servers work?

Authentication Servers can be set up in a variety of ways, depending upon the security scheme of the network they are serving. The basic process for authenticating a user includes the following steps: a user dials into a network through a communications server, or Network Access Server (NAS); the NAS forwards the user identification and password to the Authentication Server; then the Authentication Server validates the user and provides access privileges to the network.

How do passwords work and what are their limitations?

Passwords are the most common form of computer security. Some networks require multiple levels of passwords to gain access to various servers or databases. Passwords become weak links when they are shared among colleagues, stolen, written down or created in such a way that they can be easily guessed. For example, users will try to create memorable passwords by using their names or social security numbers.

How does callback work?

Callback is a security feature that works in the following way: a user dials into a communications server and enters a user name and password; the communications server then hangs up the modem connection, searches its database to authenticate the user and then calls the user back at a predefined number. Callback provides good security and cost savings to users who remotely access networks from one location. However, it is inconvenient for traveling executives.

How does packet filtering work?

Packet filters allow network administrators to limit a user's access to specific services on the network. For example, a user may be allowed to send electronic mail, but not copy data files from the network. Packet filtering on the communications server analyzes each message being sent from a remote client. The filter can determine the computer and service the user is attempting to reach and either permit or deny access to that service.

What is encryption?

Data encryption uses a secret code to scramble information so that it can be read only by computers using the same code, or encryption technology. While encryption reduces the risk of unauthorized access, it doesn't create a totally safe networking environment on its own. Code "crackers" are excited by the challenge of breaking an encryption code.