RADIUS协议在AAA系统中的应用研究

王军号,陆 奎
(安徽理工大学,安徽 淮南 232001)

摘 要:RADIUS协议在宽带网络认证授权计费解决方案AAA认证系统中得到了广泛应用。介绍了RADIUS协议的结构特点、报文内容、AAA系统架构和802.1x标准,讨论了RADIUS认证的工作流程,研究了RADIUS协议的认证机制以及在Linux环境下RADIUS服务器的配置方法,建立了RADIUS认证服务器的功能模型,分析了RADIUS协议所采取的安全措施以及存在的安全隐患,并对其安全性的进一步完善提出了建议。

关键词:RADIUS;AAA;802.1x;安全性
中图分类号:TP393.07 **文献标识码**:A **文章编号**:1673-629X(2009)07-0199-04

Research on Application of RADIUS in AAA

WANG Jun-hao, LU Kui
(Anhui University of Science and Technology, Huainan 232001, China)

Abstract: The RADIUS protocol has been widely used in the AAA authentication system for authentication authorization and accounting in the wide band network. Introduced the RADIUS protocol structure and characteristic, packet content and the authentication procedure, the AAA system construction and the 802.1x standard, has studied the RADIUS authentication mechanism as well as under the Linux environment the RADIUS server disposition method, took the security measure and its existence security hidden danger to the RADIUS has been analyzed, built function model of RADIUS server, and further put forward the proposal to its security.

Key words: RADIUS; AAA; 802.1x; security

0 引 言

RADIUS(Remote Authentication Dial In User Service),远程认证拨号用户服务,是一种在网络接入设备和认证服务器之间承载认证、授权、计费和配置信息的协议。RADIUS协议是在认证、授权、计费方面应用最为广泛的协议之一,具有以下特点:

(1)基于客户端/服务器结构。

(2)采用共享密钥保证网络传输安全性。

(3)良好的可扩展性。

(4)认证机制灵活。

因此为提供一套完整、安全的宽带网络认证授权计费解决方案,该协议广泛应用于AAA认证系统中。

1 AAA系统

1.1 802.1x标准

IEEE 802.1x标准定义了一种基于"客户端-服务器"(Client-Server)模式,实现了限制未认证用户对网络的访问。客户端要访问网络必须先通过认证服务器的认证。在客户端通过认证之前,只有EAPOL报文(Extensible Authentication Protocol over LAN)可以在网络上通过。在认证成功之后,正常的数据流便可顺利地通过以太网端口在网络上通行。

1.2 AAA系统结构

AAA是Authentication、Authorization、Accounting的缩写,即验证、授权、计费,是对网络安全访问控制的一种管理,提供了验证、授权和计费三种安全功能。AAA是一个用来对验证、授权、计费这三种安全功能进行配置的一致的管理框架。

如图1所示,AAA系统的体系结构中采用了"可控端口"和"不可控端口"的逻辑功能,利用二层IEEE 802.1x协议,不需要到达三层,由RADIUS和交换机利用不可控的逻辑端口共同完成对用户的认证与控制,业务报文直接承载在正常的二层报文上通过可控端口进行交换,从而可以实现业务与认证分离[1]。采用客户/服务器结构,客户端运行于被管理的资源侧,服务器上则集中管理用户信息,这种结构既具有良好

收稿日期:2008-10-27;**修回日期**:2009-01-17
基金项目:安徽省自然科学基金(2005KJ083)
作者简介:王军号(1970-),男,江苏赣榆人,硕士,实验师,研究方向为计算机网络与多媒体技术。

的可扩展性又便于用户信息管理。

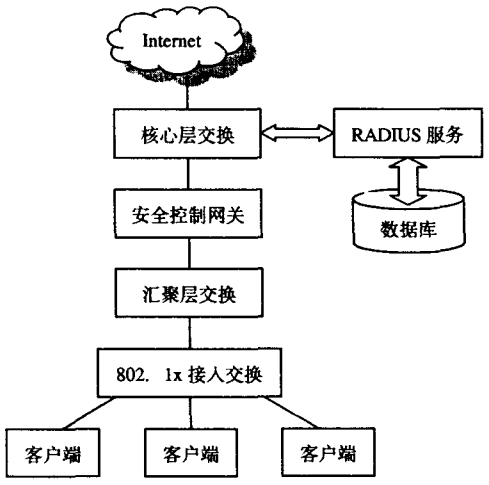

图 1 AAA 系统架构

当用户想要通过局域网与 NAS(Net Access Server)建立连接从而获得访问 Internet 的权限或取得使用某些网络资源的权限时,NAS 起到了验证用户和对应连接的作用,NAS 负责把用户的验证、授权和计费信息透传给 RADIUS 服务器,RADIUS 协议规定了 NAS 与 RADIUS 服务器之间如何传递用户信息和计费信息。

服务器负责接收用户的连接请求、完成验证并把用户所需的配置信息返回给 NAS,NAS 和协议模块之间的验证信息的传递是通过密钥的参与来完成的。

1.3 NAS 基本配置

在 AAA 系统架构中,基于以太网端口认证的交换机连结着认证服务器与客户端,可以用作 NAS,所以应首先配置。在认证服务器上添加交换机,完成 NAS 设备与 RADIUS 服务器之间进行认证报文交互的设置。在认证服务器上开设用户帐户并付费,完成在服务器上关于用户信息的设置,并在客户端与交换机连接的端口上启用 802.1X 端口认证协议。客户端使用已经在服务器上保存的帐号及密码进行认证登录。交换机的主要配置命令如下:

radius - server host 配置认证服务器地址

aaa authentication dot1x 交换机打开 802.1X 认证

aaa accounting server 配置记账服务器

aaa accounting 开启记账

radius - server key 配置认证 key

dot1x port - control auto 开启端口认证

2 RADIUS 协议的认证机制

2.1 RADIUS 数据包格式

RADIUS 协议承载于 UDP 之上,官方指定端口号为:认证授权端口 1812,计费端口 1813。RADIUS 协议数据包格式如图 2 所示。RADIUS 数据包分为五个部分[2]:

(1)编码(Code):一个八位字节,用来标志 RADIUS 包的类型。当收到的包的编码域非法时,该数据包将被自动丢弃。

(2)标识符(Identifier):一个八位字节,用于标记请求和应答数据包的匹配。

(3)长度(Length):两个八位字节,表明该包的总长度。包的最小长度为 20,最大长度为 4095。超出范围的数据包将被丢弃。

(4)鉴别码(Authenticator):十六个八位字节,用于鉴别客户端和服务器端间的信息。

(5)属性(Attributes):不限定长度,用于描述 RADIUS 协议的属性。

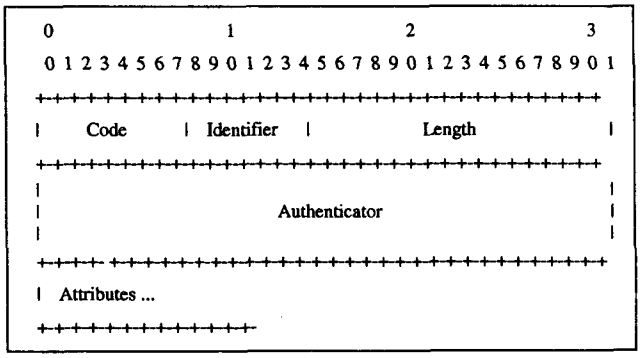

图 2 RADIUS 数据包格式

2.2 RADIUS 的认证过程

RADIUS 认证协商过程是首先客户端将用户帐号和口令传送到 NAS,NAS 生成认证请求包(Access - Request)向 RADIUS 服务器发送,RADIUS 服务器就要先对用户名和口令进行认证;若认证成功,RADIUS 服务器向 NAS 发送接受请求包(Access - Accept),否则,RADIUS 服务器向 NAS 发送拒绝请求包(Access - Reject),NAS 接收到 Access - Reject,拒绝用户的连接请求;NAS 接收到 Access - Accept,允许建立连接,对用户服务授权,接着发送授权用户的开始记帐请求包(Accounting - Request Start),RADIUS 服务器接收请求开始记帐,RADIUS 服务器向 NAS 发送记帐回应信息(Accounting - Response),直到用户与 NAS 的连接断开就发送停止记帐请求包(Accounting - Request Stop),RADIUS 服务器接收请求停止记帐[3],并向 NAS 发送记帐回应信息(Accounting - Response)。整个认证报文交互流程如图 3 所示。

一个 RADIUS 报文中包含一个或多个 RADIUS 属性,这些属性包含了认证计费信息。RADIUS 服务器收到后利用这些属性进行认证和计费[4]。认证计费用到的主要属性如表 1 所示。

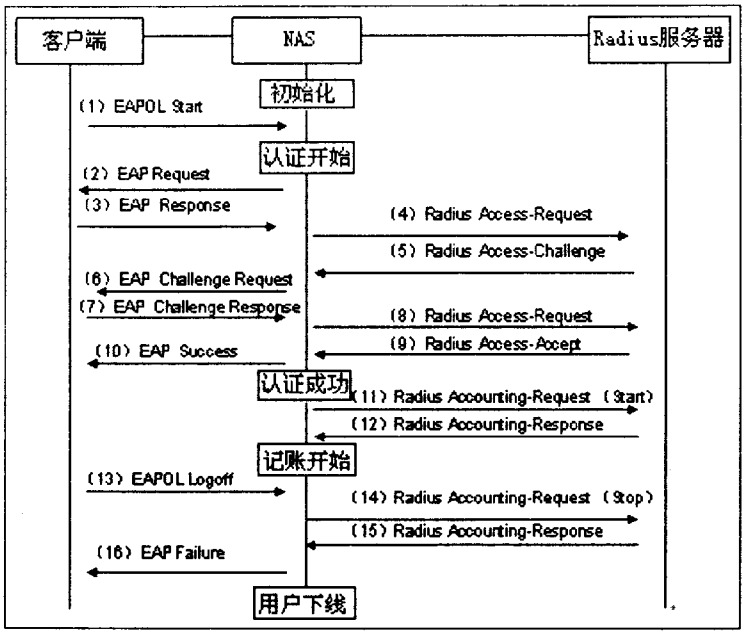

图 3　RADIUS 认证报文交互流程

表 1　认证计费用到的属性

属性名	属性类型	属性含义
User - Name	1	用户名
User - Password	2	用户密码
Acct - Status - Type	40	计费包类型
Acct - Session - ID	44	计费会话 id
Acct - Session - Time	46	计费会话时间

3　RADIUS 服务器配置

由于 Freeradius 是一个开放源代码的软件,所以这里采用 Freeradius - 1.0.2 来搭建 RADIUS 服务器,实现 RADIUS 协议。在 Linux 环境下 RADIUS 服务器配置文件有四个:radiusd. conf, cilents. conf, users, sql. conf。主要配置过程如下[5]:

(1)radiusd. conf 配置。

```
# radiusd. conf 为 RADIUS 服务启动时所读的配置文件
$ INCLUDE $ {confdir} /sql. conf # 引入 sql 模块
authorize {files ldap eap} # 用户授权时用到的模块
authentication {eap} # 用户认证时用到的模块
accounting {sql} # 用户记账时用到的模块
```

(2)clients. conf 配置。

```
# 添加 NAS, ip 为 192. 168. 1. 2, secret 是 RADIUS 服务器和 NAS 的共享密钥
client 192.168.1.2 {
        secret = key
        shortname = westb
}
```

(3)sql. conf 配置。

```
sql {
        server = "server_ip"
        login = "root"
        password = "mysql123"
        radius_db = "radius"
        ...
}
```

这个配置文件主要是关于 RADIUS 与数据库交互的配置信息,采用 MySQL 数据库,root 与 mysql123 分别是登录数据库的用户名与密码,radius_db 是数据库的名字。

(4)users 文件配置。

```
# 添加一个用户,用户名是 test,用户密码是 test
test Auth - Type: = local, User - Password = = "test",
        Service - Type: = Framed - User,
        Framed - IP - Address : = 10.0.0.1,
        Framed - IP - Netmask : = 255.255.255.0
```

通过以上各步骤的配置,RADIUS 服务器就搭建好了,使用以下指令即可运行服务器:radiusd - X。

4　RADIUS 协议的安全性

从 RADIUS 协议内容来看,它所采取的安全机制主要有以下两个方面:

(1)通信双方的身份认证。认证系统的每对实体之间都有一个共享密钥 K,双方在交互报文中附加 MD5(Info + K)放在 Authenticator 字段,通过 Authenticator 字段认证通信双方身份。MD5 算法是不可逆的,因此,攻击者不能从 MD5(Info + K)中推导出 K。接收者通过验证 Authenticator 字段可以验证发送方身份,可以防止欺骗攻击。

(2)用户口令的加密传输。用户口令以密文方式传输且是单向密文,加密算法为 MD5(K + Request Authenticator)XoR User - Password。由于 MD5 算法的不可逆性,能够保证口令在传输中的安全,可有效地解决安全问题。另外,用户口令在用户数据库中的存放也应以单向密文形式,即加密方式存储,以提高安全性和保密性[6]。

但是,RADIUS 协议有很多的脆弱之处,这包括协议本身的原因,如用户口令、共享密钥的生成和保护的不完善及恶意的攻击等。

RADIUS 安全主要表现在以下几个方面[7,8]:

1)密钥的安全:用户口令及 NAS 和 RADIUS 服务器之间的共享密钥 key 是协议中的重要参数,如果双方通信被非法侦听,攻击者就会窃取合法的用户帐号及口令。

2)信息包的重放:攻击者窃听传输过程中的信息包,假冒 RADIUS Server,向 NAS 作出响应,用于重放攻击,因此是否可防重放攻击是协议安全的一个重要因素。

3)加密算法:如果攻击者不能直接得到密钥的信息,就会考虑攻击算法来破解用户口令,由上面的流程中可以看出,User - Password,Access - Accept 及 Response - Auth 会成为攻击者的切入点。

因此,RADIUS 协议的安全性是影响认证系统能否安全认证、安全授权和安全计费的关键问题。从以上的分析可以看出,由于在认证过程中传输的数据容易被窃听,系统易引起重播攻击,而且密码算法的弱点使得用户口令及 NAS 和 RADIUS 服务器间共享密钥的保护成为关键。因此就要从体系结构上进行合理设计,同时,在服务管理策略上,从数据传输、认证计费流程设计等方面都采取了相应的改进措施,以尽可能地弥补 RADIUS 协议在安全性上的缺陷。

5 结束语

基于 RADIUS 的 AAA 计费和认证管理系统能够为网络时代提供安全可靠和高效的网络服务,这些都是由它合理的体系结构和特点以及开放性和可扩展性所决定的。

文中研究了 RADIUS 协议的认证机制以及在 Linux 环境下 RADIUS 服务器的配置方法,同时它的缺陷也是不容忽视的,文中对 RADIUS 协议的安全性作了分析。对那些对用户的控制、计费与管理要求较高的网络来说,可以考虑从协议自身进行优化扩展以提高其安全性,这些还都有待于进一步研究。

参考文献:

[1] 李 倩. AAA 认证协议的分析[J]. 北京工商大学学报,2006,24(4):45 - 47.

[2] Rigney C, Willens S, Rubens A, et al. Remote Authentication Dial in User Service (RADIUS)[S]. RFC 2865,2000.

[3] Rigney C. RADIUS Accounting[S]. RFC 2866,2000.

[4] 张 琪,喻占武,李 锐,等. 基于 AAA 服务的协议分析与比较[J]. 计算机应用研究,2007(2):296 - 298.

[5] 黄永锋,王 滨,许晓东. RADIUS 在 802.1x 中的应用[J]. 计算机工程与设计,2006,27(5):798 - 801.

[6] 兰丽娜,石瑞生. RADIUS 协议安全机制研究及改进办法初探[J]. 信息安全与通信保密,2007(6):118 - 120.

[7] 鄢野春,佘 望,聂为清,等. 利用 RADIUS 进行 FTTH 宽带网络认证[J]. 计算机技术与发展,2006,16(5):310 - 312.

[8] 梁 根. 基于 RADIUS 的校园网认证管理系统的研究与实现[J]. 计算机技术与发展,2006,16(6):43 - 44.

(上接第 165 页)

4 结束语

通过对 SharePoint 中的 RBAC 体系进行研究,使我们熟悉了 SharePoint 门户的层次结构,以及基于该层次结构的权限继承与管理,可以通过结合网站层次结构和权限继承原理[3],来优化 SharePoint 门户的权限分配管理。除此之外,还可以结合操作系统的活动目录数据库,来对 SharePoint 用户组的嵌套功能进行扩展。

由于 SharePoint 采用了层次式结构的网站架构,从而实现了文档和列表项级别的权限管理,即条目级的权限。每个文档和列表项都包含若干个属性,甚至可以扩展现有的类来实现属性的权限管理,从而实现完整的基于角色的访问控制体系,构筑安全的门户网站。

参考文献:

[1] 崔松健. 基于 WebLogic 的企业门户安全设计[J]. 实验科学与技术,2005(1):43 - 45.

[2] 景栋盛,杨季文. 一种基于任务和角色的访问控制模型及其应用[J]. 计算机技术与发展,2006,16(2):212 - 214.

[3] PattisonT, Larson D. Inside Microsoft Windows SharePoint Services Version 3.0[M]. USA: Microsoft Press,2007.

[4] Osborn S,Sandhu R,Munawer Q. Configuring role based access control to enforce mandatory and discretionary access control policies[J]. ACM Transactions on Information and System Security,2000,3(2):123 - 132.

[5] 孟庆荣. 协同编辑中访问控制模型的设计与实现[J]. 计算机技术与发展,2007,17(2):72 - 74.

[6] 任善全,吕 强,钱培德. 基于角色的权限分配和管理中的方法[J]. 微机发展(现更名:计算机技术与发展),2004,14(12):65 - 66.

[7] English B. Microsoft Share Point Server 2007 Administrator's Companion[M]. USA: Microsoft Press,2007.

[8] 戴有炜. Windows Server 2003 用户管理指南[M]. 北京:清华大学出版社,2007.

[9] 覃章荣,王 强,欧镇进,等. 基于角色的权限管理方法的改进与应用[J]. 计算机工程与设计,2007,28(6):1282 - 1284.