

支持第三方认证的 RADIUS 系统设计

于周锋¹, 蒋泽军², 王丽芳²

(1 西北工业大学 软件与微电子学院, 陕西 西安 710072; 2 西北工业大学 计算机学院, 陕西 西安 710072)

摘 要: 分析了 RADIUS 工作原理及体系结构, 指出其安全性存在的不足. 提出了支持第三方认证的 RADIUS 系统结构, 详细分析了系统的设计、数据流程以及加密机制. 利用该结构, 设计了支持第三方认证的 RADIUS 服务器, 给出和分析了设计方法和策略, 从而扩展了 RADIUS, 增强了认证机制的安全性和灵活性.

关键词: RADIUS; NAS; 第三方认证

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2010)07-0210-04

Supported for the Third-Party Authentication's RADIUS System Design

YU Zhou-feng¹, JIANG Ze-jun², WANG Li-fang²

(1 College of Software and Microelectronics, Northwestern Polytechnical University, Xi'an 710072, China;

2 College of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Analyze the RADIUS principle and the structure of the system. Indicate the security issue. Design the new RADIUS architecture which support for the third-party authentication, detailed analysis of the system design, data flow and encryption mechanisms. Used this thought, design the RADIUS server that also support for the third-party authentication, and give the design methods and tactics. Thus, Expand RADIUS and enhance the authentication mechanism's security and flexibility.

Key words: RADIUS; NAS; third-party authentication

1 引言

为了保障网络管理、服务的安全性, 网络运营商提出了远程拨入用户认证服务 RADIUS (Remote Authentication Dial In User Service), RADIUS 现在所支持的认证包括密码认证协议, 质询认证协议, 扩展认证协议等基本认证方式, 是安全性较高的模式^[1]. 通过认证授权来提高安全服务, 通过记账来收集、记录用户对网络资源的使用, 在 RADIUS 服务器中, 用户的认证信息集中在服务器管理, 这种方式增大了服务器的压力, 同时为了确保企业级认证更高的安全性、灵活性的要求, 扩展了 RADIUS 协议, 使得 RADIUS 可以支持第三方认证方式, 并设

计了动态加载第三方认证方式的 RADIUS 系统.

2 RADIUS 系统结构

认证、授权与计费体系 (Authentication, Authorization, Accounting, AAA) 是通信网络的基本功能, RADIUS 是架构 AAA 的基本协议, 现在的移动互联网, 有线接入和无线接入网都采用了基于 RADIUS 协议的 AAA 技术架构. RADIUS 定义了在网络接入服务器 (network access server, NAS) 和集中存放认证信息的 RADIUS 服务器之间传输认证、授权和配置信息^[2]. 远程登录用户通过网络接入服务器与 RADIUS 服务器相连, NAS 作为 RADIUS 的客户端运行, 如图 1 所示. 当用户要求接入

网络时要在 RADIUS 服务器进行认证,所以远程登录用户必须要向 RADIUS 的客户端 - NAS 提供认证信息. NAS 为了实现用户认证,首先要创建一个“登录 - 请求”数据包,其中包括用户名、密码、客户端的 ID 号和用户接入的端口信息. 其中密码部分已经经过 MD5 算法加密^[3]. 所以在登录认证过程中,并不是远程登录用户直接与 Radius 服务器认证,而是通过网络接入服务器 NAS 对用户信息进行认证.

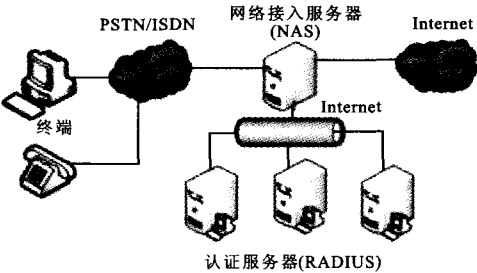


图 1 RADIUS 系统结构

用户接入 NAS, NAS 向 RADIUS 服务器提交用户数据,使用 Access - Require 数据包传输,双方使用共享密钥,这个密钥不经过网络传播. RADIUS 服务器对用户名和密码的合法性进行检验,必要时可以提出一个盘问 (Challenge), 要求进一步对用户认证,也可以对 NAS 进行类似的认证;如果合法,给 NAS 返回 Access - Accept 数据包,允许用户进行下一步工作,否则返回 Access - Reject 数据包,拒绝用户访问;如果允许访问, NAS 向 RADIUS 服务器提出计费请求 (Account - Require), RADIUS 服务器响应 Account - Accept, 对用户的计费开始,同时用户可以进行自己的相关操作.

3 支持第三方认证的 Radius 服务器认证体系结构

当客户要求接入网络系统时,通过 NAS 将数据包发送给 RADIUS 服务器^[4], RADIUS 服务器解析数据包,根据请求,调用第三方服务器的认证机制进行认证,第三方认证服务有自己的认证机制、认证管理、资源统计等. 第三方认证服务器同样有其用户信息的数据管理、数据维护、数据分析.

远程登录用户通过 NAS 与 RADIUS 服务器相连,在整个体系结构中接入了第三方认证服务器,与 RADIUS 服务器公共组成验证、授权系统. 如图 2.

当请求认证包发送给第三方认证服务器,它对请求数据信息进行分析,对分析结果进行验证,如果

成功,则授权访问网络;如果不成功,则拒绝访问.

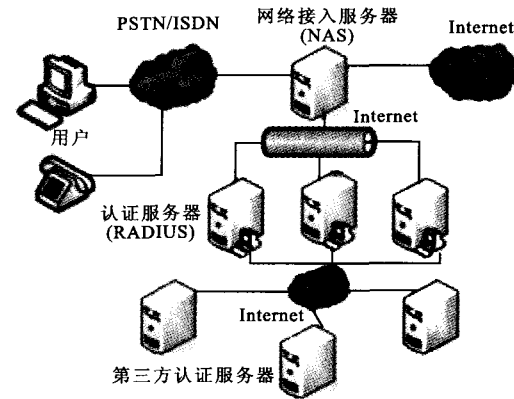


图 2 支持第三方认证的 RADIUS 体系

4 RADIUS 系统数据加密

RADIUS 系统中,为了防止网络窃听,攻击等,传输数据包必须加密,在系统中使用 MD5 加密算法对 RADIUS 数据包加密^[5],首先分析 RADIUS 数据包的格式,如图 3 所示. RADIUS 包共有 5 个域,分别是编码域、标识符域、长度域、请求鉴别码域、属性域.

8 位	8 位	16 位
Code	Identifier	Length
Authenticator (128 位随机数)		
Attributes... (不定长)		

图 3 RADIUS 数据包格式

编码域标示数据包的类型,接收到一个无效编码域的数据包后,该数据包只是会被简单的丢弃. 编码域为 1,为 Access - Request 包,编码域为 2 是 Access - Accept 包,编码域为 3, RADIUS 包为 Access - Reject 包, 11 表示 Access - Challenge 包等.

标识符用来确定请求是否重复,如果在较短时间内,一个请求有相同的客户源 IP 地址、源 UDP 端口号和标识符则 RADIUS 认为是重复请求.

长度域标示这个数据包的长度,如果包的长度比指定的短,则此包会被直接丢弃.

请求鉴别码域是非常重要的,这个值被用于验证来自 RADIUS 服务器的回复,和密码隐藏算法等,在 MD5 加密过程中起着至关重要的作用.

分析了 RADIUS 数据包的格式,对数据包中的信息使用 MD5 加密过程如下:

在数据传输中, NAS 会在 RADIUS 包的请求鉴别码域中产生 128 位的随机数,分析被加密信息,在末尾用 nulls 填补,形成多个 128 位的二进制. 现在

将 NAS 与 RADIUS 服务器的共享密钥与请求鉴别码组成字节流,将这个字节流与被加密信息的第一个 128 位相异或,将结果保存在被加密信息字符串中的第一组 128 位中。

重复以上的加密过程,从第二次循环开始,将第一次加密的结果与共享密钥组成字节流,再与被加密信息的第二组 128 位进行异或。同样将结果保存在被加密信息的第二组 128 位中。

循环加密,直至被加密信息的全部 128 位被计算过一遍,加密结束。

使用上面的加密算法,可以对 RADIUS 包中 User-Name, User-Password 等属性进行加密。保证了网络信息的安全性,提高了系统的可靠性。

5 服务器认证的数据流程

RADIUS 采用的 UDP 传输协议^[6],RADIUS 服务器是 UDP 模型的服务器,包括接收模块,和发送模块和处理模块。RADIUS 服务器封装数据报流程:

① Radius 服务器接收 UDP 数据包,Radius 协议规定的其传输协议是 UDP 协议,所以网络上发送和接收的是 UDP 包^[7]。

② Radius 服务器从 UDP 包中解析 Radius 数据包,获得认证部分信息。

③ 验证包的有效性、完整性,如果有数据丢失,或密钥错误,则 RADIUS 服务器简单丢弃该包。

④ 提取包中的用户信息,一般包括用户名、密码、以及相关配置信息。

⑤ 对用户信息进行认证,连接第三方认证服务器,对信息进行分析验证。

⑥ 返回认证的信息,表明包的合法性与否。

⑦ 创建相关属性,用属性表明 RADIUS 服务器对用户认证的答应。

⑧ 把返回的各种信息、属性、封装成 RADIUS 数据包。

⑨ 把 RADIUS 数据包封装成 UDP 数据包,并将包发送。

5.1 接收、处理模块认证

接收、处理模块的认证流程如图 4, RADIUS 服务器收到 Radius Request 数据包,首先验证 RADIUS 包的合法性,提取 Message 交由认证模块处理,然后根据认证模块返回的认证信息,决定向认证者发送 Challenge, Accept, Reject 数据包。模块数据流程过程分析如下:

① 通过 PSTN/ISDN, NAS 将 UDP 数据包传送到 RADIUS 服务器,接收数据包。

② 分析解析 UDP 包,得到 RADIUS 包。

③ 判断是不是认证包,如果是,进行下一步,否则,丢弃。

④ 根据标识符提取站点信息,并检查属性。

⑤ 根据数据包的属性,确定数据包的类型。

⑥ 数据包是“接入允许”,“接入拒绝”,“接入盘问”,这三种情况之一。

如果是“接入允许”判断标识符域,如果符合则通过,否则,丢弃。“接入盘问”,用户提供的信息不详,提取盘问信息。“接入拒绝”,非法数据包,提取拒绝信息。

⑦ 重新封装数据包以新的标识符和鉴别码进行发送。用户根据发送信息,重新接入,再次循环调用验证。

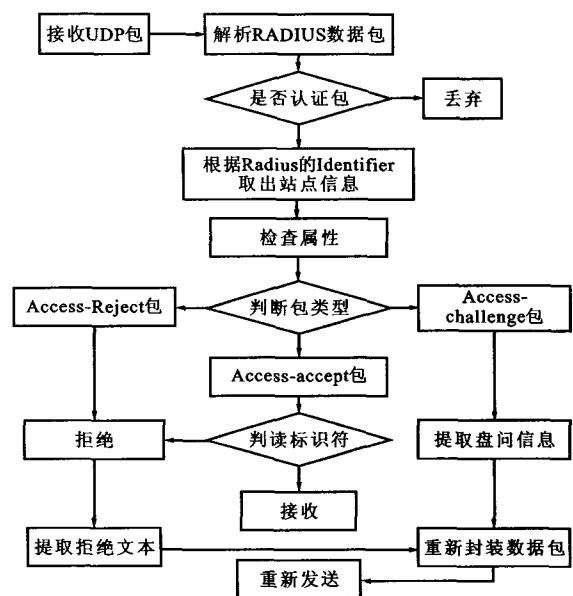


图4 接收、处理模块数据流程

5.2 发送模块数据封装

发送模块数据封装如图 5 所示。RADIUS 协议流封装在 UDP 数据报中实现远程的接入认证服务^[8]。

① 若为认证数据包,封装 RADIUS 数据包。

② 封装 RADIUS 包头,创建 Request Authentication,请求鉴别码是由 NAS 生成的 16 个字节的随机数

③ 创建 Radius 属性,如 User-Name, Framed-Routing 等。

④ 封装为 UDP 包,发送 UDP 数据包。

对请求的报文的回复分,可以应答,也可以不应

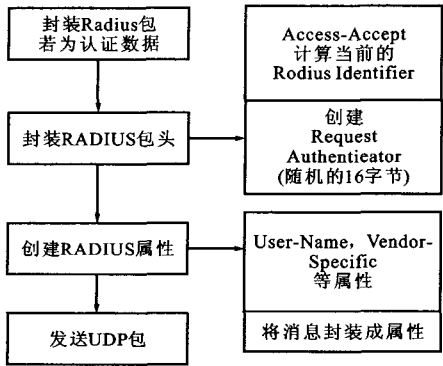


图 5 发送模块数据封装

答,可以代理到其他服务器,也可以只是把他备份到另外一台服务器上.

6 动态加载第三方认证的 RADIUS 服务器的结构

以级联的方式实现多重认证,RADIUS 服务器加载第三方认证,可以根据用户的配置信息,实现组合认证.用这种方式有利于用户的认证选择和灵活,有利于加载其他的第三方认证.

用户提供认证配置,包含认证的方式、认证信息等,通过网络接入服务器连接到 RADIUS 服务器,服务器分析用户信息,根据分析结果,连接第三方认证服务器,动态加载第三方认证机制.

这个工作框架结构如图 6 所示.在此方式下,RADIUS 服务器主要维护关于认证方式的相关信息,动态调用和加载第三方的认证库,这样提高了 RADIUS 服务器及认证信息的安全.在系统中方便实现级联多重认证.

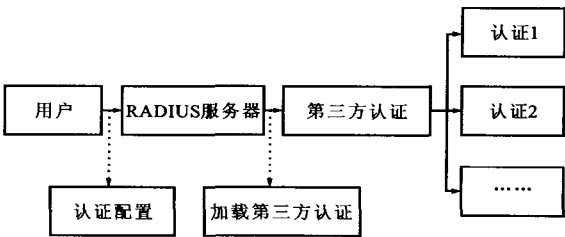


图 6 支持第三方认证的 RADIUS 服务器结构

具体的过程如下:用户输入自己的用户名,密码等认证信息,经过 RADIUS 客户端,将信息传送到 RADIUS 服务器.同时 RADIUS 服务器加载了用户需要的第三方认证的信息,这样 RADIUS 服务器可以决定,用户是准备用怎样的,哪些方式认证. RADIUS 服务器首先对用户的信息进行认证,加载所有的第三方认证方式,根据用户的认证配置信息,调用第三方认证.

根据以上的认证过程,返回认证结果,决定用户是否认证成功,是否可以接入网络等.

7 支持第三方认证模块

使用策略模式的思想,实现支持第三方认证的 RADIUS 服务器的模块

(1) 认证父类

父类中最主要包含一个认证函数 Auth()和得到本类指针的纯虚函数 GetAuth(). 父类主要提供接口,和实现被调用的作用,利用多态的原理来实现对子类的调用.

(2) 子类模块

第三方认证全部继承于父类,并且必须实现父类的两个基本函数,子类的 Auth()实现的是自己的认证,GetAuth()函数返回的是自己的类指针.

(3) RADIUS 服务器模块

在 RADIUS 服务器中,主要调用 LoadDriver (* .dll)函数,实现对所有的第三方认证的动态库的加载,以及应用 GetProcAddress()得到具体第三方类指针.

GetProcAddress()函数的具体实现如下所示:

```
FARPROC GetProcAddress(  
HMODULE hModule, // DLL 库的句柄  
LPCSTR lpProcName // 实现第三方认证函数的名字  
);
```

用 GetProcAddress()得到父类指针.根据用户的认证配置信息,实现得到第三方认证类的指针.

8 结束语

对支持第三方认证的 RADIUS 服务器的设计进行了详细分析,提出了支持第三方认证的 RADIUS 体系结构.它吸收了 RADIUS 的优势,扩展了 RADIUS,减轻了 RADIUS 服务器的压力.增强了认证机制,增加了认证的灵活性.同时实现了动态加载第三方认证以及级联认证的功能,给出了实现策略.

参考文献:

[1] Seungwon Shin, Kiyoung Kim, Jong - soo Jang. D - SAT: detecting SYN flooding attack by two - stage statistical approach[C]// Symposium on Applications and the Internet. Italy: Trento, 2005:430 - 436.
[2] Ringey C, Willens S, Rubens A, et al. RFC 2865 Remote authentication dial in user service (RADIUS)[S]. ISOC, 2000.

(下转第 217 页)

确性.由于文中采用 Verilog 对 SystemC 模型的顶层模块进行实例化,所以, SystemC 的仿真速度上有所损失.若全部采用 SystemC 进行仿真,则可以达到更快的仿真速度.

5 结束语

多核处理器是未来处理器发展的重要方向,快速对多核处理器进行建模、仿真可以在设计的早期就寻找出系统的性能瓶颈.而 SystemC 对 C++ 进行了扩展,使之具有了模拟多线程的能力,适用于多核处理器的建模.文中对多核处理器进行了建模,并且分别给出了通讯、同步等模块的实现,给出了 Verilog 和 SystemC 仿真平台速度上的差异,证明 SystemC 具有较好的处理器建模能力.

参考文献:

- [1] Jiang Xu, Wolf W, Henkel J, et al. A methodology for design, modeling, and analysis of networks - on - chip [C]// Proceeding of 2005 IEEE International Symposium on Circuits and Systems. Kobe, Japan: IEEE press, 2005:1778 - 1781.
- [2] Gorder P F. Multicore processors for science and engineering[J]. IEEE Trans on Computing in Science & Engineering, 2007,9(2):3 - 7.

- [3] Benini L, De Micheli G. Networks on chips: a new SoC paradigm[J]. IEEE trans on Digital Object Identifier, 2002,35(1):70 - 78.
- [4] 张雅琦,李镭. Verilog HDL 高级数字设计[M].北京:电子工业出版社,2006:47 - 238.
- [5] Peterson G, Ashenden P, Teegardern D. System C user's guide and system C language reference manual(version 2.0)[EB/OL]. [2009 - 03 - 10]. <http://www.systemc.org>.
- [6] 王兆菊,张洵颖,龚龙庆.应用 SystemC 的 AMBA 总线系统级模型的设计与实现[J]. 微电子学与计算机,2005,25(5):95 - 98.
- [7] 张奇,曹阳,李栋娜,等.基于 SystemC 的 SoC 行为级软硬件协同设计[J]. 计算机工程,2005,31(19):217 - 219.
- [8] 陈绍贺,赵明,王京.基于 SystemC 的片上系统设计[J]. 微电子学与计算机,2005,22(4):51 - 56.

作者简介:

奚杰 男,(1982 -),博士研究生.研究方向为多核处理器.

陈杰 男,(1963 -),博士生导师.研究方向为通信、多媒体处理、VLSI 设计.

朱玥 男,(1985 -),博士研究生.研究方向为多核处理器.

(上接第 213 页)

- [3] 丰艳.基于 RADIUS 协议的 VOLP 认证/计费系统的设计与实现[J]. 计算机工程与设计,2008(7):3480 - 3481.
- [4] 杨建军,贾晨军,冉立新.基于 RADIUS 协议的网络认证技术研究[J]. 浙江大学学报:工学版,2005(2):235 - 236.
- [5] 李春科,李伟华.MD5 加密算法及其在 RADIUS 协议中的应用[J]. 微电子学与计算机,2004,21(2):21 - 22.
- [6] 张琪,喻占武,李锐.RADIUS 服务器安全性分析及其改造[J]. 计算机工程,2007(3):146 - 147.

- [7] Rigney C, Willens S. Remote authentication dial in user service[S]. IETF, RFC2865, 2000.

- [8] 陆谊,张红.改进 802.1x 认证技术的研究[J]. 微电子学与计算机,2005,22(6):163 - 164.

作者简介:

于周锋 男,硕士研究生.研究方向为网络工程与技术.

蒋泽军 男,教授.研究方向为嵌入式计算、网络软件和嵌入式软件开发技术等.

王丽芳 女,教授.研究方向为电子商务、计算机应用等.