

基于 802.1x 的无线园区网 AAA 系统的设计与实现

王 斐¹, 陈 玲², 陆建德²

(1. 苏州大学 计算机科学与技术学院, 江苏 苏州 215006;

2. 苏州大学 江苏省计算机信息处理技术重点实验室, 江苏 苏州 215006)

摘 要:无线网接入安全是网络安全的重要课题之一。回顾了 802.11i 中采用的 802.1x EAP 认证技术,对无线园区网如何实现安全接入与认证进行深入研究,提出采用 FreeRadius 实现 AAA 功能的无线网体系结构,实现了采用数字证书的 EAP-TLS 方式服务器和客户端双向认证,提高无线网安全,保护无线网资源。还对无线园区网采用 802.1x EAP 认证的几种方案进行了深入分析比较,对根据不同园区网应用环境选择适当 EAP 设计方案提出了建议。

关键词:无线园区网;AAA;802.1x;RADIUS;EAP-TLS

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2008)10-0143-05

Design and Implementation of 802.1x Based AAA System in Wireless Campus Network

WANG Fei¹, CHEN Ling², LU Jian-de²

(1. School of Computer Sci. & Tech., Soochow University, Suzhou 215006, China;

2. Jiangsu Province Computer IT Key Lab., Soochow University, Suzhou 215006, China)

Abstract: Wireless access and authentication are important issues in wireless network security. Reviewed the 802.1x EAP authentication technique in IEEE 802.11i, then explored the methods of secure access and authentication in wireless campus network, and brought out a WLAN AAA architecture with FreeRadius. Realized the EAP-TLS bidirectional authentication between server and client with digital certificates, so as to get more WLAN security and more protection to the WLAN resources. Has also made analysis and comparison to several solutions with 802.1x EAP authentication in wireless campus network and given out the recommendations for appropriate EAP solution according to different application environment.

Key words: wireless campus network; AAA; 802.1x; RADIUS; EAP-TLS

0 引 言

无线园区网具有灵活性、可移动性及较低的投资成本等优势,作为传统有线网络的补充和发展,得到了快速的应用。但 IEEE802.11 系列无线技术本身存在的缺陷和不安全因素, WEP 使用的 RC4 加密算法密钥过短导致加密强度不够,容易被破解。IEEE 任务组 TG4 于 2004 年 6 月正式推出了新一代安全标准 802.11i,防止未授权用户访问无线网络。WPA 作为 802.11i 标准的子集,包含了认证、加密和数据完整性校验三个组成部分。最新公布的 WPA2 更采用了 AES 等更高强度的加密算法,其认证方式采用 802.1x。

IEEE 于 2004 年 12 月发布的 802.1x-2004 对 WLAN 的认证和密钥管理提出了更为安全的解决方案,用于对 WLAN 进行认证和密钥管理。文中结合 IEEE 802.1x 协议课题设计和实现了无线园区网的 AAA 系统。采用 EAP-TLS 方式提供了客户端和认证服务器之间的双向认证,采用基于 RADIUS 协议的 FreeRADIUS 实现管理和计费功能。有效保证合法用户使用无线网络资源,阻止未授权用户访问无线网络,完善无线园区网的网络管理。

1 AAA 与 802.1x/EAP 总体分析

AAA 是验证、授权和记账 (Authentication, Authorization, and Accounting) 的简称。它提供了一个用来对验证、授权和记账这三种安全功能进行配置的一致的框架。AAA 的配置实际上是对网络安全的一种管理,主要指访问控制。

收稿日期:2008-01-16

基金项目:江苏省自然科学基金项目(BK2004039)

作者简介:王 斐(1981-),男,山东烟台人,硕士研究生,研究方向为计算机网络与信息安全;陆建德,教授,研究方向为计算机网络与网络安全。

(1)验证:验证用户是否可以获得访问权。认证的关键方面是允许两个不同实体间形成一种信任关系——两者都被认定为有效的用户。

(2)授权:授权用户可以使用哪些服务。授权包括用规则的集合或其他的模板以决定在一个系统里被认证的用户可以做什么。

(3)记账:记录用户使用网络资源的情况。计费测量和证明一个用户访问时使用的资源,包括在一次会话中系统时间的总和或用户发送/接收数据的总量。计费通过记录会话统计和使用信息实现,并且被用作授权控制、倾向分析和资源利用等。

802.1x 是一种基于端口的认证协议,是一种对用户进行认证的方法和策略。802.1x 的体系架构包括三个部分:a. 请求者,通常是支持 802.1x 认证的用户终端设备,用户通过启动客户端软件发起 802.1x 认证;b. 认证系统:通常为支持 802.1x 协议的网络设备,WLAN 下一般为接入点 AP。它对认证请求者进行认证处理;c. 认证服务器:为认证系统提供认证服务的实体,通常使用 RADIUS 服务器实现认证服务器的认证和授权功能。

基于 802.1x 的无线认证系统在客户端和认证系统间使用 EAPoW^[1](Extensible Authentication Protocol over WLAN)格式封装 EAP 报文,认证系统与认证服务器间通过 RADIUS 协议传送认证信息。EAP 协议有很强的扩展性,基于 EAP 协议的认证系统可使用很多不同的认证算法,如 EAP-MD5, EAP-TLS, EAP-PEAP 等。

2 AAA 系统的核心服务 RADIUS 分析及 FreeRadius

RADIUS^[2]是 Lucent 实验室开发的基于 Client/Server 的拨号安全认证协议,其最新标准定义在 RFC2865 和 RFC2866 中。它通过授权认证来提供安全服务。RADIUS 服务器把用户的认证信息集中在一台服务器处理,支持 RADIUS 协议的客户端把用户要求的认证信息(用户名和口令)选到 RADIUS 服务器认证,只有在和服务器上用户数据库中信息一致时,才被允许进入网络。认证信息以加密的方式在客户端和服务器间传送。同时 RADIUS 服务器也可对每个用户进行安全和计费管理。RADIUS 是基于挑战/应答方式检验和鉴别用户的一种访问控制协议,可以提供集中式认证、可控制的授权以及详细的计费信息。RADIUS 认证使用 1812 端口,计费使用 1813 端口。RADIUS 是应用层的协议,在传输层它被封装在 UDP 的报文中,进而封装进 IP 包。

RADIUS 数据包分为 5 个部分:

Code:一个字节,用于表示 RADIUS 包的类型:常用类型有:Code=1,接入请求(Access-Request);Code=2,接入应答(Access-Accept);Code=3,接入拒绝(Access-Reject);Code=4,计费请求(Accounting-Request)等。

Identifier:一个字节,用于请求和应答包的匹配。

Length:两个字节,表示 RADIUS 数据区(包括 Code, Identifier, Length, Authenticator, Attributes)的长度,单位是字节,最小为 20,最大为 4096。

Authenticator:16 个字节,用于验证服务器端的应答以及用户口令的加密。RADIUS 服务器和 NAS 的共享密钥(Shared Secret)与请求认证码(Request Authenticator)和应答认证码(Response Authenticator),共同支持发、收报文的完整性和认证。另外,用户密码不能在 NAS 和 RADIUS 服务器之间用明文传输,而一般使用共享密钥(Shared Secret)和认证码(Authenticator)通过 MD5 加密算法进行加密隐藏。

Attributes:不定长度,最小可为 0 个字节,描述 RADIUS 协议的属性,如用户名、口令、IP 地址等信息都是存放在本数据段。

RADIUS 协议工作流程^[3]如图 1 所示。

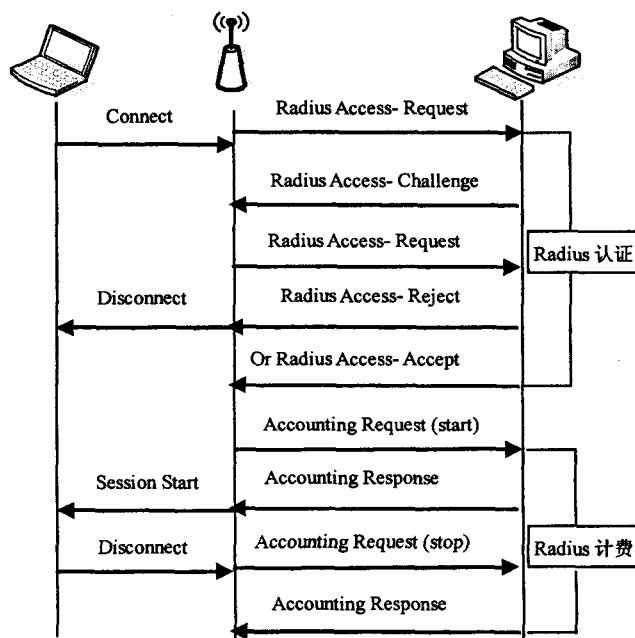


图 1 RADIUS 的工作流程

(1)当用户有上网需求时,在客户端输入用户信息,AP 收到后,向 RADIUS 服务器发出 Access-Request 包。发出 Access-Request 包的同时启动计时器和计数器,若超时计数器会激发 AP 重发 Access-Request 包。

(2)RADIUS 服务器收到 Access-Request 包后,

首先验证 AP 的共享密钥与 RADIUS 服务器中预先设定的是否一致,以确认是否是所属的 RADIUS 客户机。查验包正确性后,RADIUS 服务器会依据包中的用户名在用户数据库中查询此用户记录。若有,则对用户的请求做进一步验证。其中包括:用户口令、用户 IP、用户登录的物理端口号等。

(3)以上各类验证条件不满足,则 RADIUS 服务器会向 AP 发出 Access - Reject(接入拒绝)包。AP 收到拒绝包后,会立即停止用户连接端口的服务请求,用户被强制退出。

(4)以上各类验证条件均满足且 RADIUS 服务器中设置了用户的 Challenge/Response 握手验证要求时,RADIUS 服务器会发出一个 Access - Challenge(接入质询)包,这时用户会看到提示告知用户名已验证成功,要用户提供用户凭证数据进一步确认登录请求 Access - Request。用户提供相关凭证数据确认后,RADIUS 服务器将再次比较两次的请求信息,决定如何响应用户。

(5)所有的验证条件和握手对话均通过后,RADIUS 服务器会将数据库中的用户配置信息放在 Access - Accept(接入接受)包中返回给 AP,AP 会根据包中的配置信息限定用户的具体网络访问能力。

所有的验证、授权完成后,AP 会定期向 RADIUS 计费服务器发送计费包。

开源软件 FreeRadius 可以实现 RADIUS 服务器的功能,它完全支持 RFC2865 和 RFC2866 中的定义,支持 EAP - MD5, EAP - SIM, EAP - TLS, EAP - TTLS, EAP - PEAP 等多种 EAP 方式。在数据存储方面支持 MySQL、Oracle 等主流数据库,根据网络的规模有灵活的配置方案,并支持使用 OpenSSL 生成的证书,本课题采用 FreeRadius 作为 WLAN AAA 服务器。

3 无线园区网 AAA 系统的设计与实现

3.1 无线园区网络认证模型

无线园区网 AAA 系统设计的各部分如图 2 所示,网络由申请者,NAS,RADIUS 服务器,数据库服务器四部分组成。其中申请者就是无线局域网中的移动终端,申请者要接入无线园区网,必须向 NAS 发出请求并向 NAS 提供自身信息。NAS 是提供网络服务的 AP,NAS 接收申请者发送的请求,将请求发送到 RADIUS 服务器进行认证,并向申请者返回服务器认证结果。RADIUS 负责处理 NAS 传来的认证信息,并在数据库中查找用户的信息进行验证,最后将结果交给 NAS 和申请者。数据库记录了合法用户的认证信息和运行时的计费信息。

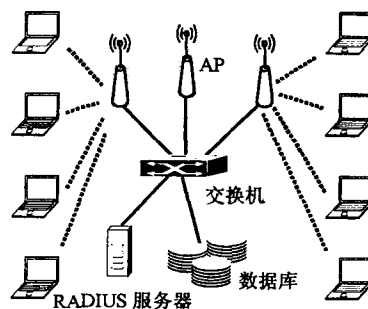


图 2 无线园区网模型

3.2 申请者软件的实现

申请者软件由 802.1x 客户端实现。本系统以开源软件 Wire1x 为基础加以修改和改进,编译生成 EAP - TLS.exe。它运行在 Windows 平台,负责发送申请者的用户信息,与 NAS(AP)交互并最终完成认证过程。Linux 平台运行开源软件 xsupplicant,在正确配置后与 NAS(AP)交互并最终完成认证过程。

3.3 NAS 的配置与实现

本课题中无线园区网 AAA 系统的 NAS 由 Cisco Aironet 1100 实现,它向无线终端提供接入服务,并且具有授权的责任。NAS 除了要传送正常的服务数据外,还要具有处理 802.1x 信息、控制用户的能力。根据 FreeRADIUS 服务器发送来的 802.1x 信息,NAS 采取适当的策略控制正常用户的访问,阻止非法用户进入无线网络。Aironet 1100 AP 使用静态 IP,将 Authentication Settings 中 Methods Accepted 设为 Open Authentication: with EAP,设置 EAP Authentication Servers 为 RADIUS 服务器的 IP 地址。在 Security: Server Manager 中将 Authentication Port 设为 1812,Accounting Port 设为 1813,将 Shared Secret 设为 AP 与 RADIUS 服务器之间的共享密码。

3.4 证书的生成与使用

所有的客户端和认证服务器端都需要事先申请一个标准的 x.509 证书并安装。证书可以从本地认证中心获取,也可以用 OpenSSL 的 /usr/bin/CA.pl 脚本生成自签证书。分别建立根证书脚本 CA.root,认证服务器端证书脚本 CA.svr,客户端证书脚本 CA.clt。然后用这三个脚本分别生成 root.der, root.p12, root.pem, radius.der, radius.p12, radius.pem, client.der, client.p12, client.pem 等证书文件。按照 RSA 实验室颁发的 PKCS#12 标准定义安全交换格式,客户端和认证服务器端对象标志符 OID 分别为 1.3.6.1.5.5.7.3.2 和 1.3.6.1.5.5.7.3.1。

将 root.der 和 client.p12 拷贝到客户端,运行 mmc 命令打开控制台,分别导入根证书存储区和个人用户证书存储区。

3.5 RADIUS 服务器的设计与实现

RADIUS 服务器具有认证、授权和计费三个功能,它处理 NAS 传送过来用户认证信息,通过检索数据库中的用户信息判断请求者的身份是否合法,并返回给 NAS 处理后的信息。

RADIUS 服务器在 Fedora Core Linux 6 平台采用开源软件 FreeRadius 1.1.2 实现,其功能包括以下方面:

认证包处理:通过监听认证端口(默认 1812)来监测 NAS 提交的认证数据包。收到认证包后,查询数据库验证用户是否合法,并把结果以 RADIUS 数据包格式从 1812 端口返回给 NAS。

计费包的处理:监听计费端口(默认 1813)。当用户的认证通过时,查询该用户计费信息,确定其计费类型、费率等。当监听到 NAS 提交计费包后,向数据库中添加“计费请求开始”包中所提交的计费信息(包括用户名、上网起始时间等)。在收到用户下网的“计费请求结束”后,根据包中提交的用户结束时间、数据流量等信息,计算用户的上网时长和数据流量,并根据用户计费类型来计算出用户本次上网费用,记录入数据库。

修改 FreeRadius 的配置文件,在 < Radius dir > /etc/raddb/radiusd.conf 文件中添加语句:authorize{eap}, authentication{eap}, 使能 EAP 认证及授权;在同目录的 client.conf 文件中设置 AP 地址及 AP 和认证服务器之间的共享密钥等,如: client 192.168.150.76 { secret = 123456 short-name = lab537 }; 在 eap.conf 文件中设置 EAP-TLS 为缺省的认证方式: eap { default-eap-type = tls }, TLS 的配置如图 3 所示;将 root.pem, root.der, root.pl2, radius.pem, radius.der, radius.pl2 证书复制到 raddb 里的 certs 目录下。

```
tls{
private_key_password=whatever
private_key_file={raddbdir}/certs/radius.pem
certificate_file={raddbdir}/certs/radius.pem
CA_file={raddbdir}/certs/root.pem
dh_file={raddbdir}/certs/DH
random_file={raddbdir}/certs/random
}
```

图 3 TLS 配置

3.6 EAP-TLS 认证过程的设计实现

EAP-TLS 认证通过基于证书的传输层安全,在

采用强加密方法的无线客户端和服务端之间提供双向认证,并生成保护无线传输的加密密钥,具有强度更高的安全性。EAP-TLS 认证流程如图 4 所示,图 4 阴影部分的 EAP-TLS 交互过程设计如图 5 所示。

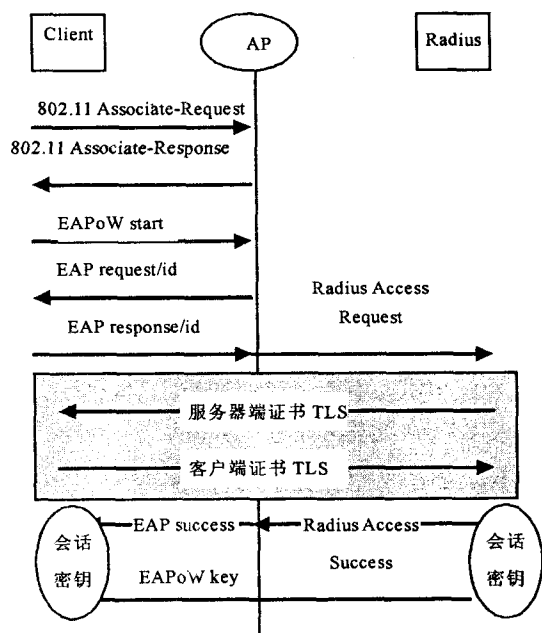


图 4 EAP-TLS 认证过程

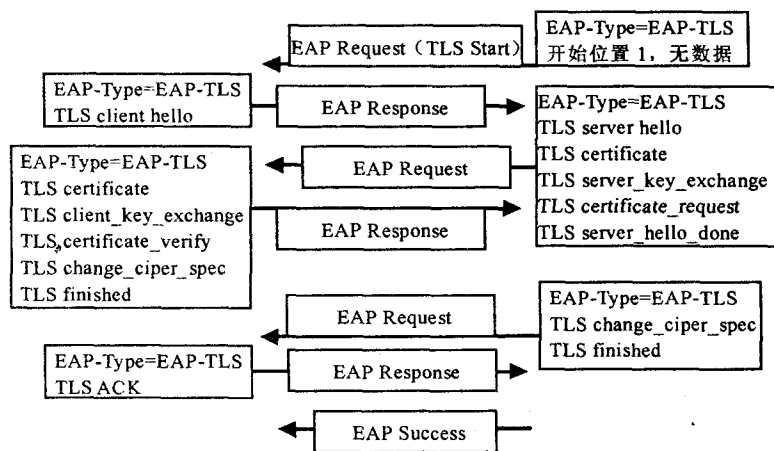


图 5 TLS 过程

基于 EAP-TLS 的全认证流程设计如下:

- (1) 无线客户端 STA 向 AP 发出 EAPoW-Start 消息请求认证;
- (2) AP 发出请求报文 EAP-Request/id, 要求 STA 输入用户名;
- (3) STA 响应请求, 将用户名信息通过 EAP-Response/id 响应帧发送给 AP;
- (4) AP 将用户名信息重新封装成 RADIUS Access Request 包发送给认证服务器;
- (5) 认证服务器将其证书通过 AP 传送给 STA;
- (6) STA 以内部存放的认证服务器证书发布者的公钥验证认证服务器的身份;

(7) STA 将自己的证书通过 AP 发送给认证服务器;

(8) 认证服务器以 STA 证书发布者公钥验证 STA 的身份;

(9) STA 与认证服务器分别生成加密用的会话密钥;

(10) 认证服务器向 AP 发送 RADIUS Accept 消息,其中包括会话密钥;

(11) AP 向客户端 STA 发送 EAP Success 消息,表示认证成功。

4 无线园区网 802.1x EAP 认证方案的分析与比较

802.1x 支持多种 EAP 类型,各种 EAP 类型各有特点。表 1 对三种典型 EAP 类型的优缺点进行了分析。

MD5 类型的身份验证由于仅使用 MD5 算法对密钥加密,并且仅能够完成服务器对申请者的单向认证,故安全性最低。但对于小型组织,基于密码的 802.1x 身份验证已足够^[4],并且实施简单,容易维护。

表 1 几种 EAP 类型的比较

功能	MD5	EAP-TLS	PEAP
相互身份验证	仅客户方身份验证	相互身份验证	相互身份验证
轮换密钥	无轮换密钥:依赖静态密钥	在每次身份验证过程中生成	在每次身份验证过程中生成
安全技术等级	弱安全技术	最强身份验证	基于密码的强身份验证
用户凭据保护	暴露于字典攻击	基于证书的身份验证	由传输层安全隧道保护
实施轻松	简单但不推荐用于无线网络	必需公钥基础结构	Windows 支持广泛
凭据灵活	仅客户方使用密码	服务器与客户方皆使用数字证书	服务器使用证书,客户方在受保护的 TLS 隧道中使用令牌、密码或证书

PEAP 是为在 TLS 保护的隧道中执行 EAP 类型而设计的,它要求基于服务器的证书,而客户方在受保护的 TLS 隧道中使用令牌、密码或证书,PEAP 还可在身份验证过程中动态生成加密无线传输的密钥。但 PEAP 目前仅能在 Windows 环境下实现,扩展性有限。

EAP-TLS 的双向数字证书认证方式提供了对服务器和客户端双方安全的认证,采用公钥基础结构,实现了最安全的接入认证,适合对安全性要求高的大型

组织^[5,6]。

5 结束语

采用基于 802.1x EAP、RADIUS 的认证、授权和计费系统可以为无线网络提供移动终端在无线园区的安全接入、安全可靠和高效的服务,阻止非法访问,保护内部资源,保证合法用户的正常访问。文中设计的采用数字证书的 EAP-TLS 方式的双向认证是安全强度很高的一种解决方案。根据具体无线园区网的应用环境,还可以另外灵活选择适当的 EAP 设计方案。

EAP-MD5 安全性较低,适合对安全要求不高的小组织,对于当前没有 PKI 的小型组织,使用基于密码的 EAP-MD5 身份验证已足够,不需使用证书。EAP-PEAP 安全性高,目前适用于 Windows 环境,PEAP 在 TLS 保护的隧道中执行 EAP,它要求基于服务器的证书,PEAP 还在身份验证过程中动态生成加密无线传输的密钥。EAP-TLS 通过基于证书的传输层安全 TLS 在采用强加密方法的无线客户端和 RADIUS 服务器间进行双方相互身份验证,并生成保护无线传输的加密密钥,这是使用 802.1x 最受欢迎、最安全的 EAP 方法之一。它要求在客户端和 RADIUS 服务器上有公钥证书。适用于对安全有较高要求的大型组织。

参考文献:

- [1] Stanley D, Walker J, Aboba B. Authentication Protocol(EAP) Method Requirements for Wireless LANs[S]. RFC 4017, 2005.
- [2] Rigney C, Willens S, Rubens A, et al. Remote Authentication Dial In User Service (RADIUS) [S]. RFC 2865, 2000.
- [3] 朱 恺,曹秀英.无线局域网中 RADIUS 协议原理与实现[J]. 微计算机信息,2004,20(9):118-120.
- [4] Microsoft. 使用 802.1 设计无线 LAN 安全性[EB/OL]. 2004-04. <http://www.microsoft.com/china/technet/security/guidance/secmod172.mspx>.
- [5] 雷怀玉,任新华.基于 EAP/TLS 的无线局域网安全认证系统的研究与实现[J]. 太原理工大学学报,2005,36(5):525-528.
- [6] 袁建国,朱 恺,方宁生,等.802.1x/EAP-PEAP 的研究与应用[J]. 计算机工程与设计,2006,27(10):1818-1820.