基于活动目录的802.1X/EAP_PEAP应用研究

龚发根,何拥军
(广东科学技术职业学院,广东 珠海 519090)

摘 要:为了解决网络由于非法接入而带来的网络安全问题,深入研究分析了802.1X协议及其具体的认证过程,通过将802.1X与活动目录技术相结合,在Windows网络环境下基于活动目录技术构建了一个高效、可靠的802.1X/EAP-PEAP接入认证应用方案。为有线网络和无线网络提供了一致的接入验证方法,并将网络接入与域登录身份验证统一起来,实现了透明统一的SSO认证。从而为用户有效解决了非法用户的接入问题,提高了网络的安全性。

关键词:802.1X;可扩展认证协议;受保护的可扩展认证协议;Radius;活动目录
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2011)01-0154-04

Study on Active Directory-Based 802.1X/EAP_PEAP Scheme

GONG Fa-gen, HE Yong-jun
(Guangdong Institute of Science and Technology, Zhuhai 519090, China)

Abstract: In order to solve the problem of network security due to illegal access to network, deeply analyzes the 802.1X protocol, and build an efficient and reliable of 802.1X / EAP-PEAP access authentication applications scheme based on Active Directory technology in Windows network environment by combination the technology of 802.1X and active directory. Provide a consistent access authentication method for the wired network and wireless network access, and implement transparent and uniform SSO authentication by unified the network access and domain logon authentication. Effective solution for users of illegal user access problem, improve network security.

Key words: 802.1X; EAP; PEAP; Radius; Active Directory

0 引 言

随着局域网,特别是无线网络的快速发展,网络安全问题日益突出。网络所面临的主要威胁之一就是外部设备非法接入到内部网络后的破坏性攻击行为。在许多企业的网络架构中,往往只注重对来自因特网的外部威胁进行防御,而忽略了来自内部的非法接入访问威胁。这种威胁在大中型IT环境中影响尤其明显,因此,建立内部网络接入防御体系势在必行。

目前,很多企事业单位已经建立了基于活动目录的信息管理系统,通过活动目录管理用户访问权限和应用执行权限。然而,基于活动目录的权限控制无法实现对用户的物理访问权限的控制,比如对网络接入方面的控制,未授权用户在物理上可随意接入网络,这将给企业的网络和应用带来很多安全隐患。为了更加有效地控制和管理网络资源,提高网络接入的安全性,通过采用802.1X接入认证和活动目录网络管理基础架构相结合的方案,为有线网络和无线网络提供一致的接入验证方法,并将网络接入与域登录身份验证统一起来,实现了透明统一的SSO认证与授权。只有通过了内部域用户验证的计算机才能正常进行网络通讯,否则其接入端口数据将被阻隔。

收稿日期:2010-05-30;**修回日期**:2010-08-10
基金项目:广东省自然科学基金项目(7007730);广东省科技计划项目(0711020400157)
作者简介:龚发根(1970-),男,江西永丰人,讲师,硕士,研究方向为网络与信息安全。

1 IEEE 802.1X协议分析

1.1 IEEE 802.1X概述

IEEE 802.1x是对802.11无线网络标准的扩展,也称为基于端口的访问控制协议(Port based network access control protocol),该协议能够对各种网络接入设备在要求连接到有线或无线局域网时提供认证和授权的手段[1-5]。利用IEEE 802.1x协议,能够在各种多点访问网络环境中提供一种类似于点对点的用户识别方法。

1.2 IEEE 802.1x总体架构

IEEE 802.1x总体架构主要由Supplicant System(申请者系统)、Authenticator System(认证者系统)、Authentication Server System(认证服务器系统)三个部分组成。整个体系架构及其相互关系如图1所示。

申请者系统代表各种网络访问客户端设备,下文

简称为客户端,该设备通过支持 EAPOL(Extensible Authentication Protocol Over LAN)协议来发起 802.1x 协议的认证过程。目前各种流行的客户端访问设备均支持这种协议,对于一些早期的客户端访问设备如果不支持,只要加装一些补丁包即可。

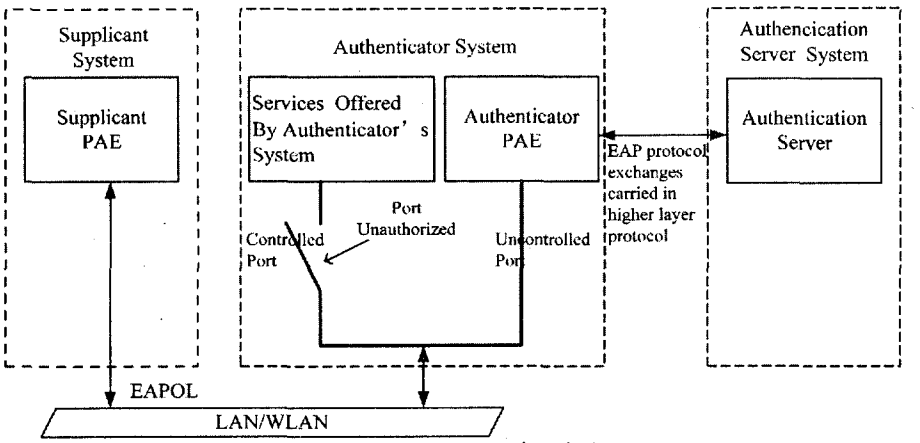

图 1　IEEE 802.1x 总体架构

认证者系统代表各种支持 802.1x 协议的网络接入设备,下文简称为接入设备,例如支持 802.1x 协议的各种无线路由器和网络交换机。这种设备的每个网络访问物理接口可以分为两个逻辑接口:受控接口和非受控接口。非受控接口始终处于双向连通状态,不需通过身份验证,可直接用来传递 EAPOL 帧,以确保客户端始终可以通过该逻辑接口发出或接受身份验证数据包。受控接口在通常情况下总是处于断开状态,只有在客户端通过身份验证的情况下才与网络连通,主要用来在客户端通过身份验证的情况下为客户端访问各种网络资源和服务传递数据包。为适应不同的网络应用需求,受控接口的工作模式可分为双向受控或仅输入受控两种。

认证服务器系统代表各种网络验证服务器,下文简称为认证服务器,该设备主要用来对客户端的身份进行验证。认证服务器通常为 RADIUS[6,7] 服务器,该服务器存储客户端身份标识信息,以及客户端网络访问控制信息等。当客户端通过认证服务器的身份验证后,客户端与接入设备之间的受控接口则处于连通状态,并利用认证服务器上的网络访问控制信息配置客户端与接入设备之间的网络连接相关参数,以控制客户端的网络访问行为。

1.3　EAP 协议

EAP 协议,即 Extensible Authentication Protocol ,定义了 IEEE 802.1x 协议框架中客户端、接入设备和认证服务器三个主要实体之间的通过机制[8,9]。通过支持该协议,接入设备只能通过非受控端口在客户端与认证服务器之间传递身份验证信,在通过身份验证后,才能通过受控接口传递业务访问数据,从而实现了认证流和业务流的分离,为各种网络应用提供了灵活性。

EAP 支持多种认证协议以保证认证过程中的信息安全,比较常用的 EAP 认证协议主要有以下几种:EAP-MD5、EAP-TLS 和 EAP-PEAP 等。EAP-MD5 是一种仅提供基本级别安全保护的 EAP 验证类型,由于其要求使用可逆密码、仅能提供单向验证以及无法动态派生 WEP 密钥,容易受到字典式攻击和欺骗攻击,一般只用于对安全性要求不高的场景;EAP-TLS 要求通过数字证书进行相互的身份验证,在认证服务器和客户端双方都需要数字证书,安全性很高,但部署成本也较高;而 EAP-PEAP 由于相对比较安全,而且部署方便,使用广泛。因此,本文将重点讨论 EAP-PEAP 认证协议。

1.4　PEAP

PEAP 也称为 Protected EAP(Protected Extensible Authentication Protocol,受保护的可扩展验证协议),该协议是由 Microsoft、Cisco 和 RSA Security 公司共同开发[10]。PEAP 在设计上类似于 EAP-TTLS,只需一个认证服务器端的数字证书来建立一个安全的 TLS 隧道,以保护对客户端的身份验证过程,并可利用服务器端的数字证书来实现对认证服务器的身份验证。然后它在客户端与认证服务器之间创建一个加密的 TLS 隧道,在加密隧道的保护下,使用 MS-CHAPv2 对客户端的进行身份验证。

1.5　IEEE 802.1X/EAP-PEAP 处理过程

以 IEEE 802.1X/EAP-PEAP 作为一种网络接入认证方案,其认证过程总体上可分为两阶段:TLS 隧道的建立与认证服务器身份的验证阶段。在 TLS 隧道的保护下通过 MS-CHAPv2 完成对客户端的身份验证,及客户端的接入。

第一阶段:TLS 隧道的建立与认证服务器身份的验证阶段,其主要处理过程如下:

1)客户端向接入设备发启 802.1x 接入认证请求。

2)接入设备向客户端请求用户身份标识,客户端向接入设备响应用户身份标识信息。

3)接入设备向客户端协商验证方式:PEAP,客户端向接入设备确认验证方式:PEAP,并通过接入设备发送"hello"信息,请求认证服务器的数字证书。

4)接入设备将请求信息发送给认证服务器,认证服务器将自己的服务器数字证书等信息返回给接入设备,接入设备将认证服务器的数字证书等信息转发给

客户端。

5)客户端验证认证服务器的数字证书,实现对认证服务器身份的验证,生成会话密钥,并以认证服务器数字证书的公钥加密相应的会话密钥及相关信息发送给接入设备,接入设备将这些信息转发给认证服务器。

至此,客户端与认证服务器之间的 TLS 隧道就建立起来了。

第二阶段:在 TLS 隧道的保护下通过 MS-CHAPv2 完成对客户端的身份验证及客户端的接入,处理过程如下:

(1)认证服务器向接入设备请求客户端身份标识信息。

(2)接到请求后,接入设备向客户端发送 EAP-Request/Identity 报文,要求客户端提供用户身份标识。

(3)客户端回应一个 EAP-Response/Identity 报文给接入设备,其中包括用户身份信息。

(4)接入设备将包含用户身份信息的 EAP-Response/Identity 报文封装成 RADIUS Access-Request 格式,并将该报文发送给认证服务器。

(5)接到上述报文后,认证服务器随机生成一个 Challenge 值,将 Challenge 值先封装成 EAP-Request/MD5-Challenge 格式,并将该报文以 RADIUS Access-Challenge 格式发送给接入设备。

(6)接入设备将包括 Challenge 值的报文拆封成 EAP-Request/MD5-Challenge 格式,然后将其转发给客户端。

(7)客户端接收到上述报文后,利用 MD5 算法对用户密码和 Challenge 值一起计算其 HASH 值生成 Challenged-Password,并将 Challenge、Challenged-Password 和用户名等信息以 EAP-Response/MD5-Challenge 的格式发送给接入设备。

(8)接到上述报文后,接入设备再将其封装成 RADIUS Access-Request 格式,并将封装好的报文发送给 RADIUS 认证服务器,以便让认证服务器验证客户端身份。

(9)认证服务器根据报文中的用户身份标识查找用户数据库,以得到用户密码信息,再利用 MD5 算法对用户密码和 Challenge 值做相同的 HASH 运算,将得到的结果与客户端发送过来的 Challenged-Password 进行比较,以判断用户身份是否合法,并将认证成功或失败的信息通过接入设备发送给客户端。如果身份验证成功,通过 RADIUS Access-Accept 报文携带协商参数,以及用户的相关业务属性给用户授权。如果认证失败,则身份验证流程到此结束 。

(10)客户端身份验证成功后(EAP-success),客户端通过接入设备获取 TCP/IP 配置信息等。

(11)接入设备可能还要通知 RADIUS 服务器开始计费等。用户上线完毕。

2 基于活动目录的 802.1X/EAP_PEAP 应用方案

如图 2 所示,给出了一个基于活动目录的 802.1X/EAP_PEAP 应用方案总体架构。

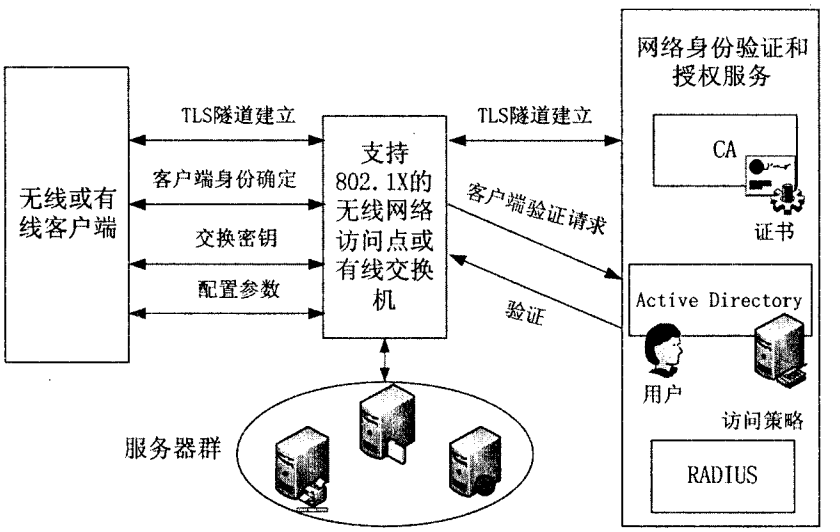

图 2 基于活动目录的 802.1X/EAP_PEAP 应用方案总体架构

1)用活动目录网络管理基础架构实现认证服务器(Authentication Server System)。

活动目录[11]是微软在 Windows 2000 Server 网络操作系统中提出的一种新技术,在后来的操作系统如 Windows server 2003、Windows server 2008 进行了更新和优化。活动目录以 Kerberos[12]为基础,本质上是为分布式网络环境设计的一种目录服务。Kerberos 的密钥分发中心正是以目录服务形式运行的域控制器上,活动目录数据库维护网络中所有安全主体的信息,其中包括每个安全主体在域中注册的秘密密钥信息等。活动目录使得组织机构可以更加有效地对有关网络资源和用户的信息进行共享和管理。另外,目录服务在网络安全方面也扮演着中心授权机构的角色,从而使操作系统可以轻松地验证用户身份并控制其对网络资源的访问。在此以 Windows server 2008 作为服务器,安装配置好活动目录域服务、DNS、DHCP、CA、IIS 等,并以该服务器的 NPS 服务作为 RADIUS 服务器。

在以 Windows server 2008 作为认证服务器的计算机上需进行的主要配置有:

(1)通过 dcpromo 在该服务器上安装 active directory domain service,以将其配置成域控制器,为网络环境提供活动目录服务。

(2)添加 DHCP 角色,并配置好相应的作用域及 tcp/ip 相关的网络参数,为客户机自动分配 IP 地址。

(3)添加 active directory certificate service 角色,为 RADIUS 服务器提供相应的 web 服务器证书。

(4)添加网络策略与访问服务角色,为授予对活动目录数据库的访问权限在 active directory 中进行注册,向 CA 为其申请相应的 WEB 服务器证书,将支持 802.1X 的交换机或无线 AP 配置成其 radius 客户,并配置好相应的网络访问策略,授予客户机相应访问策略,并以 PEAP-MS-CHAP V2 方式进行身份验证。

(5)在 active directory users and computers 中添加客户账户,并授予相应的访问权限。

2)用支持 802.1X 的交换机或无线路由器作为接入设备(Authenticator System)。

在支持 802.2X 的交换机或无线访问点上需进行的主要配置有:

· 通过 Radius-server 指定 Radius 服务器、服务端口以及共享密码等。

· 通过 aaa new-model、aaa authentication 配置与 802.1X 相关的 AAA 设置。

3)用带 802.1x 的客户端系统作为客户端 Supplicant System,目前 Windows xp、Windows vista 以及 Windows 7 均带有 802.1X 客户端。

在 Windows XP 客户端系统上需进行主要配置:

在以太网卡的连接属性中选择"Authentication"选项卡,勾选"Enable IEEE 802.1x authentication for this network",EAP type 选为"Protected EAP(PEAP)",勾选"Authenticate as computer when computer information is available",然后单击 Properties 按钮,在 EAP 属性窗口中选择"Validate server certificate",同时在"Trusted Root Certification Authorities:"窗口中选择对应的 ROOT CA,Authentication Method 选成"Secure password (EAP-MSCHAP v2)"。再点 Configure 按钮确保"Automatically use my Windows logon name and password (and domain if any)"选项已被选中。

3　结束语

为了解决网络由于非法接入而带来的网络安全问题,深入研究分析了 802.1X 协议及其具体的认证过程,通过将 802.1X 与活动目录技术相结合,在 Windows 网络环境下基于活动目录技术构建了一个高效、可靠的 802.1X/EAP-PEAP 接入认证应用方案。为有线网络和无线网络提供了一致的接入验证方法,并将网络接入与域登录身份验证统一起来,实现了透明统一的 SSO 认证与授权。从而为用户有效解决了非法用户的接入问题,提高了网络的安全性。

参考文献:

[1] IEEE Standard 802.1x-2001. standard for port based network access control[S]. 2001.

[2] 王　斐,陈　玲,陆建德. 基于 802.1x 的无线园区网 AAA 系统的设计与实现[J]. 计算机技术与发展,2008,18(10):143-147.

[3] 彭　伟. 使用 802.1x 实现校园网认证[J]. 计算机应用,2003,23(3):25-26.

[4] 郑晓蕾,曹秀英. 802.1x:基于端口的网络接入控制标准[J]. 通信技术,2002,6(6):101-103.

[5] 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):163-166.

[6] 王军号,陆　奎. RADIUS 协议在 AAA 系统中的应用研究[J]. 计算机技术与发展, 2009,19(7):199-202.

[7] 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):43-47.

[8] RFC3748 - 2004 - Cb. Extensible Authentication Protocol (EAP) [S]. 2004.

[9] 陈　群,周　健. 无线局域网安全认证的 EAP 策略[J]. 计算机技术与发展, 2008,18(9):123-126.

[10] 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.

[11] Spealman J, Hudson K, Microsoft corporation. Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure[M]. US:Microsoft press, 2004.

[12] Neuman C, Yu T, Hartman S, et al. The Kerberos Network Authentication Service (V5) [S]. RFC 4120 (Proposed Standard), 2005.

(上接第 153 页)

[8] Lin C Y, Chang S F. Semi-fragile watermarking for authentication JPEG visual content[C]//In: Proceedings of SPIE Security and Watermarking of Multimedia Contents Ⅱ. San Jose, CA, USA: [s. n.], 2000:140-151.

[9] 孙见青,汪荣贵,李守毅. 一种用于图像内容认证的数字水印新方法[J]. 计算机工程与应用,2007,43(17):34-37.

[10] GU Qin-long, YAO Ming-hai. A research of digital image encryption based on logistic chaotic sequence[J]. Computer Engineering and Applications, 2003,39(23):114-116.

[11] 王宏霞,何　晨,丁　科. 基于混沌映射的鲁棒公开水印[J]. 软件学报,2004,15(8):1245-1250.

[12] 李东勤, 林克正. 基于混沌映射的半脆弱图像水印算法[J]. 计算机技术与发展,2008,18(11):156-159.