无线局域网安全认证的EAP策略

陈 群[1,2],周 健[1]
(1.合肥工业大学 计算机信息学院,安徽 合肥 230009;
2.安庆师范学院 网络中心,安徽 安庆 246011)

摘 要:IEEE 802.11i协议使用基于802.1x和可扩展认证协议EAP的认证方案,但标准中并没有指定具体的EAP类型,采用何种EAP策略,直接关系到无线局域网的安全性能。介绍了802.1x和可扩展身份验证协议EAP在保障网络访问安全方面的工作原理,通过对EAP协议分析以及常用的EAP方法比较,提出了部署安全无线局域网的EAP策略;EAP-TLS是用于大型机构无线局域网解决方案的EAP类型,PEAP是用于中小型企业无线局域网解决方案的EAP类型。

关键词:无线局域网;802.1x;EAP;认证;安全;策略
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)09-0123-04

EAP Strategy of WLAN's Security Authentication

CHEN Qun[1,2],ZHOU Jian[1]
(1.School of Computer and Information, Hefei University of Technology,Hefei 230009,China;
2.Network Center of Anqing Teachers' College,Anqing 246011,China)

Abstract:The IEEE802.11i protocol uses a way based on 802.1x and EAP, but the standard doesn't point out the EAP type and what kind of EAP strategy is adopted, which directly relates the security performance of WLAN. Begins with a description of how 802.1x and extensible authentication protocol work to secure access to the network, brings out the EAP strategy of developing WLAN though the analysis of EAP through comparison of common used EAP methods. EAP-TLS is primarily intended for large and enterprise organizations, PEAP is primarily for small and medium organizations.

Key words:WLAN;802.1x;EAP;authentication;security;strategy

0 引 言

无线局域网(WLAN)技术的发展,使人们能更方便、灵活、快捷地访问网络资源,摆脱了传统有线网络的束缚。由于无线设备的可靠性不断提高、价格不断下降,加快了人们对无线局域网的消费需求,个人智能手机、数字助理(PDA)、笔记本电脑已成为越来越多的人享受无线工作和无线生活的工具。为增强WLAN的数据加密和认证等安全性能,2004年6月,美国电气电子工程师协会(IEEE)正式通过了802.11i标准,802.11i标准中使用802.1x认证和密钥管理方式。802.1x标准中引入EAP协议,但并没有指定具体的EAP方法,采用何种EAP策略,直接影响到无线局域网的安全性能。

收稿日期:2007-12-15
基金项目:安徽省自然科学研究项目(KJ2007B043)
作者简介:陈 群(1969-),男,安徽太湖人,讲师,硕士研究生,研究方向计算机网络安全及应用;周 健,副教授,硕士生导师,研究方向为计算机网络、管理与信息系统。

1 802.1x概述

802.1x被称为基于端口的网络访问控制协议(Port Based Network Access Control Protocol),尽管802.1x标准最初为有线以太网设计,并在有线以太网中得到广泛应用,但它也适用于符合802.11标准的无线局域网,它对无线局域网的认证方式和认证体系结构进行了优化。802.1x技术结合EAP认证,可以为无线局域网提供灵活多样的安全技术解决方案。

1.1 802.1x的体系结构

802.1x协议的体系结构包括三个重要的部分:客户端系统、认证系统和认证服务器,无线局域网中802.1x的拓扑结构如图1所示[1]。

客户端系统(Supplicant System)即申请者,一般为一个用户终端系统,在无线局域网中即为无线工作站,该系统通常要安装一个客户端软件,用户通过启动这个客户端软件发起802.1x协议的认证过程。认证系统(Authenticator System)即认证者,在无线局域网中就是无线接入点AP(Access Point),在认证过程中起

"透传"作用。认证服务器(Authentication Server System)通常为 RADIUS 服务器,该服务器可以存储用户信息,如用户名和密码、访问控制列表等。认证服务器对申请者进行鉴别,然后告知认证者,该申请者是否为授权用户。

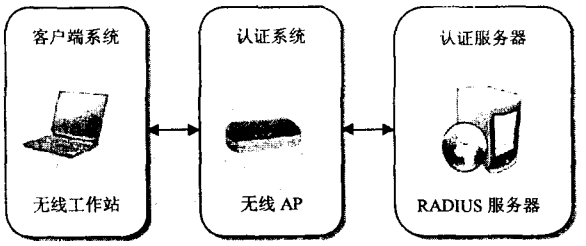

图 1 802.1x 的拓扑结构图

1.2 802.1x 端口控制原理

无线局域网中 802.1x 端口控制原理如图 2 所示[2]。认证者(AP)有两个逻辑端口:受控端口(Controlled Port)和非控制端口(Uncontrolled Port),非控制端口始终处于双向连通状态,不管是否处于授权状态都允许申请者与局域网中设备进行数据交换,主要用来传递 EAPOL(EAP Over LAN)协议帧,可保证随时接受无线客户端发出的 EAPOL 认证报文;受控端口只有在客户端认证通过的状态下才打开,此时,端口切换到授权状态,允许客户端通过该端口进行正常通信,以便访问网络资源及获取服务。

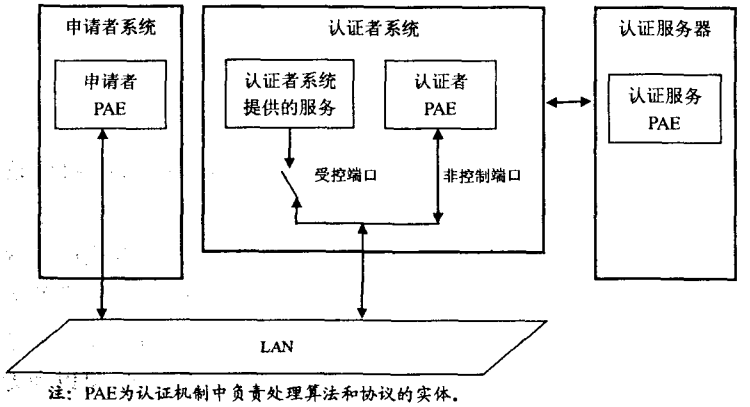

图 2 802.1x 认证的体系结构

2 可扩展认证协议 EAP

可扩展认证协议 EAP(Extensible Authentication Protocol)是 PPP(Point - to - Point)认证中的一个通用协议,其特点是 EAP 在链路控制阶段(Link Control Protocol,LCP)没有选定认证机制,而是把这一步推迟到认证阶段,这样就允许认证者在确定某种特定认证机制前请求更多的信息,还可以采用一个后端服务器来实际实现各种认证机制,认证者仅仅需要传递认证信息。无线局域网中 802.1x 技术结合 EAP 认证,可以允许申请者和认证者之间采用灵活的方案进行认证,并且对将来出现的更先进合理的认证技术具有很好的兼容性,以满足无线局域网的安全需要。

2.1 EAP 数据包的格式及认证过程

EAP 数据包的结构在 RFC 2284 中进行了定义,如图 3 所示[3]。图中各域的含义如下:

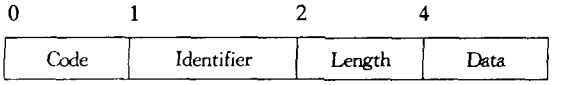

图 3 EAP 数据包格式

* Code:长度为 1 个字节,指明 EAP 包的类型,其值为十六进制,共有四种;

01 - 请求包 Request

02 - 响应包 Response

03 - 成功包 Success

04 - 失败包 Failure

* Identifier:长度为 1 个字节,辅助进行 Request 和 Response 消息的匹配;

* Length:长度为 2 个字节,指明 EAP 包的长度,包括 Code,Identifier,Length,Data 域的全部长度;

* Data:由 Code 域决定,Success 和 Failure 类型的包没有 Code 域,相应 Length 值为 4;Request 和 Response 类型的包格式由所选的 EAP 认证类型决定。

EAP 认证过程为:

(1)在链路建立阶段完成后,认证者发送一个或多个请求(Request)数据包来进行认证,该数据包中有一个类型域表明请求的类型;

(2)对方发送一个响应(Response)数据包对每一个请求做出应答,响应包中类型域和请求包中的类型域相对应;

(3)认证者发送成功(Success)或失败(Failure)数据包结束认证。

2.2 EAPOL 消息的封装

在 802.1x 中 EAP 消息包含在 802.1x 消息中,被称为 EAPOL(EAP Over LAN)——基于局域网的扩展认证协议,EAPOL 在申请者和认证者之间传输,EAPOL 数据包格式如图 4 所示。认证者和认证服务器同样运行 EAP 协议,EAP 帧中封装了认证服务器消息,将该协议封装在高层协议 RADIUS 中,以便穿越复杂的网络到达认证服务器,称为 EAP Over RADIUS。

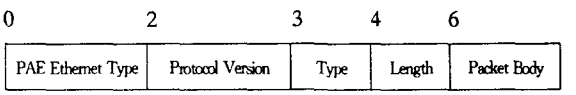

图 4 EAPOL 数据包格式

图中各域的含义如下:

* PAE Ethernet Type:长度为2个字节,表示认证实体表示的网络类型。在802.1x中其值一般为16进制的888E,表示基于端口接入的以太网类型;

* Protocol Version:长度为1个字节,表示EAPOL的版本号,实际应用中其值一般为16进制的01;

* Packet Type:长度为1个字节,表示数据帧的类型,其值有以下5种,见表1。

表1　EAPOL数据包类型

值	名称	说明
00	EAP-Packet	认证信息帧
01	EAPOL-Start	认证发起帧
02	EAPOL-Logoff	退出请求帧
03	EAPOL-Key	密钥信息帧
04	EAP-Encapsulated-ASF-Alert	用于支持ASF的警告信息

* Length:2个字节,表示该数据包体即Packet Body域的长度,单位为字节;

* Packet Body:数据包体,封装了有效的数据,可以包括EAP数据包、EAPOL开始或请求退出、EAPOL-Key的密钥描述符等信息。

3　EAP策略

802.1x中引入可扩展认证协议EAP,但标准中并没有指定具体采用何种身份认证方法,而实际上EAP只是一种封装协议[4],它允许高层使用不同的身份认证协议,如MD5,TLS,TTLS和PEAP等,EAP在802.1x中应用的层次如图5所示。

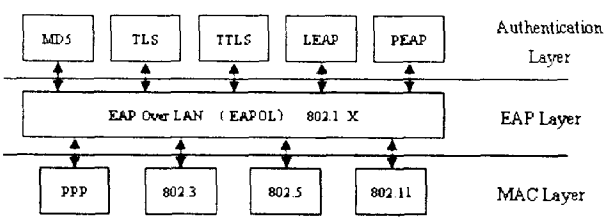

图5　EAP在802.1x中应用的层次

3.1　常用的EAP方法[5]

1)MD5:消息摘要质询,它是一种提供基本级别EAP支持的EAP认证类型。MD5通常不建议用于无线局域网,因为它仅提供单向认证,无法进行无线客户端和网络之间的互相认证。更为重要的是,它不支持自动分配和转动WEP密钥,无法减轻手动WEP密钥维护的管理负担。

2)TLS:传输层安全,它是一个IETF标准(RFC 2716),并可能是在无线客户端和RADIUS服务器上最受支持的一个标准。该方法使用公钥证书对无线客户端和RADIUS服务器进行身份认证,方法是在两者之间建立加密的TLS会话。EAP-TLS的不足之处在于必须由客户端和服务器端双方管理证书,对于较大的无线局域网安装,则是比较重的任务。

3)TTLS:隧道传输层安全,它是由Funk公司开发的,作为EAP-TLS的扩展。此安全方法通过加密通道(或"隧道")为客户端和网络之间提供基于证书的相互认证,与EAP-TLS不同,EAP-TTLS仅需要服务器方面的证书,除去了在客户端安装证书的麻烦。但TTLS主要由Funk销售,而且需为请求者和认证服务器软件付费。

4)LEAP:轻型可扩展认证协议,是一个由Cisco开发的专有EAP方法,它使用密码对客户端进行身份认证,LEAP也具有多个已发布的安全漏洞,例如容易遭受脱机字典攻击和中间人攻击,在LEAP用于认证时,应执行强密码策略。在域环境中,LEAP只能对访问WLAN的用户进行身份认证,而不能对计算机进行身份认证,由于不能对计算机进行身份认证,计算机组策略将无法正确执行,软件安装设置、漫游配置文件和登录脚本可能都会失败,并且用户可能无法更改到期的密码。

5)PEAP:受保护的可扩展认证协议,它是一个两阶段的身份认证方法:第一阶段建立与服务器的TLS会话,并使客户端可以通过使用服务器的数字证书对服务器进行身份认证;第二阶段需要在PEAP会话中为第二个EAP方法建立隧道,以对访问RADIUS服务器的客户端进行身份认证。PEAP的部署只需安装服务器端证书,不需要客户端证书。

3.2　无线局域网EAP策略

尽管理论上任何EAP方法都可以和802.1x一起使用,但并非所有的方法都适合于和无线局域网一起使用,在无线局域网中,所使用的EAP方法必须适合于在未受保护的无线环境中使用,并且可以生成加密密钥。在802.1x中常用的EAP方法比较见表2[6]。

表2　常用EAP方法比较

特点 \ EAP类型 / 功能	MD5	TLS	TTLS	LEAP	PEAP
客户端证书	否	是	否	否	否
服务器证书	否	是	否	否	是
密钥管理	否	是	是	是	是
主要提供商	MS	MS	Funk	Cisco	MS
部署难易程度	容易	难	一般	一般	一般
无线安全性	差	很高	高	较高	高

在无线局域网802.1x中,应用哪一类EAP取决于用户所需的安全级别、标准化组织和厂商对协议的支持情况以及期望的部署难易程度。通过以上分析表明,MD5由于安全性差,不适合于无线局域网的安全认证。TTLS虽然除去了安装客户端证书的麻烦,能

提供较高的安全性能,但协议为 Funk 公司专有,用户需为请求者和认证服务器软件付费,增加了无线局域网的部署成本。LEAP 以前是 Cisco 专有协议,仅与 Cisco 无线适配器一起使用,虽然后来其它制造商经授权也可使用 LEAP,但即使在 LEAP 认证时执行强密码策略,也无法满足高安全要求的无线局域网部署。在上述各 EAP 类型中,TLS 安全性最高,TLS 是一个 IETF 标准,是无线客户端和 RADIUS 服务器上最受支持的一个标准,但 TLS 不仅需要在服务器端安装证书,而且在各个无线工作站上也要安装客户端证书,增加了无线局域网的部署难度,TLS 适合于对安全性有较高要求的大型无线局域网部署中。PEAP 是一种基于安全密码的认证协议,得到了 Microsoft、Cisco 和 RSA Security 等软、硬件厂商的广泛支持,PEAP 可以兼容几乎全部厂商的全部设备,拥有了相当规模的市场占有率;由于 PEAP 使用服务器单边证书来认证无线局域网客户端,且 PEAP 与 Windows 操作系统的良好协调性,以及可以通过 Windows 组策略进行管理的特性,从而简化了安全无线局域网的部署和管理。

4 结束语

802.11i 标准中,采用 802.1x 结合 EAP 并选择高级加密标准 AES,可以为无线局域网提供强健的安全保障。具体应用哪一类 EAP,要综合考虑协议的安全性、通用性以及能否更方便部署等因素。由于 EAP-TLS 和 PEAP 自身的特点,使其成为部署无线局域网时优先考虑的 EAP 类型。Windows Server 2003、Windows XP 以及 Windows Vista 都提供了对 EAP-TLS 和 PEAP 的内置支持,Microsoft 公司提供了两套无线局域网安全解决方案[7]:使用 EAP-TLS 的"确保无线 LAN 的安全-证书服务解决方案"和"使用 PEAP 和密码确保无线 LAN 的安全",分别用于信息技术环境相对比较复杂的大型机构和中、小型企业部署高安全性的无线局域网。

参考文献:

[1] IEEE. IEEE standard for local and metropolitan area networks-Port-Based Network Access Control[S]. USA:[s.n.], 2001.

[2] 袁建国,方宁生,姜 浩. 802.1x:基于端口的访问控制协议[J]. 微机发展(现名:计算机技术与发展),2005,15(12):160-161.

[3] 周 晓,王芙蓉,郭 毅. 802.1x 在分布式防火墙中的应用[J]. 计算机技术与发展,2006,16(12):245-246.

[4] 楼颖明,罗汉文. 802.11 无线局域网的安全方案分析[J]. 通信技术,2002(9):79-80.

[5] Microsoft. 选择无线 LAN 的安全策略[EB/OL]. 2004-05-27. http://www.microsoft.com/china/technet/security/guidance/peap-int.mspx.

[6] Intel. 无线安全—802.1x 和 EAP 类型[EB/OL]. 2006-10-18. http://www.intel.com/support/cn/wireless/wlan/sb/cs-008413.htm.

[7] Microsoft. 使用 PEAP 和密码确保无线 LAN 的安全[EB/OL]. 2004-05-27. http://www.microsoft.com/china/technet/security/guidance/peap-1.mspx.

(上接第 114 页)

两题应该很快也能解决 P374,P495 两题。由此可见,概念相似度在对选手训练程序设计也是有帮助的。

4 结束语

概念相似度的计算除了在上一节描述以外,还有许多领域有着广泛的应用,例如信息检索,它是机器理解概念进行推理的重要一步。在国内外相关研究基础上,通过 FCA 的概念,根据笔者多年对程序设计算法的研究,巧妙地结合了网络流算法,提出基于属性的概念相似度的算法,这也是文中创新之处。通过实验可以看出,所提出的算法是可行的。当然该算法也有进一步挖掘的地方,比如与语义距离三角形原理结合使最终结果更人性化、更贴合实际情况。

参考文献:

[1] Borst W N. Construction of Engineering Ontologies for Knowledge Sharing and Reuse [D]. Enschede: University of Twente, 1997.

[2] Studer R, Benjamins V R, Fensel D, et al. Knowledge engineering, principles and methods[J]. Data and Knowledge Engineering, 1998, 25(1-2):161-197.

[3] Ganter B, Wille R. Formal Concept Analysis: Mathematical Foundations[M]. Heidelberg: Springer, 1999.

[4] Wille R. Restructuring lattice theory: An approach based on hierarchies of concepts[C]//In: Rival I. Oredered sets. Dordrecht-Boston: Reidel, 1982: 445-470.

[5] Ivkovic I, Kontogiannis K. Towards Automatic Establishment of Model Dependencies Using Formal Concept Analysis[J]. International Journal of Software Engineering and Knowledge Engineering (IJSEKE), 2006, 16(4): 499-522.

[6] 刘 群,李素建. 基于《知网》的词汇语义相似度计算[J]. Computaional Linguistics Chinese Language Processing, 2002, 7(2): 59-76.

[7] 胡运权,郭耀煌. 运筹学教程[M]. 第 3 版. 北京:清华大学出版社,2007.