文章编号:1001 - 9081(2008)05 - 1146 - 03

数字化校园中统一身份认证系统研究

李小雪,吴中福,钟 将,李国柱
(重庆大学 计算机学院,重庆 400030)
(wiremickey@163.com)

摘 要:给出了一种基于 IEEE 802.1X 协议和 Diameter 协议的校园网统一身份认证系统。通过对 EAP-PEAP 协议进行扩展,并且采用 Diameter 的消息路由机制,该系统能够支持域间身份认证和统一认证令牌的发放,从而解决了校园网身份认证中用户漫游和单点登录的问题。对于此身份认证系统易遭受的攻击类型作了分析,并提出了相应的解决方案。

关键词:统一身份认证;跨域;802.1X;受保护的可扩展的身份验证协议;Diameter 协议
中图分类号: TP393.08 **文献标志码**:A

Research into unified authentication system of digital campus

LI Xiao-xue, WU Zhong-fu, ZHONG Jiang, LI Guo-zhu
(*College of Computer Science, Chongqing University, Chongqing* 400030, *China*)

Abstract: Campus authentication system is a key part of digital campus. After analyzing the demands of authentication system, a campus unified authentication system based on IEEE 802.1X protocol and Diameter protocol was proposed. By extending EAP-PEAP protocol and introducing message routing mechanism in Diameter protocol, this authentication system can provide cross-domain authentication and authentication ticket distribution, thus solving the roaming authentication and single sing-on problems in campus network authentication system. At last, some means of attack were analyzed, and corresponding solutions were proposed.

Key words: unified authentication; cross-domain; 802.1X; Protected Extensible Authentication Protocol(PEAP); diameter protocol

0 引 言

在数字化校园建设中,校园网的接入身份认证系统处于十分重要的地位。一个好的身份认证系统应该满足可靠性和易用性两方面需求。可靠性有两点:第一,身份认证系统具有抵抗网络攻击(窃听、篡改、伪造、拒绝服务等)的能力;第二,考虑到在有多个校区的学校中,如果采用全校集中的网络接入身份认证系统,大量的认证数据流会造成校区间网络负载的增加,且唯一的身份认证服务器易形成单点故障,所以认证系统应该采用支持用户漫游的分布认证方式。易用性则是指认证系统支持单点登录,即一次接入认证之后就可访问校内的应用系统(例如网络接入和图书馆借阅管理系统)而不再重复认证。

在接入认证协议中,IEEE 802.1X[1] 协议作为一个基于端口的访问控制协议,近年来已经被广泛采用。特别是由于新的无线局域网安全标准 802.11i 以 802.1X 为基础,使得它更加适合校园网中有线网络和无线网络并存的环境。IEEE 802.1X 采用 Internet 工程任务组(Internet Engineering Task Force, IETF)提出的可扩展认证协议(Extensible Authentication Protocol, EAP)[2]。EAP 定义了一种可以扩展支持多种认证方法的认证协议框架,可以运用于不同协议之上,如点对点协议(Point-to-Point Protocol, PPP)或 IEEE 802 等标准数据链路层协议、拨入用户远程认证服务(Remote Authentication Dial-In User Service, RADIUS)或 Diameter 等认证、授权、计费(Authentication, Authorization, Accounting, AAA)协议,为不同协议之间认证信息的传递提供了统一平台。EAP 支持多种认证协议,例如 MD5、传输层安全协议(Transport Layer Security, TLS)等,以提供认证过程中的信息安全,安全的特点和加密的强度因不同的认证协议而异,其良好的扩展性为身份认证系统功能的扩展提供了很好的途径。

现阶段认证系统中认证服务器普遍采用的是 RADIUS 协议,但是由于协议本身的缺陷,比如基于用户数据报协议(User Datagram Protocol, UDP)的传输、简单的丢包机制、没有关于重传的规定和集中式计费服务,都使得它不太适应当前网络的发展。IETF 在 2003 年提出了 Diameter[3] 协议作为替代 RADIUS 的下一代 AAA 协议标准。该协议充分考虑了未来 AAA 服务对安全性、可靠性和移动性方面的需求,通过引入代理(Agent)设备,很好地解决了跨域身份认证的问题。

基于上述的校园网身份认证系统的需求和当今身份认证系统的发展,本文提出了一个校园网统一身份认证系统。该身份认证系统基于 Diameter 协议和 802.1X/EAP-PEAP 协议,并且对 EAP-PEAP 协议进行了扩展,支持单点登录和用户漫游,并且同时提供有线/无线网络的认证服务。

1 系统介绍

身份认证系统需要有丰富的认证功能。在本文的设计

收稿日期:2007 - 11 - 27;**修回日期**:2008 - 01 - 16。 **基金项目**:国家发改委基金资助项目(CNGI-04-6-2T)。

作者简介:李小雪(1981 -),男,重庆人,硕士研究生,主要研究方向:计算机网络安全; 吴中福(1938 -),男,四川安岳人,教授,博士生导师,主要研究方向:网络安全、网格计算与远程教育; 钟将(1974 -),男,重庆人,博士,主要研究方向:计算机网络安全、免疫计算; 李国柱(1982 -),男,重庆人,硕士研究生,主要研究方向:计算机网络安全。

中,安全认证接入交换机需要提供 802.1X 认证功能,同时能够与 Diameter Server 紧密结合,实现对接入用户的控制,达到用户名、IP、MAC、VLAN ID、交换机 IP 和端口号的捆绑,从而防止 IP 盗用、IP 篡改、私设服务器等行为出现,从而防止校园网中非法用户行为[4]。

本文所设计的身份认证系统的网络拓扑如图 1 所示。

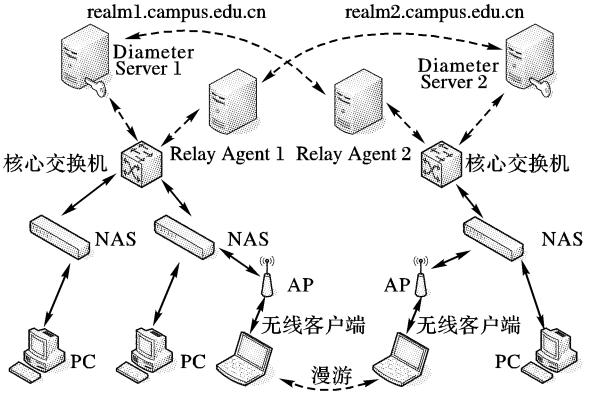

图 1　基于 Diameter 和 802.1X 的校园网跨域身份认证系统[5]

图中,PC 和无线客户端为 802.1X 的申请者(supplicant),需要安装支持 802.1X 的接入客户端;NAS(Network Access Server,网络接入服务器)为支持 802.1X 协议和 Diameter 协议的接入交换机,作为 802.1X 协议中的认证者(authenticator),同时也是 Diameter 客户端;而 Diameter Server 则作为 802.1X 协议中的认证服务器(Authentication Server, AS),包含用户信息及权限的数据库。考虑到管理和部署的统一性,无线访问接入点(Access Point,AP)仅作为网桥连接有线局域网和无线局域网,不作额外的认证设置。图中标示出两个域:realm1. campus. edu. cn 和 realm2. campus. edu. cn,代表同一学校内的校区 1 和校区 2。

2　身份认证系统流程

本统一身份认证系统的认证流程分为域内认证和域间认证两种类型。

2.1　域内身份认证流程

对于使用有线网络的域内用户,认证流程如下:

首先由 PC(作为申请者)向 NAS(作为认证者)发送 EAPoL-Start 消息,发起认证请求。NAS 回复给 PC 一条 EAPoL-Request-ID 消息,表示认证请求开始并要求申请者提供身份。申请者回应 EAPoL-Response-ID 应答消息,其中包含用户身份信息,该消息由 NAS 重新封装成 Diameter-EAP-Request 请求消息转发给认证服务器 Diameter Server(作为认证服务器)。然后,通过 NAS 转发,PC 和 Diameter Server 进行 EAP 认证过程。若认证成功,Diameter Server 向 NAS 发送 EAP-Success 消息,允许该 PC 接入网络,NAS 收到该消息后转发 EAPoL-Success 消息给 PC,并同时将自己的 802.1X 受控端口设置为授权状态。之后,经过认证的 PC 就可通过 NAS 的授权端口接入网络。

无线局域网的用户接入认证方式与有线局域网用户类似,但无线客户端在与 NAS 通信之前需要首先与 AP 进行无线关联,而在 EAP 认证时产生的对等主密钥(Pairwise Master Key,PMK)被用来进行 802.11i[6] 协议中的强安全网络(Robust Security Network,RSN)关联。经过四步握手密钥协商体制,无线客户端最终可与 NAS 建立起安全的加密信道,保证了无线传输数据的私密性,避免了无线局域网中窃听、非法接入等安全隐患。

2.2　域间身份认证流程

Diameter 代理分为实现服务域(Realm)间消息路由功能的中继代理(Relay Agent,RA)、实现管理域(Domain)间消息路由的委托代理(Proxy Agent,PA)、实现消息重定向功能的重定向代理(Redirect Agent,RDA)以及实现不同 AAA 协议间转换的翻译代理(Translation Agent,TA)。本身份认证系统中引入中继代理,提供跨域认证功能。中继代理的作用是转发域内多个 NAS 的跨域认证请求。设置中继代理有几个方面的好处:首先,中继代理汇聚了域内所有 NAS 的跨域认证请求,这样就不必在域内所有 NAS 上配置与属于其他域的认证服务器建立安全连接所需的信息,同时也减轻了认证服务器与太多域外 NAS 建立连接的压力;其次,当增加或减少 NAS 时,中继代理的存在也减少了在认证服务器上的配置任务。

跨域数据流程如图 2 所示。

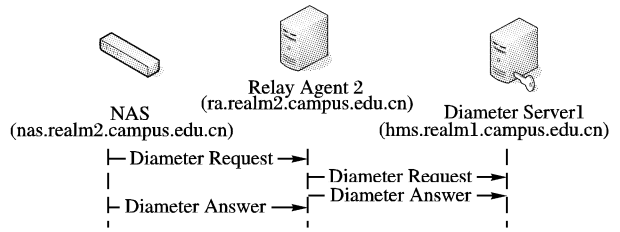

图 2　中继代理实现跨域认证

当属于校区 1 的无线客户端漫游到校区 2 并与校区 2 的 AP 完成无线关联后,它向校区 2 的 NAS(nas. realm2. campus. edu. cn)发起认证请求,其中包含本人的身份 user@ realm1. campus. edu. cn。处于 realm2 中的 NAS 作为 Diameter 客户端,根据用户身份中的“realm1. campus. edu. cn”字段查找自身域路由表,确定申请者不属于本域,就将认证请求向 realm2 域内的中继代理 Relay Agent 2(ra. realm2. campus. edu. cn)转发。该中继代理收到请求,同样进行域路由表查找,根据对应“realm1. campus. edu. cn”的表项,发现需要 realm1 中的认证服务器提供认证,于是将认证请求转发至位于 realm1 域的认证服务器 Diameter Server 1(hms. realm1. campus. edu. cn),这样就完成了认证请求的跨域过程。而认证应答消息经由反方向路径返回,从而实现了用户身份的跨域认证。

如果校区较多,还可考虑设置重定向代理。重定向代理位于域间,它并不负责认证数据的转发,而是集中储存各个域的路由配置信息,以便各个域的中继代理在需要时查询。重定向代理的好处是实现了集中管理,如果认证系统有变动,例如认证服务器的增减,只需要改动重定向代理内的路由信息,而不需修改所有中继代理的设置,大大减轻了配置任务。

3　认证令牌分发

统一身份认证系统通常采用认证令牌的方式实现单点登录,但认证令牌的分发普遍都采用的是 Web 方式。结合本认证系统特点,本文提出一种采用扩展 EAP-PEAP 认证协议的方式实现的认证令牌分发方式。它工作于数据链路层上,能够在认证成功的同时分发认证令牌,与 Web 方式相比,具有集成度高、易用性高、资源开销小等优点。

受保护的 EAP 协议(Protected EAP Protocol, PEAP)[7] 是一种混合式 EAP 认证协议。它分两个阶段进行:第一阶段建立单项服务器认证的 TLS 隧道;第二阶段在该隧道保护下,

对客户方进行 EAP-OTP、EAP-MD5 或 EAP-MS-CHAPv2 等基于 EAP 的方式认证。与 EAP-TLS 采用的证书方式相比，PEAP 仅需要服务器装有公钥证书，这既消除了对客户方公钥证书的要求，符合校园网络的特点，简化了身份认证系统的布署，又使对客户方进行的认证处于 TLS 加密信道的保护之下，保证了之后的通信内容的安全。

PEAP 协议在第二阶段采用了类型长度值(Type Length Value，TLV)格式封装数据，有 Result-TLV、NAK-TLV、Error-Code TLV、EAP-Payload TLV 等多种类型，这意味着 PEAP 协议第二阶段并不局限于传输 EAP 认证数据。本系统设计了一个称之为 Token TLV 的新 TLV 类型，加入到 PEAP 第二部分的传输过程中，使之支持认证令牌的请求和传输。扩展后的 PEAP 协议第二阶段的层次结构如图 3 所示。

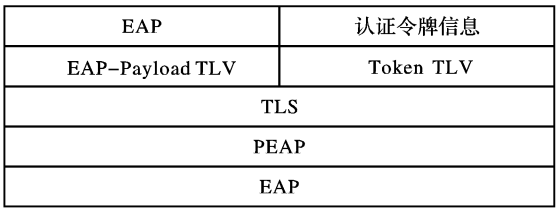

图 3 PEAP 协议第二阶段层次结构

Token TLV 遵循 TLV 标准，图 4 为具体格式。

图 4 Token TLV 消息格式

1)M 位：设为 0，表示为可选 TLV。

2)R 位：保留位，设为 0。

3)TLV Type：长度 14 位，在此选取未定义的编号 21 作为其值。

4)Length：长度 16 位，为 TLV 消息除 4 字节包头后的长度。

5)F、K 位：00 保留，01 为客户端发送的请求认证令牌消息，10 为服务器端发送的认证令牌消息，11 为客户端发送的认证令牌确认消息。

6)认证令牌字段：服务器发送的认证令牌内容，该字段仅存在于服务器端发送的认证令牌消息中。

扩展后的 EAP-PEAP 认证过程包含认证令牌发放过程，流程如图 5 所示。

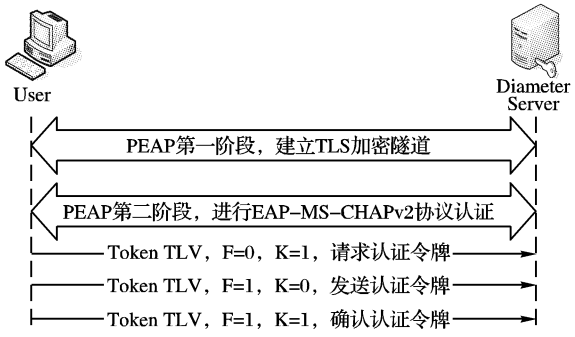

图 5 扩展后的 EAP-PEAP 认证及令牌发放流程

客户端在 PEAP 第二阶段的认证完成之后，向认证服务器发送认证令牌请求，同时启动超时计时器。认证服务器接到请求，根据数据库中用户权限生成相应的认证令牌，并封装到 Token TLV 中发送。客户端收到认证令牌，发送确认消息，整个认证过程结束；或客户端在计时器超时后重新发送认证令牌请求。整个过程都处于 TLS 隧道中，有效地避免了窃听、篡改等安全隐患。客户端在获得认证令牌之后，就可以将其用于其他应用系统的登录中，从而实现了统一的单点登录。

4 安全性分析

本认证系统采用 EAP-PEAP 认证协议，保证了认证数据的完整性和机密性，同时也能够防止中间人攻击和重放攻击。但对于拒绝服务攻击(Deny of Service，DoS)，有下列两种情况分别讨论：

4.1 针对认证服务器的 DoS 攻击

针对认证系统的 DoS 攻击是指通过反复发送虚假的身份认证信息，消耗认证服务器资源，增加认证服务器负载，使其由于资源耗尽而导致拒绝服务。对于此类攻击，本文考虑采用过滤的方法，将攻击阻止在 NAS 处，减轻认证服务器的压力。

NAS 对每个发送 EAPoL-Start 消息开始认证过程的用户记录其 MAC 地址和尝试登录次数。在达到尝试次数上限后，启动计时器，在一段时间内对于该 MAC 地址发出的请求认证消息 EAPoL-Start 直接丢弃，使其无法连接到认证服务器，由此保护认证服务器不受 DoS 攻击。

4.2 针对 802.1X 协议的 DoS 攻击

802.1X 协议中的 EAP 协议容易遭受的 DoS 攻击[8]有：反复发送虚假 EAPoL-Start 报文阻止正常用户认证成功；伪造某个特定用户的 EAPoL-Logoff 报文发送到认证服务器，使服务器将该用户的对应的 NAS 受控端口状态转为未授权，终止向用户提供服务。

对于第一种攻击，可以采用 4.1 节中的方法解决。而对应第二种攻击需要采用数字签名方式，具体实现过程如下：

1)客户端在发送 EAPoL-Logoff 等非加密报文之前，生成一个随机数 R。记之前认证过程中获得的认证令牌为 T。

2)客户端生成字符串 $S = R + T$，计算 $H = \mathrm{md5}(S)$。

3)在 EAPoL-Logoff 等非加密报文中添加 R 和 H 字段，发送到认证服务器。

4)认证服务器在认证过程中也保存认证令牌 T。在收到 EAPoL-Logoff 等非加密报文后，取出报文中的随机数 R，同样计算 $H1 = \mathrm{md5}(R + T)$。若 $H1 = H$，则可证明报文为合法客户端所发。

由于认证令牌仅由认证服务器和通过认证的客户端所有，而且分发过程避免了窃听和篡改，因此能够作为签名，证实 EAPoL-Logoff 等非加密报文的合法性。

5 结语

认证计费系统对校园网络的管理及运行来说是至关重要的。目前校园网使用较多的身份认证方式主要有 Web Portal、以太网承载点对点协议(PPP over Ethernet，PPPoE)和 802.1X 三种。相对于普遍采用的 Web 认证方式，802.1X 认证方式能够减轻网络封装开销，消除网络瓶颈，实现认证流与业务流的分离，保证网络传输效率。同时，IEEE 802.1X 作为二层协议，对网络的整体性能要求不高，能够有效降低建网成本。而且在无线局域网安全标准 802.11i 中，也要求使用 802.1X 协议进行身份认证。

(下转第 1151 页)

如果客户端是 IDV 的受信方,也可由客户端代为验证。

7)用户 BC 验证:用户需要身份认证时,客户端将此用户的 BC 发往 IDV。IDV 可以到发证的权威机构查证其真伪。如果客户端是 IDV 的受信方,也可由客户端代为验证。

8)如果以上检查、验证都没有问题,IDV 可以接受远端的 BPU 的处理结果。

3　实例

以电子商务中一种典型的例子来说明认证框架的应用。例子中包含两个 BPU:1)生物认证设备,内置数据采集、信号处理、匹配和决策模块,可以完成一次完整生物认证;2)存储设备,为 STOC 卡(Store On Card),如智能卡,内含 BC 和 AC。生物认证设备在客户端一侧,用户持有 STOC 卡。客户端的作用是为用户提供服务界面,还可以存储和转发 BPU 以及服务器的信息。此外还有 SP 和 IDV。

一种可能的认证方式的主要过程如下:

1)用户需要 SP 的某项服务时,客户端向 SP 提出申请服务请求。

2)SP 同意请求后,将 IDV 的 URL 返回给客户端。

3)客户端向 IDV 发申请认证请求消息。

4)IDV 同意后生成一个随机串作为“挑战”,连同同意认证消息一起发给客户端,IDV 记录此随机串。

5)客户端提示用户插入 STOC 卡并确认。

6)客户端向生物认证设备发出请求认证消息,并把 IDV 的挑战传送给生物认证设备。

7)生物认证设备采集用户生物特征,进行信号处理,生成现场样本。

8)生物认证设备向客户端发送要求要求模板的消息。

9)客户端向 STOC 卡发送要求模板的消息,并把 IDV 的挑战传送给 STOC 卡。

10)STOC 卡把 IDV 挑战作为应答,生成 ACBio Instance。

11)STOC 卡将 ACBio Instance 连同 BC 和 AC 发到客户端。

12)客户端存储以上内容,并把STOC卡的ACBioInstance 和 BC 发到生物认证设备。

13)生物认证设备验证上述 Instance 的完整性。将 BC 中模板与自己产生的现场样本进行比较,得出身份验证结果。然后生成自己的 ACBio Instance。

14)生物认证设备将自己的 ACBio Instance 发到客户端。

15)客户端接受上述信息,并将 2 个 BPU 的 Instance、BC 和 AC 传送给 IDV。

16)IDV 收到以上信息后:(1)核查 Instance 中 BPU 证书的合法性;(2)核查 BC 和 AC 的真实性;(3)检查 Instance 的应答是否为自己的挑战;(4)IDV 核查 Instance 的数字签名;(5)根据 AC 中的权限,找出 BPC 中对应的认证策略,检查 Instance 中的功能报告和安全报告中记录的内容是否符合认证策略;(6)如果以上验证都通过,则接受生物认证设备的认证结果。

4　结语

生物认证的应用方兴未艾,从其传统应用领域,如门禁、考勤、司法系统等,已经逐步扩展到更广泛应用领域,如进出境管理、金融、福利金领取、国民身份管理等,但目前基本是局部的、实验性的。随着有关国际标准的建立和应用框架的完善,生物认证在未来身份认证中的大规模应用才能变为现实。本文提出的开放式网络环境进行身份认证的框架正是希望在这方面做出一些探索性工作。

参考文献:

[1] ITU-T SG17. Proposed draft Recommendation for X. tsm[S]. Geneva: 2005.

[2] ITU-T SG17. Revised draft Recommendation X. tai: Telebiometrics Authentication Infrastructure(TAI)[S]. Seoul: 2007.

[3] ISO/IEC 1st CD 24761. Information technology-Security techniques-Authentication context for biometrics[S]. Berlin: 2006.

[4] ISO/IEC 19785-1. Information Technology-Common Biometric Exchange Formats Framework-Part 1: Data Element Specification[S]. 2006.

(上接第 1148 页)

本文提出的基于 802.1X 和 Diameter 协议的校园网统一身份认证系统具有良好的效率和很高的安全性。它采用的新一代的认证计费协议 Diameter 能够很好地支持跨域需求,而扩展后的 PEAP 认证协议则实现了 802.1X 协议下的认证令牌同步发放,并且有对应拒绝服务攻击的解决方案。因此,该统一身份认证系统可以广泛适应校园网络的各种需求。

参考文献:

[1] IEEE-SA. IEEE Std 802.1X-2004, Port-based network access control[S]. Washington DC: IEEE Computer Society, 2004.

[2] ABOBA B, BLUNK L J, VOLLBRECHT J R, *et al*. IETF RFC 3748, Extensible Authentication Protocol(EAP)[S]. Reston, VA, USA: The Internet Society, 2004.

[3] CALHOUN P R, LOUGHNEY J, GUTTMAN E, *et al*. IETF RFC 3588, Diameter base protocol [S]. Reston, VA, USA: The Internet Society, 2003.

[4] 冯雯,郑炳伦,吴江. 基于 802.1X 的校园网身份认证系统的设计与实施[J]. 四川大学学报:自然科学版,2006,43(6):1236 - 1241.

[5] MENG FANG, AN CHANG-QING, YANG JIA-HAI. Implementing a secure AAA system in IPv6 network[C]// Proceedings of the 2006 International Conference on Communication Technology(ICCT'06). Washington DC: IEEE Computer Society, 2006:1 - 4.

[6] IEEE-SA. IEEE Std 802.11i. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements[S]. Washington DC: IEEE Computer Society, 2004.

[7] PALEKAR A, SIMON D, SALOWEY J, *et al*. Protected EAP Protocol(PEAP) Version 2[S]. California: [s. n.], 2004.

[8] HE CHANG-HUA, MITCHELL J C. Security analysis and improvements for IEEE 802.11i[C]// Proceedings of the 12th Annual Network and Distributed System Security Symposium(NDSS'05). Reston, VA, USA: The Internet Society, 2005:90 - 110.

[9] 马建峰,朱建明,赖晓龙,等. 无线局域网安全—方法与技术[M]. 北京:机械工业出版社,2005.