基于接入控制器模式的公共无线局域网安全体系设计

宋宇波, 胡爱群, 杨晓辉
(东南大学信息安全研究中心, 南京 210096)

[摘要] 公共无线局域网面临网络安全、用户数据保护、身份认证、移动管理及网络服务等多方面的挑战。将现有的公共无线局域网分为 WISP—owned, Operator—owned以及 for Enterprise 3种类型, 并分别讨论了各种类型的特征及其架构。在此基础上提出一种基于接入控制器模式的通用安全体系, 可应用于目前大多数类型的公共无线局域网。提出了一种 802.1X和 Web认证的混合型认证协议, 该协议在进行 Web认证时将利用 802.1X协商后产生的密钥进行, 可有效地抵抗窃取服务、基站伪装、消息窃听等攻击, 并与现有公共无线局域网 Web认证相兼容。

[关键词] 公共无线局域网; 安全体系; 认证; 接入控制器
[中图分类号] TP393.17 [文献标识码] A [文章编号] 1009—1742(2008)08—0056—04

1 前言

随着无线应用和无线网络技术的快速发展, 人们希望能够降低网络基础设施的成本, 同时也能享受随时随地的移动网络应用, 得到高效率、高质量、低商业成本的网络服务。网络连接将从公司、学校等私有网络扩展到诸如机场、宾馆、公园、商业区等人群密集的公共热点地区。由于无线局域网技术在传输速率、设备成本、网络复杂度、可管理性、室内短距无线通信等方面无疑具有优势, 因此基于 IEEE802.11[1]标准无线局域网技术的公共无线局域网络 (public wireless local area network, PWLAN) 无疑是目前提供高速公共无线网络连接的理想解决方案。近年来, 国内外已有很多网络运营商架构了公共无线局域网, 提供 11~54 Mb/s的无线宽带网络服务。

公共无线局域网是在机场、车站、酒店、旅馆、超市、剧场、公园、会议场所等人口密集的公共热点地区部署基于无线局域网技术, 提供高带宽无线互联网接入服务的无线网络系统。它面临着网络安全、用户数据保护、身份认证、移动管理及网络服务等多方面的挑战。现有的公共无线局域网又不同的运营商经营, 其体系结构差别较大。使得用户无法在不同运营商之间的无线局域网间进行自由切换和漫游。另外, 现有的公共无线局域网没有专门的安全认证机制, 目前网络运营商一般采用基于 Web认证实现用户的认证授权、接入和计费。然而这存在较大的安全漏洞, 攻击者可以通过 IP或 MAC地址欺骗窃取服务, 底层的数据缺乏加密和完整性保护, 同时这种认证方式无法抵抗基站伪装攻击。

将现有的公共无线局域网分为 WISP—owned, Operator—owned以及 for Enterprise 3种类型, 并分别讨论了各种类型的特征及其架构。在此基础上提出一种基于接入控制器模式的通用安全体系, 可应用与目前大多数类型的公共无线局域网。另外, 提出了一种 802.1X和 Web认证的混合型认证协议, 该协议可有效地抵抗窃取服务、基站伪装、消息窃听等攻击, 并与现有公共无线局域网 Web认证兼容。

[收稿日期] 2006—11—04; 修回日期 2007—03—29
[基金项目] 信息产业部 242资助项目 (2005A14)
[作者简介] 宋宇波 (1977—), 男, 江苏无锡市人, 博士, 东南大学信息安全研究中心讲师

2 公共无线局域网架构

从现有的应用上看,目前的公共无线局域网结构上基本相似,都是基于现有互联网的事实标准架构,其采用的无线局域网技术为 IEEE802.11或者是 HIPERLAN。其提供服务模式基本上是有线网络服务的扩展和延伸。从应用模式和体系结构上看,可将公共无线局域网定义为以下 3种类型:

1) WISP—owned PWLAN是由无线互联网服务提供商(wireless internet server porvider,WISP)架构的公共无线局域网。其主要特点为公共无线局域网是有线互联网接入服务的延伸,网络运营商提供主要向用户提供互联网接入服务,网络运营商拥有自己的基于互联网的认证授权计费管理系统。其架构由无线接入点、接入控制器、IP核心网络、网关、管理系统和本地网络应用构成。

2) Operator—owned PWLAN是由蜂窝网络运营商(cellular network operator)架构的公共无线局域网。这种公共无线局域网体系结构最先由 Juha Ala—Laurila[2] 等人在 2001年提出,其主要思路是充分利用蜂窝网络的基础设施和资源架构公共无线局域网。无线局域网传输速率高,成本低廉,部署简单,但覆盖距离小,只能部署在特定的公共热点地区;而蜂窝网络具有覆盖范围大,并已得到广泛的部署和应用,拥有良好的计费漫游管理设施和庞大的客户群,但数据传输速率低而且费用高。因此,两种网络有着很好的互补性,两者结合可以满足那些需要宽带无线接入又需要随时随地的移动网络连接的用户需求。目前已有面向 GSM、GPRS、CDMA2000、3G蜂窝网络运营商的 PWLAN架构方案。

欧洲电信标准协会定义了该结构的两种模式[3]:紧耦合模式和松耦合模式。在紧耦合模式中,WLAN通过标准化接口或者一个特别用于优化WLAN性能的新接口连接到蜂窝网络的服务节点(如 GPRS网络的 SGSN节点),用户 IP数据和鉴权计费等数据都要通过服务节点进入蜂窝网络的核心网。这种方式的耦合度较高,可以很方便地重用蜂窝网络提供的 AAA基础设施;在松耦合模式中,WLAN的用户数据是通过 WLAN连接到运营商的 IP网,没有经过蜂窝网络的核心网,只有鉴权、计费信令从蜂窝网络网关节点或专门的设备进入蜂窝网络核心网。

3) PWLAN for Enterprise是面向企业的公共无线局域网。上述两种类型主要针对的用户群是那些希望访问互联网的普通用户群,而这种类型的公共无线局域网主要面向企业用户。这种类型的公共无线局域网体系结构与第一种类型类似,主要不同的是接入控制器应支持 VPN网关功能,以使企业用户可以安全的访问企业内部网。

3 公共无线局域网安全体系结构设计

在讨论公共无线局域网安全体系结构设计之前,有必要考虑公共无线局域网面临的安全威胁。公共无线局域网由于自身的特点,比有线网络面临更广泛的安全威胁:a 易受窃听,攻击者难以发现;b 易受插入攻击,攻击者无需切开电缆就可向网络发送数据;c 易受拒绝服务攻击(DoS),攻击者可大量发送垃圾信息阻塞信道或对某个移动设备发送虚假服务请求,使该设备始终处于全额工作状态而迅速耗尽电池中的电能;d "基站"伪装,攻击者可用自己的大功率"基站"覆盖真正的基站,而使得无线终端错误地与之连接。

通过对现有公共无线局域网的体系结构的分析,提出一个基于接入控制器的通用安全体系结构,该体系结构可以应用于大多数类型的公共无线局域网。图 1显示了一个通用的公共无线局域网安全体系结构,该体系结构基本上满足上述 3种类型的公共无线局域网类型。该体系主要由移动终端、无线接入点、接入控制器、Web认证服务器、AAA服务器/AAA代理等关键部件构成。

1) 移动终端。移动终端主要指的是用于接入 802.11网络的用户设备。其主要功能包括无线网络搜寻功能、无线网络连接功能、无线网络认证功能、无线网络连接管理。

2) 无线接入点。这里的无线接入点一般指的是提供 802.11无线网络接入的接入点。提供无线接入网与固定网之间的网桥功能,认证信息转发功能,提供基于 802.1X的接入控制功能,把移动终端的认证信息转发给 AAA服务器,链路层的加密功能,用户 MAC地址接入控制及用户二层隔离功能。

3) 接入控制器。接入控制器位于无线接入网与互联网的交界处,主要提供移动终端连接互联网的接入控制功能。它的主要功能包括:提供移动终端连接互联网的接入控制功能;充当 Internet网关;提供如 DHCP、DNS、VLAN、VPN等本地网络服务;实施对网络的业务控制;网络数据的监控和网络设备的管理。这里的接入控制器是个逻辑上的概念,

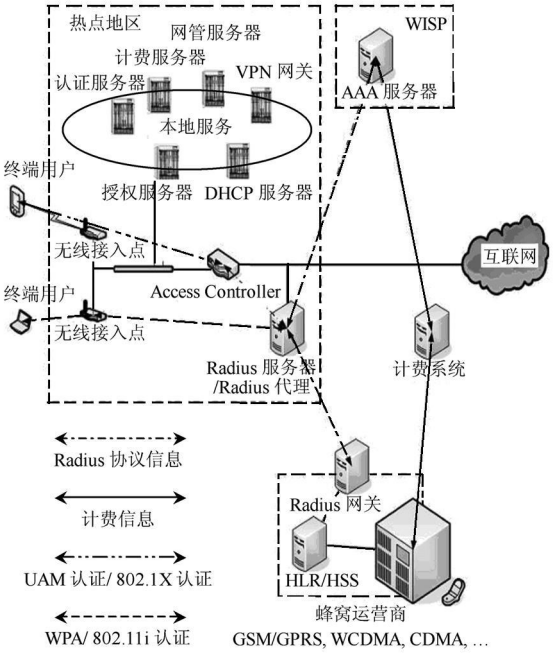

图 1 公共无线局域网安全体系结构

Fig. 1 The security architecture of PWLAN

在实际情况中可能由多个部件构成。

4) Web认证服务器。主要负责 Web认证、用户信息查询以及整个系统的管理功能模块, Web服务器通过 SSL确保信息安全。

5) AAA服务器/AAA代理。主要向用户提供 AAA功能, 或者向那些漫游用户提供 AAA代理功能。处理或转发用户的认证和计费信息。如果认证使用的是 802.1X协议, AAA服务器通过 EAP和移动终端进行认证, 并生成 WPA会话密钥分发给 AP和移动终端。对于蜂窝运营商而言, AAA服务器隐藏了蜂窝网的结构。它既是蜂窝网中归属位置寄存器(HLR)身份认证的网关, 也是蜂窝网 AAA系统的网关。认证模块采用 7号信令(SS7)向 HLR传送标准的 GSM/GPRS认证信令。蜂窝网用存储在 SIM卡中的 GSM/GPRS国际移动用户识别码(IMSI)来认证用户。

4 公共无线局域网混合认证协议设计

4.1 协议流程设计

为了确保公共无线局域网认证的安全性, 提出一种基于 802.1X和 Web的混合型认证协议, 该协议在进行 Web认证时将利用 802.1X协商后产生的密钥进行, 可在不改变现有公共无线局域网 Web认证方式下实现, 并且可以弥补 Web认证方式存在的漏洞。

802.11i/WPA采用基于端口控制技术的 802.1X[4]认证标准实现 802.11无线局域网的认证和接入控制, 802.1X为申请者、认证者和认证服务器的三方接入控制模式, 其本身并没有定义具体的认证协议, 它利用上层的认证协议进行身份认证, 认证者和认证服务器之间采用 RADIUS协议。

协议流程如图 2所示, 第一步首先建立 802.11连结; 第二步利用 802.1X认证交换用户认证信息, 这里使用 EAP—TLS认证方式, 客户端和认证服务器通过证书来证明自己的身份, 用于加密的密钥在密钥交换过程中生成; 第三步认证通过后终端用户和无线接入点通过四步握手交换生成 802.11会话密钥 KEY, 同时无线接入点用 RADIUS协议将该会话密钥 KEY传输给 RADIUS服务器, RADIUS服务器将用户的 MAC地址和会话密钥的摘要 HASH(KEY)发送给 Web服务器。之后所有链路层的通信都采用会话密钥加密保护; 第四步终端用户和 Web服务器之间完成 Web认证, 用户通过网页向 Web服务器发送 Web认证信息{ID, credential, MAC, HASH(KEY)}, Web服务器将校验 MAC, HASH(KEY)进行校验以确定用户身份, 若认证通过则通知接入控制器允许用户访问公共网络, 同时给用户返回一个 Web认证响应。

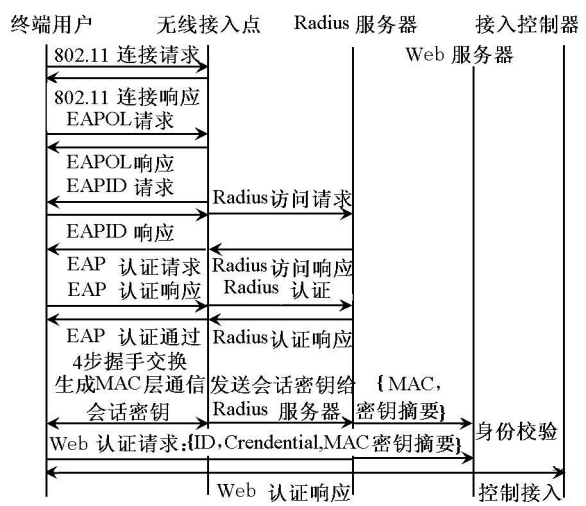

图 2 公共无线局域网混合型认证流程

Fig. 2 The mixed authentication procedure of PWLAN

4.2 安全分析

1) 窃取服务。在该认证协议中, 攻击者无法通过地址欺骗方法来获得 WLAN服务。在整个

802.1X客户认证过程中每个用户都必须使用自己的密钥对认证信息进行加密,接入点将丢弃非法数据报。

2) 基站伪装。首先,用户终端通过 EAP—TLS 协议和接入点间实现双向认证。Web服务器间通过检测{MAC, HASH(KEY)}防止该攻击行为。攻击者无法更改 Web认证请求消息中的 MAC地址或者 HASH(KEY),因为该消息是经过 SSL加密的。

3) 消息窃听。除了最开始的802.11网络连接,认证过程的第二步至第三步由 802.1X确保认证信息的隐秘性和完整性;当会话密钥建立后,第四步的 Web认证的 MAC层数据由上述步骤生成的会话密钥加密保护,所以攻击者获取该会话密钥和攻击802.1X认证协议一样困难。

4) 拒绝服务。在 802.11无线局域网中有好几种 DoS攻击方法,例如,向合法用户发送拒绝认证/取消连接帧;欺骗用户进入功率节省模式等,这些攻击方法利用了 802.11协议的自身漏洞,该认证协议无法抵御。可通过入侵检测系统来检测 DoS攻击,并及时通知网络管理服务器。

5 结语

通过安全分析表明,该体系结构可以很好地应用于各种类型的公共无线局域网。笔者提出的基于802.1X和 Web认证的混合型认证协议可有效地抵抗窃取服务、基站伪装、消息窃听等攻击,并可在现有的公共无线局域网 Web认证体系上实现,适合公共无线局域网环境的应用。

参考文献

[1] IEEE 802.11, Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[S]. Technical Report IEEE, 1999

[2] Juha A—L, Jouni M, Jyri R. Wireless lan access network architecture for mobile operators[J]. IEEE Communications Magazine, 2001, 39(11): 82—89

[3] 3rd generation partnership project; technical specification group services and system aspects; feasibility study on 3gpp system to wireless local area network (WLAN) interworking (release 6)[S]. Technical Report TR 22.934 V6.2.0, 3GPP, September 2003

[4] IEEE802.1x: IEEE Standard for Local and Metropolitan Area Networks— Port—Based Network Access Control[S]. IEEE, 2001

The design on the security architecture of public WLAN based on access controller mode

Song Yubo, Hu Aiqun, Yang Xiaohui

(Research Center of Information Security, Southeast University, Nanjing 210096, China)

[Abstract] The security problem, such as network security, user data protection, authentication, mobile management and network services are becoming more and more important in Public WLAN. This paper focuses on the design research of the PWLAN security architecture. A security model based on access controller is proposed in this paper. Furthermore, a compound 802.1X and Web authentication scheme is provided to ensures cryptographically protected access while preserving pre—existing public WLAN payment models.

[Key words] public WLAN; security architecture; authentication; access controller