基于 IEEE 802.1x 协议的无线局域网安全性的改进思路*)

熊 江
(重庆三峡学院 计算机科学系 重庆万州 404000)

摘 要 无线网络系统的迅速发展和广泛应用令市场对该系统的安全要求不断提高,本文通过分析现有无线局域网安全性解决方案的基础上,提出并实现了"基于 IEEE 802.1x 协议的无线局域网的安全体系"的解决方案,极大地增强无线局域网内通信数据的安全性。

关键词 无线局域网,MAC, WEP,IEEE 802.1x

IEEE 802.1x Protocol Based Wireless LAN Secure Improvement Mentality

XIONG Jiang
(Department of Computer Science, Chongqing Three Gorges College, Wanzhou 404000)

Abstract Rapid development and the widespread application of wireless network systemare have unceasingly enhanced the market to this system safe request, this text, on the basis of analyzing present wireless local-area network security solution, proposes and realizes of solution," wireless local-area network security system based on IEEE 802.1x protocol", which has strengthened the security of the communication data in the wireless LAN greatly.

Keywords Wireless local-area network, Media access control, Wired equivalent privacy, Port based network access control protocol

1 IEEE 802.1x 协议介绍

IEEE 802.1x 又名为基于端口的访问控制协议(Port based network access control protocol),它源于 IEEE 802.11 无线以太网(EAPOW),它可提供对无线网络的用户验证及访问权限的控制,协议仅仅关注端口的打开与关闭,对于合法用户接入时,该端口打开,而对于非法用户接入或没有用户接入时,则该端口处于关闭状态。该协议对网络性能的极大改进以及对认证计费问题的圆满解决,IEEE 802.1x 引起了国内网络用户的充分重视,目前微软也在大力推广,并在 Windows XP 已经整合 IEEE 802.1x 客户端软件,无需要另外安装客户端软件。IEEE 802.1x 协议的体系结构包括三个重要的部分:Supplicant System 客户端、Authenticator System 认证系统、Authentication Server System 认证服务器。

1.1 IEEE 802.1x 协议技术特点

协议实现简单 IEEE 802.1x 协议为二层协议,不需要到达三层,对设备的整体性能要求不高,可以有效降低建网成本。

认证和业务分离 IEEE 802.1x 的认证体系结构中采用了"可控端口"和"不可控端口"的逻辑功能,从而可以实现业务与认证的分离。用户通过认证后,业务流和认证流实现分离,对后续的数据包处理没有特殊要求,业务可以很灵活,尤其在开展宽带组播等方面的业务有很大的优势,所有业务都不受认证方式限制。

和其他认证方式的比较 IEEE 802.1x 协议虽然源于 IEEE 802.11 无线以太网(EAPOW),但是,它在以太网中的引入,解决了传统的 PPPoE 和 Web/Portal 认证方式带来的问题,消除了网络瓶颈,简轻了网络封装开销,降低了建网成本。

1.2 IEEE 802.1x 优点

简洁高效 纯以太网技术内核,保持 IP 网络无连接特性,去除冗余昂贵的多业务网关设备,消除网络认证计费瓶颈和单点故障,易于支持多业务。

容易实现 可在普通 L3、L2、IP DSLAM 上实现,网络综合造价成本低。

安全可靠 在二层网络上实现用户认证,结合 MAC、端口、账户和密码等;绑定技术具有很高的安全性。

行业标准 IEEE 标准,微软操作系统内置支持。

易于运营 控制流和业务流完全分离,易于实现多业务运营,少量改造传统包月制等单一收费制网络即可升级成运营级网络。

2 IEEE 802.1x 存在的问题

IEEE 802.1x 协议并不十分安全,仅仅提供了一种用户接入认证的手段,并简单地通过控制接入端口的开/关状态来实现。但是 IEEE 802.1x 并不提供真正的认证机制,当利用 IEEE 802.1x 时,需要选择一种 EAP 的类型来定义认证,如传输层安全协议(EAP-TLS)或隧道传输层安全协议(EAP-TTLS),而支持特定 EAP 类型的软件是认证服务器和用户的操作系统或应用软件,接入点 AP 只是 IEEE 802.1x 数据报的传输通道而已。研究发现 802.1x 易受会话"掠持"。会话"掠持"是当攻击者接管已存在的会话时,则意味着攻击者可依赖存在的认证连接来获得对网络资源的访问。

图 1 显示攻击者等待一合法用户 Susan 认证通过后,再

*)重庆市教委科研项目(编号:kj061107)和重庆三峡学院校级科研项目(2005-Sxxyyb-002)资助。熊 江 副教授,硕士,研究方向为计算机网络及硬件。

通过各种形式的拒绝服务攻击来取消或阻止 Susan 的连接随后假扮为 Susan 攻击者为了维持连接需要骗取认证用户的 IP 地址。

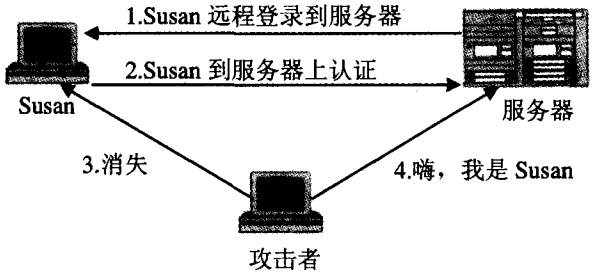

图 1　会话"掠持"

3　已有的无线局域网安全性解决方案

3.1　Cisco 的无线局域网安全解决方案

Cisco LEAP 是基于 802.1x 的解决方案，它使用了一个专用算法以支持移动台（用户）和认证（AAA）服务器的相互认证，为此，AAA 服务器必须支持 LEAP 算法。其核心为：

• 可扩展身份验证协议（EAP），是使无线客户机适配器与 RADIUS 服务器进行通信的远程访问拨号用户服务（RADIUS）的扩展。

• IEEE 802.11X，用于控制端口通信的推荐标准。

3.2　Agere 的无线局域网安全解决方案

Agere 的解决方案提供了在移动台（用户）和无线接入点 AP 使用非标准对话来完成标准的 PPP 认证方法。

3.3　Symbol Technologies 的无线局域网安全解决方案

Symbol Technologies 支持基于 Kerberos 的认证服务器。

3.4　WindowsXP 部署的安全无线网

Microsoft 在 WindowsXP 中支持 IEEE 802.1X 用于需要验证的网络访问的标准协议，在以太网和 802.11 网中支持用户和机器的验证使用 Radius 验证，Windows 2000 Internet Authentication Server 可以和 Active Directory 用户数据集成，网络访问的级别由管理员控制分为禁止访问（即使获得了 IP 地址）、完全访问和 Guest 访问，并支持向客户分发加密密钥。

4　提出基于 IEEE 802.1x 协议的无线局域网安全性的改进思路

网络的安全性可以从三个要素分析：访问控制、身份验证、数据保密性。如果这三个要素都没有问题了，就不仅能保护传输中的信息免受危害，还能保护网络和移动设备免受危害。无线局域网的安全需要考虑三个基本的服务：审计、认证和机密性，以上的企业和组织有的只考虑了这三者之一，有的虽然考虑了这三个方面，但没有提供一个统一的、方便的、集成的安全监管工具，所以，在 IEEE 标准 802.1x 中所暴露的瑕疵，都曾经遭受猛烈攻击，表示以上无线网络安全措施无法获得高级别的安全，还需要进一步加强。

项目组提出一种针对基于 IEEE 802.1x 协议的无线局域网的安全体系（图 2）。

本无线局域网的安全体系是基于多层安全技术的可扩展无线安全管理平台（Extensible Security Management Platform），在系统中，我们把安全体系分为三个等级，每一级都提供了不同的安全层次和用户访问权限。最低的安全等级称为"无安全级"，在这一层次上仅提供了网络的 ESSID 参数认证；第二级的安全策略需要验证移动台的 ESSID 参数、对移动台的 MAC 地址进行过滤、对传输的数据采用静态 WEP 进行加密；第三级的安全策略也就是最高级的安全，它除了采用第二级的全部安全策略外，还利用 RADIUS 服务器对每一用户进行认证。

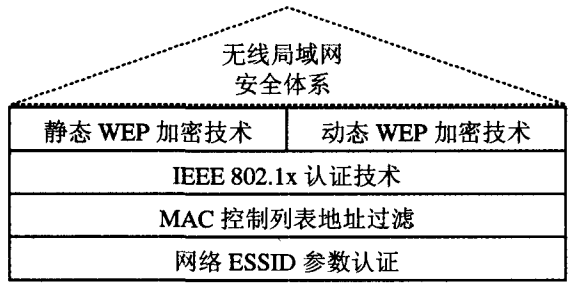

图 2　基于 IEEE 802.1x 协议的无线局域网的安全体系

"基于 IEEE 802.1x 协议的无线局域网的安全体系"不是采用现有的某一安全技术开发的，而是容纳了各种安全手段对无线传输的信息进行保护，并对现有的及今后出现的安全措施实行"即插即用"，并在基于 IEEE 802.1x 协议的无线局域网的安全体系的基础上提出了"全面的无线局域网的信息安全保护"解决方案：在实现中采用 RADIUS 认证机制对无线以太网用户进行认证、采用 ESSID 认证机制和 MAC 地址访问限制列表对访问者进行过滤、采用 WEP 会话安全密钥对传送的数据进行保护，以此来充分保护用户数据的私密性。所以无线安全管理平台和全面的信息安全保护能适应今后无线技术的发展。更重要的是该系统实现全面地信息安全保护，对无线网卡、用户和 AP 设备进行全面地认证、监管和保护，可以随着无线安全技术的不断发展而提升自身的安全性能，达到全面保护无线局域网安全的目的。

总结　在无线局域网络市场迅猛发展的今天，用户迫切要求为无线局域网络的使用提供全面的网络安全保证，提出的基于 IEEE 802.1x 协议的无线局域网的安全体系经过实践证明能极大地增强无线局域网内通信数据安全，并且管理方便，控制容易，扩展性好，维护方便。

参 考 文 献

1　IEEE SA Standards Board. IEEE Std 802. Ix. Port-Basel network access control [S]. 2001

2　(美)Jim Geier. 无线局域网. 北京：人民邮电出版社. 2001,04

3　Monly M. Pautet M-B. The GSM system for mobile communications. ISBN7-5053-3634-7/TP. 1499，电子工业出版社，1996. 259～271

4　Macaulay T . Hardening IEEE 802.11 wireless networks. 2002

5　http://www. chinawlan. net/articleDetail. asp? CatID = 12&NewsID=5513《无线局域网安全挑战自由》，2002. 2. 17

6　Macaulay T. Hardening IEEE 802.11 wireless networks. http://www. ewa-canada. com. 2002,2

7　Fluhrer S, Mantin I, Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4. http://www. drizzle. com/～ aboba/IEEE/rc4_ksaproc. pdf. 2001,7

8　熊江. 无线局域网络安全性的研究. 计算机科学，2003,7

9　吴晓伟. 增强网络安全的 802.1X. 计算机世界报，2002,23