

基于 IEEE 802.11bWLAN 安全技术研究

梁宝龙, 李文阁, 陈 阳

(广西大学 计算机与电子信息学院, 广西 南宁 530004)

摘 要:随着无线局域网(WLAN)技术的迅速发展,其安全问题日益受到人们的关注。由于传输的特殊性,WLAN 始终面临严峻的安全考验。无线网络攻击技术的不断翻新,基于 IEEE 802.11b 的攻击技术会越来越多,复杂性将越来越高。所以与有线网络相比,保护 WLAN 安全的难度要远大于保护有线网络。文中介绍了基于 IEEE 802.11b 协议下的 WLAN 可能面临的非法登录、拒绝服务、字典攻击等安全威胁,分析了如何提高 WLAN 下的几种安全机制及 802.11 协议下的 802.11i 安全标准。提出了现有无线设备使用中一些可提高 WLAN 安全性的解决措施,在一定程度上提高了 WLAN 的安全性。

关键词:无线局域网;IEEE 802.11b;攻击技术;安全标准;802.11i

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2010)12-0170-03

Security Technology Based on IEEE 802.11bWLAN

LIANG Bao-long, LI Wen-ge, CHEN Yang

(College of Computer and Electronic Information, Guangxi University, Nanning 530004, China)

Abstract: As wireless LAN (WLAN) technology is developing rapidly, their safety has attracted increasing attention. As the transmission of particularity, WLAN security has always been facing a severe test. As the wireless network attack techniques are constantly devised, based on IEEE 802.11b technology will attack more and more complexity will more and more. Therefore, compared with the wired network, WLAN security protection is far greater than the difficulty of protecting cable network. Described in detail under the agreement based on the IEEE 802.11b WLAN may face illegal log, refused to accept service, dictionary attacks and other security threats, and a detailed analysis of how to improve WLAN security mechanisms and several under the 802.11 protocol under the 802.11i security standard. Put forward some of the existing wireless devices can improve WLAN security solutions, to some extent, these measures effectively improved WLAN security.

Key words: WLAN; IEEE 802.11b; attack techniques; security standards; 802.11i

0 引 言

WLAN 是 Wireless LAN 的简称,即无线局域网。所谓无线网络,顾名思义就是利用无线电波作为传输媒介而构成的信息网络。由于 WLAN 产品不需要像有线网络那样需要铺设通信电缆,无线设备部署较之有线灵活。WLAN 技术为用户提供更好的移动性、灵活性和扩展性,在难以重新布线的区域提供快速而经济有效的局域网接入,无线网桥可用于为远程站点和用户提供局域网接入。但是,当用户对 WLAN 的期望日益升高时,其安全问题随着应用的深入表露无遗,并成为制约 WLAN 发展的主要瓶颈。

1 WLAN 的安全面临严峻的威胁

随着无线技术的广泛应用,无线网络的安全问题越发备受人们的关注。由于传输的特殊性,WLAN 始终面临严峻的安全考验。随着攻击技术的不断翻新,基于 802.11b 的攻击技术会越来越多、复杂性将越来越高,但目前基于无线网络技术 802.11b 协议的威胁主要有以下几类:非法登录,非法侦听和非授权的监督,人为干扰,端到端攻击,对接入点的密码暴力攻击,加密攻击、错误配置等使 WLAN 的安全受到极大威胁。因此需要采取一系列安全措施,以防止信息被恶意攻击者轻易地截获,防止对业务的欺骗接入等等^[1,2]。

2 WLAN 几种主要攻击技术

WLAN 使用无线电波作为媒体,所以在任何无线信号覆盖的地方,无线收发器都可以收发数据包。由于 WLAN 技术通过射频无线电传输的特性和 IEEE

收稿日期:2010-05-10;修回日期:2010-08-11

基金项目:国家自然科学基金(60963022);广西自然科学基金(0991059)

作者简介:梁宝龙(1986-),男,海南临高人,硕士研究生,研究方向为高性能计算与网络系统。

802.11b 标准中存在安全机制的缺陷,严重影响了 WLAN 系统的安全性能。所以基于 IEEE 802.11b 标准中安全机制的缺陷导致的 WLAN 可能遭受的攻击主要有下述几类:非法接入点和未授权用户攻击,中间人攻击,拒绝服务攻击,对 IP 地址发起的主动攻击,字典攻击等。

2.1 非法接入点和未授权用户攻击

这类攻击主要是针对正在部署没有通过安全认证或者是新建立的网络未及时进行安全更新的网络进行攻击。攻击者试图通过连接一个无线客户端,尤其是一台笔记本电脑或 PDA,一旦连接上无线客户端攻击者未经授权就进入了 AP(Access Point)。AP 可以配置成为要求客户端通过密码来进行访问。如果没有密码,入侵者可以连接到内部网络只需通过启用一个无线客户端与 AP 通信。但是,有些 AP 所有客户端访问使用相同的初始密码,所有客户端用户第一次成功访问后都提示修改密码。

2.2 中间人攻击

由于 802.11 是单向认证,攻击者插入一个会话的中间,同时伪装成会话的双方,分别对会话的双方伪装成对方。这样,攻击者既可以读到会话中的私有数据,也可根据需要篡改数据,从而达到攻击目的。攻击者可伪装成 AP 接受移动工作站的请求,如果该会话没有加密,则攻击成功;否则攻击者可以使用 IV(Initialization Vector)字典来窃听会话内容。

2.3 拒绝服务攻击

拒绝服务攻击 DoS^[3](Denial of Service)很容易被应用到无线网络中。攻击者可以发送与无线局域网频率相同的干扰信号来干扰网络的正常运行,从而导致正常的用户无法使用网络。拒绝服务是指当攻击者占用了主机或网络几乎所有的资源的时候,使合法的用户无法获得这些资源。拒绝服务攻击另一种的攻击手段就是发送大量的非法的身份请求。如果 AP 受困于成千上万的伪装认证的请求的话,那么任何用户在提交身份验证请求时,要想获得一个合法的会话过程是非常困难的。

2.4 对 IP 地址发起的主动攻击

针对 IP 地址发起的攻击目的是破解数据报的头字节,从中得到 IP 地址。获得数据包 IP 地址后,攻击者将 IP 地址修改指向被控制的客户端的主机,然后通过受控客户端接收来自互连网络经 AP 和路由器发过来的明文。

2.5 字典攻击

在字典攻击中,攻击者使用一个很大的字典,或者数据库,它包含所有可能的密码。由于 IV 字节的空

间太小,所以成功建立字典相对简单。只要攻击者获得了由此次所使用的 RC4 密钥流,就能对所有使用此初始向量(Initialization Vectors, IV)的数据包进行解密。由于 IV 只有 24bit,可以破解 IV,从而破解 WEP 加密。攻击者可以构建密钥流对 IV 的“字典”。因为密钥空间是 2 的 24 次方,即整个字典将占用 1500 个字节(平均 IEEE802.11 密钥流长度)乘以 2 的 24 次方,或者大约 24GB^[4]。那么如果有足够大的硬盘空间,攻击者只需要花点时间和精力来对照该“字典”就可以破解了。

3 WLAN 的几种安全机制

3.1 服务区标识符(SSID)过滤

服务区标识符 SSID^[5]是一个可选项,许多实际的无线设备产品中默认允许任何 SSID 都可以登录 AP。IEEE802.11b 标准允许 SSID 有 AP 通过信标帧定期以明文形式广播,SSID 是一个基本服务集(BSS)中所有工作站(STA)共享的秘密,STA 越多,秘密被泄露的可能性越大。SSID 过滤使用户所使用的无线客户端服务集标识必须与被访问的无线接入点 AP 相匹配,否则就无法通过此无线接入点 AP 进行数据通信。因此可以认为 SSID 是一个简单的口令,从而提供认证机制,实现一定的安全^[6]。

3.2 物理地址(MAC)过滤

MAC 地址过滤可以将无线局域网只设定为给定的无线用户使用。每一个无线工作站网卡都由唯一的物理地址(MAC)标识,MAC 由厂家出厂前设定,无法更改。网络管理员可以在无线局域网接入点 AP 中手工设置一组允许或拒绝访问的 MAC 地址列表,通过这个列表决定访问用户是否可以数据进行通信,从而实现 MAC 地址访问的过滤^[7]。

3.3 共享密钥验证

共享密钥验证是一种要求双方必须有一个公共密钥,密钥验证过程中只能使用 WEP(Wired Equivalent Privacy)机制的工作站之间进行,避免明文传输。使用共享密钥验证的鉴别过程^[8]包含 4 个步骤:

- (1)无线客户端向无线接入点 AP 发送验证请求;
- (2)无线接入点 AP 发布一个随机产生的无格式文本,从无线接入点清晰地发送到无线客户端;
- (3)无线客户端响应这个请求,并使用自身的密钥加密这个请求,然后将其发回无线接入点;
- (4)无线接入点解释明白无线客户端的加密响应,识别通过一个匹配的 WEP 密钥。如果无线客户端的 WEP 密钥是正确的,无线接入点进行响应,并标记无线客户端为关联。否则,无线接入点将否定当前响应,

并且标记无线客户端未鉴别或为关联。

3.4 WEP 加密

为了提供与有线网络相近的安全性, IEEE 802.11 标准提供了 WEP 算法来进行数据保密, WEP^[9,10] 算法是基于 RC4 密码算法。RC4 是一种流式加密算法, 用 RC4 加密的数据流失一位后, 该位后的所有数据都会丢失, 这是因为 RC4 的加密和解密失去了同步。在 WEP 中明文通过和密钥流进行异或产生密文^[11]。WEP 加密主要作用是在信息的提供上使得无线与有线网络具有同等级的机密性。

WEP 加密过程如图 1 所示。

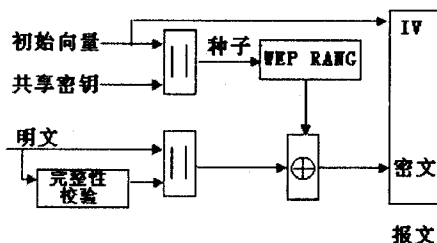


图 1 WEP 加密过程

图 2 为 WEP 帧的结构。

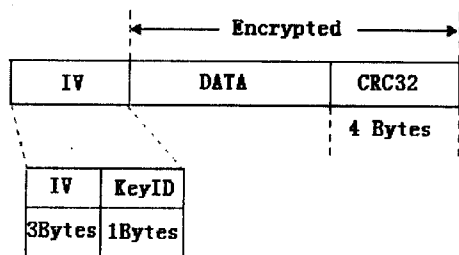


图 2 WEP 的帧结构

3.5 802.11i 安全标准

IEEE 802.11i 安全标准完成于 2004 年 7 月, 是为了弥补 802.11WEP 脆弱的安全加密功能而制定的修正案。IEEE 802.11i 标准定义了基于 AES 的全新加密协议 CCMP (Counter - Mode/ CBC - MAC Protocol), 使用向前兼容 RC4 的暂时性密钥完整协议 TKIP (Temporal Key Integrity Protocol) 和 WRAP (Wireless Robust Authenticated Protocol) 三种加密机制, 增加了攻击者破解难度。为了提供更高级别的加密保护, 802.11i 安全标准采用了新的 WLAN 架构, 支持新的 AES (Advanced Encryption Standard) 标准。

802.11i 协议结构如图 3 所示。

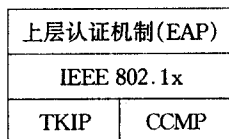


图 3 802.11i 标准结构图

1) TKIP 是包裹在 WEP 外面的一套算法, 它添加

以下 4 算法: 消息完整性校验码; IV 序列; 数据包加密; TKIP 的加密和解密。

2) CCMP 是基于 AES 的 CCM (Counter with CBC - MAC Mode) 模式。该模式采用了 Counter 模式用于数据保密和 CBC - MAC 模式用于认证。

3) IEEE 802.1x 和可扩展认证协议 (Extensible Authentication Protocol, EAP), IEEE 802.1x^[12] 协议是一种基于端口的网络访问控制方案。它不仅提供访问控制功能, 还能提供用户认证和计费能力。

它的核心是扩展认证协议 (EAP), 包含三个主体: 申请者, 认证者和认证服务器。其认证过程如图 4 所示, 认证步骤如下:

- (1) 用户向 AP 发送一个认证请求帧;
- (2) AP 发送一个回应帧, 要求用户提供身份信息;
- (3) 用户向 AP 提交自己的身份信息;
- (4) AP 将用户身份信息转交给认证服务器;
- (5) 认证服务器通过查询用户身份信息验证用户身份的合法性, 合法则通过认证, 否则认证失败。

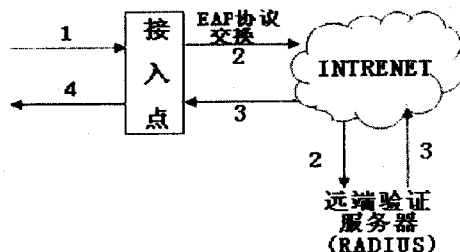


图 4 IEEE 802.11X 认证过程

4 结束语

WLAN 是一项新兴的技术, 由于传输的特殊性, WLAN 始终面临严峻的安全考验, 需要从加密技术和密钥管理技术两方面来提供保障, 业界为此制定了众多的无线局域网安全技术和标准, 但任何一种技术和标准都有其局限性。所以为了对付不断出现的新的安全威胁, 需要不断研究相关的关键技术来搭建增强的、有足够安全的 WLAN 网络, 并且将 WLAN 安全管理和这些技术有机地结合起来, 才能构建一个相对安全的无线网络。

文中回顾了基于 802.11b 协议下的 WLAN 安全威胁, 详细分析了 WLAN 安全机制, 理清了安全技术发展的脉络, 在一定程度上提高了 WLAN 的安全性。同时, 随着 802.1x 和 802.11i 的标准发布, 逐步减少了设备间的非兼容性、统一技术市场。我们认为, 随着新的安全技术的出现和应用领域的无限增长, 各种 WLAN 的安全技术和安全标准最终会以某种方式走

(下转第 204 页)

梯度和图像强度分布的分割方法,通过实验显示可以有效地对脑部肿瘤进行分割。文中的算法还可以扩展到多个时间点图像的分割,根据前一个时间点病人的图像和分割结果,来指导下一个时间点图像的分割,这样可能会得到更好的分割结果。这将是下一步研究的方向。

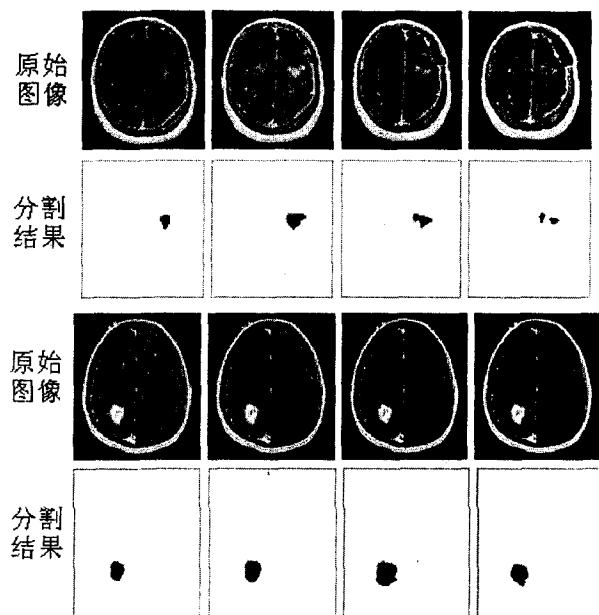


图 3 分割结果显示(白色区域为肿瘤区域)

参考文献:

- [1] Clark M C, Hall L O, Goldgof D B. MRI segmentation using fuzzy clustering techniques: integrating knowledge[J]. IEEE Engineer in Medicine and Biology, 1994, 13(5): 730 - 742.
- [2] Kaus M R, Warfield S K, Nabavi A, et al. Automatic segmentation of MR image of brain tumors[J]. Radiology, 2001, 218: 586 - 591.
- [3] Osher S, Sethian J A. Fronts propagating with curvature - dependent speed: algorithms based on Hamilton - Jacobi formulation[J]. Journal of Computational Physics, 1988, 79: 12 - 49.
- [4] 王志豪, 汪继文. 一种新的基于 Snake 模型的水平集图像分割方法[J]. 计算机技术与发展, 2008, 18(12): 130 - 133.
- [5] 钱芸, 张英杰. 水平集的图像分割方法综述[J]. 中国图像图形学报, 2008, 13(1): 7 - 13.
- [6] Ho S, Bullitt E, Gerig G. Level set evolution with region competition: automatic 3D segmentation of brain tumors[C]//International Conference on Pattern Recognition. [s. l.]: [s. n.], 2002: 532 - 535.
- [7] Prastawa M, Bullitt E, Ho S, et al. A brain segmentation framework based on outlier detection[J]. Medical Image Analysis, 2004(8): 275 - 283.
- [8] Xie K, Yang J, Zhang Z G, et al. Semi - automated brain tumor and edema segmentation using MRI[J]. European Journal of Radiology, 2005, 56: 12 - 19.
- [9] 张宁, 秦安, 陈武凡. 一种新的心脏磁共振图像分割方法[J]. 计算机工程与应用, 2008, 44(31): 224 - 227.
- [10] Li C, Xu C, Gui C, et al. Level set evolution without re - initialization: a new variation formulation[C]//IEEE Conference on CVPR. [s. l.]: [s. n.], 2005: 430 - 436.
- [11] Chan T, Vese L. Active contours without edge[J]. IEEE Transactions on Image Processing, 2001, 10(2): 266 - 277.
- [12] Cremers D, Osher S, Soatto S. Kernel density estimate and intrinsic alignment for shape prior in level set segmentation[J]. International Journal of Computer Vision, 2006, 69(3): 335 - 351.
- [1] Clark M C, Hall L O, Goldgof D B. MRI segmentation using fuzzy clustering techniques: integrating knowledge[J]. IEEE Engineer in Medicine and Biology, 1994, 13(5): 730 - 742.
- [2] 段水福, 历晓华, 段炼. 无线局域网(WLAN)设计与实现[M]. 杭州: 浙江大学出版社, 2007: 159 - 169.
- [3] 林秉忠, 陈彦铭. 无线网络安全白皮书[M]. 台湾电脑网络危机处理暨协调中心, 2004: 64 - 116.
- [4] Arbaugh W A, Shankar N, Justin Wan Y C. Your 802.11 Wireless Network has No Clothes[J]. IEEE Wireless Communications, 2002(12): 44 - 51.
- [5] Ow Eng Tiong. IEEE 802.11b Wireless LAN: Security Risks[M]. [s. l.]: SANS Institute, 2001.
- [6] Beniwal V, Sonal, Kharb S. A Study of IEEE 802.11b Wireless LAN Security Issues[EB/OL]. 2007. URL: http://www.rimtengg.com/coit2007/proceedings/pdfs/103.pdf.
- [7] 李庆超, 邵志清. 无线网络的安全架构与入侵检测的研究[J]. 计算机工程, 2005(2): 143 - 151.
- [8] Wong S. The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards[M]. [s. l.]: SANS Institute, 2001.
- [9] 王鹏卓, 张尧弼. 802.11WLAN 的安全缺陷及其对策[J]. 计算机工程, 2004(5): 133 - 136.
- [10] Gast M. Seven Security Problems of 802.11 Wireless[EB/OL]. 2002. URL: http://www.oreillynet.com/lpt/a/2404.
- [11] Uskela S. Security in Wireless Local Area Networks[EB/OL]. 2007. URL: http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/wireless_lan.html.
- [12] 赵礼红, 吴昊, 黄清. 无线局域网[M]. 北京: 科学出版社, 2004: 201 - 206.
- [13] Wireless LAN Security 802.11b and Corporate Networks. Internet Security Systems[EB/OL]. 2001 - 09 - 16. URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

(上接第 172 页)

向统一。

参考文献: