现代计算机技术与应用
2022 年 8 月第 4 卷第 3 期

浅析无线网络安全

郑　华

辽宁农业职业技术学院，营口

摘　要 | 随着网络的日益普及，强大的市场推动力导致无线网络技术的发展越来越快，随之而来的安全问题也越来越突出，这给无线网络的研究又提出了新的课题。从分析无线网络的结构着手，讨论无线网络存在的非授权访问、信息易篡改等安全隐患以及解决这些隐患的主要技术，具有重要的意义。

关键词 | 无线网络；信息安全

近年来网络技术取得了巨大的进步。传统的有线局域网由于受到布线的限制，给移动办公用户带来了很大的不便。因此，高效快捷、组网灵活的无线局域网应运而生。无线网络的应用扩展了用户的自由度，使网络结构更方便、更灵活、更经济，但其数据安全却存在重大问题。

1　无线网络的结构

无线局域网由无线网卡、无线接入点（AP）、计算机和有关设备组成，它采用单元结构，将整个系统分成多个单元，每个单元称为一个基本服务组（BSS）。

作者简介：郑华，辽宁农业职业技术学院助教。
文章引用：郑华．浅析无线网络安全［J］．现代计算机技术应用，2022，4（3）：103-107.
https://doi.org/10.35534/mcta.0403015c

BSS 的组成有三种方式：无中心的分布对等方式、有中心的集中控制方式以及这两种方式的混合方式。在分布对等方式下，无线网络中的任意两站之间可直接通信，无须设置中心转接站，这时，MAC 控制功能由各站分布管理。在集中控制方式下，无线网络中设置一个中心控制站，主要完成 MAC 控制以及信道的分配等，网内其他各站在该中心的协调下与其他各站通信。在分布式与集中式的混合方式下，网络中的任意两站均可直接通信，而中心控制站完成部分无线信道资源的控制。

2　无线网络的特点

无线网络更容易受到恶意攻击。被攻击端的电脑与攻击端的电脑并不需要网线设备上的连接，只要在无线路由器或中继器的有效范围内，就可以进入内部网络，访问资源。如果内部网络传输的数据并未加密的话，更有可能被窥探数据隐私。一般的家庭无线网络都是通过一个无线路由器或中继器来访问外部网络。通常这些路由器或中继器设备制造商都会提供一个管理页面工具。这个页面工具可以用来设置该设备的网络地址以及账号等信息。而很多用户都不会去修改设备默认的用户名和密码，这使得黑客有机可乘。只要通过简单的扫描工具就很容易找出这些设备的地址，并尝试用默认的用户名和密码去登录管理页面，如果成功则立即取得该路由器或交换机的控制权。无线链路使网络更易受到从被动窃听到主动干扰的各种攻击。而无线网络没有一个明确的防御边界，攻击者可能来自四面八方和任意节点。无线网络的这种开放性带来了非法信息截取、未授权信息服务等一系列信息安全问题。

无线网络的信息容易遭到篡改。信息篡改是指攻击者将窃听到的信息进行修改（如删除或替代部分或全部信息）之后再将信息传给原本的接受者，其目的有两种：恶意破坏合法用户的通信内容，阻止合法用户建立通信链接；将修改的消息传给接受者，企图欺骗接受者相信修改后的消息。信息篡改攻击对物理网络中的信令传输构成很大的威胁。

无线网络的安全管理难度更大。无线网络终端不仅可以在较大范围移动，而且还可以跨区域漫游，这意味着移动节点没有足够的物理防护，从而易被窃听、

破坏和劫持。攻击者可能在任何位置通过移动设备实施攻击，而在全球范围内跟踪一个特定的移动节点是很难做到的；另一方面，通过网络内部已经被入侵的节点实施攻击而造成的破坏更大，更难检测到。因此，对无线网络移动终端的管理要困难得多。

3 无线网络的安全措施

3.1 对传输数据进行限制

通过无线网络传输的数据信号可能被非法攻击者窃取到，为此，有必要对传输的数据信号进行加密限制，以阻止非法攻击者轻易窃取到其中的内容。

目前，无线局域网分为两大阵营：IEEE802.11 系列标准和欧洲的 HiperLAN。IEEE802.11b、IEEE802.11a 以及 IEEE802.11g 协议中都包含了一个可选安全组件，名为无线等效协议（WEP），它可对每位企图访问无线网络的人的身份进行识别，同时对网络传输内容进行加密。不过，在默认状态下不少无线节点设备都会禁止使用 WEP 加密技术，那样非法攻击者就能轻松扫描到各类无线网络信息，同时能将捕获到的无线数据内容轻松破解。所以，我们必须及时修改无线节点设备的数据加密参数，确保对无线上网信号进行安全加密。

3.2 设置 MAC 地址过滤

基本上每一个网络接点设备都有一个独一无二的标志，称之为物理地址或 MAC 地址。当然无线网络设备也不例外。所有路由器、中继器等路由设备都会跟踪所有经过他们的数据包源 MAC 地址。通常，许多这类设备都提供对 MAC 地址的操作，这样，我们可以通过建立自己的准通过 MAC 地址列表来防止非法设备（主机等）接入网络。

3.3 防止入侵者访问网络资源

这是用验证算法来实现的。在这种算法中，适配器需要证明自己知道当前的密钥。这和有线 LAN 的加密相似。在这种情况下，入侵者为了将他的工作站

https://doi.org/10.35534/mcta.0403015c

和有线 LAN 连接，必须满足这个前提。

3.4 利用认证

认证提供了关于用户的身份的保证，这意味着当用户声称具有一个特别的身份时，认证将提供某种方法来证实这一声明是正确的。用户在访问无线局域网之前，首先需要经过认证验证身份以决定其是否具有相关权限，再对用户进行授权，允许用户接入网络，访问权限内的资源。目前，无线局域网中采用的认证方式主要有 PPPoE 认证、WEB 认证和 802.1X 认证。PPPoE 认证是出现最早、最为成熟的一种接入认证机制。在无线局域网中采用 PPPoE 认证，只需对原有的后台系统增加相关的软件模块就可到达认证目的，大大节省了投资，因此使用较为广泛。WEB 认证相对于 PPPoE 认证，一个非常重要的特点就是客户端除了 IE 浏览器外，不需要安装认证客户端软件，给用户免去了安装、配置与管理客户端软件的烦恼，也给运营维护人员减少了很多相关的维护压力。同时，WEB 认证配合 Protal 服务器，还可在认证过程中向用户推送门户网站，有助于开展新的增值业务。

参考文献

[1] 仇芒仙. 无线网络的安全技术的探讨 [J]. 电脑开发与应用，2007（4）：43—47.

[2] 包延芳. 浅析网络防火墙技术 [J]. 今日科苑，2008（2）：202.

[3] 李安宁，马晨生. 入侵检测技术探析 [J]. 内蒙古科技与经济，2008（21）：40–42.

Analysis of Wireless Network Security

Zheng Hua

Liaoning Agricultural Vocational and Technical College, Yingkou

Abstract: With the increasing popularity of the network, the strong market force leads to the development of wireless network technology faster and faster, followed by more and more prominent security issues, which to the wireless network research and put forward a new topic. Starting from the analysis of wireless network structure, it is of great significance to discuss the security risks of wireless network such as unauthorized access and easy tampering of information, and the main techniques to solve these risks.

Key words: Wireless network; Information security

https://doi.org/10.35534/mcta.0403015c