IEEE802.11访问控制与MAC地址欺骗

冯柳平[1,2]　刘祥南[3]　刘明业[1]
（1 北京理工大学信息科学技术学院，北京 100081）
（2 桂林电子工业学院 通信与信息工程系，广西 桂林 541004）
（3 厦门大学计算机与信息工程学院，福建 厦门 361005）

摘　要： 对无线网络的访问控制机制进行了讨论，分析了目前所采用的 IEEE 802.11b 无线网络设备在访问控制方面的不完善性，以及 MAC 地址访问控制的漏洞。采用序列号分析法对 MAC 地址欺骗进行检测，从而对无线网络的非授权访问进行监控。

关键词： 无线网络，地址访问控制，MAC 地址欺骗，序列号
中图法分类号： TP393.08　　**文献标识码：** A　　**文章编号：** 1000-7180(2005)10-025-03

IEEE 802.11 Access Control and MAC Address Spoofing

FENG Liu-ping[1,2], LIU Xiang-nan[3], LIU Ming-ye[1]
(1 School of Information Science and Technology, Beijing Institute of Technology, Beijing 100081)
(2 Dept.of Communication and Information Engineering, Guilin University of Electronic Industry, Guilin 541004 China)
(3 School of Computer and Information Engineering, Xiamen University, Xiamen 365001 China)

Abstract: Access control mechanism on wireless network is discussed. Faultiness of wireless network equipment adopted presently and flaw of MAC address access control are analysed. MAC address spoofing is detected using sequence number analysis method and unauthenticated access on wireless network is monitored.
Key words: Wireless network, Address access control, MAC address spoofing, Sequence number

1　引言

网络的安全性主要集中在访问控制和数据加密两方面，访问控制保证敏感数据只能由授权用户进行访问。对于有线网络来说，访问控制以物理端口接入方式进行监控，它的数据通过物理电缆传输到特定的目的地，一般情况下，只有在物理链路遭到破坏的情况下，数据才有可能被泄漏。无线局域网的数据是利用无线信号在空气中进行传输的，它最大的问题在于无法通过对传输介质的接入控制来保证网络的安全，通过无线信号传输的数据很容易被未经授权的用户获取，因此无线网络面临一系列的安全问题。本文将对地址访问控制及漏洞进行讨论，并提出解决方案。

2　地址访问控制与漏洞检测

2.1　无线网络访问控制的不完善性

为了防止用户对无线网络的非授权访问，IEEE 802.11 定义了两种认证方式：开放系统认证和共享密钥认证。开放系统认证主要以 SSID 值作为最基本的认证方式。只要客户能给出正确的 SSID 值，访问接入点 AP(Access Point)就能接受客户的请求。而且 AP 会对空白的 SSID 做出回应，回应的内容则是该 AP 的 SSID 值。在这种认证方式下，任何人都可以取得 SSID 值并且与 AP 进行连接，因此如果攻击者想渗透进入，都可畅通无阻，可以说是完全没有安全防护的认证方式。共享密钥认证以 WEP(Wired Equivalent Privacy)算法为基础。当前的共享密钥认证协议很容易被攻击者所利用，他们通过被动攻击来窃听交互认证的过程，这主要是由于 WEP 算法的漏洞和 IEEE 802.11 认证协议的固定结构(不同的认证过程的区别仅在于随机的质询信息)。

2003 年底我国发布了无线局域网鉴别与保密基础结构(WAPI WLAN Authentication and Privacy Infrastructure)安全协议。从认证的角度看来，IEEE 802.11 是一种单向的认证，即服务器端对客户端的认证，而 WAPI 强调的是双向认证，身份凭证为公钥数字证书。WAPI 采用 ECC(椭圆曲线)算法，其参数由政府掌控，对于信息的安全提供了保障。但在

收稿日期：2005-03-14
基金项目：厦门市科技局项目(3502Z20021021)

2004 年 4 月下旬的中美商务会议上,双方达成协议中国无限期推迟 WAPI 标准的实施。

无线局域网新的安全标准 IEEE 802.11i 于 2004 年 6 月获得 IEEE 标准委员会通过。IEEE 802.11i 标准草案中主要包含加密技术:TKIP(Temporal Key Integrity Protocol)和 AES(Advanced Encryption Standard),以及认证协议 IEEE 802.1x。该标准通过 Wi-Fi 的基础上增加一个安全层,使得企业与家庭在无线接入中的安全性得到大大加强。

IEEE 802.11i 无线局域网安全标准向前迈进了一大步,但是无线局域网还无法抵御各种攻击。而且目前世界上采用的最主流的无线设备是基于 IEEE 802.11b 协议,因此加强无线网络的访问控制就显得尤为突出。另一种限制非授权访问的方法是基于 MAC 地址的访问控制,地址访问控制在 IEEE 802.11 标准中并没有定义,而是由厂商提供的。但是采用 MAC 地址欺骗,攻击者也很容易通过地址访问控制,进入到网络中。

2.2 地址访问控制

2.2.1 MAC 地址

MAC 子层在物理层和数据链路层的逻辑链路子层之间提供了一个统一的接口。为了简化网络通信的传递,为 MAC 层分配了一个唯一的 48 位地址,即 MAC 地址。MAC 地址前三个字节为 OUI(Organizationally Unique Identifier)标识符,由 IEEE 控制,并分配给网络设备生产厂商;其余三个字节由厂商分配,网络设备在出厂的时候就被赋予了一个唯一的 MAC 地址。MAC 地址是网络设备在全球的唯一编号,可用于直接标识某个网络设备,是网络数据交换的基础,这就确保了网络上不存在重复的 MAC 地址。

2.2.2 地址过滤

现在大多数的二层交换机都可以支持配置 MAC 地址过滤表,限定只有与 MAC 地址过滤表中规定的一些网络设备有关的数据包才能使用该端口进行传递。通过 MAC 地址过滤技术可以保证授权的 MAC 地址才能对网络资源进行访问。

在无线网络中,每个 AP 可以把网络的客户限制为在过滤表中出现的 MAC 地址。如果客户的 MAC 地址在列表中,就允许对网络进行访问;如果地址不在列表中,对网络的访问就被拒绝。当客户端试图连接到无线网络时,首先要通过 IEEE 802.11 的认证协议,向 AP 请求身份认证。当认证成功后,客户端可与 AP 进行连接。若设置了 MAC 地址过滤,则只允许指定的 MAC 地址进行连接(如图 1 所示)。

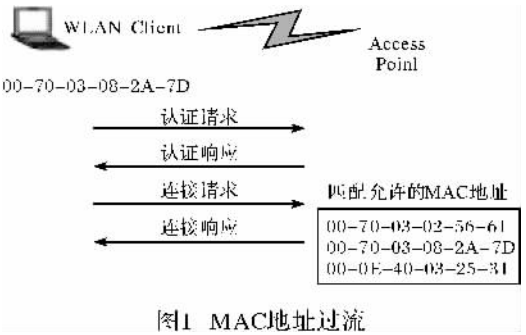

图1 MAC地址过滤

MAC 地址过滤表位于 AP 中,起到阻止非授权客户访问的作用。在客户试图与 AP 连接之前,MAC 地址过滤会识别出非授权的 MAC 地址,并阻止通信通过 AP 到达网络。

2.2.3 MAC 地址欺骗与身份假冒

由于每块无线网卡拥有唯一的 MAC 地址,地址访问控制相当于在无线网络的入口增加了一把锁,限制非授权客户对网络资源的使用,提高了无线网络的安全性。从理论上来说,地址访问控制提供了相当的安全性,然而事实并非如此,由于网络设计上的问题,我们无法防止 MAC 地址欺骗。

首先,MAC 地址很容易被攻击者嗅探到。即使采用了 WEP 加密手段,MAC 地址也是以明文的形式在空中传播,攻击者通过窃听的方式就可确定授权的 MAC 地址。另外,几乎所有的无线网卡都允许通过软件的方式修改 MAC 地址,攻击者想要成功伪造一个 MAC 地址并不需要许多复杂的工具。如果攻击者得到一个授权的 MAC 地址,他们就可以重新配置接口,把网卡的 MAC 地址进行修改,伪装成授权的客户,通过访问控制,对"被保护"的网络进行访问。

3 MAC 地址欺骗检测

3.1 帧序列号

攻击者通过盗用 MAC 地址假冒成授权客户,并利用这种独特的方式进入到无线网络。由于攻击者行为的隐蔽性,采用普通的监控手段很难检测到。但某些技术,如序列号分析法可对客户的这种非授权访问进行检测。

IEEE 802.11 MAC 层的设计比原先的 IEEE 802 的设计要复杂得多,这样设计是为了保证传输的可靠性和漫游的透明度,因此在 IEEE 802.11 的头部增加一个新的字段——帧序列控制字段。通过

使用帧序列控制字段,对大的管理帧和数据帧实行分片。IEEE 802.11 在每个帧中用 2 个字节来作为序列控制字段:4 位作为分片号,12 位作为序列号(如图 2 所示)。

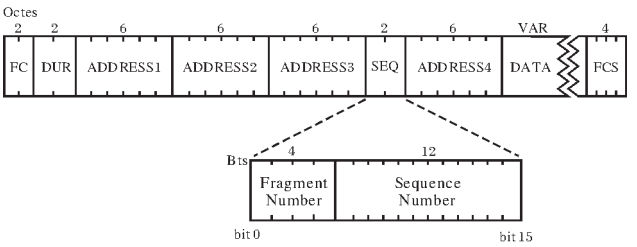

图2 IEEE 802.11 帧中的序列号

管理帧和数据帧进行传输时,若需要分片,则在该帧的每个分片中带有一个相同的序列号和一个递增的分片号,序列号字段从 0 开始连续记数,模为 4096。若帧未分片,则分片号为 0。对于在序列控制字段中具有相同序列号的所有传输,接收站将进行重组。

3.2 检测

IEEE 802.11 的 MAC 帧序列控制字段和网络层的 IP 标识字段很相似。然而,和 IP 标识字段不同的是,序列控制字段的值不能通过软件或程序的方式去修改。因此,攻击者能伪造一个 IEEE 802.11 的 MAC 帧,但却没有能力把序列控制字段设置为任意值。通过分析序列号分析,就能识别采用 MAC 地址欺骗的非授权客户。

对授权的 MAC 地址,建立一个序列号基线,捕获信号范围内的所有无线网络传输,并对与该 MAC 地址相同的帧进行序列号跟踪,将其序列号与序列号基线进行比较,若超出了一定的阈值,就视为 MAC 地址欺骗。

在对序列号监控的过程中,会出现一些异常的情况。当客户漫游到监控的区域之外,然后又返回到监控区域,中间有很多序列号值没有记录,序列号将会出现异常。为了避免虚报,对序列号的延时必须进行处理。当客户改换频道或网卡重新初始化时,序列号可能发生跳值或重新设置的现象。出于这个原因,如果单个的序列号出现异常或出现少量的缺口,则不应进行报警。在大多数情况下,攻击者假冒客户的 MAC 地址,它和原客户的序列号将会有很大的差别。

4 结束语

在目前市场主要采用 IEEE 802.11b 网络设备的情况下,采用 MAC 地址欺骗,攻击者可以很容易地通过无线网络的地址访问控制,窃取授权无线客户的合法身份,进入到无线网络,甚至进入到内部网,对网络资源进行访问和入侵。序列号分析法可对这种攻击进行有效的监控,加强无线网络的安全。

参考文献

[1] LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11,1999 Edition, 1999

[2] Nikita Borisov, Ian Goldberg, David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. Proceedings of the Seventh Annual International Conference, Rome, Italy, 2001, 7: 180~189

[3] William A Arbaugh, Narendar Shankar, Y C Justin Wan. Your 802.11 Network has No Clothes. First IEEE International Conference on Wireless LANs and Home Networks, Suntec City, Singapore, 2001, 12: 131~144

[4] Matthew S. 802.11 Wireless Networks: the Definitive Guide, 北京: 清华大学出版社, 2002.11

[5] Tom Karygiannis, Les Owens. Wireless Network Security: 802.11, Bluetooth, and Handheld Devices. NIST Special Publication SP 800-48, National Institute of Standards and Technology. 2002.12. http://csrc.nist.gov/publications/nistpubs/800-48/NIST SP 800-48. pdf

[7] Joshua Wright, GCIH, CCNA. Detecting Wireless LAN MAC Address Spoofing. http://home.jwu.edu/jwright/. 2003.1

冯柳平　男,(1964-),博士生,副教授。研究方向为网络安全。

刘祥南　男,教授。

刘明业　男,教授,博士生导师。