无线局域网保密性分析

姚 靖 姚 嘉 金心宇 浙江大学信息与电子工程系(310027)

Abstract

Because of the opening of wireless medium, we need more secrecy when we communicate with WLAN, the paper firstly analyzes the deficiency of WLAN in the secrecy at present,then it introduces some latest measures about the secrecy of WLAN.

Keywords:WLAN (Wireless LAN),WEP (Wired Equivalent Privacy),DLS (Dynamic Security Loop),VPN(Virtual Private Network)

摘 要

由于传输媒体的开放性,利用无线局域网进行通信要求其具有更高、更完善的保密性能。本文首先分析了当前无线局域网在保密性上的不足,然后简单介绍了一些现在最新的保密性措施。

关键词:无线局域网,有线等效保密算法,动态安全链路,虚拟专用网

无线局域网由于其传输媒体是辐射到空中的电磁波,它无所不在并且没有固定的路由,因此在一定的范围内,由它所传送的信息可被任何人所截获。利用无线局域网进行通信更需要其有较高的通信保密能力。当我们使用无线局域网技术,却没有采取适当的保密措施时,即使一些初级黑客都有可能利用容易得到的廉价设备对网络进行攻击,取得网络的访问口令,登录到服务器上窃取信息,控制 Web 站点,甚至中断整个网络的运行。

1 无线局域网的保密性漏洞

1.1 信息的窃听/截收

由于无线局域网使用 2.5GHz 范围的无线电播进行网络通讯,任何人都可以用一台带无线网卡(NIC)的 PC 机或者廉价的无线扫描器进行窃听。为了符合 802.11b 标准,无线网卡必须工作在全杂乱模式下(full promiscuous mode)才能监听整个网络的通讯。这类似有线局域网中以太网的 sniffer。无线局域网的不同之处在于,要截收电文,可以不必添加任何具体的东西。

当然,无线传输技术使截收更加困难,特别是当局域网采用专用的或特有的方式传送数据。所增加的难度的确有助于减少泄密。然而,一个主动的攻击者是可以找到途径进行窃听的。例如,根据有关的技术规格,攻击者很可能从生产厂家那里找到所需的消息,也不必利用一般的接收机或监测器从头做起,他可以从无线局域网的生产厂家的标准 NIC 入手,通过硬件或软件对它进行修改,以提供所收到全部数据。

1.2 数据的修改/替换

数据的修改或替换需要改变节点之间传送的信息或抑制信息并加入替换数据,由于使用了共享媒体,这在任何局域网中这都是很难办到的。一个局域网节点一般不能修改另外一个节点的数据,或者脱离共享媒体,取走数据并插入自己的数据来代替。

但是,在共享媒体上,功率较大的局域网节点可以压过另外的节点,从而产生伪数据。如果某一攻击者在数据通过节点之间的时候对其进行修改或替换,那么信息的完整性就丢失了。打个比方,就像一间房子挤满了讲话的人,假定 A 总是等待其旁边的 B 开始讲话。当 B 开始讲话时,A 开始大声模仿 B 讲话,从而压过 B 的声音。房间里的其他人只能听到声音较高的 A 的讲话,但他们认为他们听到的声音来自 B。

在无线局域网上采用这种方式替换数据比在有线网上更容易些。利用增加功率或定向天线可以很容易使某一节点的功率压过另一节点。较强的节点可以屏蔽较弱的节点,用自己的数据取代,甚至会代其他节点的反应。

另一个可能出现修改或替换问题的地方是网络中的业务集中点。例如,使用网桥在两段局域网之间传送数据。由于这两段局域网之间的每条信息都必须通过这个装置,它就成为修改业务的理想地点,从而影响局域网中数据的完整性。当信息在这两段局域网之间通过时,就可以利用网桥对其进行修改,见图 1。

1.3 伪装

伪装即某一节点冒充另一节点。尽管这在数据替换的过程中同样发生,但伪装更容易些,因为被冒充的节点不在附近。由于被冒充的节点并没有发送信息,伪装的节点就不必急于阻止其他发送。通过改换自己的标识,可以很容易冒充另一节点。

伪装出现的原因是,某些网络服务的允许与否是

根据请求节点的地址来决定的。例如,在许多 UNIX 计算机上都提供的“rlogin”服务,用户不用口令就可注册,只要他们来自指定的网络地址。对于无线局域网,从事伪装会更容易些,这是因为不必与网络进行实际连接。这样,在无线局域网的工作范围之内,攻击可以来自任何节点。

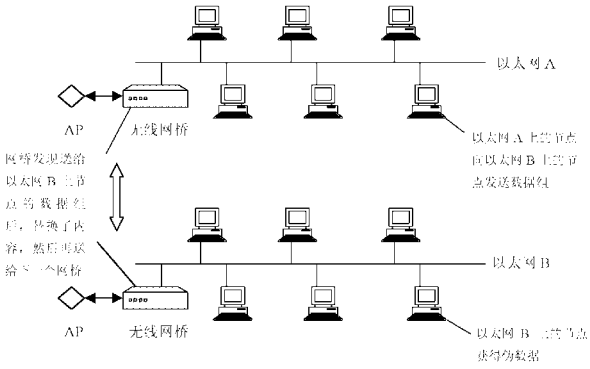

图 1 在网桥出替换数据

另一方面,由于无线局域网传送信息的复杂性增加,伪装另一节点就更加困难了。特别是当使用一般传输设备的时候,将网络地址信息与特别设计的硬件(例如在 NIC中写入特殊号码)联系一起的方案使伪装更加困难。但是,伪装虽然说不是件易事,却可以实现。例如,一个可行的方法事修改与被冒充节点来自同一个厂家的无线局域网节点。

1.4 干扰/抑制

不怕麻烦地监视无线 LAN 的数据,或者试图改变它,或者假冒它来自另一个源,所有这些均是有意的、试图破坏保密性的行为。然而,最令人头疼的很可能是纯粹无意的行为——来自其他电磁辐射的干扰。

噪声或其他形式的干扰可阻碍节点之间的接受,使整个传输瘫痪,信息系统彻底失效。根据所使用的无线局域网的类型,许多干扰都可以影响用户。附近办公室的另一个无线局域网可以屏蔽用户的局域网。同样,办公室的微波炉也能如此。干扰使误码率上升,导致网络流通速度降低,因为信息必须重新发送。在某些地方,无线节点之间的通信可能全部终止。

蓄意干扰,被称作抑制,就是有意制造电磁辐射来破坏通信。其效果同样使局域网瘫痪,或者至少是性能下降。

尽管在无线传输中产生的误码、干扰或抑制能破坏数据的完整性,但是用户可以通过在无线通信中定期使用差错检验码来发现这些威胁,因为噪声和干扰总是可以突然冒出的,对于抑制,我们所面对的主要问题一般是网络有效性的丧失。

2 无线局域网的保密性措施

2.1 屏蔽辐射

采取网络隔离和设置网络认证措施可以防止不同局域网之间的干扰与数据泄漏,因为某些电磁波的辐射频率不擅长穿透物体,因此采取网络隔离可以有效地屏蔽辐射,使之不能到达某一限定的、希望保密的区域。网络认证则主要是针对网间干扰而设置的,通过网络认证,不属于本网络的信号不会得到认证,从而也不会对本网络构成干扰。

确定某一无线局域网屏蔽效果的最简单的方法是在主要工作区的外面设一节点。如果它不能从外面共享该局域网,但当靠近时工作良好,则该无线局域网可能是安全的。为了更确切一些,有无线电和微波通信经验的电子设备工程师可以使用测量装置测量无线局域网信号在工作区外面各处的场强。

2.2 OSI 模型分层保密措施

一般人们很少依赖单一的万能保密措施来提供需要的保护。一个设计良好的保密安全系统将以分层方式采取多种不同的保密措施,具体如图 2 所示。

图 2 一种分层保密方法

所以我们可以根据 OSI 模型的分层结构采取不同层次上的加密措施。

2.2.1 物理层

在物理层采用适当的传输措施,如采用直接序列扩领 DSSS、跳频扩频 FHSS、直接序列跳频扩频 FH/DS 等扩频技术。扩频技术具有很强的抗干扰性:DSSS 技术用伪随机码将要传送信息的功率扩展到很宽的频带上去,使信号功率谱密度随频谱的展宽而降低,甚至可以将信号淹没在噪声中;在接收端用与发端相同的伪随机码对接收到的扩频信号进行相关处理,恢复出发送的信息.而干扰由于与伪随机码不相关,经扩频后落入信号通频带的干扰功率大大降低,达到抗干扰的目的;FHSS 技术使载波频率在伪随机码的控制下不断地、随机地跳变,而干扰不知道跳频频率的变

化规律,经混频后被排斥在信号通频带之外,提高了抗干扰能力;FH/DS 则综合了两者的优点。要截获、窃听或侦察经过扩频技术处理的信号是非常困难的,除非采用与发送端所用的扩频码相同的伪随机序列且与之同步后进行相关检测,否则对扩频信号是无能为力的。

2.2.2 数据链路层

(1) WEP(有线等效保密算法)

无线局域网最关键最独特的保密措施是在网络的媒体访问控制层使用 802.11 定义的 WEP 保密算法对数据进行加密,WEP 能提供与有线网所固有的物理安全属性相等同的效能,具有较强的抗攻击性。WEP 使用了 40 位的 RC4 算法,它属于流密码,这是一种一次将 1byte 明文变化为 1byte 密文的对称密码,密文通过把明文与密匙流(伪随机序列)进行异或运算产生,解密时把相同的密匙流与密文异或即可。由于流密码具有这样的特点,它对消息的完整性要求很高。此外,在流密码实现时一定要防止出现密匙重用的现象。因为如果攻击者拦截了两段用同一密匙流加密的密文。他就可以对这两段密文进行异或,从而得到两段明文的异或值,再辅以统计学手段,攻击者就有可能得到明文。而如果存在大量的重复密匙流的话,攻击成功的可能性就大大增加了。而且。这时只要一段明文被破译,其它的明文也将面临被破译的巨大危险。因此,WEP 的安全性是很不理想的,采用 IEEE802.11 标准的用户最好不要采用聊算法 (目前 IEEE 802.11 标准还没有严格的约束力),目前市场上已经出现了很多支持其它算法的产品,只不过 WEP 仍然占主流。

(2) 动态安全链路(DSL)技术

针对 WEP 的不足之处,对 WEP 加以扩展,提出了动态链路安全技术。动态安全链路技术采用 128 位钥匙,但与 WEP 截然不同的是,动态安全链路技术采用的钥匙是动态分配的,而 WEP 采用的钥匙是手工输入和维护的。动态安全链路技术针对每一个会话(session)都自动生成一把钥匙,并且即使在同一个会话期间,对于每 256 个数据包,钥匙将自动改变一次。采用动态安全链路技术时,要求无线访问点 AP 中维护一个用户访问列表,而在用户端请求访问网络时进行用户名/口令的认证,只有认证通过之后才能连通。

(3) 端口访问控制技术(802.1x)

802.1x 协议是由 IEEE 定义的,用于以太网和无线局域网中的端口访问与控制。该协议定义了认证和授权,可以用于局域网,也可以用于城域网。802.1x 引入了 PPP 协议定义的扩展认证协议 EAP。大家都知道,传统的 PPP 协议都采用 PAP/CHAP 或 Microsoft 的 MS-CHAP 认证方式,它们都是基于用户名/口令或 Challenge/Response(对口令加密)方式,而作为扩展认证协议,EAP 可以采用更多的认证机制,比如 MD5,一次性口令,智能卡,公共密钥等等,从而提供更高级别的安全。实际上 802.1x 是运行在无线网设备关联之后,其认证层次包括两方面:客户端到 802.1x 认证端,认证端到认证服务器。802.1x 定义客户端到认证端采用 EAP over LAN 协议,认证端到认证服务器采用 EAP over Radius 协议。802.1x 要求无线工作站安装 802.1x 客户端软件,无线访问点要内嵌 802.1x 认证代理,同时它还作为 Radius 客户端,将用户的认证信息转发给 Radius 服务器。

2.2.3 应用层

虚拟专用网络(VPN)

虚拟专用网是指在一个公共 IP 网络平台上通过隧道以及加密技术保证专用数据的网络安全性,目前许多企业以及运营商已经采用 VPN 技术。只要具有 IP 的连通性,就可以建立 VPN。VPN 技术不属于 802.11 标准定义,因此它是一种增强性网络解决方案。严格来讲,VPN 可以替代连线对等保密解决方案以及物理地址过滤解决方案,也可以与 WEP 协议互补使用。VPN 协议包括第二层 PPTP/L2TP 协议以及第三层的 IPsec 协议。实际上,VPN 只涉及发起端,终结端,因此对无线访问点 AP 来讲是透明的,并不需要在无线访问点支持 VPN。IPsec 是标准的第三层安全协议,用于保护 IP 数据包或上层数据,它可以定义哪些数据流需要保护,怎样保护以及应该将这些受保护的数据流转发给谁。由于它工作在网络层,因此可以用于两台主机之间,网络安全网关之间,或主机与网关之间。在无线局域网环境,主要采用客户端到网关组网方式。IPsec VPN 可以提供目前最高级别的 168 位 3DES 加密算法,其安全程度明显好于 WEP 协议。

3 结束语

一种最适合的安全的 WLAN 解决方案,一方面要确保用户数据的安全,另一方面也要考虑成本及效率,因为使用加密技术及 VPN 解决方案,不仅要有硬件资金的投入,还会有系统开销。另外,由于目前各厂家的安全解决方案不同,设备的互操作性存在问题,我们希望新的 WLAN 标准能尽快出台,从根本上解决 WLAN 的保密性,也能解决各厂家设备的兼容性。

参考文献

1 郭峰,等.无线局域网.北京:电子工业出版社,2001

2 [美]Peter T.Davis.Craig R.McGuffin 著.宋荣,等译.无线局域网——技术、问题和策略.电子工业出版社,2001

3 Wireless LAN Security,Internet Security System (ISS), 2002

[收稿日期:2002.7.5]