从802.11、802.1x论无线网络的安全性

彭红 （武汉中南财经政法大学工商管理学院 430064）

摘要：随着无线网络的迅速发展，网络安全问题已也逐渐引人注意。本文从802.11和802.1x协议安全机制的角度，分析了他们在无线网安全中存在的缺陷和问题。

关键词：802.11 802.1x 无线局域网 安全性 认证

1 802.11 安全机制

IEEE 802.11的安全是通过两种类型的认证服务和一种编码协议来实现的，这些认证服务和编码机制是固有的，有些不可修补的缺陷。下面描述和分析这些安全机制：

1.1 有线对等保密（WEP：Wired Equivalent Privacy）协议

(1) WEP简介

WEP只是802.11标准中指定的一项保密协议，但不是必需的，其目的用来保护无线LAN用户，防止偶然的偷听，它以RC4序列密码为基础，即加密和解密使用相同密钥的对称密码，RC4是应用软件中最广泛使用的序列密码。术语“有线对等”表示：WEP提供的安全只是提供等同于传统有线网络的保密级别。然而，有线局域网能通过许多物理机制而受保护，并不等同于无线传输。

WEP在安全性方面可达到三个目的：

· 机密性，例如预防通过使用编码来偷听；

· 接入控制，通过拒绝不正确的密码包和通过认证机制来实现；

· 数据完整性，例如通过使用数据效验和预防传送中篡改。

(2) WEP结构(如图1)

WEP使用通信器之间共享的秘钥。一些版本使用最初用于制定标准的40位密钥，而其他较新的版本则使用128位（实际上是104位）密钥。

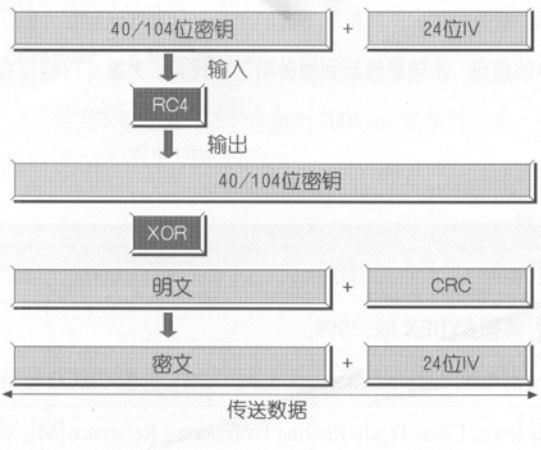

图1 WEP图解

WEP执行如下过程：

① 一个密钥（40或104字节的）与24位初始向量（IV）连接形成64位或128位的密钥。在每个信息包中把IV加到密钥里以确保各信息包的密钥不同；

② 把①形成的密钥输入到RC4 PRNG（伪随机数生成器）中，然后生成和初始密钥长度相同的（不是64位就是128位）伪随机密钥流；

③ 明文通过完整性效验算法进行运算产生一个效验和（即CRC），然后把此效验和与明文连接；

④ 数据向量（即第③步中的明文+效验和）与第②步形成的密钥流进行XOR（异或）加密，最终形成密文。

⑤ 把IV附加到密文上，其结果在无线网上进行传输。

1.2 802.11的认证

客户在传送数据前应先进行认证并与接入点AP建立关联，这种关联仅是把客户与AP绑定起来。802.11标准提供了两种认证类型：开放系统认证（Open systems authentication）和共享密钥认证（Shared-key authentication）。开放系统认证是802.11标准必备的且对大多数AP而言是缺省的，它允许任何客户只要SSID（服务集标识）匹配就能与AP建立关联，即只要连接到无线网络的任何人都被授予访问权，实际上他根本就没认证；共享密钥认证方法要求在无线设备和接入点AP上都使用WEP算法，如果用户有正确的共享密钥，那么就授予对WLAN的访问权。

2 802.11存在的安全性问题

2.1 WEP存在的缺陷

WEP的几个缺陷已被普遍证实和广泛扩散，每个缺陷都允许在无线传输中被动或主动受攻击，或者允许攻击者破译信息，或者是在传送信息里插入伪造信息。下面就描述几个主要的WEP缺陷：

(1) IV冲突

IV冲突简单来说就是无线传输信息的许多点重复使用IV，前面提到，IV是加到每个包的密钥中以确保各包有不同的RC4密钥，一般给定的密钥并不经常改变。众所周知，两个信息包使用相同的IV进行加密是很容易破译的。

IV冲突主要由以下几个因素决定。首先，24位的IV密钥空间难以保证在任何合理的时间内免受冲突，在11Mbps传输速率上发送1500字节包的AP仅在5小时内将耗尽IV的密钥空间；其次，有些无线网卡在初始化时IV复位成零，然后每传输一个信息包，IV值就加1，这意味着传输的信息首先是已知和重复的IV，这就为更多的IV冲突导致了机会或者允许攻击者来猜测IV；第三，WEP安全是基于密钥要频繁改变的假设，实际上密钥并不经常改变，主要因为它是手工处理且耗费时间：密钥被分发且输入到每个用

户软件以及AP中，任何人每5小时就改变一次密钥是不可能。基于上述这些因素，IV冲突经常发生几乎是肯定的。

(2) 缺少密钥管理

WEP标准中没有规定密钥管理方案，这意味着运营商可以按自己喜欢的方式管理密钥，实际上，密钥管理通常由系统管理员或用户自己来操作。在缺乏能共同使用的密钥管理方案的情况下，密钥经常长时间使用并且质量不佳，大多数使用WEP的网络在网络节点之间共享一个WEP密钥。

(3) 其他攻击

· RC4的弱密钥：当在多个明文上同时使用带有相同WEP密钥的相同的IV时，IV冲突就产生了所谓的"弱"WEP密钥。它可让攻击者根据起始的少数传送包来分析和猜测密钥，从而捕获隐藏的WEP密钥。

· 产生CRC数据指纹的完整性效验值的线性算法允许攻击者在加密数据时输入数据以确定CRC值是如何改变的，从而可以为后面的明文破译提供线索。

2.2 认证存在的问题

很明显开放认证存在严重的问题，因为只要知道SSID（服务集标识）就能访问网络，事实上，发现AP的SSID也很容易，每个AP传送的质询帧都包含它的SSID，共享密钥相对要安全些，但仍存在问题，因为所有的客户均使用相同的密钥，要识别单个用户是不可能的；同样，WEP使用的密钥与认证使用的共享密钥相同，因此，攻击者只要盗取一个密钥就可达到一箭双雕：即能进行访问认证，又可编码和解密。

另一方面，AP可认证一个用户，但用户不可也不能认证一个AP，即没有双向认证。如果在WLAN上放置一个"无赖"AP，它能通过"掠持"合法用户成为拒绝服务攻击的发射台。

3 802.1x协议

由于WLAN应用的不断增加以及当前安全协议的一些弱点，必需要有新的、更好的安全机制来保护无线传输，新的IEEE 802.1x标准正是其中之一。

802.1x是一个基于端口的网络访问控制（Port-Based Network Access Control）协议，旨在对最初颁布的802.11标准的安全性加以改进。802.1x可用来提供更强的认证、访问控制和密钥管理，同时允许WLAN对无线用户或工作站实行集中认证。

802.1x基于已存在的认证协议EAP（Extensible Authentication Protocol，可扩展认证协议），而EAP本质上是PPP（点对点）协议的扩展。802.1x不局限于任何特殊的网络结构，而是作为物理网络定义认证用户方式的依据，并不考虑内在的网络协议，即802.1x把EAP配置到物理媒体，而不管媒体是以太网（Ethernet）、令牌网（Token Ring）或无线网（WLAN）。802.1X也支持多种认证方式，这包括令牌卡、Kerbero、一次口令、证书和公共密钥认证。

3.1 802.1x认证机制

802.1x认证包括三个主要的部分：客户端（Supplicant）、认证系统（Authenticator）和认证服务器（Authentication Sever）。客户端一般为一个用户终端系统，该终端通常要安装一个客户端软件，用户通过启动这个客户端软件发起IEEE 802.1x协议的认证过程；认证系统在以太网中指认证交换机，在无线网中指AP，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口；认证服务器通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机或AP发出打开或保持端口关闭的状态；它通常为远程认证拨号用户服务器（RADIUS）。

3.2 802.1x和动态密钥管理

802.1x仅仅提供了认证，并没有指出特定认证类型或任何编码类型，因此，几个供应商使用802.1x作为传递机制提供动态密钥管理的私有版本，通过动态密钥交换，认证服务器能把会话密钥与认证通过信息一起返回给AP。

动态密钥管理提供的机制比手工维护密钥要安全的多，802.1x允许客户端通过使用动态密钥管理来自动改变编码密钥，以使被动攻击的可能性减到最小。

3.3 802.1x存在的问题

802.1x协议并不十分安全，已有研究者发现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2显示攻击者等待一合法用户Susan认证通过后，再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。

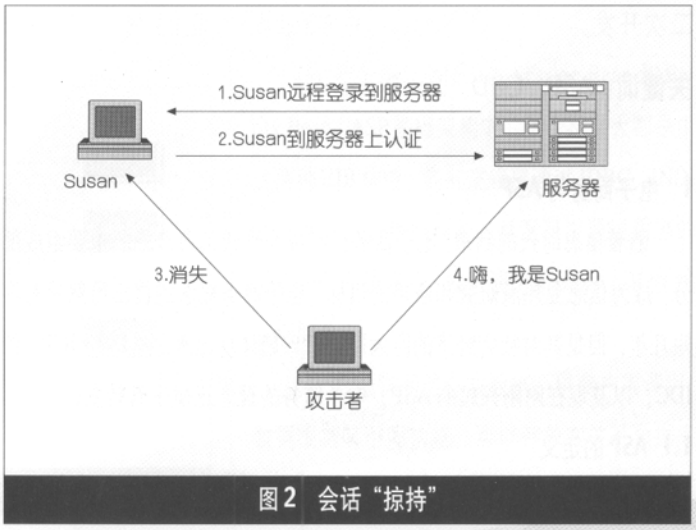

图2 会话"掠持"