申请上海交通大学工程硕士专业学位论文

无线局域网的安全机制、漏洞破解以及解决方案

学　　校： 上海交通大学

院　　系： 信息安全工程学院

班　　级： Z0803623

学　　号： 1080362061

工程硕士生： 颜炳风

工 程 领 域： 计算机技术

导　　师 I： 李小勇

导　　师 II： 邓玉成

上海交通大学信息安全工程学院

2010 年 9 月

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

A Dissertation Submitted to Shanghai Jiao Tong University for

Master Degree of Engineering

WLAN SECURITY, VULNERABILITIES AND SOLUTIONS

Author : Yan BingFeng

Specialty : Computer Technology

Advisor I : Prof. Li XiaoYong

Advisor II : Deng YuCheng

School of Information Security Engineering

Shanghai Jiao Tong University

Shanghai, P.R.China

September 26, 2010

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

上海交通大学
学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：

日期：2010年11月17日

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

上海交通大学
学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权上海交通大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保密□，在___年解密后适用本授权书。

本学位论文属于

不保密☑。

（请在以上方框内打“√”）

学位论文作者签名：颜炳叶

日期：2010年11月17日

指导教师签名：李士勇

日期：2010年11月18日

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

无线局域网的安全机制、漏洞破解以及解决方案

摘 要

无线局域网（WLAN）在很多个重要的领域中，一直被认为是一种非常重要的网络连接方式，其发展前景极其广阔，是未来网络发展的一个重要方向。

但是在无线局域网中，窃取数据会变得很容易，因为入侵者不需要接入物理网络，而只需要把具有无线网络功能的装置放在无线局域网信号范围内即可。这就变得像是通过“空气”进行“网络入侵”、“数据窃取”。正因为如此，无线局域网的安全问题已经变得刻不容缓，亟需解决。

正如上面所述，无线局域网的发展前景极其广阔。但是它的安全问题，成为限制了无线局域网的蓬勃发展的重要因素。了解、研究、以及解决无线局域网的安全性问题，成为当今一个非常重要的研究课题。

本课题就是从无线局域网的安全这一个研究角度入手，深入分析当前无线局域网所以用到的几种主要安全协议。其中涉及到的主要有三种安全认证机制，分别是：

1、Wired Equivalent Privacy（WEP）

2、Wi-Fi Protected Access（WPA）

3、WPA Security Protocol（WPA2）

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

对这几种协议加以分析，详细阐述 WEP 安全协议和 WPA 安全协议的安全机制，找出存在的安全漏洞。并且完成课题中两个重要的任务：

（1）针对 WEP 协议的两个安全漏洞，RC4 算法问题和初始向量问题，实施实验对其进行破解。

（2）分析 WPA 协议的安全机制，找出 WPA 的安全漏洞，配对主密钥（PMK）以及服务集标识符（SSID）的安全隐患，阐述一个完整的 WPA 破解过程。

最后结合本课题中实验结果，以及现有的安全漏洞解决方法，分析并得出最合适的解决方案：

（1）对于 WEP 协议的两个漏洞问题，采用短期的解决方法（TKIP）和长期的解决方法（CCMP），最终实现无线局域网的安全。

（2）对于 WPA 协议的主要漏洞，采用高级加密标准（AES）和添加轮次密钥，实现无线局域网的安全。

通过本课题的研究，实现加深对无线局域网安全机制的理解，找到存在的安全漏洞，并得出合理解决方案，从而使无线局域网变得更加安全可靠。相信无线局域网的发展前景不可限量。

关键词：无线局域网，无线破解，WEP，WPA，WPA2

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

WLAN SECURITY, VULNERABILITIES AND SOLUTIONS

ABSTRACT

Wireless Local Area Network (WLAN) is expected to continue to be an important form of network connection in many business areas. With widen prospect, it become an important research field.

In the WLAN, sniffing becomes easier because the way of connection alter that the intruder only need put the wireless enable terminal in the coverage of the WLAN. It means that the attacker can sniff data and crack via the air. Because of this, the security problems of WLAN become urgent need to resolve.

As mentioned above, the prospects of WLAN is limitless. But the security problems become the biggest factor to restricting WLAN rapid develop. Understanding, research, and solve the security problem of WLAN, is a very important research topic.

This issue is starting with the security problem of WLAN, and in-depth analysis several major security protocol of the current WLAN network. The three main authentication mechanisms are:

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

WPA Security Protocol (WPA2)

Then, to analyze these different kinds of protocol, expatiate on WEP

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

security protocol and security protocols WPA security mechanisms. Finally, find out the existing vulnerabilities, and to complete two important tasks:

1st. Use two security vulnerabilities of WEP protocol, RC4 algorithm problem and the initial vector problem, and implement experimental cracking WLAN.

2ed. Analysis the WPA security mechanisms, identify WPA security vulnerabilities, matching master key (PMK) and the Service Set Identifier (SSID) problems, and described a complete process of WPA.

Finally, along with the experiments, it will discuss the solution for against the cracking methods:

1) The two vulnerabilities of WEP protocol, using short-term solution (TKIP) and long-term solution (CCMP), the ultimate wireless LAN security.

2) The major vulnerabilities of the WPA protocol, using Advanced Encryption Standard (AES) and add the Round key of wireless LAN security.

Through this research topic, the purpose is to deeper understanding of WLAN security mechanisms, to find security loopholes, and to work out a reasonable solution to make WLANs more security. The future of WLAN must be beautiful.

KEY WORDS: Wireless LAN, wireless crack, WEP, WPA, WPA2

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

目 录

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第一章 引言

1.1 背景和意义

当今无线局域网（WLAN）在很多重要的领域中被广泛使用，它被认为是一种非常重要的、无法替代的网络连接方式。而且随着无线网络迅速普及，越来越多的优势被体现出来，并且被市场广泛认可。乐观的预计，在不远的将来无线局域网将会覆盖所有的家庭、中小企业中，以及所有主要城市的中心城区范围。例如现在的纽约，就已经开始逐步实施采用无线网络覆盖所有五个行政区域；又比如在上海，政府已经开始着手建设一个覆盖整个嘉定区的无线局域网。

但是无线局域网的安全问题已成为限制无线局域网发展的重要因素。解决无线局域网的安全性问题，成为当今一个重要的研究课题。

正如上面所述的情况，无线局域网的发展前景极其广阔，是未来网络发展的一个非常重要方向。但是无线局域网的安全问题，制约了无线局域网的蓬勃发展。本文正是针对目前无线局域网安全认证协议存在的几个突出问题，分析研究相关资料，并在这些研究基础上，进一步探讨如何设计实现适用于现有 WLAN 网络的安全认证管理系统。

1.2 课题的目标

本课题将尝试实现下列几点目标：

通过研究 IEEE 安全协议，从而充分理解 IEEE 802. 11 安全协议的相关知识，以及找出破解现有无线局域网安全协议漏洞的方法。

然后，通过实施两个相关实验，阐述如何破解 WEP 和 WPA。

最后根据实验结果，探讨解决破解无线局域网的方法，并设计一个切实可行的无线局域网安全认证管理系统。

在完成本课题时，将会得到下列内容：

（1）此课题报告，其中包括用于完成该课题的所有资料。

（2）软件破解过程的相关图片会展示在本报告中。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（3）实验的相关结果将在本报告中展示。

1.3 本文的结构与安排

本课题大致分为六个章节。

第一章：介绍课题的背景和意义，以及课题所要完成的目标。

第二章：简单介绍无线局域网的现状，目前 IEEE 802.11 主要的安全协议，包括 WEP、WPA 和 WPA2。

第三章：介绍破解无线局域网的主要方法和手段。

第四章：分析 WEP 和 WPA 存在的安全漏洞，并通过具体实验阐述完整的破解 WEP 和 WPA-PSK 过程。

第五章：讨论针对 WEP 和 WPA 安全漏洞进行破解的解决方案，以及切实可行的无线局域网安全管理解决方案。

第六章：对全文进行总结。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第二章 无线局域网综述

2.1 无线局域网介绍

无线局域网 WLAN（Wireless Local Area Networks）是目前一种相当便利的数据传输系统，它利用射频 RF(Radio Frequency)技术，取代采用铜轴双绞线所构成的局域网络。根据 Frost & Sullivan 公司统计，无线局域网市场在 1998 年有 3 亿美金，到 2005 年的时候已经达到 16 亿元。如今的无线局域网（WLAN）已经在大学、机场和其他主要的公共场所得到应用。另外，由于目前无线局域网设备的成本逐步降低，使得很多个人用户也能负担得起，因此有很多家庭用户也开始安装使用无线局域网，摆脱有线网络那些繁琐的连接。但是目前无线网络接入的基础建设成本仍然较高，虽然各大运营商已经在加快无线城域网基础建设，无线网络的覆盖范围也已经得到极大的扩展，但是目前在公共场所使用无线网络连接还是受到很大的限制。除了成本问题，安全性问题也是无线局域网发展的重要制约因素。

随着信息技术的不断发展，人们对通信的要求也在不断提升。家庭和小型办公网络用户对移动连接的需求是无线局域网市场增长的无穷动力。与此同时，在实现移动办公，可以随时随地地获取信息的时候，确保 WLAN 的安全性也就成了这项技术的焦点。

2.2 无线局域网的优点和缺点

由于无线局域网为人民带来了很多的好处，因此它现在已经被应用在许多的中小型企业和家庭中。无线局域网优点在于：灵活性、易用性等等。接下来简单地说明一下无线局域网的优点：

（1）灵活性：

无线局域网的用户，可以在任何有无线信号覆盖的范围内获取无线信号， 在启用 802. 11b 协议的计算机，搜索范围可达 30 米的，而 802. 11g 传播的距离更

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

远。此外，无线网络可应用在用户不能安装新的网络电缆的地方，终端工作站可以自由移动，并加入到新的网络接入。

（2）易于使用：

无线局域网用户只需要用具有无线网卡的计算机连接到基站便可以使用无线局域网。用户无需配置无线局域网（WLAN）。例如无线局域网卡将自动搜索无线访问点。然后无线局域网网卡便可以从访问点自动获得 IP 地址，并访问网络资源。

（3）鲁棒性：

用户可以从一个无线接入点移动到另一个无线接入点，并且保持他们的终端设备无需停止工作。另外，在无线接入点信号覆盖重叠的范围内，在当前无线局域网接入点停止工作时，用户可以继续保持网络连接。正因为无线网络的这个特点，可以解决在传递某些重要的数据包时网络中断的问题。例如在一个重要的网络会议上，企业想要确保互联网的连接，可以设置无线局域网。

（4）价格：

近年来，无线网络设备的价格已经不是一个主要的因素限制无线网络在世界各地应用。根据 2000 年的统计资料，无线网卡的成本约为 100 欧元。但是，到了 2004 年年底，相同网卡的成本仅为 30 欧元。因此，无线局域网比较适合有线网络铺设非常昂贵的地方，或者不方便使用有线网络的地方。例如大型的露天场所，比如临时性的展会，或仅一次性使用的情况。

但是，无线局域网也有它的一些不足之处，这些问题制约了无线局域网的发展。主要有以下的几个方面问题：

（1）安全性：

安全性是一个重要的问题，它阻碍了无线局域网大规模推广。因为只要在无线接入点覆盖范围内，攻击者能使用某些工具（例如，AirCrack，AirSnort）轻松地截获数据包。即使数据包应用了无线加密，攻击者也能偷听数据通信。

（2）无线电波的覆盖范围：

无线访问是通过一系列特定的微波射频。例如典型 802. 11b 和 802. 11g 接入点覆盖范围大约为 100 英尺。但是，很多障碍物会降低无线信号传播。此外，多个重叠的微波无线访问点，会导致信号冲突。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（3）数据传输速率：

目前无线局域网数据传输速度还远不如现有的主要有线局域网速率。通常，无线局域网的带宽是 11Mbit/s 或 54Mbit/s。这样的数据传输速率并不合适大量的数据传输。然而有线局域网（LAN）的带宽已普遍达到 100Mbit/s，甚至 1000Mbit/s。虽然在 2004 年电气与电子工程师（IEEE）宣布，成立了一个新的 802. 11 专题小组，新 802. 11 标准（802. 11n）的无线局域网络。预计 802. 11n 的标准数据吞吐量，将会达到 540Mbit/s 的理论值，但该标准还没有最终确定，至少到今天为止尚未全面实现。

2.3 无线局域网的基本体系结构

一个基本的无线局域网网络，包括访问点、无线客户端、基本服务集、扩展集和分布式系统。

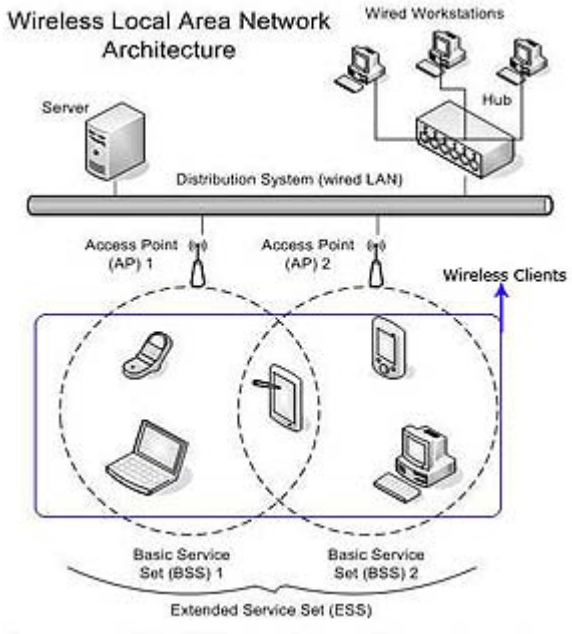

图 2-1 无线局域网基本体系结构

Figure 2-1 WLAN Architecture

（1）访问点（AP）：访问点是无线局域网的基站。访问点的功能是：传输和接收已启用无线射频设备的信号。

（2）无线客户端：无线客户端可以解释为移动设备，如便携式计算机，个人掌上电脑（PDA）或具有无线网络接口卡的桌面设备。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（3）基本服务集（BSS）：基本服务集（BSS）是一组可以彼此通信的站点。在 BSS 可以被分为两种类型：Independent BSS 和 Infrastructure BSS。

Independent Basic Service Set：由一个基本服务集组成一个独立网络，在这个网络中，不能访问其他已有的分布式网络

Infrastructure Basic Service Set：一个基础设施服务集可以与其他站点通信。但是，它不能在同一个基本服务集内通过访问点进行通信站彼此通信。

（4）扩展服务集（ESS）：ESS 是一组被关联起来的 BSS 和局域网。在一个扩展的服务集中，分布式系统控制访问点的连接。否则，每个 ESS 有一个的标识，称为服务集标识号（SSID）。其中 SSID 是一个 32 字节的字符串。

2.4 无线局域网的类型

无线局域网根据组网方式，可以分为两个主要的类型：

第一类：点到点（对等网）或 ad-hoc 无线局域网。

第二类：访问点或基础设施无线局域网。

2.4.1 点到点（对等网）或 ad-hoc 无线局域网

这种方式构成一种特殊的无线网络应用模式，多台计算机通过无线网卡即可以实现相互连接，实现组网需求。无需透过 Access Point。

无线设备直接在这种类型的无线网络中相互通信、资源共享。并不需要中央访问点。通常这个方法被应用在两台或几台计算机之间。见图 2-2。

图 2-2 点对点无线局域网

Figure 2-2 Peer-to-Peer WLAN

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.4.2 访问点或基础设施无线局域网

这种类型的无线局域网允许无线客户端通过访问点连接网络。在这种类型的无线局域网中，访问点可能是一个集线器或路由器，可以发送和接收无线频率，或桥接无线网络和有限网络。

这种方式的无线局域网实现了点到多点的接入方式。实现的时候必须有一台 Access Point 设备。见图 2-3。

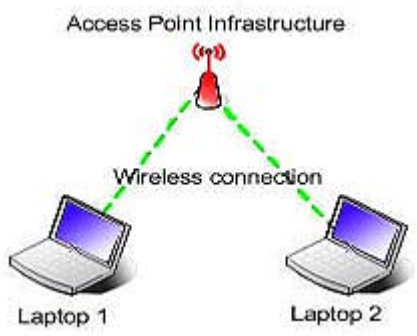

图 2-3 无线局域网访问接入点

Figure 2-3 Access Point WLAN

2.5 IEEE 802.11（Wi-Fi）

IEEE 802. 11 的 Wi-Fi 标准是最初无线局域网的标准，由 IEEE 有线局域网/城域网标准委员会于 1997 年 6 月确定下来的。该标准描述了一个媒体访问控制（MAC）协议和三个可选的物理层（PHY）协议。在 1999 年年底，IEEE 发表两个项 802. 11 标准的补充协议：802. 11a 与 802. 11b。两个版本的目的是实现更高的带宽。在 1999 年 IEEE 发表了新的内容，这是 IEEE 802. 11b 的新增内容。在 2. 4GHz 频段，指定物理层高的比率的扩展的直接序列扩频（DSSS）。在 1Mbps 和 2Mbps 速率下，这个 DSSS 扩展系统可提供 5. 5Mbit/s 和 11Mbit/s 的数据负载率。在 IEEE 802. 11a 是 1999 原始年标准的补充。在 5 GHz 频段，它可以提供高速率，采用正交频分复用（OFDM）系统。另外，该标准正成为基础标准。此外，正交频分复用系统最大能提供无线局域 54Mbit/s 的网络数据负载率。

在 2003 年，IEEE 定义了 802. 11g 协议，采用该协议可以使得无线设备达到 54Mbps 的速率，并保持向下兼容 IEEE 802. 11b。这项重大的突破使得流媒体、视频、下载等应用更为方便，同时允许更多用户可以互不干扰使用无线网络。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

此外，IEEE 802.11i 标准在 2004 年被明确下来。该标准提供了在用户访问前，公共网络访问点和同用户设备之间的连接身份验证。它提供了认证协议，密钥管理协议和数据保密性协议。无线保护访问（WPA）是一个重要的 IEEE 802.11i 协议，它包括更好的暂时密钥集成协议（TKIP），更容易安装程序使用一个预共享的密钥（PSK），还可以使用基于 802.1X 的远程验证拨号用户服务（RADIUS）的用户身份验证。

另外在 2004 年 1 月，IEEE 宣布它已成立一个新的 802.11 专责小组开发一种新的修订版，用以完善 802.11 标准的本地无线网络。实际数据量理论值可达 540Mbit/s，它要求在物理层可以达到更高的原始数据速率，相当于比 802.11a 或 802.11g 快 10 倍，高于 802.11b 近 40 倍。预计 802.11n 亦会提供比当前网络的更好地覆盖距离。

IEEE 802.11 协议列表

表 2-1 IEEE 802.11 协议

协议	发行日期	频率	最大带宽
IEEE 802.11	1997	2.4 GHz	1,2 Mbps
IEEE 802.11a	1999	5 GHz	54 Mbps
IEEE 802.11b	1999	2.4 GHz	11 Mbps
IEEE 802.11g	2003	2.4 GHz	54 Mbps
IEEE 802.11i	2004	2.4 GHz	54 Mbps
IEEE 802.11n	2007	2.4 GHz 或 5 GHz	540Mbps

2.6 无线安全技术概述

从 WLAN 第一代以来，无线局域网已经被部署许多在小型企业和一些个人用户的家中。由于早期有很多访问点（AP），不能确定用户在访问网络时是否有得到安全认证，这时候无线局域网的安全问题就出现了。面对这种情况，IEEE 和其他（如 Wi-Fi 联盟）的组织出版了很多的安全标准，以应对不同的安全漏洞。在这里我们将介绍几个主要的无线局域网安全协议：

Wired Equivalent Privacy（WEP）

Wi-Fi Protected Access（WPA）

WPA Security Protocol（WPA2）

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.6.1 Wired Equivalent Privacy（WEP）

WEP 是一种基于 64bit RC4 的数据加密算法，由 IEEE 802. 11b 标准定义的无线局域网安全标准。采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。此外，标准的 64 位 WEP 被定义了两个主要功能，通过使用 40 位密钥，连接到 24 位初始向量（IV）来产生 RC4 密钥。WEP 的第一个功能是避免被无意窃听到受保护的数据。第二个功能是避免未经授权访问无线网络。

WEP 支持 64 位和 128 位加密。对于 64 位加密，加密密钥为 10 个十六进制字符（0–9 和 A–F）或 5 个 ASCII 字符；对于 128 位加密，加密密钥为 26 个十六进制字符或 13 个 ASCII 字符。64 位加密有时称为 40 位加密;128 位加密有时称为 104 位加密。152 位加密不是标准 WEP 技术，没有受到客户端设备的广泛支持。WEP 依赖通信双方共享的密钥来保护所传的加密数据帧。

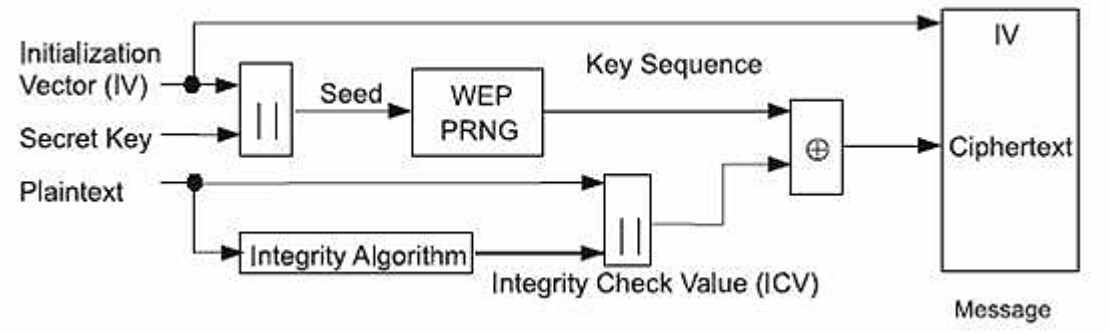

图 2-4 WEP 加密过程

Figure 2-4 WEP Encryption process

在具体实施中,这样的算法广泛采用 104 位密钥以代替 40 位密钥。然而 WEP 的封装和解封装机制是一样的，无论使用 40 位或 104 位密钥。这个算法将生成一个移动设备和访问点之间共享的密钥。数据包传输前通过密钥加密，并检查数据包,确保在传输期间数据包的完整性。虽然这个标准并不涉及如何共享该密钥，但由于大多数系统使用单密钥，并且该密钥被所有移动站点和访问点所共享。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

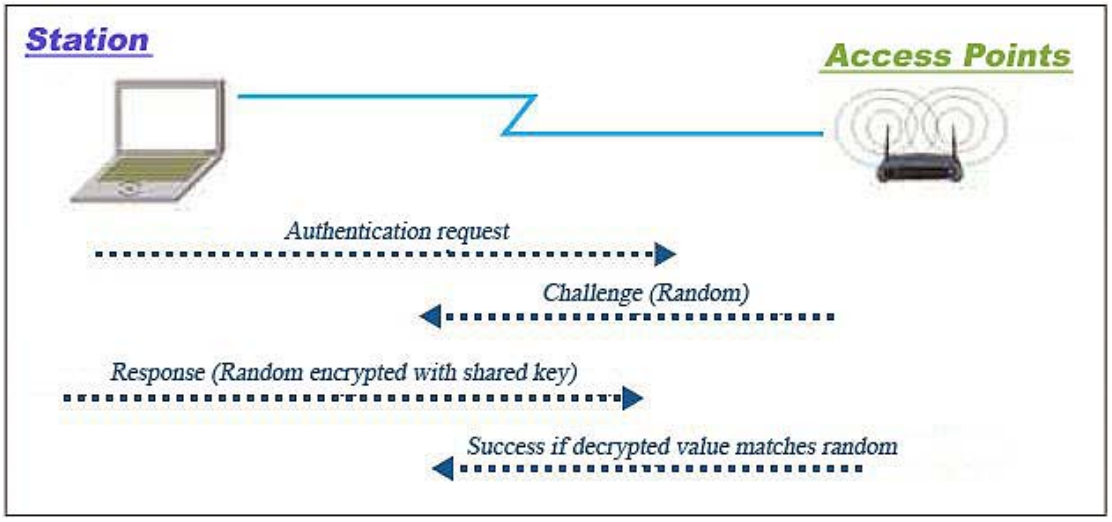

图 2-5 无线站点使用 WEP 认证

Figure 2-5 Wireless Station Authentication Using WEP

WEP 的漏洞

根据图 2-5 所示，在认证信息交换过程中，挑战信息（Challenge）通过无线网络进行传递，这正式中间人攻击的一个漏洞，图 2-6 描述了一个典型的中间人攻击的情形。攻击者可以截获包括纯文本和响应的密码文本。在进行攻击的过程中，攻击者可以通过破解明文，以识别 WEP 密钥。有一些软件，例如 WEPCrack 和 AirSnort，可以识别“弱”WEP 密钥，这样便会使得无线局域网的安全攻击过程变得比较容易，而且速度很快。

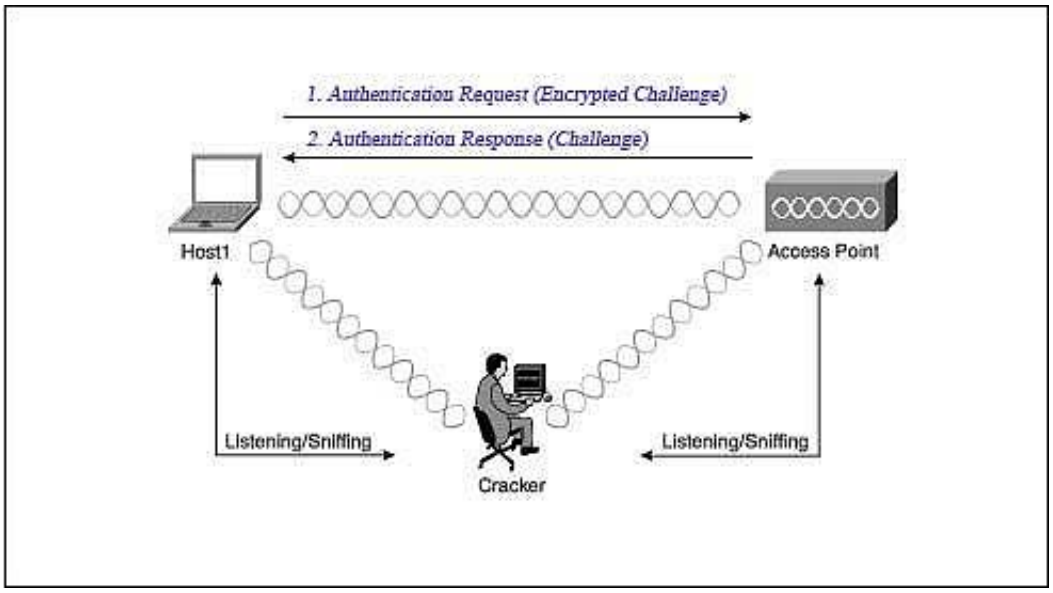

图 2-6 WEP 弱点：中间人攻击

Figure 2-6 WEP vulnerability: Man-in-the-middle Attack

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

从图 2-6 中可以看出，一个入侵者正在进行典型的中间人攻击。获取主机：Host1 和无线接入点 Access Point 的通信信息。当获取了明文和对应的密钥后，可以通过简单的异或运算，便可以对明文和密文进行转换。

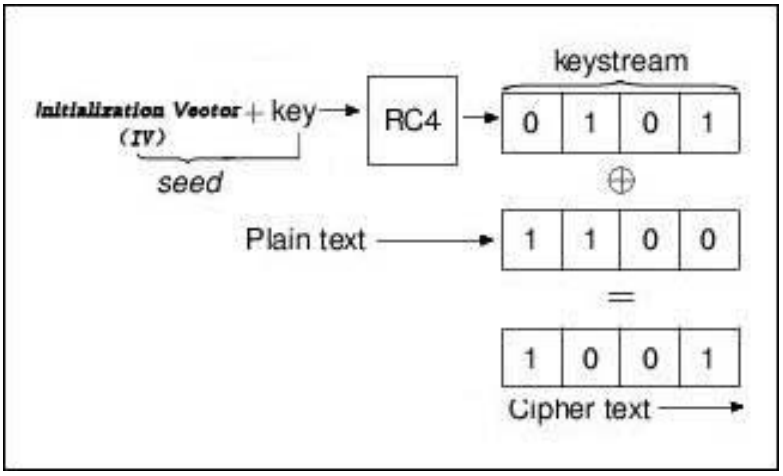

图 2-7 执行一次异或（XOR）运算

Figure 2-7 the performing an exclusive OR (XOR)

如图 2-7 表明，WEP 加密应执行一个独占的异或（XOR）函数生成加密的挑战的关键流的纯文本。异或（XOR）的功能可以将其定义为：“A 或者 B，但不能两者同时”。如此一来，异或（XOR）函数生成逻辑 1 的输出，只有两个输入值不同。如果输入相同，输出就是逻辑 0。

这样就很清楚了，结果是一个密钥流，如果异或（XOR）函数运行在纯文本以及加密的挑战方式时。这样，攻击者可以通过共享密钥认证过程，嗅探认证信息，并生成密钥。同时，攻击者还可以利用这个方法实现无线局域网的入侵。比如：修改消息、插入消息和重定向 IP 等等。

其数据的解密过程如下：

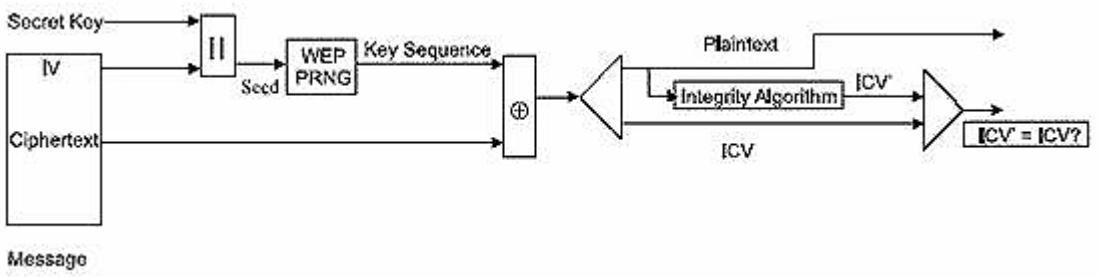

图 2-8 WEP 解密过程

Figure 2-8 WEP Decryption process

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

除此以外，初始向量（IV）重用攻击也应该提一下，每次初始通过 PC 网卡重置初始向量为零，然后通过每一次使用后递增。在这种情况下，便会导致密钥流被反复使用。

另外，在 2001 年 Newsham 使用上文所述的 keystreams 消息身份验证，成功地建立了一个脱机字典，用来攻击 WEP。

2.6.2 Wireless Protected Access（WPA）

在过去的几年，与 IEEE 一起工作的 Wi-Fi 联盟提出了一个 Wireless 与 Wi-Fi 互操作的安全受保护访问协议 WPA。WPA 协议大大改进了之前的无线网络安全保护能力和访问控制技术，使无线网络数据的安全级别提高。2001 年推出的 WEP 加密协议的弱点已经被普遍知道。因此，WPA 协议旨在克服所有已知的 Wired Equivalent Privacy（WEP）的“弱点”。虽然没有一个安全解决方案可说是“防弹”的，但是 WPA 在无线安全方面实现了一个大飞跃。

WPA 协议旨在保护 802. 11b、802. 11a、802. 11g、multi-band 以及多模的 802. 11 设备的所有版本。WPA 作为 802. 11i 的子集，可以向前和向后全部兼容，并且设计成可以作为一个软件下载到现有的无线设备上运行。

WPA 使用一种强大的新的加密算法以及用户身份验证方法，处理 Wi-Fi 的安全性，这是在 WEP 上很缺少的。WPA 提供高级别的保障，始终严格地保护用户的数据安全，只有获得授权的用户才可以访问网络。使用 WPA 协议可以简单、灵活地提供无线安全保护。

此外，无线因特网服务提供商（WISP）也可能会发现 WPA 增强加密和身份验证方案可以使用在公共“热点”，并为服务提供商和移动用户提供更高级别的安全，而不需要进行额外的部署。同时也可以为公司，家庭和小型办公室/家庭办公室（SOHO）的使用者提供一个强大的安全性网络。

WPA 安全机制：

WPA 解决 WEP 的两个主要的漏洞：在客户端和缺乏身份验证的访问点之间使用相同的静态密钥，只有获得授权的用户可以访问无线网络。

WPA 使用一个非常强大的加密方案：暂时密钥集成协议（TKIP）。加上 802. 1X 身份验证，可扩展的身份验证协议（802. 1X / EAP），TKIP 采用了增强型保护密钥。它还添加了一个消息完整性检查代码（MIC），用以防止数据包伪造。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

WEP 与 WPA 的比较

表 2-2 WEP 与 WPA 的比较

	WEP	WPA
加密	被科学家和黑客攻破	修复所有 WEP 缺陷
	40 位密钥	128 位密钥
	静态密钥 网络上的所有人使用相同密钥	动态会话密钥。 一个用户/一个数据包/一个会话
	密钥手动输入到每个设备	密钥自动部署
身份验证	使用预设的 WEP 密钥进行身份验证 有缺陷	利用 802.11X 和 EAP 进行身份认证 强大的用户身份验证

加密

TKIP 扩展的 48 位初始化向量（IV）和 IV 顺序规则，提高密钥大小从 40 到 128 位，并由身份验证服务器动态生成密钥，替代 WEP 的一个静态密钥。此外 TKIP 应用一个密钥管理替代可预测 WEP 密钥。

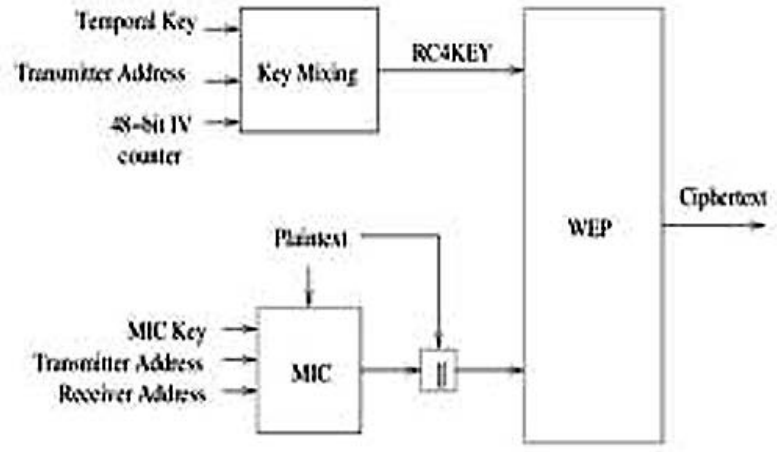

图 2-9 WPA 封装过程

Figure 2-9 WPA encapsulation process

TKIP 使用的是 802.1X／EAP 框架。身份验证服务器使用 802.1X 生产一个唯一的主密钥或“配对”密钥，由此来加密获得授权的用户的会话。然后，TKIP 分发给客户端和访问接入点，设立密钥管理系统。此外使用配对密钥，动态生成唯一的数据加密密钥，用来加密无线通信期间用户的每一个数据包。

此外，消息完整性检查（MIC）可以阻止入侵者拦截、数据包被篡改和重新发送。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

身份验证

WPA 使用 802. 1X 其中一种可扩展的身份验证协议（EAP）。802. 1X 是一种基于端口的网络访问控制安全协议。2001 年 8 月它被 IEEE 作为标准使用。

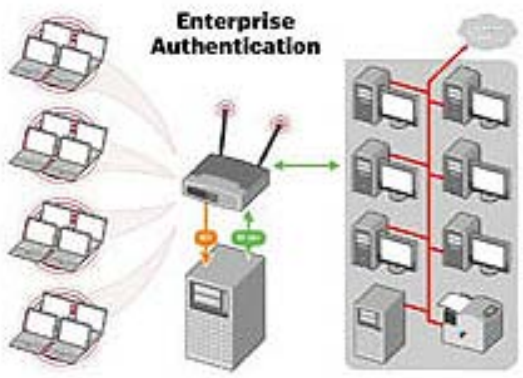

图 2-10 WPA 企业认证

Figure 2-10 WPA Enterprise Authentication

EAP 可以使用被互联网广泛使用的数字证书作为处理用户的身份信用的凭据。区别于用户名和密码的认证方式，以及其他的身份证明措施，由 IT 管理员统一部署和管理。WPA 灵活接受两种类型的身份验证。具体实施的时候通常采用基于标准的 EAP 方式实现，包括：

（1）EAP-Transport Layer Security（EAP-TLS）

（2）EAP-Tunneled Transport Layer Security（EAP-TTLS）

（3）Protected Extensible Authentication Protocol（PEAP）

此外，802. 1X 通过 EAP 服务器进行身份验证，创建客户端和工作站之间的身份验证框架。相互身份验证可以保护用户避免一些“意外连接”或未经授权的访问，还可以确保访问网络的用户访问的资源是经过授权的。当用户请求访问该无线网络，客户端发送用户授权到身份验证服务器。如果身份验证服务器接受用户认证授权，则身份验证服务器会发送主 TKIP 给客户端及访问点。

另一方面，由于那些小型办公室和 SOHO 的用户环境，使用预共享密钥（PSK）或密码的情况下，使用 WPA 会有许多优点。PSK 提供小型办公室和 SOHO 用户使用相同的 TKIP 加密每个数据包以及提供密钥管理。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

图 2-11 WPA SOHO 认证

Figure 2-11 WPA SOHO Authentication

WPA 的弱点

在 2003 年 11 月 ICSA 实验室高级技术专家——Robert Moskowitz 申称：只要一个简单的公式，通过执行 WPA-PSK 字典攻击，就可以显示无线网络的密码。这个漏洞是根据这样一个事实：配对主密钥（PMK）通过比较密码字段、服务集标识符（SSID）进行确认。这些信息通过哈希算法计算 4096 次，生成一个 256 位的值。这些信息在会话密钥创建和验证时被请求，而这个密钥信息是通过通常的广播方式传播，并且是可随时都可以获取到的。Moskowitz 进一步解释：配对密钥（PTK）是基于 PMK 的，是一个 HMAC 函数。通过抓取“四次握手”认证信息，攻击者可以通过字典攻击，获取需要的数据。

在 2004 年年底 Takehiro 发布 WPA 破解器。此外网络工程师 Josh Wright 制作了 coWPAtty 软件。这两个软件都是基于 Linux 系统的，并强制执行 WPA-PSK 字典攻击，试图确定网络共享密码。他们两人都需要用户提供一个词典文件和一个包含 WPA-PSK 四个握手的转储文件。这两个软件是基本相同的，但是 coWPAtty 包含一个 WPA 自动解析器，而 WPA 需要用户手动执行字符串提取。此外，coWPAtty 已优化 HMAC-SHA1 函数，使它变得更快速。两个工具都使用 PBKDF2 算法，控制 PSK 哈希攻击，并确定密码。

目前 WPA 加密方式的这个漏洞，使攻击者可利用 sniff 工具，搜索到合法用户的网卡地址，并伪装该地址对路由器进行攻击，迫使合法用户掉线重新连接，在此过程中获得一个有效的握手包，并对握手包批量猜密码，如果猜测密码的字典中有合法用户设置的密码，即可被破解。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.6.3 WPA Security Protocol（WPA2）

IEEE 已经认识到 WEP 不是一种足以保护无线通讯的安全协议。于是开始着手建立一个新的安全标准——802. 11i，也称为 WPA2。802. 11i 在 2004 年年初就开始起草了，该标准包括一组鲁棒性很强的安全标准集。802. 11i 体系结构包括：802. 1X 身份验证和基于端口的访问控制，AES（高级加密标准）加密模块和 CCMP，用来保持关联性的跟踪，并提供保密、完整性和源身份验证。

像 WPA 安全协议一样，WPA2 将应用 802. 1X/EAP 框架，以确保集中身份验证和动态密钥管理。WPA2 同时支持个人和企业模式。在个人模式，预共享密钥与 SSID 组合来创建成对的主密钥（PMK）。客户端和 AP 使用 PMK 来交换消息以创建成对的临时密钥（PTK）。

在企业模式中，在成功认证后——使用其中一种 EAP 方法——客户端和 AP 都收 801. 1z 服务器接收消息，并用于创建 PMK。然后它们交换消息以创建 PTK。然后 PTK 被用以加密和解密消息。

在个人和企业两种情况中，都有一个组临时密钥（GTK）在客户端和 AP 的消息交换过程中被创建出来。GTK 被用于解密广播和多播消息。

因为 AES 加密算法的优点，希望用 AES 建立新的 WLAN 安全加密协议。但是，AES 并不接受现有的 802. 11b/g 硬件和后续的无线局域网设备。因此必须衡量使用 WPA2 增强安全新带来的好处和相比之下带来的成本。

此外，WPA2 提供了一个从 WPA 迁移非常完善的方式。WPA2 会提供一个高度安全的“混合模式”，支持 WPA 和 WPA2 的两种客户端工作站。这将允许在一个企业在短时间内有序地升级无线网络。但是 WPA2 的混合模式不同于 WEP/WPA 混合模式，它只支持 WPA 和 WPA2，旨在提供较高的安全级别。

WPA2 除了使用 802. 1X/EAP 框架以确保身份验证外，“四次握手”是另一项重要的 WPA2 的身份验证程序。

四次握手

身份验证过程剩下两个考虑因素：访问点（AP）仍需进行本身对客户端（STA）的身份验证，加密密钥被需要发送来。先前 EAP 交换提供了共享安全密钥 PMK。该密钥的开销在持续的整个会话过程中应尽可能小。因此，在四次握手中另一个键名为 PTK。PTK 由以下属性组成：PMK，AP 生成值（ANonce），STA 生成

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

值（SNonce），访问点 MAC 地址和 STA 的 MAC 地址。生产一个加密的哈希函数。

握手还生成 GTK（Key 组时间）用于解密多播和广播的信息。在图 2-11 中解释握手交换的实际过程：

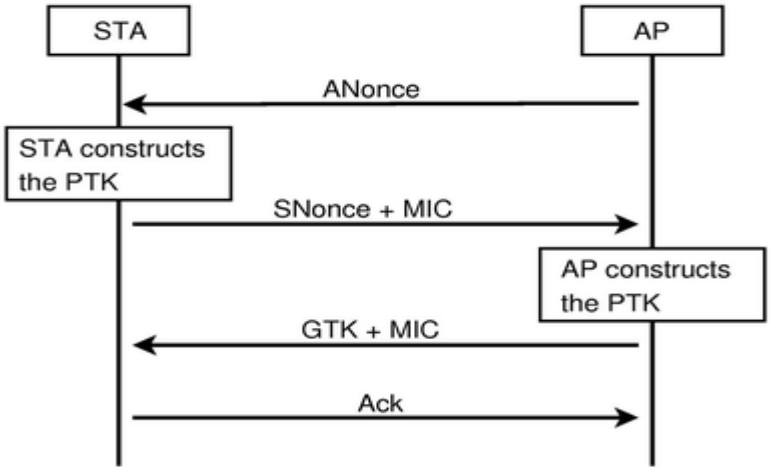

图 2-11 在握手过程期间的实际信息交换

Figure 2-11 Actual messages exchanged during the handshake

（1）AP 发送一个当前值（ANonce）给 STA。客户端这时便有了 PTK 所有属性。

（2）STA 将自己的当前值（SNonce）发送给 AP。

（3）AP 发送 GTK 和一个序列号。该序列值将被用在下一次的组播或广播帧，这样接收端的 STA 可以执行基本的回应探测。

（4）STA 向 AP 发送确认信息。

当 PTK 得到以后，它被划分为三个单独的项：

（1）EAPOL-Key 确认密钥（KCK），这个密钥被用于计算 EAPOL-Key 数据包的 MIC 值。

（2）EAPOL-Key 加密密钥（KEK），这个密钥被用于加密 EAPOL-Key 数据包。

（3）临时密钥（TK），用于实际的无线通信进行加密的密钥。

组密钥握手

使用 GTK 的网络，可能需要更新预设的计时器以免过期。当一个设备离开网络，GTK 也需要更新。这是为了避免设备接收来自接入点的多余多组播或广播信息。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

为了处理更新，802.11i 定义一组密钥握手，其中包含一个双向握手：

（1）AP 将新的 GTK 发送到网络中的每个 STA。GTK 使用 KEK 加密，分配给 STA 和保护数据不被篡改。

（2）STA 通知新的 GTK 并回复 AP。

WEP 与 WPA2-PSK 的比较

表 2-3 WEP 与 WPA2-PSK 的比较

	WEP	**WPA2-PSK**
安全性	不安全，易破解	除暴力破解，尚未有破解方法
加密算法	RC4	AES，128 位加密算法
连接	单次，Open System 和 Shared Key 模式	四次握手，只能 Open System 模式
密钥	静态，无派生	动态，任意两设备间密钥不一样
完整性校验	CRC-32，线性算法，易篡改	CCM，密码区块链信息认证，对 MIC 加密，无法篡改
初始化向量	24 位，线序排列	48 位数据包编号
身份认证	无	IEEE 802.1x 身份认证
重播保护	无	数据包编号作为计数重播保护

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第三章 破解无线局域网的基本方法

在本章节中将提出针对无线局域网的几种攻击方法。根据 Lisa Phifer 理论，这些主要的攻击方法可以分为以下几个主要类型：机密性攻击，授权攻击以及针对访问控制攻击。这里将会较为详细阐述每一种攻击类型的工作原理，以及使用会使用到的工具。

3.1 机密性攻击

机密性攻击试图截取在无线连接中传输的私人信息。无论这些信息在 802. 11 或者更高层级的协议中，已经加密或者未经加密方式传输的都可以截取。本节分为 3 个部分：无线局域网嗅探（窃听），SSID 截取和 WEP 秘钥破解。

3.1.1 无线局域网嗅探（窃听）

在有线局域网中，传统的“嗅探”是指窃听相互通信的计算机之间的电子信号。

通常，如果入侵者使用网络设备或专用软件，通过物理方式接入了该有线网络，那么这种方法通常可以收集到整个局域网中所有数据流。

然而在无线局域网中，“嗅探”会变得相对更加容易，因为入侵者不需要通过物理方式接入网络，而只需要把具有无线网络功能的计算机放置在无线局域网信号覆盖的范围内即可。这就意味着攻击者可以通过“空气”进行嗅探。并且现在的攻击者可以从互联网上可以轻易地找到很多商业的或者免费的嗅探工具，这些软件可以自动对数据进行拆包，分析出数据类型，获得详细的用户数据信息。

嗅探工具

在互联网高度发达的今天，入侵者能够轻易找到许多嗅探工具，例如 Sniffer Pro、Prismdump、Kismet、WildPacket’s Airopeek 以及 WildPacket’s Omnipeek 等等。这些工具都可以用来嗅探无线局域网的数据，而且每个软件都有其自身的独特特点。这里图示的就是通过 WildPacket’s Omnipeek 4. 0 截取的无线局域网数据，见图 3-1 及 3-2。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

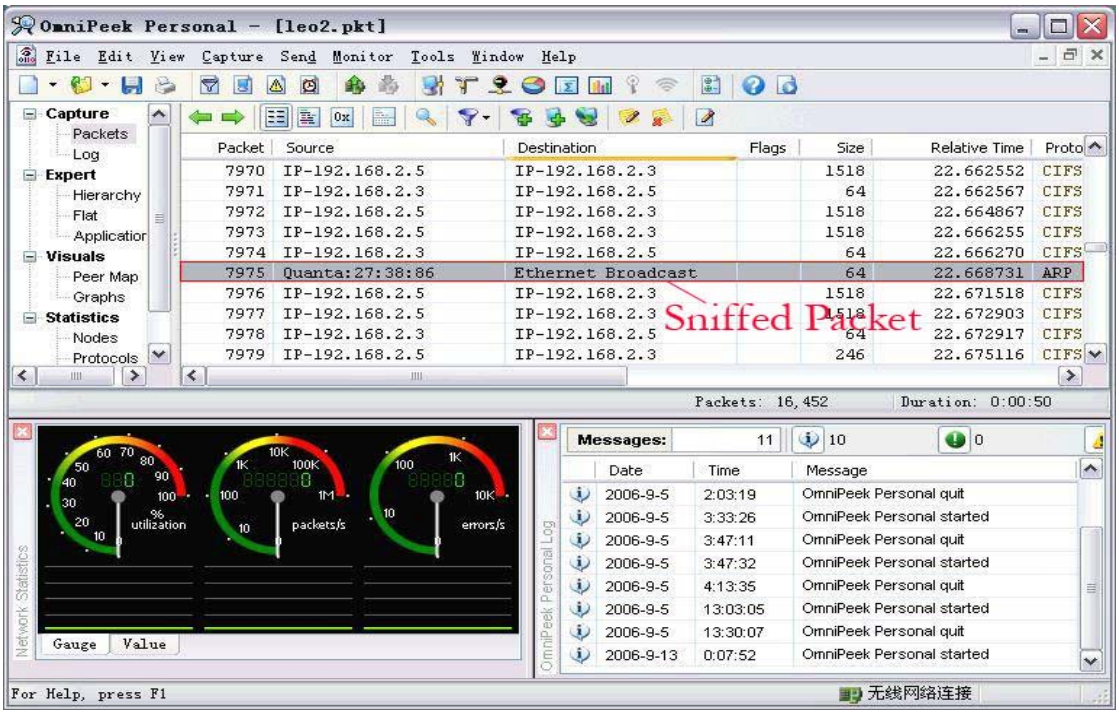

图 3-1 OmniPeek 4.0 嗅探数据截屏

Figure 3-1 OmniPeek 4.0 sniffing data, Screenshot

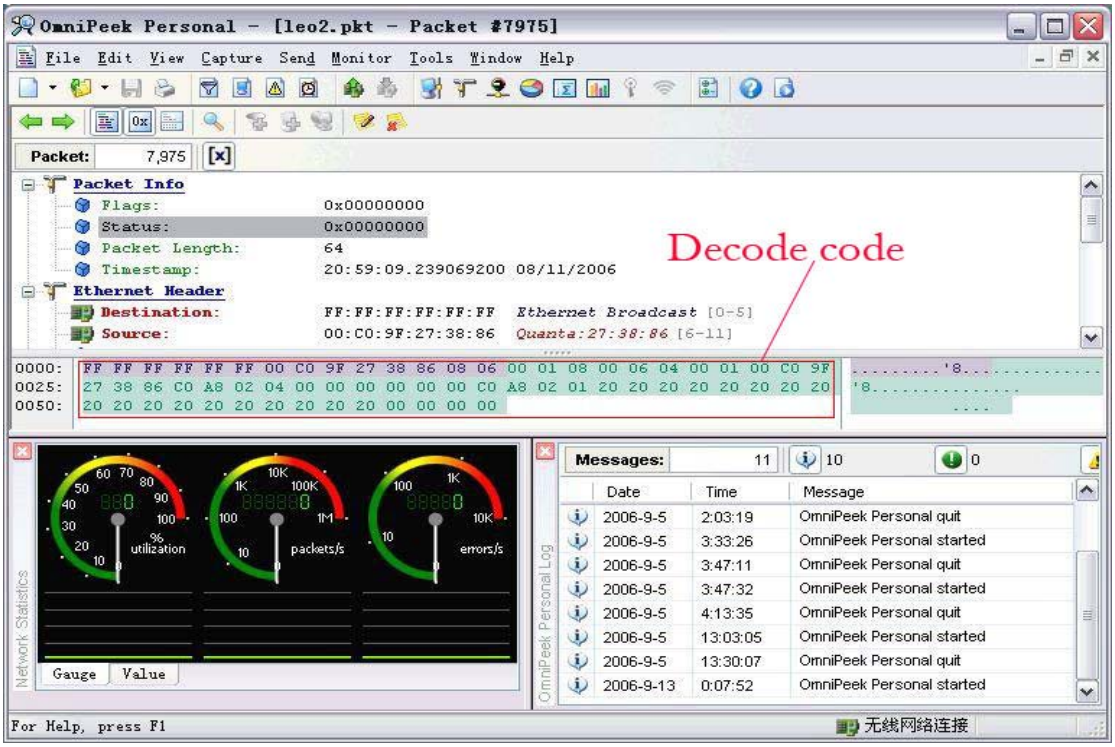

图 3-2 OmniPeek 4.0 数据包解码截屏

Figure 3-2 OmniPeek 4.0 Packet Decode, Screenshot

嗅探数据

在未加密的无线局域网中，入侵者很轻易地通过 WildPacket’s AiroPeek 获取很多无线局域网重要信息，例如 SSID。使用 AiroPeek 分析这些数据包，并且

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

针对无线局域网的不同类型的数据包来生成日志文件。使用 802. 11 协议的无线局域网，通常具有三种基本类型：数据包，网络信息和管理控制信息。

数据包提供了进一步进行分析的原始数据。管理控制信息包含了网络状态信息，比如握手、授权、联接和同步。举例来说，通过一个所谓“Beacon”管理包，可以嗅探得到一个接入点的 SSID。Beacon 包是一种定期从接入点发出的管理包。这个数据包包含了该接入点及其服务的识别信息。在这个例子中，由于管理包是采用无格式文本进行传输的，入侵者可以通过嗅探工具找到无线局域网的 SSID。就算该网络使用了 WEP 加密方式，入侵者同样可以通过嗅探该管理包来获取网络中的 SSID，见图 3-3。

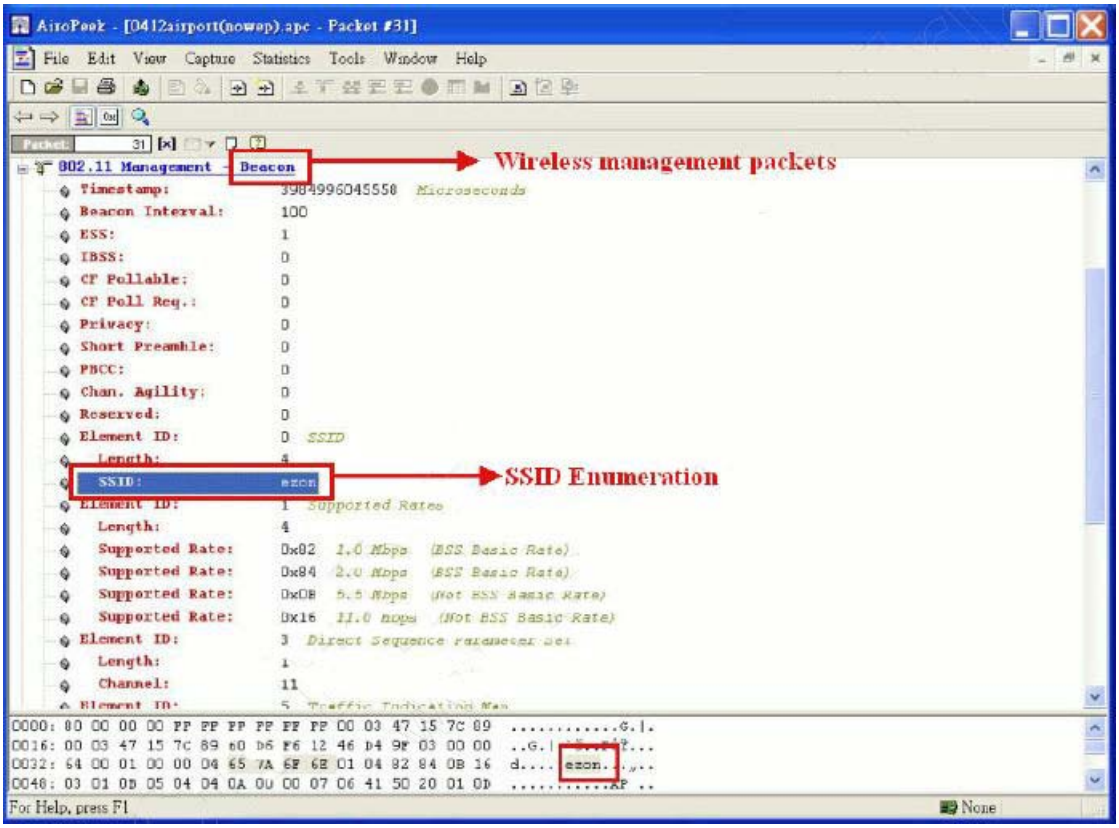

图 3-3 AiroPeek 嗅探数据截屏

Figure 3-3 AiroPeek sniffing data, Screenshot

另一方面，SmartSniff 是一款可以截取网络适配器间传输的 TCP/IP 数据包的工具，并且可以将捕获的数据按照客户端和服务器端的会话顺序进行察看。破解者可以用 ASCII 码的形式（对于基于文本的协议，如 HTTP，SMTP，POP3 和 FTP）或者 16 进制数查看 TCP/IP 会话。另外它还提供了以 HTML 页面形式显示数据包流的功能，包括协议、端口、数据大小和内容，见图 3-4。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

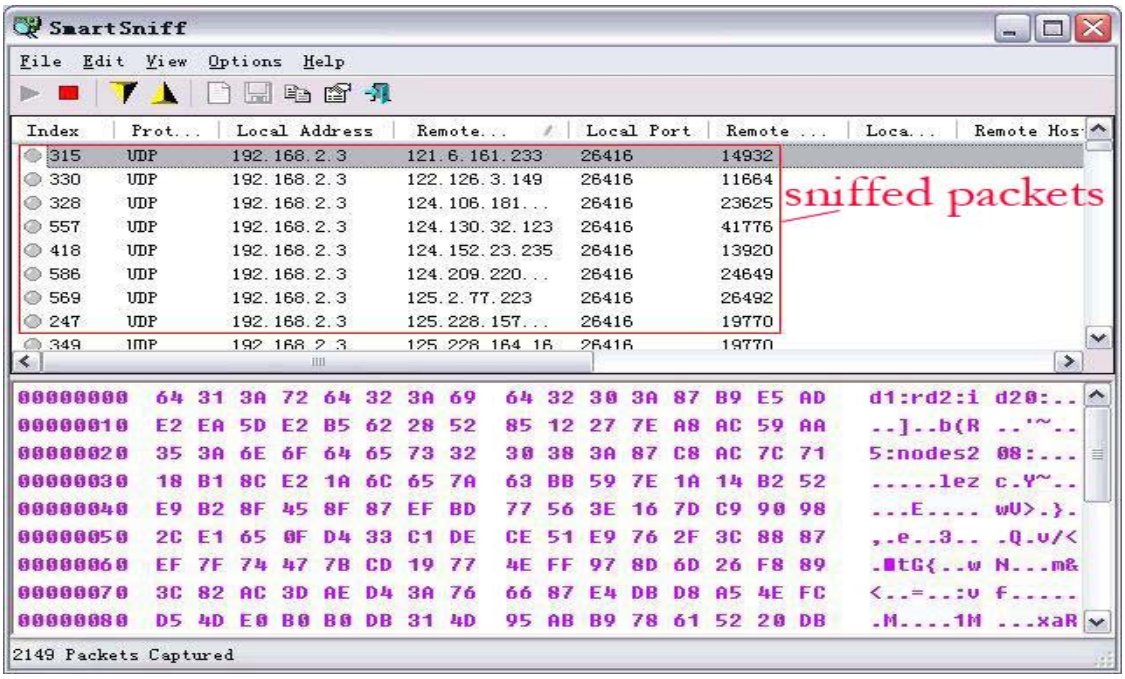

图 3-4 SmartSniff 嗅探数据截屏

Figure 3-4 SmartSniff sniffing data, Screenshot

此外，Ufasoft Sniffer 是一款局域网/无线局域网分析软件。它能截取并分析网络中的包。通过使用包驱动器，它能从网卡驱动中请求所有的包，见图 3-5。

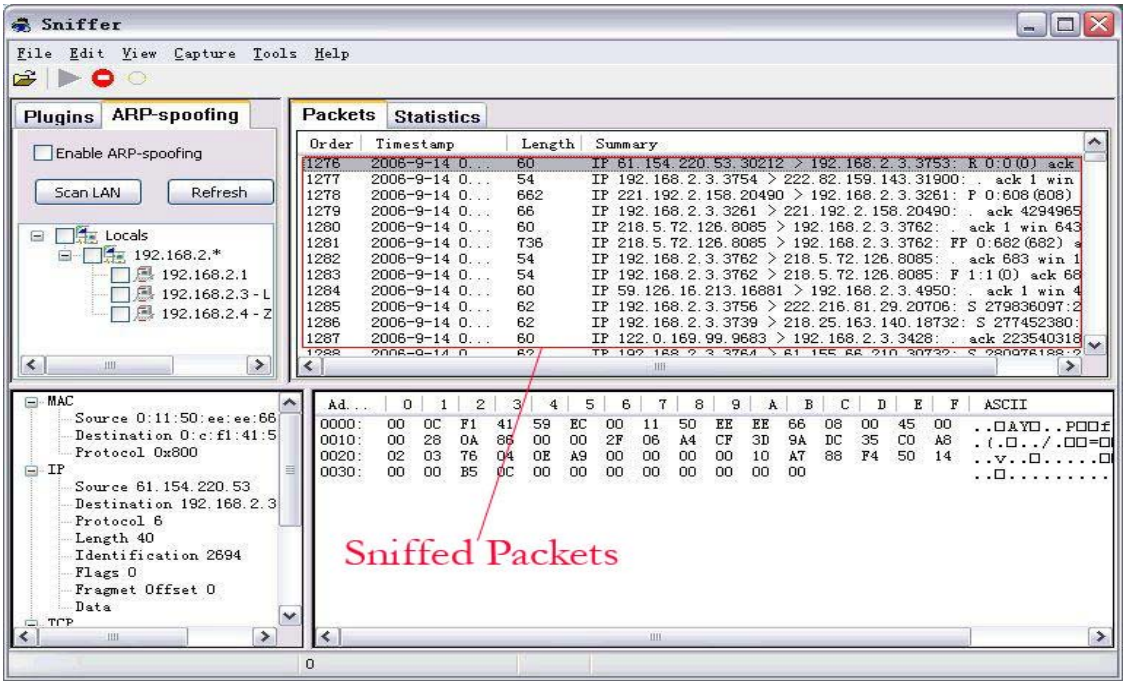

图 3-5 Sniffer 嗅探数据截屏

Figure 3-5 Sniffer sniffing data, Screenshot

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

3.1.2 SSID 截取

SSID 是附属在无线网络中所有包上的一个代码，用来标示这些包是该网络中的部分。此外，所有试图进行相互通信的无线设备都需要分享相同的 SSID。因此，入侵者可以通过 SSID 广播更容易得获得 SSID；即便无线局域网关闭了 SSID 广播，入侵者还是可以使用一些合适的工具来破解 SSID。如果窃听者在一台客户机上设置了 SSID，那么它会自动获取广播信息并且通过同样的工具加入到无线网络中。随后的一节将会描述一种可以窃听 SSID 的工具。

NetStumbler

NetStumbler 是一款用于 Windows 系统的工具，可以用来发现使用 802. 11b, 802. 11a 和 802. 11g 协议的无线局域网。它能让使用者发现无线网络的 MAC 地址、SSID、信道和是否使用了类似 WEP 的加密方法。见图 3-6

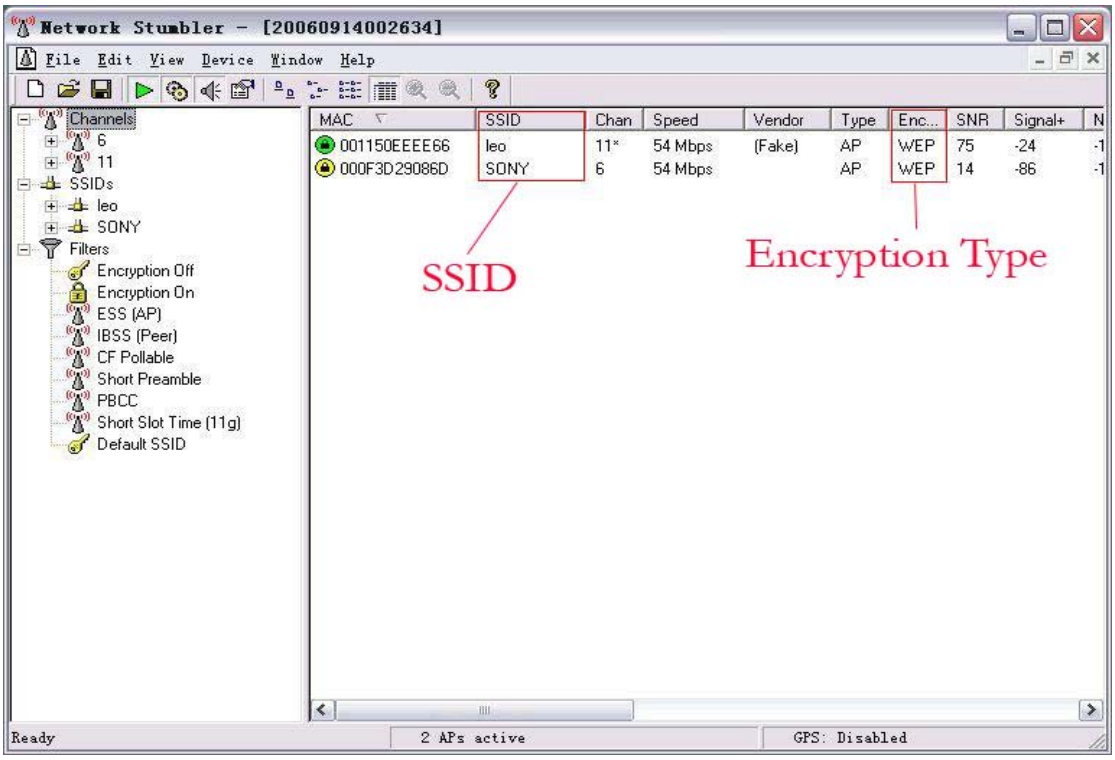

图 3-6 NetStumbler SSID 窃听截屏

Figure 3-6 NetStumbler SSID Interception, Screenshot

3.1.3 WEP 秘钥破解

WEP 秘钥破解是指获得数据并通过暴力译码或 Fluhrer-Mantin-Shamir（FMS）译码攻击来复原 WEP 秘钥。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

暴力译码攻击

暴力译码攻击基本上由使用一组秘钥对获取的 802. 11 包的加密有效载荷进行解密和通过观察 32 位校验和匹配来确定正确性。

攻击者需要一个已知的纯文本来使密钥重用。为了达到这个目的，攻击者要生成一本密钥“词典”，由一组组的初始向量空间（IVs）组成。从本质上来说，这种攻击最重要的事情就是如何优化这个“词典”的产生。多数的接入点都是用基于密钥生成算法的密码。利用这个弱点，可以更有效的破解 40 位和 100 位的无线网络。但是，如果用使用优化方法，攻击者会在对一台机器的 40 位密钥空间花上几天或者对一个分布式网络中的机器花上相当可观的时间后感到迷茫。

虽然这个攻击可以应用到很多网络中，它还是不能攻击一个 104 位 WEP 加密的网络。这项富有挑战的任务激励攻击者去改进他们的破解办法，使其更有效。因此就有了下一节所说的新的破解方法。

Fluhrer-Mantin-Shamir（FMS）译码攻击

在 WEP 中，加密密钥可以通过译码进行复原，因为 WEP 使用了一个通用的流密码 RC4。但是在非标准情况下，WEP 将基础密钥和一个 24 位的头包串联在一起，称为 WEP 初始化向量。并把这个结果用作头包 RC4 密钥。基于这点，在 2001 年 8 月 Fluhrer，Mantin，Shamir（FMS）声称一个监听器可以获得数百万个加密的包，这些包的第一个纯文本字节是已知的。这样可以通过发现 RC4 密钥的属性来削弱 RC4 密钥。根据这个步骤，入侵者可以找到一些密钥泄漏的包来计算密钥。通过检测这些解析过的包，入侵者可以找到初始化向量的弱点并且输出获得密钥。每个被解析的包都只能释放一个密钥字节。但是，通过 RC4 密钥计划运算法则，入侵者可以找到每个被解析的包都只能提供 5%的机会来获得正确的密钥字节。最近的 FMS 攻击实践已经可以从大约 100 万个包中获得静态 WEP 密钥。

此外，FMS 攻击对 WEP 是致命的。一旦 WEP 密钥被发现了，全部的安全性就丢失了。安全风险包括：

（1）破解者可以对窃听到的包进行解密并读取加密的通信，摧毁 WEP 的机密性目的。

（2）破解者可以仿制加密的包，用来被接入点接受，进入无线网络，或者攻击主机，摧毁 WEP 的完整性和授权目的。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

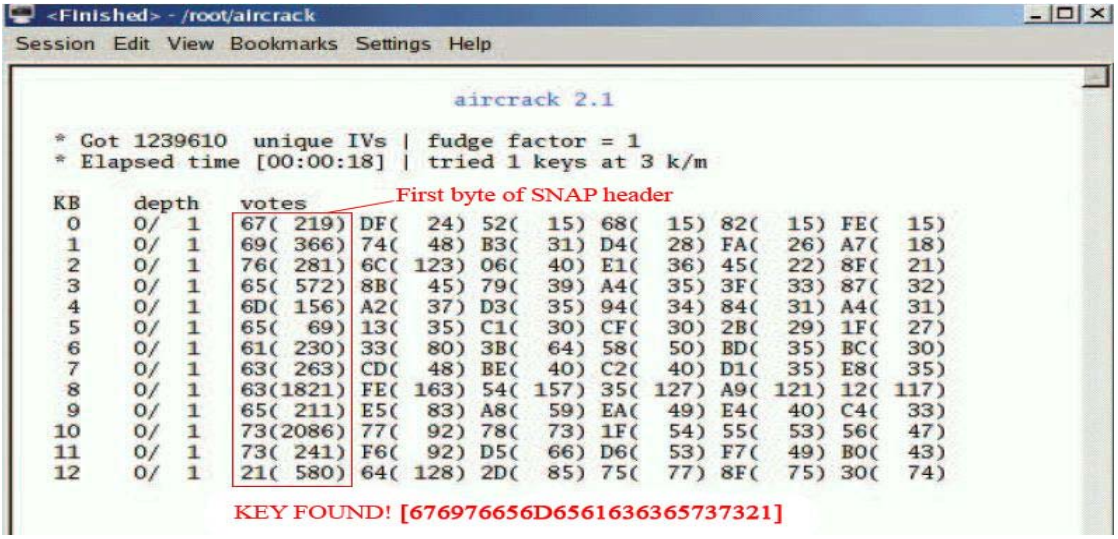

图 3-7 使用 AirCrack 进行 FMS 攻击

Figure 3-7 FMS attack using AirCrack

3.2 授权攻击

入侵者可以使用授权攻击来窃取合法用户的身份和机密信息，并进入私人网络和服务。本节中，将解释实施授权攻击的两种方法。

3.2.1 共享密钥猜测（WEP）

在 WEP 中，授权方法是通过使用带有口令和回复的公共密钥实现的。授权过程需要 4 个信息。站点通过共享密钥请求授权，接入点则回复一个 128 位的随机生成的口令。然后，口令被送回请求的站点。站点使用公共密钥和 RC4 加密法则将这个口令加密。同时，站点将加密后的口令送回接入点。接入点对加密的口令进行解密，并检查其是否符合先前随机生成的值。

问题是，攻击者可以窃听这一过程，并获得明文文本（随机口令）和相应的加密文本（加密的回复），用来找出加密算法。由于攻击者可以同时获得明文和密文，这样就可能制造出一个假的加密信息。另外破解者可以通过嗅探无线网络，从明文和密文中获得许多授权信息。这可以用来生成一个假的授权信息，而这些信息是接入点发送给正在合法有效用户的。

3.2.2 PSK 破解

虽然 WPA 提供了 802. 1x 授权框架下的暂时密钥集成协议（TKIP）可以用来防止未授权的网络访问，但许多中型的公司和小型办公室/家庭办公室

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（SOHO）用户仍然使用 WPA 预共享密钥方式，而不是基于用户的由授权服务器生成的密钥。在 WPA-PSK 中，用户必须共享一个 8 到 63 个 ASCII 字符或者 63 位 16 进制数（256 位）。和 WEP 类似，这个密码对于网络中的所有用户是一样的，并且储存在接入点和客户计算机中。攻击者可以通过截取 4 次通信的授权握手信息来找到这个密码，并用于攻击。

另一方面，在 2004 年末，WPA Cracker 由 Takehiro Takehashi 和 Georgia Tech 发布了，同时 coWPAtty 也由 Josh Wright 发布。这两个工具都是基于 Linux 系统，并且对 WPA-PSK 进行暴力穷举攻击来获得共享密码。

3.3 访问控制攻击

这些攻击通过入侵无线局域网的访问控制来进入网络。比如接入点的 MAC 过滤器和 802. 1X 端口接入控制。

3.3.1 媒体访问控制（MAC）地址欺骗

MAC 地址对于计算机网络中的网络设备来说是唯一标识。在 802. 11 无线网络中还使用了客户追踪和授权。如果入侵者可以识别出这点，那么他们就能成为无线网络的一部分并进行攻击。虽然 MAC 地址过滤通过只允许有效 MAC 地址进入网络提供了良好的安全性，仍然有许多方法可以破解 MAC 地址授权。首先，攻击者通过修改他们的 MAC 地址来试探目标无线局域网。其次，就算不是很熟练的攻击者可以修改 MAC 地址来掩盖他们的存在。此外，攻击者还可以把他们的 MAC 地址改为可以进入网络的授权地址。下面的小节将会阐述如何修改 MAC 地址，包括使用工具（如 SMAC、Technitium MAC Address Changer）或者手动来修改 MAC 地址。

修改 MAC 地址

在 Windows 系统下，MAC 地址可以通过以太网适配器的属性菜单修改。在“高级”选项中，“MAC 地址”，“本地管理地址”，“以太网地址”，“物理地址”或者“网络地址”。可能有些驱动程序并不支持这种修改 MAC 地址的方式，不过攻击者有一个更好的解决方法，就是修改系统注册表。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

这个主键包含了每个网络适配的设置。字符串的内容称为“网络地址”，并应用到适配器的 MAC 地址设置中。

在 Liunx 系统中，修改 MAC 地址更加容易，只要修改网卡配置文件即可达到修改 MAC 地址的目的。编辑“/etc/sysconfig/network-scripts/ifcfg-eth0”文件，修改其中的“HWADDR=”字段即可，如图 3-8 所示。

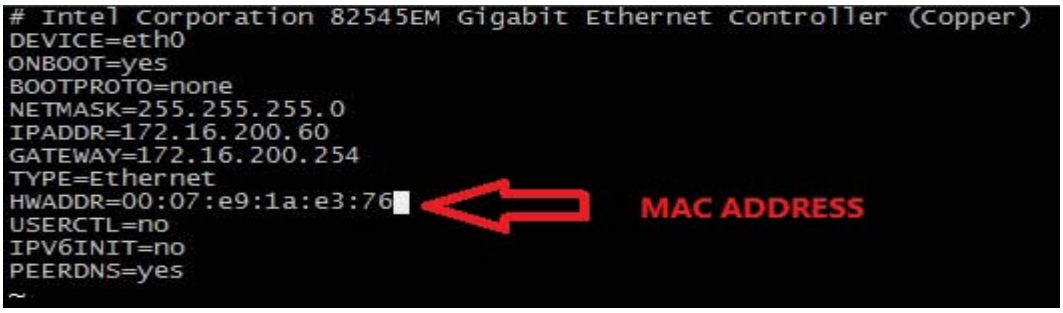

图 3-8 MAC 地址修改

Figure 3-8 MAC address Changing

使用工具修改 MAC 地址

（1）SMAC 是一款强大的，容易使用的 MAC 地址修改器，它允许用户修改 Windows2000，XP 和 VISTA 上几乎所有的网卡地址，无论生产商是否允许这样做。不过，SMAC 不能修改硬件烧入的 MAC 地址。它只能修改软件设定的 MAC 地址，新的 MAC 地址会在重启后生效。此外 SMAC 还可以在 Wi-Fi 网络中，通过隐藏 MAC 地址来保护用户的隐私。

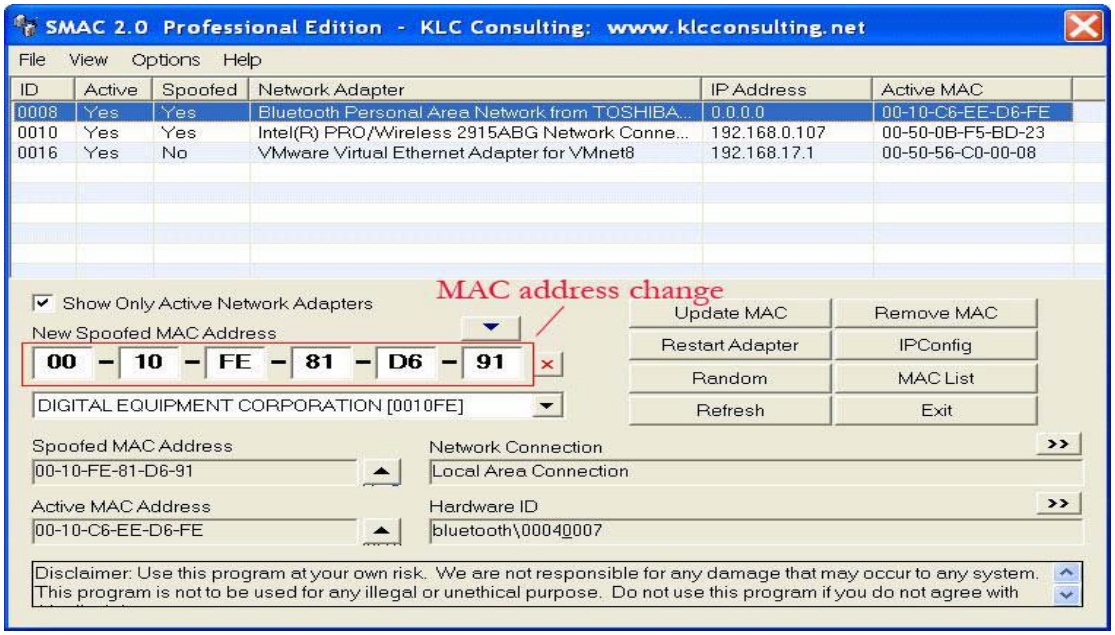

图 3-9 SMAC 2.0 更改 MAC 地址

Figure 3-9 SMAC 2.0 Changing MAC address

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（2）Technitium MAC 地址修改器，它允许用户可以忽略网络适配器的生产商和驱动来修改网络适配器的 MAC 地址。它的界面非常简单，并且提供了机器上每个网络适配器的信息。每个网络适配器的 MAC 地址都是由生产商固化在电路中的。这些固化的 MAC 地址被 Windows 驱动用来连接以太网（局域网）。这个工具可以给网卡设定新的 MAC 地址，并且忽略原有固化的 MAC 地址。

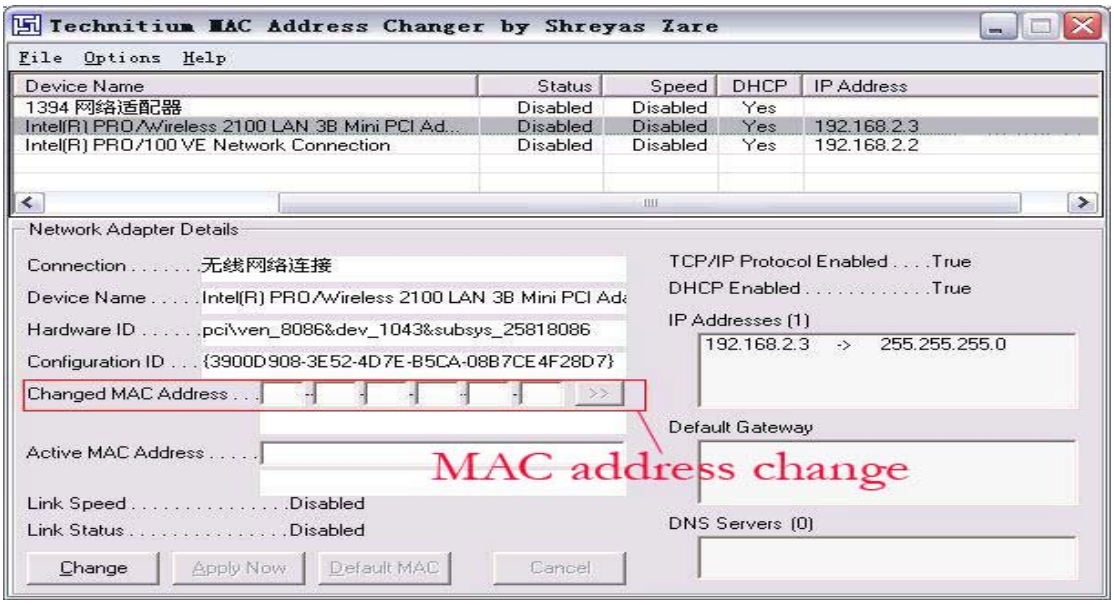

图 3-10 Technitium MAC 地址修改器

Figure 3-10 Technitium MAC Address Changer

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第四章 WEP 和 WPA 破解实验及分析

在本章中，将会阐述 WEP 破解实验，并完整地叙述一下 WPA-PAS 破解的过程。

4.1 WEP 破解试验

在试验之前，先要简要说明 WEP 安全协议的完整的加密和解密过程，以及这个两个过程中所存在的两个弱点，而这两点正是将会被用于破解 WEP 协议的关键之处。

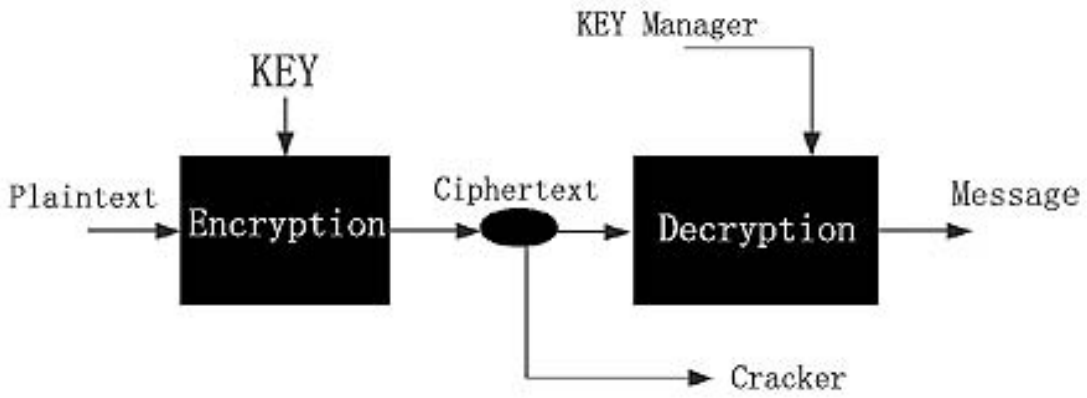

图 4-1 WEP 破解示意图

Figure 4-1 WEP Crack illustration

4.1.1 WEP 加密过程

1、计算校验和(Check Summing)

(1)对输入数据进行完整性校验和计算。

(2)把输入数据和计算得到的校验和组合起来得到新的加密数据，也称之为明文，明文作为下一步加密过程的输入。

2、加密

在这个过程中，将第一步得到的数据明文采用算法加密。对明文的加密有两层含义：明文数据的加密，保护未经认证的数据。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

⑴将 24 位的初始化向量和 40 位的密钥连接进行校验和计算，得到 64 位的数据。

⑵将这个 64 位的数据输入到虚拟随机数产生器中，它对初始化向量和密钥的校验和计算值进行加密计算。

⑶经过校验和计算的明文与虚拟随机数产生器的输出密钥流进行按位异或运算得到加密后的信息，即密文。

3、传输

将初始向量和密文串接起来，得到要传输的加密数据帧，在无线链路上传输。

4.1.2 WEP 解密过程

加密数据帧的解密过程只是加密过程的简单取反。解密过程如下。

1、恢复初始明文。

重新产生密钥流，将其与接收到的密文信息进行异或运算，以恢复初始明文信息。

2、检验校验和。

接收方根据恢复的明文信息来检验校验和，将恢复的明文信息分离，重新计算校验和并检查它是否与接收到的校验和相匹配。这样可以保证只有正确校验和的数据帧才会被接收方接受。

4.1.3 WEP 的弱点

RC4 弱点

RC4 流加密是由一个秘密密钥和初始化向量（IV）组成的，密码的输出字节数是取异或（用⊕表示），以及用来生成加密文本的纯文本：

$$C = (M \cdot c(M)) \oplus RC4(IV \cdot k) \qquad 4\text{-}1$$

真正的 WEP 数据是在每个密文数据包 C 之前添加初始化向量（IV）。

RC4 流加密调度算法由两部分组成，一个密钥计划算法和一个输出生成器。在 WEP 中，密钥计划算法使用 64 位分组密钥（40 位密钥再加上 24 位初始化向量）或 128 位密钥（104 位密钥加 24 位初始化向量），来设置 RC4 状态阵列，S。这个“S”是一个涉及 {0 … …255}的置换。输出生成器使用状态阵列 S 创建一个伪随机序列。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

攻击者可以使用第一个字节从伪随机序列推断出 RC4 密钥，因为伪随机序列是其主要弱点。这第一个字节的方程为[S+S[1][S[1]]。因此，在关键密钥生成阶段，第一个字节依赖于状态阵列中的三个值（S[1]、S[S[1]]、S[S[1]+S[S[1]])。然后，攻击者可以通过观察这些值获取密钥相关的信息。

总之，RC4 算法中伪随机序列输出的第一个字节是易受攻击的弱点。因为第一个字节的输出只取决于三个状态阵列中的值（S[1]、S[S[1]]、S[S[1]+S[S[1]])。 攻击者可以通过观察这三个值，从而分析密钥的信息。

初始化向量弱点

每个数据包都包括有 24 位的初始化向量（IV）。WEP 密钥在加密和解密无线传输的数据时，每个数据包数据包的初始化向量都会改变。初始化向量用于确保相同的纯文本数据帧。初始化向量的变化取决于提供方如何实施。许多计算机在每次当网卡初始化时，会将初始化向量置为 0，然后每次使用时增加 1。这种情况会导致密钥流将被重用，并导致针对简单口令攻击的可能性。

初始化向量是 WEP 的主要弱点。因为，初始化向量是 WEP 作为纯文本传输及作为 WEP 加密帧的前缀。这使破解者在无线局域网中窃听、拦截带有纯文本的初始化向量信息的可能性。另一方面，窃听者可以捕获数据帧，以及使用相同的初始化向量的相同密钥的加密包。此外，如果入侵者通过收集许多重复使用过的初始化向量，他就能知道纯文本内容，就可以解密加密的数据。

在 RC4 密钥计划算法中，它从基本的 WEP 密钥中生成初始化向量。在 WEP 中实施 RC4 的一个缺陷就是允许创建“弱”初始化向量空间（IVs）来解密加密文本。

通过密码学分析 RC4 算法，初始化向量的弱点可以表示为：

（A+3，N−1，X） 4−2

“A”代表入侵者知道加密密钥的前 A 个字（A = 0 初始）。“N”是 KSA（密钥计划算法）的循环。“X”是 RC4 在 IP 网络输出的数据的第一个字节。在 KSA 中，这也意味着没有元素得到交换。因此通过很多弱初始化向量，入侵者可以获得密钥恢复状态阵列。

使用状态阵列进行置换 WEP 的 KSA，弱初始化向量可表示成：

X=SB+3[1] < B+3 4−3

X+SB+3[X] = B+3 4−4

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

“S”是状态阵列。“B”是恢复用的密钥字节。

总之，一个弱的初始化向量可以从它的输出字节得到密钥信息。因为第一个初始化字节是用明文传输的。一旦获得了第一个密钥字节，就可以用来破解后面的字节。

数据完整性校验算法

WEP 加密使用的 ICV 是一种基于 CRC-32 的用于检测传输噪声和普通错误的算法。但 CRC-32 是信息的线性函数，攻击者可以篡改加密信息和 ICV，使信息表面上看起来是可信的。一旦攻击者能够实现篡改加密数据包，那么就使得各种非常简单的攻击成为可能。

因此，破解者可以设计软件来检查并收集弱初始化向量。在后面的章节中，将介绍使用弱初始化向量来破解 WEP 密钥。

4.1.4 破解工具

针对 WEP，将使用的是 AirSnort。AirSnort 可以恢复加密密钥。它通过被动地监控传输来运作，然后使用足够的数据包来计算的加密密钥。一旦收集到足够的数据包，它就可以在秒钟级别内“猜测”加密密码。AirSnort 依靠被称为“感兴趣的数据包”来捕获数据。感兴趣的数据包是指含有破解无线局域网的弱初始化向量的数据包。执行一个成功的破解所需的密钥长度依赖的感兴趣的数据包数。事实上，密钥长度是攻击无线局域网的重要考虑因素，捕获线程宽度是破解的另一个重要因素。这两个因素影响了 AirSnort 猜测正确密钥。通过设置适当的线程广度参数设置，攻击者可能会节省很多破解时间。

4.1.5 WEP 破解试验结果

AirSnort 是一个高效率的工具，因为它适用并行捕获。此外，AirSnort 会自动捕获相关联的 SSID。因此，在入侵者并不需要截取额外数据，可以节省大量的宝贵时间。

硬件和软件

（1）破解 WEP 的实验环境需要使用以下硬件设备：

笔记本电脑： CPU：1. 9GHz, Ram 1024MB

无线 AP 接入： D-Link DWL-1000 access point

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

无线网卡：　　Broadcom 802.11b/g WLAN

Cisco 340 Series Client

（2）破解实验使用到的软件：

操作系统：　　Redhat Linux（Kernel：2.6.28）

WEP 工具：　　AirSnort 0.2

模拟无线数据：　　UDP Flood

WEP 破解描述

因为要破解的是无线网络的 WEP 密钥，所以设置一台装有无线网卡的便携式计算机称之为“发送者”，用来模拟用户和必要的网络流量。同样另外设置一台便携式计算机称为“破解者”，用来嗅探破解的数据包。

首先使用“teleport”软件使“发送者”访问网站并与接入点频繁通信（模拟常见的公司通信）。然而，通信量似乎太低不足以破解（获取大约 10 个感兴趣的数据包需要 1 小时）。采用“UDP Flood”软件制作每秒 250 个数据包，等待一段时间，此时获取 10 个感兴趣的数据包的只需要 1 分钟左右。这种情况下，可以有效地捕获无线的数据包。

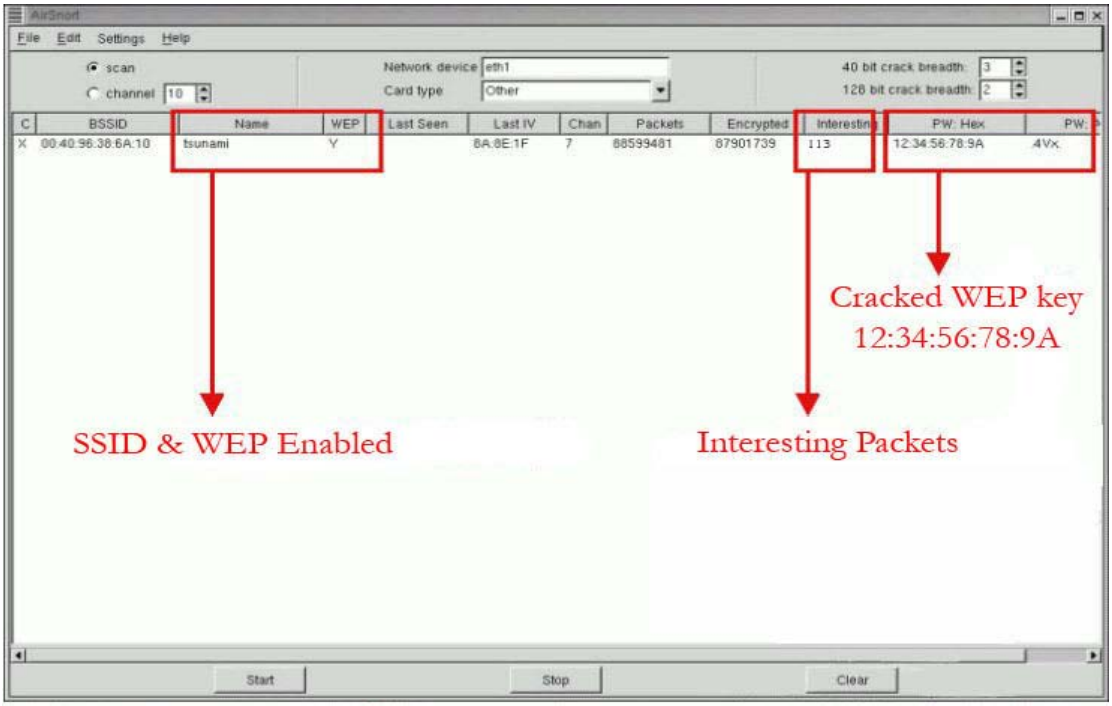

图 4-2 AirSnort WEP 破解截屏

Figure 4-2 AirSnort WEP Cracking

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

试验结果

破解时间约 1 小时。因为 AirSnort 不会记录它破解所用的时间。默认情况下捕获宽度设置为 40 位中破解 3 个。WEP 密钥是 40 位的，因为已知 64 位 WEP 加密（24 位初始化向量）。下表显示了对客户端和 D-link DWL 1000 接入点 WEP 秘钥破解的结果。

D-Link DWL-1000 访问点的 WEP 破解结果：

表 4-1 WEP 破解结果

Date	Cost time	Interesting packets	WEP key（Hex）	Success
4. 1-4. 3	71hr.	113	123456789A	Y
4. 4-4. 6	52hr	96	123456789A	N
4. 7-4. 9	44hr.	Hang up	123456789A	N
4. 10-4. 12	55hr.	Hang up	1111111111	N
4. 13-4. 15	33hr	96	1111111111	N
4. 16-4. 18	37hr	108	1111111111	Y

分析：

“感兴趣”的数据包捕获总是容易受到干扰。一开始捕获数会上升，然后随着时间的增加会有所下降。其中弱初始化向量的出现是随机的。

D-Link DWL-1000 接入点和 Cisco 340 Series 客户端，有时候会只收到 96 个感兴趣的包。发现 Cisco 的无线客户端有时候会比较安全。这其中的原因需要更多进一步的工作，从而分析出得到该结果的原因。个人推测，很可能在某些特定情况下，Cisco 的客户端会和其他品牌的接入点设备生成出较少的弱初始化向量。

4.2 WPA-PSA 破解方案

就像先前提到的（章节 2. 6. 2 和 3. 2. 2），WPA-PSK（预先共享密钥方式）是其无线局域网的弱点所在。因为设备只为一个扩展服务集（ESS）提供一个 PSK，就像他们为 WEP 密钥所作的一样。当 PSK 代替了 802. 1x，PSK 就是用来进行四次握手程序的 PMK 以及全部的层级结构 PTK。下面的部分会阐述 WPA 中如何使用 PSK，以及如何通过 coWPAtty 破解 WPA-PSK。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

4.2.1 在 WPA 中使用 PSK 的过程

首先与使用 802. 1X 生成的 PMK 相比，PSK 提供了一个更容易实施的选择。256 位的 PSK 可以直接用作 PMK。

当采用该 PSK 作为密码时，PMK 通过下面的方法可以获得：

PMK = PBKDF2（Passphrase, SSID, SSIDLength, 4096, 256） 4-5

这意味着密码、SSID 和 SSID 长度串联的字符串，通过 4096 次哈希运算将生成 256 位的值。SSID 和密码的长度对操作速度的影响很小。

PTK 是一个 keyed-HMAC 函数，使用 2 个 MAC 地址的 PMK，以及从四次握手程序中得到的两个数据包。这就是为什么整个加密层级结构变成了 PSK 中的每个处理过程。其他的信息也是可知的。

4.2.2 破解 WPA-PSA 的过程

由于时间限制，并没有足够的时间来执行破解 WPA-PSK 的试验。因此本章节中后续的 WPA 破解报告，通过叙述方式阐述使用 coWPAtty 破解工具，暴力破解 WPA-PSK 的完整过程。coWPAtty 可以系统地通过一次性测试无数的密码来尝试破解 WPA-PSK。使用 coWPAtty 的原因在于 coWPAtty 能快速排除标准的弱密码。

使用 coWPAtty 是比较简单的。攻击者需要提供一个密码组列表，一个完整的 EAP 四次握手过程，以及目标网络的 SSID 捕获文件。以下部分将说明收集四次握手和 SSID 的步骤。

收集数据

在运行 coWPAtty 之前，破解者需要在访问点和一个节点之间进行 WPA-PSK TKIP/EAP/802. 1X 协商会话。并在那里部署监听工具，例如使用 Ethereal 或者 WireShark 之类的嗅探工具来截获包含 WPA 握手信息的 cap 文件，再使用“eapol”进行过滤，此时可看到抓取的 Key 数据，如图 4-3 所示，并将其保存。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

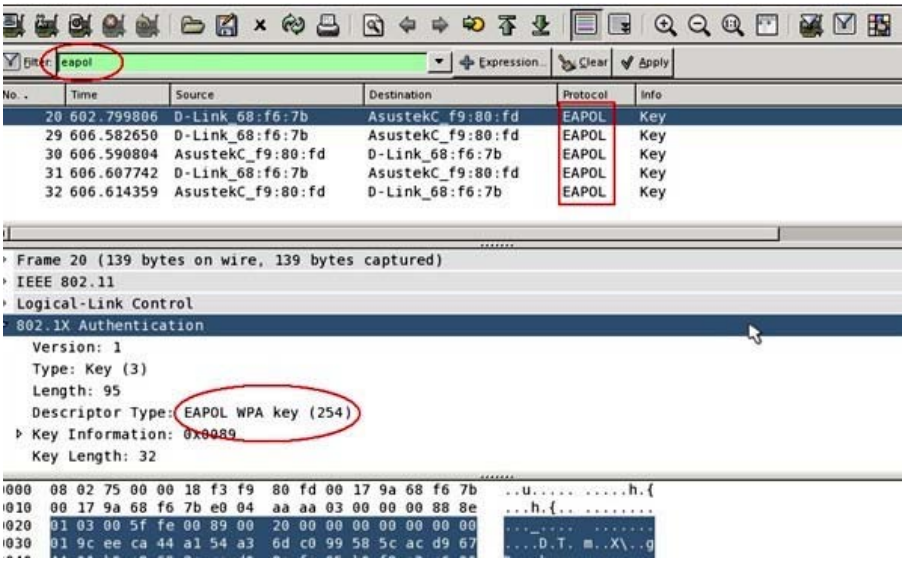

图 4-3 截取数据

Figure 4-3 Sniff Data

下面用一个已高度筛选的捕获结果举例，其中只有四个数据包。每个包都代表了四次握手过程中的一个环节。在一个正常的捕获中，破解者会看到会无线局域网管理包，以及来自其它设备的加密通信连接。攻击者必须获得所有与握手通信相关联的四个数据包。

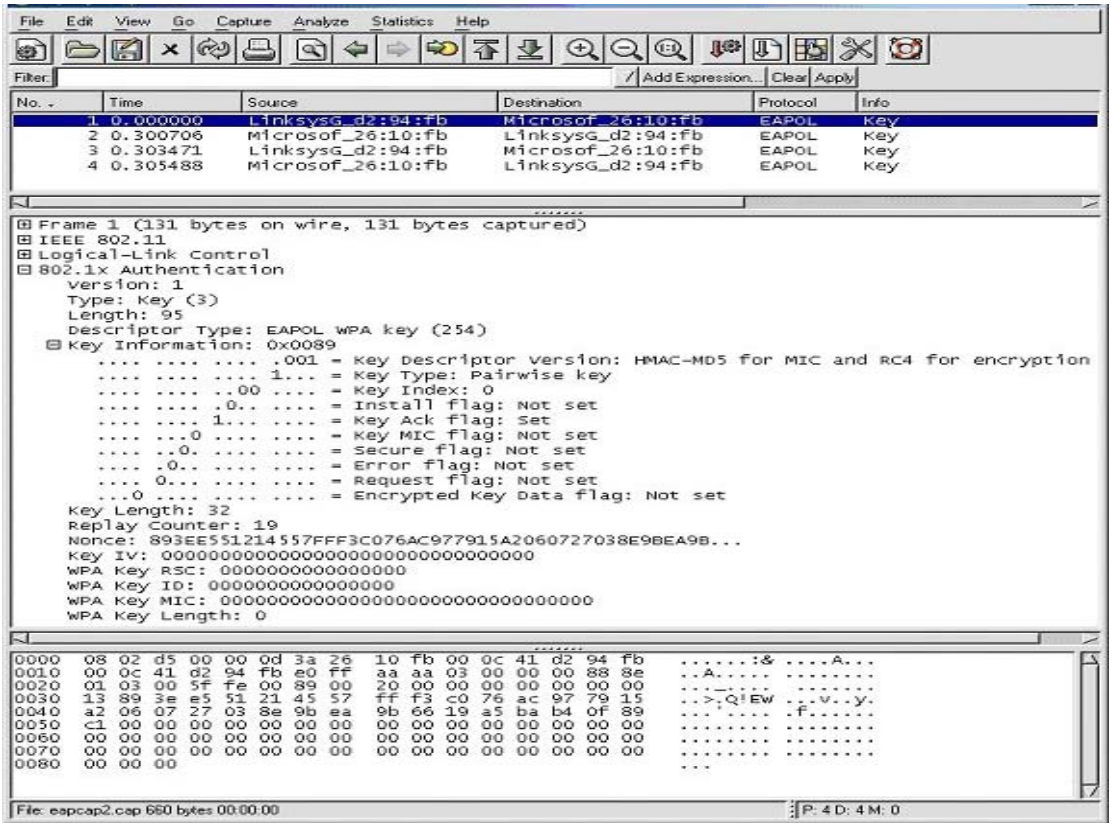

图 4-4 数据包 1

Figure 4-4 Packet 1

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

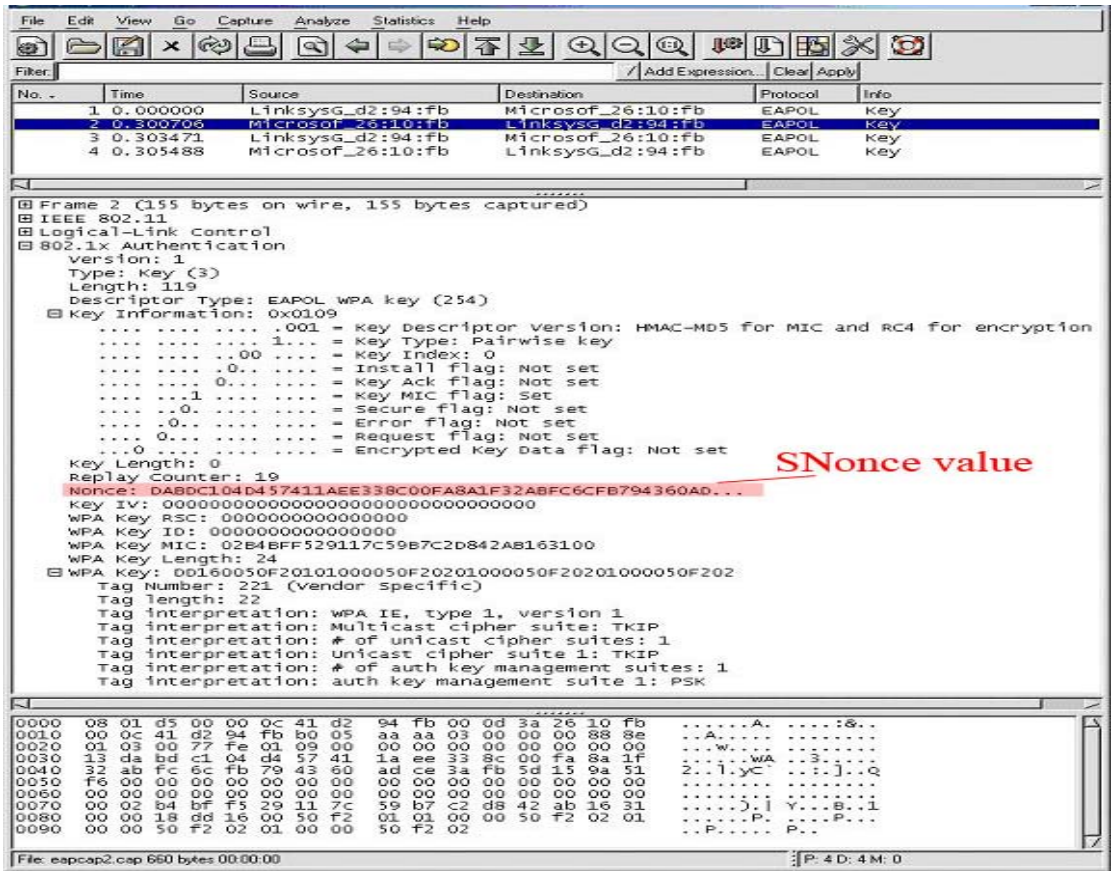

图 4-5 数据包 2

Figure 4-5 Packet 2

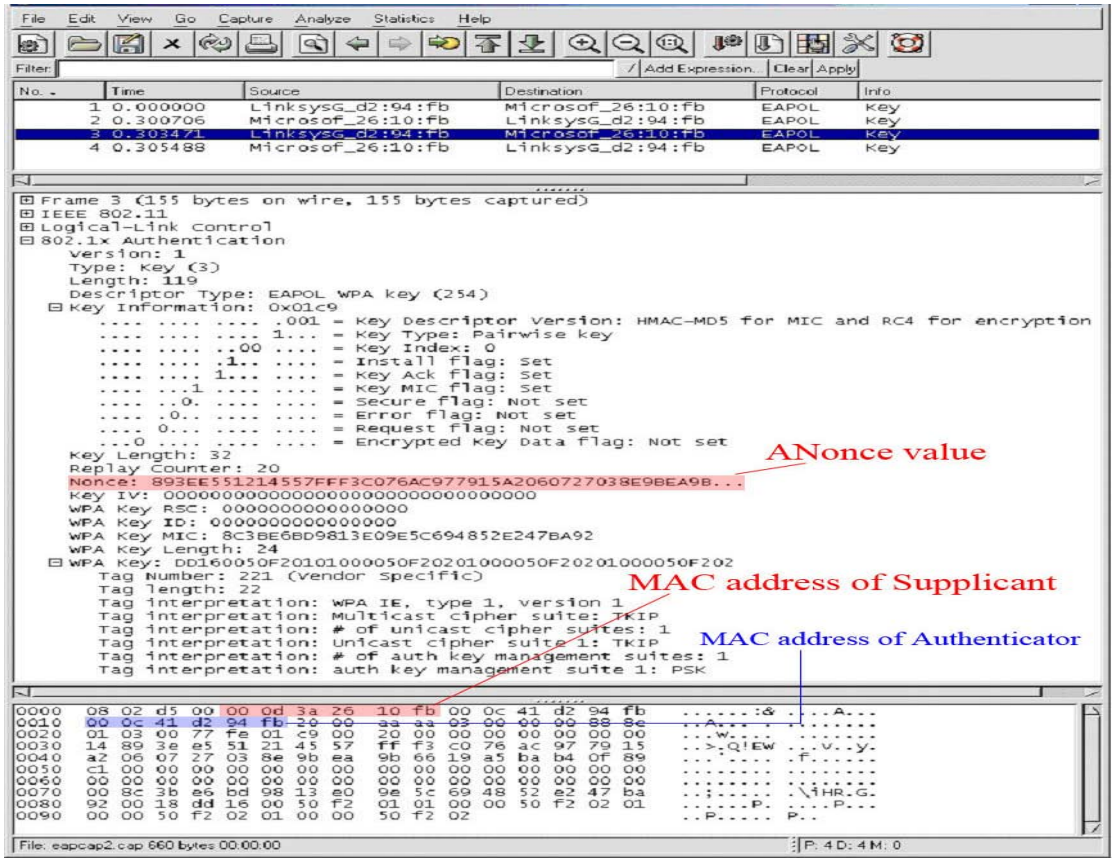

图 4-6 数据包 3

Figure 4-6 Packet 3

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

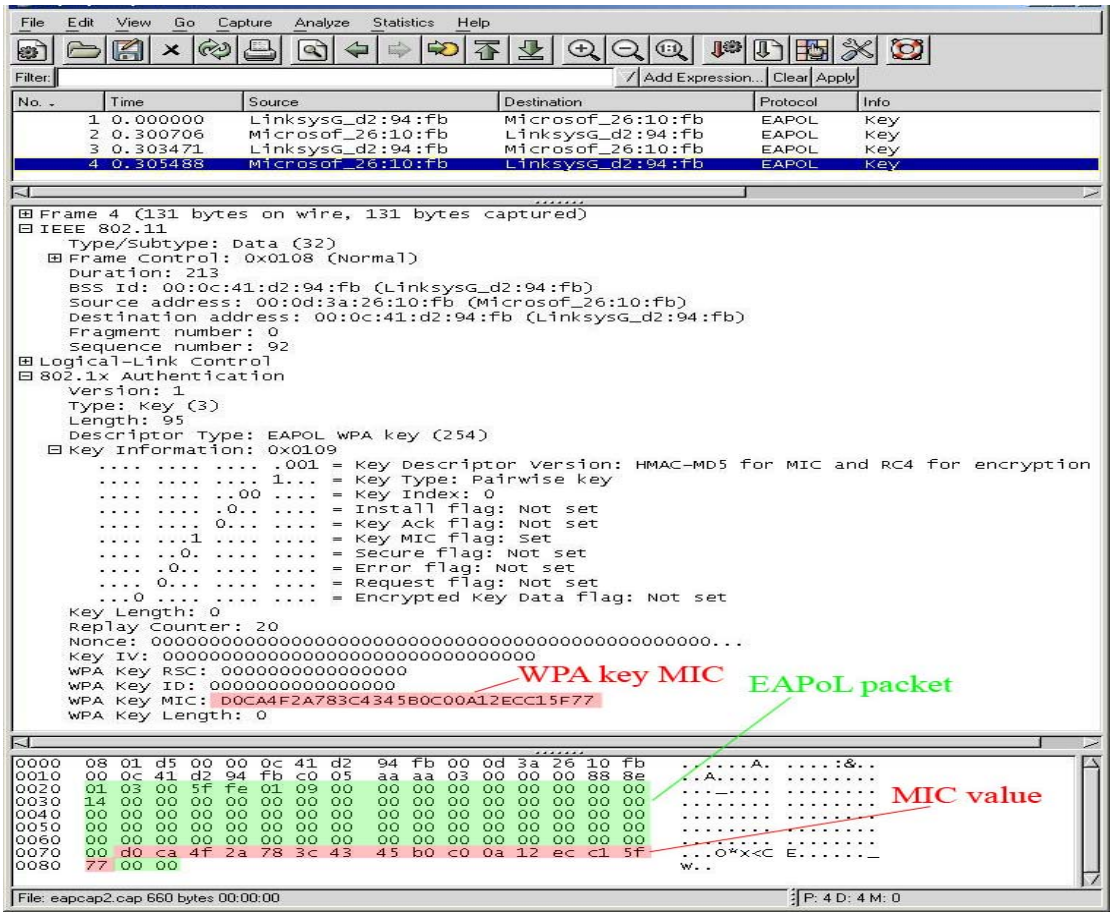

图 4-7 数据包 4

Figure 4-7 Packet 4

四个数据包通过 Ethereal 提供每个单独的数据包的详细信息。攻击者可以从数据包 2 和 3 中获得加密信息。（参见图 4–5 和 4–6）此外，数据包 3 种还提供了安装标志位。

查找 SSID

像所有的破解密码工具一样，coWPAtty 需要一个 SSID。有两种主要方法来找出 SSID。

1、通常使用程序监控一段时间的通信后，SSID 将通过用户下一次的交互发出。

2、然后使用程序（如 wlan_jack 或 essid_jack），迫使用户从网络中完全断开连接，此时不存在认证。

3、接下来无线设备会自动尝试重新身份验证，并且发送文本的 SSID，攻击者就可以通过监听获得 SSID。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

破解

假设破解者已知 SSID（linksys54gh），SSID 长度（11），从词典文件（radiustest）中生成的测试密码，以及通过 Ethereal 捕获的四次握手过程（数据包 1-4）。

然后攻击者可以使用 coWPAtty 软件，按照下列步骤来计算 PSK。

1）破解者可以通过 coWPAtty 验证所有所需的包。目的是筛选出所有的数据包中不涉及 802. 1X 身份验证类型标志的包。此外，数据包将进行检查以确保捕获了完整的四次握手过程。

2）破解这些通过 coWPAtty 捕获的所有相关信息包。

数据包 1：没有提供实际有效的数据用于破解过程

数据包 2：提供了 SNonce 值，用绿色标出，参见图 4-8。

```
0000   08 01 d5 00 00 0c 41 d2   94 fb 00 0d 3a 26 10 fb
0010   00 0c 41 d2 94 fb b0 05   aa aa 03 00 00 00 88 8e
0020   01 03 00 77 fe 01 09 00   00 00 00 00 00 00 00 00
0030   13 da bd c1 04 d4 57 41   1a ee 33 8c 00 fa 8a 1f
0040   32 ab fc 6c fb 79 43 60   ad ce 3a fb 5d 15 9a 51
0050   f6 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0070   00 02 b4 bf f5 29 11 7c   59 b7 c2 d8 42 ab 16 31
0080   00 00 18 dd 16 00 50 f2   01 01 00 00 50 f2 02 01
0090   00 00 50 f2 02 01 00 00   50 f2 02
```

图 4-8 数据包 2 中有 SNonce 值（绿色字段）

Figure 4-8 Packet 2 with SNonce value（green）

数据包 3：提供了 ANonce 值，用绿色标出。以及验证端和请求端的 MAC 地址，分别用蓝色和红色标出，参见图 4-9。

```
0000   08 02 d5 00 00 0d 3a 26   10 fb 00 0c 41 d2 94 fb
0010   00 0c 41 d2 94 fb 20 00   aa aa 03 00 00 00 88 8e
0020   01 03 00 77 fe 01 c9 00   20 00 00 00 00 00 00 00
0030   14 89 3e e5 51 21 45 57   ff f3 c0 76 ac 97 79 15
0040   a2 06 07 27 03 8e 9b ea   9b 66 19 a5 ba b4 0f 89
0050   c1 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0070   00 8c 3b e6 bd 98 13 e0   9e 5c 69 48 52 e2 47 ba
0080   92 00 18 dd 16 00 50 f2   01 01 00 00 50 f2 02 01
0090   00 00 50 f2 02 01 00 00   50 f2 02
```

图 4-9 数据包 3 中有 ANonce 值（绿色字段）和 MAC 地址（蓝色、红色字段）

Figure 4-9 Packet 3 with ANonce value（green）and MAC addresses（blue and red）

数据包 4：提供了用于计算的 MIC 值时用到的，MIC 测试值和 EAP 数据包，分别用红色和绿色标出。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

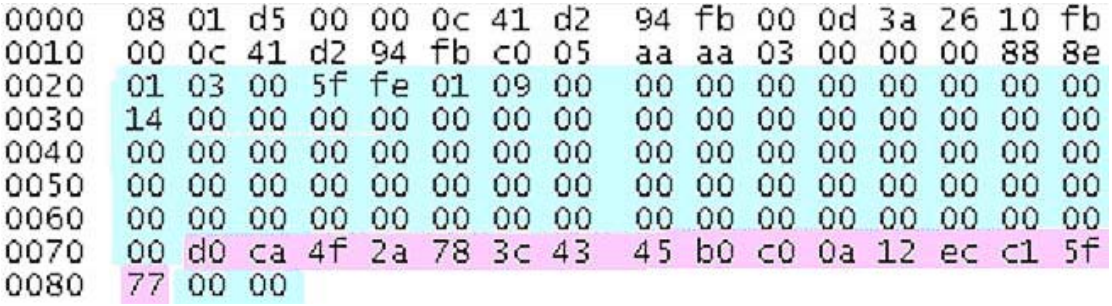

图 4-10 数据包 4 中有 EAP 数据帧（绿色字段）和 MIC 值（红色字段）

Figure 4-10 Packet 4 with EAP frame data（green）and MIC value（red）

3）破解者将通过 coWPAtty 软件检查选定的测试密码，以确保它不是少于 8 个或大于 63 个字符

4）破解者从测试密码中获得 PMK

PMK = pdkdf2-sha1（radiustest，linksys54gh，11，4096） 4-6

5）破解者使用 coWPAtty 软件从 PMK 中生成 PTK

6）破解者使用 coWPAtty 软件，根据之前获得的 PTK 中 MIC 密钥和 EAPol 信息来计算 MIC 值：

Calculated MIC=d0ca 4f2a 783c 4345 b0c0 0a12 ecc1 5f77 4-7

7）破解者通过 coWPAtty 软件把计算得到的 MIC 和捕获的 MIC 进行比较

PSK =“radiustest”

这里注意攻击往往不是一次就能成功的。有时为了可以成功截获需要反复进行攻击。破解时间取决于密码难易程度、字典包含程度、内存及 CPU 等。

分析：

破解 WPA-PSK 的过程如上所述，并不是简单的事情。因为破解者必须了解包是如何创建的，以及它们的数据是如何保护 WPA-PSK 网络的。此外，破解者还需要一个大词典文件，一台性能强大的计算机和一点“耐心”，最终得以破解、并获取想要的无线局域网密码。关于更详细的信息，可以参考“Cracking Wi-Fi Protected Access（WPA），Part 2”。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第五章 改进 WEP 和 WPA 的弱点

通过前几章的分析，目前使用的无线局域网安全认证协议都或多或少存在一些安全漏洞，需要结合多方面的策略加以完善。包括技术方面的，寻找性能更好的加密手段，然后采用双向认证，可以有效防止非法用户进入。另外加强管理，如加强控制接入点 AP 的安全，合理设置 SSID 等，经常更换并使用随机的密钥，还需要尽量掌握要使用 WLAN 的用户个数、业务类型，制定加密和使用制度。

在本章节中，将会给出几个安全对策，应对 WEP 和 WPA-PSK 现有的安全问题，实现无线网络的安全可靠。

5.1 WEP 协议漏洞的对策

正如本文 2. 6. 1 章节所分析的，WEP 安全协议存在着中间人攻击，初始向量 IV 重用，RC4 密码流算法等安全隐患，使得 WEP 协议极易被破解。因此必须对其进行改造。例如 WEP 应重新设计一个更强的密钥文本块，应用密码和加密的 MAC 函数。本节将会探讨如何解决 WEP 的脆弱性。

5.1.1 强加密散列函数替代和向量空间划分区域

对于加密的 WEP 数据包的攻击，就是先前提到过的初始向量（IV）重用攻击。由于初始化向量只有 24 位，且在数据帧中是明文传输。为避免初始化向量重用攻击，系统应确保每个初始向量针对每个密钥只用一次。否则当基站和移动节点两者都需要更新密钥时，必然产生初始向量空间（IVs）将被耗尽的问题。给攻击者提供了可乘之机。

由于在 802. 11 标准中并没有明确规定何时更换 IV 和如何更换 IV 的法则，而且 IV 采用明文直接传送。多数制造厂商在设计时为了方便，通常将 IV 的初始值设置为 0，然后往上递增，这样小数值的 IV 使用频率增大，密码流重用的几率也增大了，同时攻击者拦截到相同密码流加密的数据包的几率也就增大了。这里设想采用以下较为可行的办法来应对。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

使用强加密散列函数替代

将初始向量和密钥一起，使用一个强加密散列函数替代。这样每个包的密钥 K 将变成：

K’ = hash（IV*K） （其中 K 代表了 WEP 密钥） 5-1

通过哈希函数转换，使得初始化向量不再是简单的明文传送。同时使初始化向量的数位得到相应的扩展。

如果采用好的哈希算法，可以保证数据传输的唯一性。避免初始化向量的碰撞。

初始向量空间（IVs）划分区域

给初始向量空间（IVs）划分区域，并为基站和通信节点各分配不同的空间区域，然后在两个方向的通信上使用不同的密钥。

如此一来，在密钥更新仍然不变的情况下，可以防止重复使用密钥流的袭击。

5.1.2 丢弃密码流首字节和两阶段 HASH 函数

对于 RC4 密码流算法，可以采用一个简单的方法使得 RC4 变得更加安全。这就是，让 WEP 硬件丢弃输出密码流的第一个字节。避免攻击者通过输出的第一个字节来推断 RC4 密钥。

这种方法的可实现性较高，对于 RC4 密码流算法来说不会产生额外的资源消耗。

另外一种安全对策的实现方法是采用两阶段 HASH 函数。

加密者和解密者共享 128bits 密钥作为临时密钥，每一方必须确保对每个临时密钥和每一个初始向量不被重复使用，IV 作为从零开始的 16 bits 计数器在执行时必须确保当时 16 bits 的 IV 耗尽时临时密钥已经到期。发送端和临时密钥混合以保证不同的站点用不同的密钥加密。

用两阶段处理临时密钥：

第一阶段混合临时密钥和发送端的左（高阶）32bits，输出会被隐藏。

第二阶混合第一阶段的输出和发送端的右（低阶）16 bits 和 IV，每包密钥在被使用前要先计算好。

这种方法的优点是可以充分利用现有的设备；缺点是每个站点需较大的计算量。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

5.1.3 改进密钥安全管理方案

RC4 算法生成秘钥脆弱的问题并不完全在算法，还在于秘钥的管理机制。

因此需要对秘钥管理进行改进，具体方法是：

（1）生成一个线性空间 M，并定义它的线性操作（+，X）以及 0 和负元素，使得满足加法和乘法约束条件。

（2）对于 M 选取一组基 E={e1，e2，…，e16}构造子空间，使子空间的数目达到最大化，但在实际情况中可以根据应用场合选取它的一个子集。

（3）双方要进行通信时，先通过 challenge–responds 方式，利用 HMAC 算法求出 challenge text 的散列值，进行认证确认。通过后，双方分别产生一个随机数，使用 Diffie–Hellman 算法，传递一个初始化的字符串 S，S 包含密钥表的第一个表项的索引。在通信初始化时双方还必须协商密钥的更新频率 n（n 是一个较小的数，n 越大安全性越低），即双方通信 n 个数据帧后，就变更使用密码表项。

（4）在双方通信了 n–1 个资料帧后，管理方主动在第 n 个帧中的明文最后附加更新信息。

（5）在双方通信了一定的数据帧、密码表项更新了相应的次数以及 S 传递的更新系数用完后，双方需要再产生随机数，分配新的更新系数集。在双方传递更新系数集前，要再次验证双方身份。为了避免攻击者利用这一过程，要求双方当前的整个密码表求散列值，核对通过后才交换更新系数。通信双方成功交换更新系统后重复这一步骤。

（6）通信结束时，双方再互相核对密码表的散列值，确认后，双方保存各自同步的密码表，供下次通信所用。

安全性分析

因为在本方案中共享密钥部分是变化的，则放入 RC4 伪随机序列产生器的种子的变化范围由 24 位（IV），扩大到 128 位（IV+key）。但由于上面提到的密码表项更新的算法对系数有非零的约束，且密码子空间个数不一定满足最大值得等的要求，所以实际伪随机序列产生器的种子的变化范围比 128 位小。

对于利用初始化向量 IV 进行的字典攻击，因为 k 不再是不变的，而只要通信双方同步。因此，如果攻击者不掌握任何关于密码表及其更新内容的信息，即使他截取了足够数量的相同初始化向量 IV 的数据包也无能为力。对于

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Main-in-Middle 攻击，双方在交换一定数量的资料帧后需要认证一次。如果攻击者想利用 MIM 攻击把自己伪装成访问接入点和基站之间的透明的桥，就必须完全掌握密码表的变化，否则无法通过认证，也就无法假装成合法的通信对等体。

复杂度分析

这一无线局域网密钥安全管理方案主要的运算开销集中于三个部分：HMAC 散列算法，Diffie-Hellman 密钥交换算法，密码表项更新算法。在密码表项更新算法中，只涉及多项式运算。但主要的问题是这里的多项式运算的加法和数乘运算受约束于硬件的运算能力。最简单的情况下，可以把加法定义为各对应向量元素相加后取模，数乘定义为各向量元素乘以一个数域上的数再取模，这样的算法复杂度就大大降低。

对于 104bits 的密钥，假设密码表项数取最大值为 12012。它的基共有 13 个，每个基都有 13 个元素，这些元素只有 0 和 1 这间取值，则储存基要 169 字节。对于 1~13 号的基，需要用 4 位二进制代码编译，而每个表项对应的密码子空间的基的数目是 6，所以在这种情况下储存整个密码表每项对应的基编号约需要 4*6*12012≈36kbits。出厂时在无线网卡或访问接入点上只需要额外增加 36k+169≈37kbits 的存储空间，这对于现在的内存容量来讲是毫无问题的。使用时，由密码表项的基和 Diffie-Hellman 算法分配得到的系数形成真正的表项，每个表项为 104bits，共有 12012 项，则存储约 156kbits，就是每对 AP-MS 通信实体只需增加 156k 的内存存储开销，假设有 256 个移动基站在一个 AP 覆盖范围内与之通信，AP 所使用的服务器也只是增加 30M 的存储开销。

5.2 FMS 攻击的解决方法

在解释对抗 FMS 攻击前，大家可以先简单回顾一下 AirSnort WEP 破解试验结果（即：4. 1. 3 章节）。该实验已经完整地描述了入侵者如何使用 FMS 攻击破解 WEP 密钥的过程。侵者能通过使用工具实现破解任何使用 WEP 所保护的无线网络。这就是利用了 FMS 攻击理论，即使用一些密钥泄漏数据包来计算密钥作为破解数据包的关键。入侵者可以找到初始化向量和输出字节来获得密钥。每个被截获的破解包都泄漏密钥中的字节。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

针对 WEP 的弱点，IEEE 成立 Task Group I 专题小组（TGi）尝试解决那些使用 WEP 协议的无线网络设备的安全漏洞。在这项计划中，IEEE TGi 具有两个步骤，包含 TKIP、CCMP 和 WRAP 等三种加密方案，包括短期的解决方法（TKIP）及长期的解决方法（CCMP）。

5.2.1 短期解决方法

IEEE TGi 定义了暂时密钥集成协议或 TKIP，提供了相对 WEP 协议而言更加强大的加密机制。TKIP 是在 WEP 的外围增加了一些机制来弥补 WEP 的缺陷，具体包括：(1)利用 Michael 算法计算的信息完整性代码(MIC/MAC)；(2)每包密钥(Per-packet Key)构建机制；(3)扩展的 48bit 初始化向量(IV)和 IV 顺序规则(IV Sequencing Rules)。作为过渡解决方案的 TKIP，与 WEP 一样，都是基于 RC4 加密算法，只是对现有的 WEP 进行了改进，采取了动态的、每个用户每次通信只用一次的 WEP 密钥，加密密钥的长度由 40 位加长到 128 位，初始化向量 IV 的长度也由 24 位加长到 48 位，在一定程度上提高了数据的保密程度。然而，WEP 算法的安全漏洞是由于 WEP 机制本身引起的，与密钥的长度无关，即使增加加密密钥和初始化向量的长度也不可能增强其安全程度，也就是说 TKIP 并没有从根本上起到提高安全性的作用。以下各段落将会叙述。

信息完整码（MIC）

为了检测伪造，MIC 有三个组件。一个秘密 64 位身份验证密钥 K 只在发送方和接收方之间共享。一个标签的函数采用密钥 K 和消息 M 来组成完整性代码 T。标签 T 跟随信息 M 发送来检测伪造。这意味着接收方输入 K、T 和 M，创建自己的标记代码 T'，M 和 K。如果这两个标记代码匹配，那么该信息是正确授权的。

初始化向量顺序记录

WEP 在攻击者可能会利用此可以通过记录有效 WEP 数据包创建伪造，并且重复发送（重播攻击）。若要解决这个问题，TKIP 采用数据包序列号、发件人与收件人之间的同步。到达数据包的初始化向量是否正确决定了是否是被重播，如果是，那么就丢弃数据包。每当新的密钥设置后，发送方和接收方都要重置他们的计数器。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

各包密钥混合

为了防止攻击者通过 FMS 攻击还原 WEP 加密密钥而得到 24 位 WEP 初始化向量。TKIP 采用新的各数据包密钥混合功能。此功能是基于通过结合基础密钥，MAC 地址发送器和包顺序数而生成新的每个数据包的 WEP 密钥。为最小化计算要求，混合功能分为两个阶段。

第一阶段使用非线性替换的表或 S 盒，结合基础密钥，MAC 地址发送器和数据包序列号生成一个中间值。该中间值可以缓存并使用最多 216 个数据包。因为它包括发射机地址，混合函数在每个主机上生成一个不同的值，即使主机间使用相同的基础密钥。

第二阶段中结合数据包序号以及中间值，并生成各数据包密钥。中间值和序列号使用小密码扩散到该项中的各数据包密钥。第二阶段对数据包序列号从各据包密钥进行反序列。使用 FMS 攻击大约每个包需要花费约一百五十个周期的时间。

对于 TKIP 密钥的混合功能并没有定量的安全分析。但是密码专家认为它达到了设计的目的。

密钥重生成机制

TKIP 密钥重生成机制的体系结构是层次结构。有三种密钥类型： 临时密钥、密钥加密密钥和主密钥。

我们较早前讨论过 WEP 的重复使用初始化向量问题。为了解决此问题，并和密钥混合机制结合，TKIP 使用了特殊的密钥重建信息作为密钥更新机制。这个信息发布从站点和接入点之间的下一组临时密钥中获得的密钥。有两种类型的临时密钥，128 位的密钥进行加密，64 位的密钥保持数据完整性。

密钥重生成信息和密钥加密密钥一起，保护了临时密钥。站点和接入点在连接和重连接的时候必须建立全新的密钥体系。

为了完成这些通信，TKIP 使用 802. 1X 授权服务器来向站点和接入点发送通用密钥体系加密密钥。主密钥被用来保护这些发布的安全。它和授权机制和授权服务器是紧密相关的。每个进程都使用一个全新的无关联的主密钥。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

5.2.2 TKIP 的不足

在上一节中，描述了 WEP 的安全解决方案。在这些方法中，对每个数据包进行密钥混合是至关重要的，因为它解决了 FMS 的进攻漏洞。攻击者可以利用输出的伪随机序列的第一个字节来推断 RC4 密钥，因为伪随机序列是主要的弱点。此输出的第一字节的等式是由 S[S[1]+S[S[1]]给出。因此在密钥建立阶段，这第一个字节依赖于三个指定的矩阵值（S[1]，S[S[1]]，S[S[1]+S[S[1]]）。然后，攻击者可以通过仔细观察，推断出关于密钥的部分信息。在第二阶段对每个数据包进行密钥混合可以解决这个漏洞，因为第二阶段的混合带有数据包序列号的中间值来生成每个数据包的密钥。这意味着数据包的序列号通过每个包的密钥被去掉了相关性。因此，攻击者就无法猜测输出的第一个字节了。

然而，对每个数据包进行密钥混合，并不是一件“防弹衣”，也不能完全确保数据包的安全。对于一些特殊情况下，它仍然会被攻破。例如，攻击者改变了数据包的序列号和每个数据包的加密密钥，使得数据包很可能出现 WEP ICV 校验失败和 TKIP MIC 不正确地解密。

在另一方面，MIC 可以通过完整性代码或标签，验证信息是否被修改。这意味着，如果接收到的完整性代码可能与标记创建功能创建的完整性代码不匹配，那么该数据包将被假定为已被修改，数据包会被丢弃。然而，MIC 也带来了一些不足之处。例如，更新初始向量（IV）可能导致的身份验证密钥即可失效。这就意味着，初始向量（IV）的密钥流会被已知明文攻击的方式致使泄漏，而且如果第二个数据包加密与用相同的初始向量（IV）加密相比缩短了，那么这个 MIC 值被泄漏了。对于这种情况下，攻击者就可以破解认证密钥。

虽然 TKIP 的解决了 WEP 的脆弱性，但是 TKIP 仍然具有一些 WEP 协议的安全隐患。因此就需要采用 Counter-Mode-CBC-MAC Protocol（CCMP）长期解决方法。

5.2.3 长期解决方法

Counter-Mode-CBC-MAC Protocol（CCMP）相对于 TKIP 来说，解决了所有已知的 WEP 不足。如果不考虑已部署的硬件，高级加密系统（AES）会被选为其核心加密算法。CCMP 提供了加密，认证，完整性和重放保护。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

使用单个密钥（块密码）主要是提供机密性和完整性，减少密钥管理开销，并使指定 AES 主要计划的时间最短。由 CCMP 提供的维持完整性的另一特色是头包纯文本，以及有效负载的机密性和完整性。CCMP 设计为两种运算模式，即计数器模式(Counter Mode)和密码区块链信息认证码模式(CBC-MAC Mode)，其中计数器模式用于数据流的加密/解密，而密码区块链信息认证码模式则用于身份认证及数据完整性校验。

计数模式（CTR）

在该计数器模式（CTR）中，计数器将会首先由一个 K-CTR 的加密密钥的块密码算法进行加密。然后，MPDU 纯文本(邮件协议数据单元)则只需用 K-CTR 生成一个 MPDU 密码进行与或运算。最后，计数器将自加一次，以加密下一个纯文本。

CCM 模式

一个称为 CCM 的新模式（密码块链接模式）被设计以满足预计的安全标准。CCM 结合了两个较为知名的，并且被广泛应用的技术。CCM 使用计数器模式进行加密，以及密码块链接消息验证码（CBC-MAC）进行完整性保护。

这两个算法只采用在发送方和接收方的加密基元。CCM 的保密性和完整性都使用相同的密钥。这通常是一个危险的做法，但 CCM 使用的 CBC-MAC 初始化向量保证与计数器模式空间不重叠，可避免这种用法的不足。

针对每个会话，CCM 需要有一个全新的临时密钥。CCM 也要求用给定的临时密钥保护的每帧数据有唯一的 nonce 值。CCM 是用一个 48 位 PN 来实现的。对于同样的临时密钥可以重用 PN，这可以减少很多保证安全的工作。

CCMP 用 16 个字节扩展了原来 MPDU 大小，其中 8 个为 CCMP 帧头，8 个为 MIC 效验码。值得注意的是 CCMP 不使用 WEP ICV。

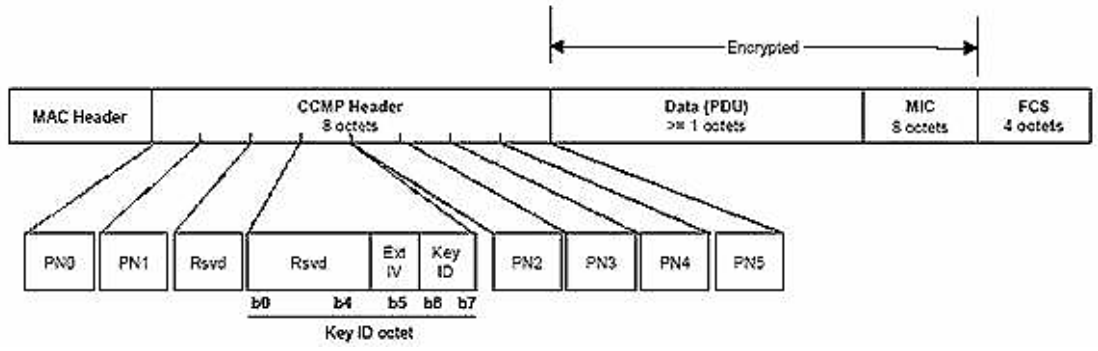

图 5-1 CCMP MPDU 扩展
Figure 5-1 Extend MPDU for CCMP

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

检查重放的规则如下：

1）PN 值连续计算每一个 MPDU。

2）每个发送者都应为每个 PTKSA，GTKSA 和 STAkeySA 维护一个 PN（48 位的计数器）。

3）PN 是一个 48 位的单调递增正整数，在相应的临时密钥被初始化或刷新的时候，它也被初始化为 1。

4） 接收者应该为每个 PTKSA，GTKSA 和 STAKeySA 维护一组单独的 PN 重放计数器。接收者在将临时密钥复位的时候，会将这些计数器置 0。重放计数器被设置为可接收的 CCMP MPDU 的 PN 值。

5）接收者为每个 PTKSA，GTKSA 和 STAKeySA 维护一个独立的针对 IEEE 802. 11 MSDU 优先级的重放计数器，并且从接收到的帧获取 PN 来检查被重放的帧。这是在重放计数器的数目时，不使用 IEEE 802. 11 MSDU 优先级。发送者不会在重放计数器内重排帧，但可能会在计数器外重排帧。IEEE 802. 11 MSDU 优先级是重排的一个可能的原因。

6）如果 MPDU 的 PN 值不连续，则它所在的 MSDU 整个都会被接收者抛弃。接收者同样会抛弃任何 PN 值小于或者等于重放计数器值的 MPDU，同时增加 ccmp 的重放计数 的值。CCMP 加密过程如下图：

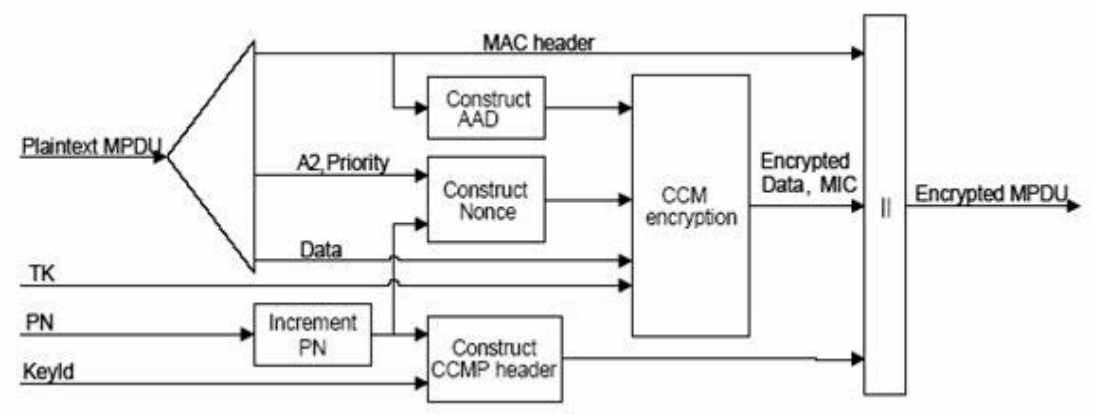

图 5-2 CCMP 加密

Figure 5-2 CMP Encryption

CCMP 加密步骤如下：

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

1）增加 PN 值，为每个 MPDU 产生一个新的 PN，这样对于同一个临时密钥 TK 永远不会有重复的 PN。需要注意的是被中转的 MPDUs 在中转过程中是不能被修改的；

2）MPDU 帧头的各个域用于生成 CCM 方式所需的 Additional Authentication Data（AAD）。CCM 运算对这些包含在 AAD 的域提供了完整性保护。在传输过程中可能改变的 MPDU 头部各个域在计算 AAD 的时候被置 0；

3）CCM Nonce 块是从 PN，A2（MPDU 地址 2）和优先级构造而来。优先级作为保留值设为 0；

4）将新的 PN 和 Key ID 置入 8 字节的 CCMP 头部；

5）CCM 最初的处理使用临时密钥 TK，AAD，Nonce 和 MPDU 数据组成密文和 MIC；

6）加密后的 MPDU 由最初的 MPDU 帧头，CCMP 头，加密过的数据和 MIC 组成。

当 AP 从 STA 接收到 802. 11 数据帧时，满足以下条件则进行 CCMP 解密；

1）WPA/802. 11i STA 协商使用 CCMP 加密；

2）Temp key 已经协商并安装完成。

CCMP 加密步骤如下：

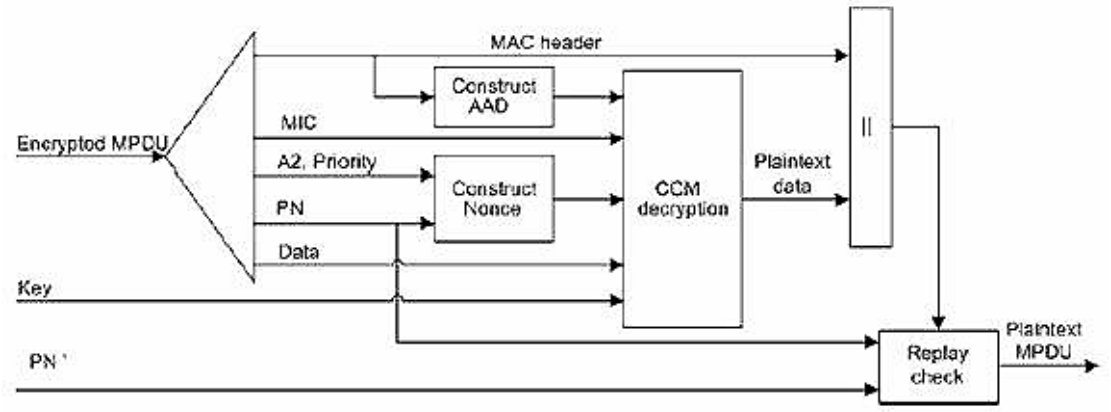

图 5-3 CCMP 解密

Figure 5-3 CMP Decryption

1）解析加密过的 MPDU，创建 AAD 和 Nonce 值；

2）AAD 是由加密过的 MPDU 头部形成的；

3）Nonce 值是根据 A2，PN 和优先级字节（保留，各位置 0）创建而来；

4）提取 MIC 对 CCM 进行完整性校验；

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

5）CCM 接收过程使用临时密钥，AAD，Nonce，MIC 和 MPDU 加密数据来解密得到明文，同时对 AAD 和 MPDU 明文进行完整性校验；

6）从 CCM 接收过程收到的 MPDU 头部和 MPDU 明文数据连接起来组成一个未加密的 MPDU；

7）解密过程防止了 MPDUs 的重放，这种重放通过确认 MPDU 里的 PN 值比包含在会话里的重放计数器大来实现，接着进行检查重放，解密失败的帧直接丢弃。

CCMP 的安全机制与 WEP、TKIP 截然不同，它除了能对数据进行保护外，还可以提供对 MAC 起始码的保护，加密引擎 AES 可靠性、安全性更高。但是 CCMP 对硬件的要求也更高。不过总的来说，CCMP 能够提供保密、鉴别、完整性及重演攻击的保护措施，是确保无线网络安全的必备条件。

5.3 WPA-PSK 攻击的解决方法

WPA-PSK 攻击是基于字典攻击的。其弱点是 PMK 是从密码，SSID，SSID 长度的组合中获得的。通过捕获四次完整的握手过程，入侵者可以使用字典攻击密码。在之前的章节中介绍了如何使用 coWPAtty 使用暴力字典攻击 WPA-PSK 完整过程。

下面提供一个改进方案，提供对抗字典暴力破解的解决方法。

5.3.1 基于 AES 的改进方案

高级加密标准（AES）是一种块密码用作加密标准。支持任意分组大小，密钥的大小为 128、192、256，可以任意组合。此外，AES 还具有应用范围广、等待时间短、相对容易隐藏、吞吐量高的优点。此算法在性能等各方面都优于 WEP 和 tkip，利用此算法加密，无线局域网的安全性会获得大幅度提高，从而能够有效地防御外界攻击。AES 提供一个 4x4 的字节阵列。当加密时，每次 AES 都有四个阶段组成：轮密钥加，字节替换，行位移变换和列混合变换。

（1）轮密钥加：

在这个步骤中，轮次的次密钥和形态结合。在每个轮次中，轮次子密钥是从主密钥中获得的，每个轮次的子密钥都接受相同的长度作为形态。轮次子密钥通过子密钥和形态的与或操作获得。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（2）字节替换：

在此步骤中，阵列中的每个自己都会用一个 8 位的 s-box 来更改。这个操作使密码不具有线性。另外，S-box 被选择用来避免固定点。

（3）行位移变换：

在此步骤中，对每行的形态都通过一定的方式进行变化。

（4）列混合变换：

在此步骤中，每个形态的每个 4 字节列将通过不变的线性变化组合在一起。

AES-CCMP 模式

下面着重讨论 AES-CCMP 模式，AES—CCMP 模式可以同时提供数据加密和数据完整性校验。AES-CCMP 数据加密部分采用 AES—CTR 模式，首先它用一个计数器产生一系列的分组作为明文输入 AES，AES 加密后输出定长密钥流，定长密钥流与信息进行异或产生密文。AES-CCMP 数据完整性校验部分采用 CBC 模式。

加密过程：

⑴将由标志，随机数和计数器构成的初始向量输入 AES 产生定长密钥流；

⑵将定长密钥流与 MAC 帧的数据部分异或，计数部分加 1；

⑶将⑵的结果作为下一个 AES 的输入，产生定长密钥流，⑶-⑵循环，直到 MAC 帧数据全部加密完为止；

⑷计数器清零，将上面得到的加密数据作为 AES 的输入，输出密钥流；

⑸将⑷得到的结果与校验码异或，完成对 MAC 帧的加密。

数据完整性校验：

⑴把由标志，随机数和计数器构成的初始向量输入 AES 产生定长密钥流；

⑵把 AES 以密码分组链接的形式对 MAC 帧头和 MAC 帧整个数据单元进行运算；

⑶将⑵得到的结果，选取一半作为 MIC（Message Integrity Code）值。

AES—CCMP 作为一个加密和数据完整性保护协议模式，很好的解决了 WEP 机制的安全问题，AES-CCMP 模式采用 AES 算法代替流密码算法 RCA，用 AES-CTR 进行加密，使加密的数据难以破解，提高了信息加密的安全强度，采用 AES CBC MAC 机制完成数据完整性校验，解决了 CRC 不能从真正意义上的信息认证问题，同时 AES-CCMP 模式在 AES-CTR 部分采用了计数器，计数

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

器产生一系列的分组作为 AES 明文的输入，解决了 WEP 机制中 Iv 重用问题。目前使用 TKIP 的 WPA 只是一个临时的过渡性方案，TKIP 与 WEP 一样基于 RC4 加密算法，但相比 WEP 算法有了很大改进，但是 TKIP 没有脱离 RCA 算法的核心机制，所以 TKIP 甚至更易受到攻击。由于考虑到产品的兼容性，采用 WPA 作为暂时过渡方案，相信 AES 成为普遍的 WLAN 安全保护技术指日可待。

5.3.2 AES 加密的不足

AES 提供了 128 位、192 位和 256 位的密钥长度。它给使用暴力字典攻击制造了难度，因为增强的密钥长度会使攻击者有比原来攻击 WPA-PSK 时更强的字典文件。除此之外，入侵者必须捕获四次通信的握手过程才能破解 WPA-PSK。AES 用户在密码中没有线性部分，并且每个字节都和每轮次的密钥进行结合。这些方法使获得四次通信的握手过程的难度大大增加。

但是，AES 并不是一个完美的标准，它还是能够通过旁路攻击被击破。攻击块密码的通常方式是使用不同版本，拥有较少轮次的密码来尝试多次攻击。例如，AES 有 10 轮 128 位的密钥，12 轮 192 位的密钥和 14 轮 256 位的密钥。另一方面，AES 不能向下兼容 802. 11b/g 硬件。因此，用户必须使用新的设备来代替 802. 11b/g 硬件。

5.4 部署多重防御

由于无线局域网数据传递的特殊性，攻击者可以轻易截获网络中各个移动站点和 AP 之间的通信数据包。从先前的章节中（4. 1. 5 和 4. 2. 2）可以得知，通过这些数据包，可以分析得到 SSID、MAC 地址、EAPol 等重要数据。攻击者可以利用这些轻易截取来的数据，对无线网络进行攻击。通过欺骗帧、截获会话帧、伪造数据帧等方式，发现 AP 中存在的认证缺陷。攻击者还可以采用被动方式监听网络流量，通过无线网络分析仪可以毫无阻碍地进行网络流量分析。

就目前情况来看，通过会话拦截实现的网络攻击是无法避免的。一旦攻击者进入无线网络，还可以通过配置快速地接入网络主干，这样使得一些边界安全设备形同虚设。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

因此对于无线局域网的安全防预，不能够仅仅依靠密码技术。根据上一章的结论，仅仅依靠 WEP 或者 WPE 来保护无线局域网依然是非常不安全的。就算采用 TKIP、CCMP，以及 AES 加密之后，无线局域网的安全依旧受到威胁。

单一的手段必然有它的不足。在实际的生产中，需要一个整体的防御架构作为安全保障。将 WLAN 的安全从单一的物理层安全延伸到各个环节，从而使用户在使用 WLAN 时能够像使用有线网络一样安全。

5.4.1 启用 Radius 认证服务

对于大型无线局域网络，要求更高的安全性。对它的管理不仅需要可以自动变更密钥安全认证机制，还需要更多安全性功能，从而满足更多用户和更复杂安全性的要求。

要组建一个能够支持上千名用户，具有先进加密和认证技术的大型系统通常需要一套能够进行集中化管理的安全性解决方案。这就需要通过 Radius（拨号用户远程认证服务）进行实现。Radius 能够对授权访问网络资源的网络用户进行集中化管理。所有这些是无法全由一台无线局域网接入点设备完成的。

支持 802. 1x 协议的 Radius 技术提高了企业级无线局域网用户的认证能力。为了提高 WLAN 服务的数据安全性，IEEE 802. 1x 和 IEEE802. 11i 中使用了 EAPOL-Key 的协商过程，设备端和客户端实现动态密钥协商和管理。同时通过 802. 1x 协商，客户端和设备端协商相同的一个密钥 PMK（参见 IEEE802. 11i），进一步提高了密钥协商的安全性。802. 1x 支持多种 EAP 认证方式，如 EAP-TLS、EAP-PEAP、EAP-TTLS、EAP-MD5、EAP-SIM 等，其中 EAP-TLS 为基于用户安全证书的身份验证。EAP-TLS 是一种相互的身份验证方法，也就是说，客户端和服务器端进行相互身份验证。在 EAP-TLS 交换过程中，远程访问客户端发送其用户证书，而远程访问服务器发送其计算机证书。如果其中一个证书未发送或无效，则连接将终断。

在无线局域网应用中，当 EAP TLS 认证成功时，客户端 PAE 和 Radius 服务器会对应产生公用的对称的 Radius Key，Radius 服务器会在认证成功消息中将 Radius Key 通知设备端 PAE。客户端 PAE 和设备端 PAE 会根据该 Radius Key，客户端 MAC 地址以及设备端 MAC 地址，产生种子密钥 PMK 以及对应的索引

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

PMKID。根据 IEEE802. 11i 协议定义的算法，设备端 PAE 和客户端 PAE 可以获得相同的 PMK，该种子密钥将在密钥协商过程（EAPOL-Key 密钥协商）中使用。

802. 1x 具体认证过程如下：

（1）无线终端向 AP 发出请求，试图与 AP 进行通讯；

（2）AP 将加密的数据发送给验证服务器进行用户身份认证；

（3）验证服务器确认用户身份后，AP 允许该用户接入；

（4）建立网络连接后授权用户通过 AP 访问网络资源；

这种方案提供较高的安全级别，比较适合用于对数据保密程度较高的网络。

5.4.2 使用 VPN 方式加密

VPN 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。用户可以借助 VPN 来解决无线网络的不安全因素。该方法可以配合 802. 1x 协议的 Radius 认证技术，一同实现较高级别的安全认证。

通常的做法是将 WLAN 设置成单独的局域网部分，并通过 VPN 网关将该部分连接到组织或机构局域网上。利用 VPN，所有无线用户在得到许可访问组织或机构局域网之前首先由 VPN 网关进行鉴权。VPN 网关只向拥有机器中所具有的有效软件证书或令牌的用户授权。客户机到 VPN 服务器的数据包使用 IPSec 加密。因此黑客将无法破解这些数据包的内容。这些安全措施需要额外的程序（如要求用户登录 VPN 网关、在所有无线机器上安装 VPN 客户端程序）。

但是 VPN 会产生瓶颈问题，而且由于 VPN 设备本身在做加密和解密的工作，也会带来的性能上的损失。但是 VPN 提供的安全级别较高，这也表示 VPN 方式可以带来更高的安全性。

5.4.3 合理隔离网络

对于安全网络来说，应该把 VPN 服务器放在非军事区（Demilitarized Zone，DMZ）中，接入点应置于防火墙外部。DMZ 是一个添加在受保护网络和外部网络之间的网络，可以将敏感信息和公用信息隔离，以便提供另外一层安全。DMZ 是分层安全设计的一个优秀实例，通过将 VPN 服务器隔离到一个网络段中，两个网络间数据共享的几率几乎为 0。对已经获得 DMZ 中某个服务器访问权限的

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

攻击者而言，这种隔离能阻止他在网络中的进一步渗透，这也是设立 DMZ 的目的所在——隔离并限制攻击者所能造成的破坏。

5.4.4 配置访问控制列表

为了进一步保护无线网络，可以使用访问控制列表 ACL。虽然不是所有的无线接入点都支持这项特性，但如果您的网络支持，您就可以具体地指定允许哪些机器连接到接入点。并且还可以设置对网络端口进行封锁，从而阻止不在允许列表内的主机接入 AP，或者直接对 AP 的端口扫描。

这样可以直接杜绝黑客对无线局域网接入点进行攻击。这种 ACL 方式可以实现对 IP、MAC、TCP 以及 UDP 等过滤。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

第六章 小结

近年来，越来越多的个人和公司开始使用无线局域网，无线局域网的安全问题已经不容回避。自从 IEEE 802.11 标准制定后，无线安全机制在不断改进和明晰，比如 WEP 和 WPA。然而，这些安全机制都有弱点。例如，一个攻击者可以通过窃听输出包的第一个字节来获得伪随机序列，进而推演出 RC4 密钥。另外，攻击者也可以通过找到密钥泄漏包来找到弱的初始化向量和输出字节而获得 WEP 密钥。另一方面，当用户实施 WPA-PSK 时，WPA 机制也暴露出了一些不足。攻击者可以利用这些不足进行 WPA-PSK 暴力攻击破解，因为所有的无线网络用户都必须在接入点和客户端之间使用共享的通关文。自从这些新的安全机制被公布以来，WEP 和 WPA 的弱点通过使用 TKIP 和 AES 来加以克服。

在本课题中，不仅描述了 IEEE 802.11 安全协议的基础知识（包括 WEP，WPA 和 WPA2）。还介绍了破解无线局域网的方法和手段。通过实验，完成了使用 AirSnort 对 WEP 密钥进行解密的实验。以及实验证明了 FMS 攻击可以通过特定工具实现。然后通过叙述一个完整的 WPA-PSK 破解过程，来说明破解 WPA 安全协议存在的安全隐患。在最后一部分，根据实验结果以及相关文献，提出了改进 WEP 和 WPA 的解决方案，以及合理化建议。从而加强无线局域网的安全性。

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

缩略语：

AAD:	Additional Authentication Data
AES:	Advanced Encryption Standard
ANonce:	AP nonce
AP:	Access Point
BSS:	Basic Service Set
CBC-MAC:	Cipher Block Chaining Message Authentication Code
CCM:	Cipher-block Chaining Mode
CCMP:	Counter-Mode-CBC-MAC Protocol
CTK:	Counter Mode
DS:	Distribution System
DSSS:	Direct Sequence Spread Spectrum
EAP:	Extensible Authentication Protocol
ESS:	Extended Service Set
FMS:	Fluhrer-Mantin-Shamir cryptanalysis attack
GTK:	Group Temporal Key
IBSS:	Independent Basic Service Set
IEEE:	Institute of Electrical and Electronics Engineers
IV:	Initialization Vector
KCK:	Key Confirmation Key
KEK:	Key Encryption Key
KSA:	Key Scheduling Algorithm
LAN:	Local Area Network
MAC:	Media Access Control
MIC:	Message Integrity Check
MPDU:	Message Protocol Data Unit
NIC:	Network Interface Card
NIST:	National Institute of Standards and Technology
OFDM:	Orthogonal Frequency Division Multiplexing
OXR:	exclusive OR
PDA:	Personal Digital Assistant
PEAP:	Protected Extensible Authentication Protocol
PHY:	Physical layer
PMK:	Pairwise Master Key
PSK:	Pre-Shared Key
PTK:	Pairwise Transient Key
RADIUS:	Remote Authentication Dial-In User Service
SOHO:	Small office/home office
SSID:	Service Set Identifier
STA:	Station
SNonce:	STA nonce
TGi:	IEEE Task Group I
TGn:	IEEE Task Group N

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

TKIP:	Temporal Key Integrity Protocol
TK:	Temporal Key
TLS:	Transport Layer Security
TTLS:	Tunneled Transport Layer Security
VPN:	Virtual Private Networks
WEP:	Wired Equivalent Privacy
WISP:	Wireless Internet service provider
WPA:	Wi-Fi Protected Access
WPA2:	WPA security protocol
Wi-Fi:	Wireless Fidelity; Wi-Fi（sometimes written Wi-fi, WiFi, Wifi, wifi）is a trademark for sets of product compatibility standards for wireless local area networks（WLANs）
WLAN:	Wireless Local Area Networ

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

参考文献

[1] Berghel, H. and Uecker, J (2005), Wi-Fi attack vectors, [Access 12th July 2006].

[2] Bhagyavati, and Summers, W. C. and DeJoie, A. (2004), Wireless Security Techniques: An Overview, [Access 1th July 2006].

[3] Borisov, N. and Goldbeerg, I. and Wanger, D. (2001), Intercepting mobile communications: The insecurity of 802.11, [Access 15th July 2006].

[4] Cam-Winget, N. and Housley, R. and Wagner, D. (2003), SECURITY FLAWS IN 802.11 DATA LINK PROTOCOLS, [Access 3rd July 2006].

[5] DeLaet, G. and Schauwers, G. (2004), Cisco Network Security Fundamentals: Wireless Security, [Access 25th July 2006].

[6] Ferguson, N. and Kelsey, J. and Lucks, S. and Schneier, B. and Stay, M. and Wagner, D. and Whiting, D. (2000), Improved Cryptanalysis of Rijndael, [Access 27th July 2006].

[7] Fluhrer, S. and Mantin, I. and Shamir, A. (2001), Weaknesses in the key scheduling algorithm of RC4, [Access 28th July 2006].

[8] Fogie, 2005, Cracking Wi-Fi Protected Access (WPA), Part 2, [Access 12th August 2006].

[9] Griffith, E. (2004), 802.11i Security Specification Finalized, [Access 5th July 2006].

[10] He, C. and Sundararajan, M and Datta, A and Derek, A. and Mitchell, J. C. (2005), A Modular Correctness Proof of IEEE 802.11i and TLS, [Access 2th September 2006].

[11] Housley, R. and Arbaugh, W. (2003), SECURITY PROBLEMS IN 802.11-BASED NETWORKS, [Access 11th July 2006].

[12] IEEE (2003a), IEEE STD 802.11 1999 Edition, [Access 15th July 2006].

[13] IEEE (2003b), IEEE STD 802.11a 1999 (R2003), [Access 15th July 2006].

[14] IEEE (2003c), IEEE STD 802.11b 1999 (R2003), [Access 15th July 2006]

[15] IEEE (2004), IEEE STD 802.11i 2004, [Access 15th July 2006]

[16] ISAAC, 2006, Security of the WEP algorithm, [Access 12th July 2006].

[17] Machta, D. (2003), Securing WLAN: from WEP to WPA, [Access 28th July 2006].

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[18] Mac Michael, J. L. (2005), Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode, [Access 5th August 2006].

[19] Moen, V. and Raddum, H. and Hole, K. J. (2004) , Weaknesses in the Temporal Key Hash of WPA, [Access 7th August 2006].

[20] Moskowitz, R. (2003), Weakness in Passphrase Choice in WPA Interface, reprinted in Wi-Fi Networking News, [Access 18th August 2006].

[21] Newsham, T. (2001), Cracking WEP keys, [Access 28th July 2006].

[22] Phifer, L. (2006), Wireless attacks, A to Z, [Access 18th July 2006].

[23] Prince, D. J. (2006), Geeks Manual Part B: Alphabet Soup: wireless standards, [Access 8th July 2006].

[24] Rogaway, P. and Bellare, M. and Black, J. (2003), OCB: a block-cipher mode of operation for efficient authenticated encryption, [Access 28th July 2006].

[25] ShanmugaLakshmi, R. and Shalini, G. and Vijayalakshmi, C. (2006), Disguising Text Cryptography Using Grey Level Modification Technique in Digital Images, [Access 18th July 2006].

[26] Stubblefield, A. and Ioannidis, J. and Rubin, A. D. (2001), Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, [Access 10th July 2006].

[27] Stubblefield, A et al. (2004), A key recovery attack on the 802.11b Wired equivalent privacy protocol (WEP), [Access 6th July 2006].

[28] Wright, J and GCIH and CCNA (2003), Detecting Wireless LAN MAC Address Spoofing, [Access 12th August 2006]

[29] Thomas, T. M. (2004), Wireless Security, [Access 15th July 2006].

[30] Wi-Fi Alliance, 2003, Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, [Access 6th July 2006].

[31] Wild Packets (2006), Real-Time Network Analytics for Enterprise WLANs, [Access 12th July 2006]

[33] 吴越、曹秀英、胡爱群、毕光国，无线局域网安全技术研究[J]电信科学, 2002,(06)

[34] 刘琦，无线局域网安全技术的分析与改进[D]. 中国人民解放军国防科学技术大学, 2002

[35] 孙宏、杨义先，无线局域网协议 802.11 安全性分析[J]电子学报, 2003,(07)

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[36] 张龙军、张明，无线局域网 IEEE802.11 标准安全机制研究[J]大连理工大学学报, 2003,(S1)

[37] 谭钦红，无线局域网安全与认证的研究和公用 WLAN 的应用[D]. 重庆大学, 2004

[38] 李林、李晖、王丹卉，基于 802.1X 协议的无线局域网安全性研究[J]电子科技, 2004,(07)

[39] 秦杰生、曹秀英，在无线局域网(WLAN)中 EAP-TLS 认证的应用[J]计算机安全, 2004,(09)

[40] 程民利，无线网络中的安全技术研究[D]. 东南大学, 2005

[41] 冯茜、王玉东、张效义，无线局域网 802.1X 认证机制安全分析及改进[J]无线电工程, 2005,(02)

[42] 李林，无线局域网安全机制的分析与研究[D]. 西安电子科技大学, 2005

[43] 赵琳，无线局域网 802.11b/11i 协议安全机制研究[D]. 解放军信息工程大学, 2006

[44] 周劼，无线局域网安全与认证系统的研究[D]. 东华大学, 2006

[45] 周贤伟、刘宁、覃伯平，IEEE 802.1x 协议的认证机制及其改进[J]计算机应用, 2006,(12)

[46] 王小军、陆建德，基于 802.11i 的四次握手协议的攻击[J]计算机与现代化, 2006,(05)

[47] 赵海霞、周庆忠，基于 WLAN 的入侵检测系统研究[J]科技广场, 2006,(05)

[48] 刘垚峰、王相林，WLAN 安全方案及 802.11i 标准研究[J]计算机工程与设计, 2006,(13)

[49] 王勇、陆际光，基于 802.11i 的 WLAN 认证机制分析及其改进策略[J]中南民族大学学报(自然科学版), 2006,(02)

[50] 余斌霄，无线网络的安全性[D]西安电子科技大学, 2006

[51] 黄玉划，无线网络安全机制中的对称密码学问题研究[D]东南大学, 2006

[52] 李兴华，无线网络中认证及密钥协商协议的研究[D]西安电子科技大学, 2006

[53] 吴振强，无线局域网安全体系结构及关键技术[D]西安电子科技大学, 2007

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

致谢

首先感谢上海交通大学的导师李小勇和陈凯博士，在完成该论文和研究工作的过程中，得到了两位导师的无私帮助和细心指导。他们深厚的科学素养、严谨的治学态度、勤勉的工作精神和谦和的待人品德，使我受益匪浅。课题的每一步进展都离不开导师的谆谆教导和鼓励，在此向两位导师表示由衷的感谢和敬意！

同时也向彭希彤老师、王京峰老师以及上海交通大学信息安全学院的各位老师，给予我的大力支持和帮助，使我顺利地完成了此项论文研究工作！

最后要在此感谢未能一一提及的所有给予我帮助和支持的朋友和同学，感谢你们！

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

攻读学位期间发表的学术论文目录

[1] 颜炳风, 《无线局域网的安全机制、漏洞破解以及解决方案》, 《科技信息》2010 年第 27 期

?1994-2017 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net