WiFi通信的安全分析

刘幸酉
上海交通大学电子信息与电气工程学院　上海　200030

摘　要　通过分析当前应用广泛的WiFi技术以及WEP的工作过程，讲述其中存在的安全问题，从发现的缺陷中讲解破解方法，同时简单介绍国产WAPI技术情况。

关键词　WiFi；WEP；WPA；WLAN；WAPI；通信安全

引言

WiFi技术自上世纪末到现在，发展不过十来年，但应用非常广泛。WiFi最初是由1999年成立的WiFi联盟而来，以后变成对无线局域网技术的统称。WiFi技术自开始到现在已经经历了多个版本，包括从最早的802.11到后面的802.11b，802.11a，802.11g，802.11i，802.11n。所以现在所说的WiFi技术代表的就是802.11协议体系。

但目前为止，应用最广泛的仍然是802.11a/b/g标准，尤其是便携式的笔记本电脑基本都有支持这三个标准的模块。其他多种电子设备如PDA、PSP、部分手机都能支持WiFi。有了WiFi确实方便了不少。在家里，不需要布置繁琐的网线，就可以将笔记本放置在家中任何地方上网；在咖啡吧里，可以一边喝咖啡一边免费上网；开会时不需要为没有够用的网线及接口而烦恼。

虽然WiFi应用广泛，但也有很多令人担忧的安全问题。

1　WiFi技术简析

WiFi技术与蓝牙技术一样，同属于在办公室和家庭中使用的短距离无线技术，主要应用于局域网中。除个别版本使用5GHz附近频段外，WiFi技术主要使用2.4GHz附近频段。当前应用的802.11协议版本，更多的功能是对有线网络的延伸。图1是802.11协议栈及其在实际使用中的简单对照[1]。

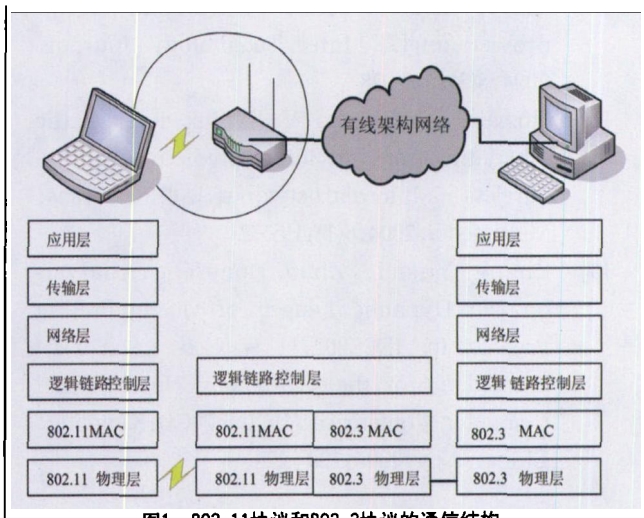

图1　802.11协议和802.3协议的通信结构

WiFi技术的定义其实只涉及数据链路层的MAC子层和物理层，上层协议和802.3的定义都遵守802.2。对于数据安全性，WiFi技术中更多使用的是WEP和WPA加密方法来实现对网络访问的验证和数据的加密，虽然这些定义的加密方法是可选的，但用户更多选择的是使用WEP方法。对于802.11的WEP加密，具体是如何实现破解的呢？下文详细讲述。

2　WEP分析

2.1　WEP介绍

WEP(Wired Equivalent Privacy) 算法在802.11协议中是一种可选的数据链路层安全机制，用来进行访问控制、数据加密等。

当无线工作站请求访问AP(Access Point)时，首先必须通过AP的访问认证。认证过程如图2所示[2]。无线

工作站发出认证请求，AP收到请求后生成随机内容，将该内容发送给无线工作站并要求无线工作站将这部分内容加密后传回。无线工作站将使用WEP进行加密，然后将加密数据传回AP。AP接收到工作站的响应后，同样使用WEP对数据进行验证。如果无线工作站的响应内容被AP验证通过，则该工作站通过验证并可以随后进行通信连接的建立，否则验证失败拒绝连接[3]。

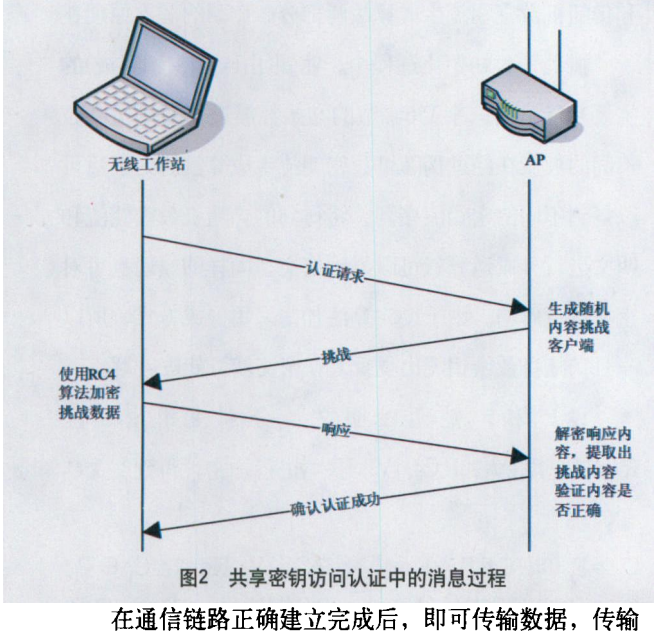

图2　共享密钥访问认证中的消息过程

在通信链路正确建立完成后，即可传输数据，传输的数据内容仍将通过WEP来加密和解密。在发送方，数据通过WEP使用共享的密钥进行加密，在接收方，加密了的数据通过WEP使用共享的相同密钥进行解密。如图3所示。

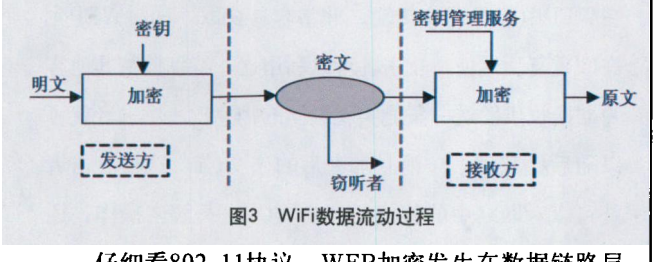

图3　WiFi数据流动过程

仔细看802.11协议，WEP加密发生在数据链路层中的媒体访问控制子层之上，逻辑链路控制子层之下，如图4所示。802.11协议与802.3协议相比，两者的不同之处在于图中虚线所框。对于上层及物理层、信号编码等，由于和内容加密无关，暂不去讨论。

2.2　WEP工作过程

具体来说，WEP的加解密是在MAC子层进行的。对于需要传输的帧，由帧头和载荷组成。WEP加密操作的全过程如图5所示[4]，而解密过程与加密过程一样，仅在解密后需要核对ICV的正确性。WEP对其载荷进行保护，主要分成4个步骤。

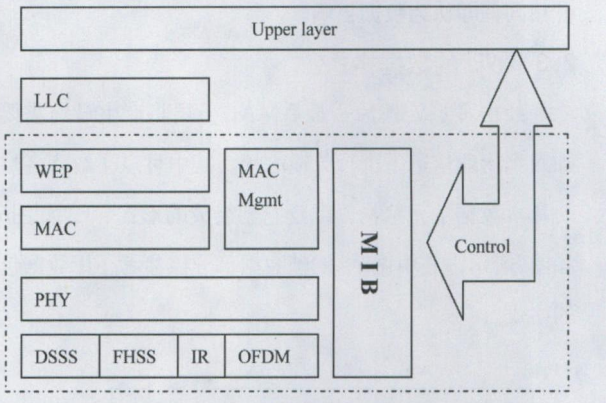

图4　802.11协议底层协议结构

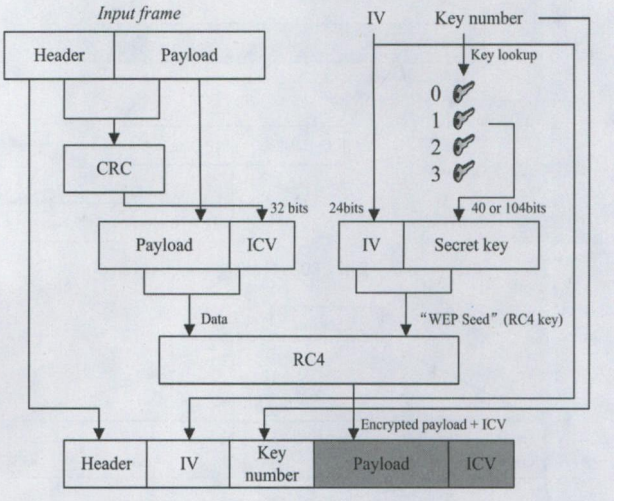

图5　WEP加密操作过程

1）对于需要传输的帧，先进行完整性效验序列计算，使用CRC算法生成32位的ICV完整性效验值，将载荷和ICV组合在一起作为将被加密的数据。

2）WEP的加密密钥分成两部分，一部分是24位的初始化向量IV，另一部分就是私密密钥。由于相同的密钥生成的帧密钥流是一样的，所以使用不同的IV来使生成的帧密钥流不同，从而可用于加密不同的需要被传输的帧。

3）生成的帧密钥流长度和被加密内容的长度是一样的，该密钥流作为RC4加密算法的密钥，使用RC4算法对帧载荷进行加密。

4）解密的时候，先进行帧的完整性效验，然后从

中取出IV和使用的密码编号，将IV和对应的密钥组合成解密密钥流，再通过RC4算法应用于已加密的载荷上，就能解析出载荷以及ICV内容。对解密出的内容再用步骤1)的方法生成ICV'，比较ICV'和ICV，如果两者相同，即认为数据正确。

2.3 WEP的数据格式

经由多层处理后，最后MAC子层将产生最终需要加载到物理信道上进行传输的帧。其中可以了解到各层的基本数据单元结构，以及它们组成的形式[5-6]。如图6和图7所示。其中图6中的帧数据部分仅参考了IP数据包的格式。

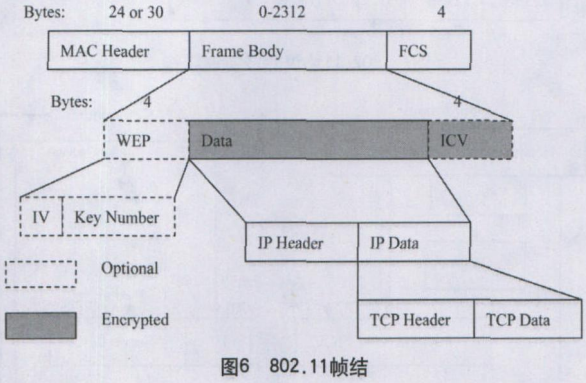

图6 802.11帧结

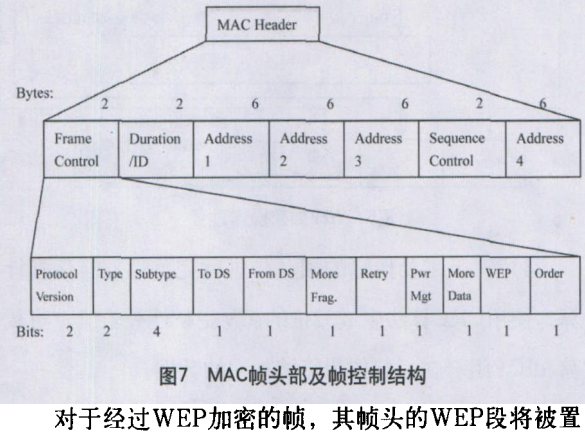

图7 MAC帧头部及帧控制结构

对于经过WEP加密的帧，其帧头的WEP段将被置为1，而帧的数据部分也会因为IV和ICV的加入被扩展8个字节。由于帧头部分的内容并未进行加密，可以被攻击者用来识别合法的客户端MAC地址。

3 WEP的缺陷

综合前面对WEP这种通过共享密钥来对数据加密的算法，仔细分析后可以看出，WEP中存在不少安全隐患。

3.1 ICV篡改

CRC-32算法是一种用于检测传输噪音和普通错误的算法。它是信息的线性函数，可以被攻击者篡改加密信息，并很容易地修改ICV使数据包合法。

3.2 RC4算法缺陷

RC4是当前最流行的加密方式之一，在许多应用程序中得到采用。它是一个流加密系统，包括初始化算法和伪随机数密钥流生成算法两部分。RC4的基本原理在于“搅乱”。初始化过程中，密钥(由IV和密钥组成)的主要功能是将一个256字节的初始数簇进行随机搅乱，不同的数簇在经过伪随机数密钥流生成算法的处理后可以得到不同的密钥流序列，将得到的伪随机数密钥流和明文进行异或运算就可以得到密文。同样的原理也可对密文进行解密。由于RC4算法加密采用异或方式，所以一旦伪随机数密钥流出现重复，密文就可能被破解。

设P_1和P_2是两段明文，分别使用密钥流RC4{IV_1,Key}和RC4{IV_2,Key}进行加密，得到密文C_1和C_2。

$$\left.\begin{aligned} C_1 &= P_1 \oplus RC4\{IV_1,Key\} \\ C_2 &= P_2 \oplus RC4\{IV_2,Key\} \end{aligned}\right\} \Rightarrow \begin{aligned} RC4\{IV_1,Key\} &= C_1 \oplus P_1 \\ RC4\{IV_2,Key\} &= C_2 \oplus P_2 \end{aligned}$$

$C_1 \oplus P_1 = C_2 \oplus P_2$，当$IV_1 = IV_2$时。

可见，在密钥流相同时，只要知道P_1，P_2，C_1，C_2中的任意三者，就能得到第四者。对于RC4算法，对于相同的密钥和IV所生成的伪随机数密钥流是唯一的。而在WEP中IV是明文传输，非常容易获取，同时WEP允许IV重复。这使得攻击者可以利用这一特点欺骗其他客户端接收或发送一条能实现预测的消息P_1，攻击者就可以随后拦截到该条消息加密后的密文C1。这样攻击者就可以对网络中的其他任何密文Cx进行解密操作，还原成Px。同时在WLAN中定义的若干协议规范，已包含若干已知的值(如IP头，IPX头，SNAP头等)。根据这些，攻击者能够从加密的数据中推算出部分密码，再逐步推算密码其他部分。

3.3 IV容易碰撞

IV在WEP中的功能是使RC4算法在使用相同的密钥生成的伪随机数密钥流不重复，而用以作为“数据包

加密密钥”。所以可简单认为，在知道用户密钥的情况下，WEP其实是使用IV来加密数据包的。根据WEP体制，发送人使用IV加密数据包，接收人也必须知道这个IV才能解密数据。WEP标准中的IV长度为24bits。而2^{24}仅有约160万个。这使得最多约160万个数据包后，将会重复IV。重复的IV可以被攻击者根据RC4的缺陷用来解析密文。有人会说160万个数据包，可是非常多了，即使按照每个数据包1500字节进行计算，有近24G字节的通信量，等待IV的重复需要多大的耐心啊。其实在通信频繁的WLAN中，这个数值并不大。有人说过“考虑到随机性的本质，只需传输不到1万个包，就可能会开始重复”。也就是说传输十多兆的文件或数据，IV就会出现碰撞。对于此点，笔者已经在自己编写的程序中进行过验证，虽然实际中并没在那么少的数据包中重复，但是6万内的数据包却出现过重复。

3.4 密钥管理机制缺乏

WEP没有密钥管理机制，只能通过手工方法对AP和工作站配置分发新的密钥。实际应用中，由于更换密钥比较麻烦，密钥并不经常被更换，所以很长一段时间内密钥都是不变的。这样，如果WLAN中一个用户丢失密钥，则会殃及整个网络的安全。

3.5 用户密钥的隐形缺陷

由于WEP的密钥标准中要求用户输入的密钥长度是固定的——40bits或104bits。如果用户选择64位加密方式，则提示用户输入5位字符或者10位十六进制符号。如果用户选择128位加密方式，则提示用户输入13位字符或者26位十六进制符号。这都是为了使密钥长度都能达到规定尺寸。一般用户在使用的时候，大多会选择64位加密方式，而输入的内容多数是5位的字符。因为不同的用户都有自己的一套密码设置习惯，如果要求用户恰好输入指定长度的密钥，由于惰性，大多用户为了设置成功往往使用占40bits的5位字符，即便使用10位十六进制符号也是简单的组合。在笔者破解的众多WLAN密钥中，就体现出这个问题。

3.6 未定义非法访问处理机制

在WEP中未定义对非法访问的控制和处理，如若攻击者使用密码字典进行攻击，对于这类频繁的非法连接请求，WEP并不做处理。而结合第3.5点的特点生成的字典，幸运地话也可以在较短的时间内破解出大多数WEP密钥。这需要结合社会工程学的弱密码学。

3.7 缺少对数据包的身份验证

由于没有针对数据包的身份验证机制来确定每个数据包的来源，这样导致非法客户端发出的数据，也会被AP所接受。虽然在AP管理端有一项MAC过滤，可以通过该功能限制非法MAC地址的访问，但MAC地址是可以被修改的，很容易伪造成合法客户端机器。

在攻击者攻击的时候，由于有的网络通信流量非常少，这就导致不能拦截到足够多的信息来分析出密钥。这个时候攻击者可以采用主动攻击的方式，拦截一个合法客户端的ARP请求包，随后攻击者向AP不断重放这个ARP请求包，在允许IV重复的基础上，AP会在接收到ARP请求包后回复客户端。这样攻击者就可以收集到更多的IV。获取ARP请求包也是非常简单的，使用无线欺骗的方法强制合法客户端和AP断线，在随后重连的过程中就有机会获得ARP请求包。

3.8 WEP安全现状

当今，网络上有多种利用WEP的各种漏洞缺陷进行解密的工具，如Aircrack，WEPCrack，Airsnort等。它们都能在高效地拦截到足够多的数据信息的前提下，快速解析出WEP的用户密钥，信息量越多，速度越快。著名的BT系统尤其集成了完整的无线破解工具，现在已经发布了BT4 beta版本。这些工具在利用漏洞推测密钥的基础上，还集成了复杂的算法来帮助缩短破解时间，减少数据资源积累量。

在解决由于WEP的缺陷所带来的安全问题上，“外套”技术被提出来。“外套”技术的软件加密方法可以将一些没有实际意义的无线数据包混杂在WEP数据包中，从而使攻击者在截获足够的数据信息后仍然无法分析出WEP的加密密钥。由AirDefence公司提供的新的外套技术，可以帮助那些大量使用便携式收款机、条码扫描器或零售网点终端和手持VoIP设备的用户，在他们常规产生的网络数据流中，AirDefense的

WEP外套模块可创建假数据流，使WEP密钥不同于实际WLAN客户端和接入点使用的WEP密钥，从而使攻击者破解的密钥无效，使用户的数据得到一定程度上的有效保护。

另外，也有如动态密钥等方案来对WEP进行改善，但这些并不能从根本上解决问题。

4 WPA

虽然说WEP之后有更安全的WPA和WPA2的加密技术，避开了WEP中的众多弱点，但是安全攻击和防范本就是天生一对，没有无坚不摧的矛，也没有坚韧无比的盾。WPA的加密方式需要四次握手，使用了多至48位的IV，防止IV重复，MIC信息编码完整性机制以及动态密钥管理机制等一系列的规则来加强通信安全。其具体细节本文不予分析。

鉴于WPA比较完善的密码体制，并不能通过破解WEP的方式来进行破解，但是由于在WPA的四次握手包中包含和密码有联系的信息，可以依靠这个信息来进行字典攻击。在这里成功破解出信息，关键依赖良好的字典。良好的字典依赖对弱密码的分析以及对曾出现过的强密码的收集，当然运算速度也是关键环节。

当前，已经公布的破解WPA的工具有一家俄罗斯软件公司出品的Elcomsoft Wireless Security Auditor(EWSA)软件，宣称可以利用GPU的运算性能快速攻破WPA-PSK和WPA2-PSK密码，运算速度比使用CPU可提高上百倍，密码尝试速度可达到5万2 400个每秒。

5 WAPI

5.1 WAPI简介

WiFi暴露的众多安全问题，是为什么中国大陆地区不支持甚至禁止WiFi手持设备进口的原因之一。中国并不是不清楚WiFi所能带来的便利，所以极力推出自己研发的WAPI技术。WAPI(WLAN Authentication and Privacy Infrastructure)，即无线局域网鉴别与保密基础结构，于2003年在中国无线局域网国家标准GB15629.11中发布。它是针对IEEE802.11存在的漏洞和隐患，利用基于数字证书的双向认证，在客户端和无线接入点之间建立一个相互验证的方法。WAPI使用已经ISO/IEC批准的0x88B4作为以太类型号。

WAPI包括WAI(WLAN Authentication Infrastructure)和WPI(WLAN Privacy Infrastructure)两部分。前者负责认证，采用基于椭圆曲线的公开密钥证书体制，无线客户端和计入点通过认证服务器进行双向身份鉴别。后者负责加密，采用国家商用密码管理委员会办公室的对称密码算法进行加密和解密。

图8介绍WAPI(2006)中无线工作站(STA)接入网络鉴别的过程[7]，与2003年发布的版本对比，可以看到在单播密钥协商阶段有很大的改变。曾经由STA发起的密钥协商请求更改为由AP发起密钥协商请求，同时加入了对所协商密钥的确认[8]。估计这点是考虑到AP可能被非法STA进行DoS攻击而进行的改善。虽然WAPI(2006)相对2003版本有诸多完善，但在证书鉴定和密钥协商过程中仍存在安全缺陷，可被攻击者利用进行被动攻击和反射攻击[9]。由于篇幅原因这里不做深入探究。

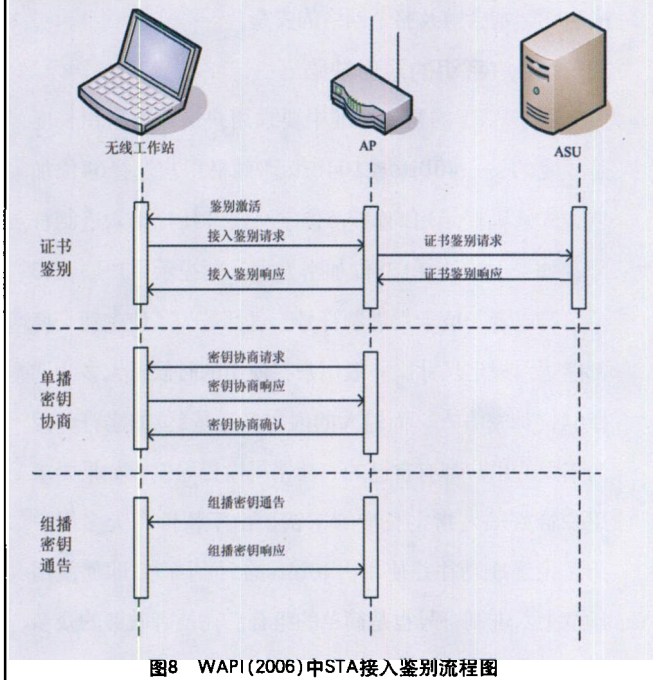

图8 WAPI(2006)中STA接入鉴别流程图

5.2 WAPI面临的现状

从1992年开始研究WAPI标准到发布，再到国际

标准的申请，一直受到IEEE802.11标准阵营的重重阻挠。可喜的是，2006年3月7日，WAPI产业联盟成立大会在北京召开，WAPI产业联盟正式成立。当前，国内众多芯片企业纷纷支持WAPI，国外WLAN芯片企业也逐步转变了对该标准的态度，纷纷跟进WAPI标准和技术并推出相应芯片产品。今年4月中旬，工信部宣布以后国内所有2G、3G手机都可以支持WAPI技术。5月，工信部在政策上已允许内置WAPI/WiFi双接入的手机入网，同时这可能也是WiFi在中国获得发展的一个新的机遇。尤其是在最近的国际标准组织ISO/IEC JTC1/SC6会议上，WAPI首次获得包括美、英、法等10多个与会国家成员体一致同意，将以独立文本形式推进其为国际标准。

虽说WAPI在认证、加密方面都弥补了当前的WiFi通信中的不足，而且使用了较新的算法，目前也未发现任何算法上的缺陷，但是谁也不能保证当前安全的算法不存在没有发现的缺陷，就好比WEP从诞生到发现弱点花费了5年时间，而后2年才发现其致命弱点。只有经过时间和市场的考验，才能证明体制的合理性和算法的健全性。希望WAPI在给人们带来便捷和安全的道路上走得更远。

6 常规安全问题

在使用WLAN中，虽然面临着众多安全问题。但有些问题仍然可以通过用户主观行为来避免或降低威胁。从笔者开始研究WEP、WPA解密到现在破解的数十个WLAN网络来看，多数密码都非常简单，而且多有实际含义；同时这些密码从笔者破解后至今，从未更改过；所以用户需要使用复杂点的密码，并经常更换密码，以增加被攻击的难度。

另外笔者还轻易进入到其中的数个路由器，原因是设置的密码太简单，如账号是admin，密码也是默认的admin。根据不同类型的AP型号就能简单猜测出账号和密码，进入路由的管理页面，宽带账号和密码就已经暴露在攻击者的视线中了。建议路由器生产商，不能将密码显示在web页面中，否则宽带账号密码将很容易从源码中拾取。对于非web页面程序，道理也是一样，密码不能轻易暴露在密码框中，即使以星号等符号遮掩也不行，否则类如Peekpass的软件将使之“原形毕露”。

密码简单多是由于用户懒惰所造成的。当然这也是有很多客观原因，在当今Internet盛行的年代，哪个人头脑中不是记着一大堆的账号和密码，比如邮箱、论坛、网站、银行卡、计算机用户。想象一下自己拥有的众多账号密码，如何能熟记于心呢？可能多数人对于这些密码的设置都已经有自己的习惯了，比如使用统一密码、密码结构一致，这样的习惯同样也成为了安全威胁。在当其中一个密码泄露后，根据各种关联性，其他密码很可能会被猜测出，另外相信有的人会使用计算机中的记事本等工具进行统一记录和保管，而WiFi网络被攻陷时，这些密码信息就很容易被窃取，因为毕竟不是每个人都是电脑高手能够使自己的计算机足够安全。

同时在突破一个网络后，就可以轻易截取到通信网络中的数据。更多的账号，更多的密码都可能暴露其中，尤其是上层明文传输的通信数据，如MSN。关于如何从多种即时聊天工具中获取敏感信息，并深入分析来达到舆情分析和监控的效果，笔者将另文专门讨论。

7 小结

虽说WEP有众多安全问题，但是WLAN中使用WEP加密仍占大多数，而且当前使用中的设备基本都支持WEP，正在不断生产及以后将生产出的设备仍然都是支持WEP的；同时IEEE的802.11i协议保持后向兼容问题，WEP仍得以继续；所以WiFi技术在安全性能上的整体升级仍有一段路。

通信安全一直存在于整个通信网络中。在无线通信中，安全问题尤为突出，如何解决好WLAN中的通信问题，需要做大量的工作从根本上避免算法中的缺陷并保证体制的健全。

8 参考文献

[1] Yan Wei.WLAN与802.11.PKU NC&IS[EB/OL].[2009-05-20]. http://net.pku.edu.cn/

webCourse/ppt/lec8.pdf

[2] Sheila Frankel. Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i[M], NIST,2007

[3] Lee Barken. Wireless Hacking:Projects for Wi-Fi Enthusiasts,Syngress,2004.10

[4] Matthew S Gast.802.11 Wireless Networks The Definitive Guide[M]. Beijing: O' Reilly, 2005

[5] Mauri Kangas. Overview of 802.11 Networks and Standards. 2004.02

[6] Gorry Fairhurst. IEEE 802.3 Logical Link Control. Internet Communications Engineering - A Tutorial[EB/OL].[2009-05-20]. http://www.erg.abdn.ac.uk/users/gorry/eg3567/lan-pages/llc.html

[7] 中华人民共和国国家质量监督检验检疫总局.GB15629.11-2003-XG1-2006, 2006

[8] 中华人民共和国国家质量监督检验检疫总局.GB15629.11-2003, 2003

[9] 吴柳飞,张玉清,王凤娇.一种新的WAPI认证和密钥交换协议[J],计算机工程,2008,34(8):164-166

作者简历

刘辛酉

上海交通大学电子信息与电气工程学院工程硕士，研究方向：通信安全、软件开发。

Security Analysis in WiFi Communications

Liu Xinyou | Shanghai Jiao Tong University, Shang hai 200030, China

Abstract This paper analyzes the WiFi technology which is widely used and the process of WEP. Based on this, some security issues and limitations are pointed out. Then this paper brings out methods of WEP cracking. At last, the situation of domestic WAPI technology is briefly introduced.

Keywords WiFi; WEP; WPA; WLAN; WAPI; Communication Security