无线局域网WPS安全机制分析

谭正东
(浙江省舟山市财政局 浙江舟山 316021)

摘要:WiFi保护设置(WPS)是由WiFi联盟2006年年末发布的一个行业标准,旨在为不精通无线局域网安全知识的普通用户提供一个统一的、简单的方法来安全配置无线网络。但WPS先天就具有可能被暴力破解的可能,特别是2011年12月底公布的PIN码漏洞,使得开启WPS功能的无线设备都极易被暴力攻击。本文简单介绍了WPS的产生背景,分析了WPS协议、PIN码漏洞和解决办法。

关键词:无线安全 WPS
中图分类号:TN929 **文献标识码**:A **文章编号**:1007-9416(2012)03-0238-02

1、WPS (Wi-Fi Protected Setup) 技术

无线局域网(WLAN)的应用越来越广,除了学校和商务场所等有公用的无线接入点外,越来越多的个人用户也开始使用WLAN。但在这些用户中,有相当比例的的用户没有对无线局域网进行安全设置的意识和知识,经常导致其无线网络是完全开放的。这对于用户来说是非常危险的,因为他们就完全没有了隐私,攻击者可以很轻松的登录他们的个人无线局域网。基于这个背景,WiFi联盟于2006年末推出了WPS(Wi-Fi Protected Setup)技术,该技术结合WPA/WPA2加密方式和简单方便的配置方式于一体, 使无线局域网的相关安全设置简便化。

在传统方式下,用户新建一个无线网络时,必须在接入点手动设置网络名(SSID)同时选择一种安全认证方式(WEP、WPA、WPA2),客户端接入该无线局域网时需输入验证密钥。这整个过程需要用户具备Wi-Fi设备的背景知识和修改必要配置的能力。WPS能帮助用户自动设置网络名(SSID)、配置强大的WPA数据编码及认证功能,用户只需输入个人信息码(PIN方法)或按下按钮(按钮设置,或称PBC),即能安全地连入WLAN。对于普通用户来说,无需了解SSID和安全密钥的概念就能实现安全连接。

支持WPS的产品目前提供两种安装解决方案:

PIN码方式 输入PIN码——对于WPS认证的设备为强制配置。

PBC方式 按钮配置——它可以是设备上的硬件按钮或软件模拟的按钮。

2、WPS先天的缺陷

WPS存在着先天的缺陷,无论PIN码方式还是PBC方式,都是基于PIN码认证。无线路由器或者接入点(AP)启用WPS功能都需要配置一个静态PIN,以允许外部访问者ER(External Registrar)的访问和配置。启用WPS后AP就会配置为使用静态PIN码,一个具有WPS认可(WPS-capable)的ER,只要提供了正确的PIN,就可加入这个无线网络。WPS的弱点就在于AP的这个静态PIN码,在理论上可能允许未经身份验证的远程攻击者用暴力计算,穷举PIN码,在较短的时间内确定AP的密码。

PIN码是无线设备生产厂家随机生成一组8位数字字符串,通常厂家会印在无线设备标签上,无线路由器或AP的管理界面中当然也会存在并可更改。

既然知道了无线路由器PIN值的范围(8位纯数字),且目前大部分设备的WPS是呈开启状态的,那么穷举PIN码以攻破无线路由器的安全防护这一暴力行为就有了理论可行性。

在实验环境下,模拟一个理想的无线网络环境,在无线接收速率3K/sec的计算机上穷举8位全数字的WPS密码需要8个小时才能完成。由于8位纯数字的穷举量为:10?8,即:10,000,000,这是一个很庞大的数字,穷举会耗费很长时间。如果PIN码是随机的8位,考虑实际环境中存在的信号不佳,噪声过大,设备负载过重,等待PIN认证结果的合理延迟(如果PIN码验证失败,程序会等待很长一段时间才会提示)等等因素,10小时内搞定WPS加密还是不太现实的。

3、WPS PIN漏洞

2011年12月28日,一位名叫Stefan Viehbock的安全专家宣布,自己发现WPS加密技术其实存在着十分重大的安全漏洞,利用这个漏洞平均只需要两小时左右,便能以不断尝试密码组合的暴力攻击(Brute Force),破解使用 WPS 密码保护的路由器。US-CERT(美国计算机应急准备小组)确认了该漏洞,并发布了VU#723755漏洞警告。

随后Stefan Viehbock又公布了自己设计的WPS破解工具。这个工具可以破解WPS的PIN码,而且将破解时间缩短到2个小时以内。这个工具都在破解之后令破解者可以获取WPA密码,即使之后WPS被关闭后也可以通过获取的WPA密码连上无线网络。

在WPS的PIN验证规范存在设计缺陷,采用 WPS 加密技术的 Wi-Fi 路由器,在用户的每次密码尝试时,会分成「前半」四码和「后半」四码。当PIN验证失败,接入点会发送一个EAP-NACK消息返回给客户端。EAP NACK消息发送的方式,使攻击者能够确定如PIN码的「前半」四码是否正确。前四码如果错误的话,那路由器就会直接送出「错误」讯息,而不会继续看后四码。

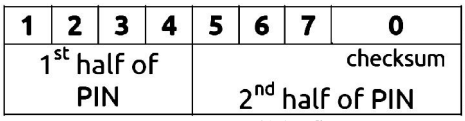

图1 PIN码的组成

图1显示PIN码由前半部分四码1st和后半部分四码2nd组成,其中2nd的最后一位为检验位。现在,PIN信息可以分为两组来看,1st和2nd,分别发送M4和M6信息,以验证1st和2nd是否正确。意味着试到正确的1st,最多只需要试 104(即10000 组号码)。一旦没有错误讯息,就表示1st是正确的,而后便可以开始尝试2nd。2nd比1st简单,因为八码中的最后一码是校验码,由前面七个数字产生,因此实际上要试的只有三个数字,即103(100组号码)。这使得原本最高应该可达108(10,000,000组)的密码组合(七位数+校验码),瞬间缩减降低为104+ 103(即11,000)总的组合,大幅降低破解所需的时间。

攻击一个开启WPS功能的无线网络,实际上需要多长时间?如果信号理想、噪声小、使用Intel酷睿芯片的笔记本来测试一下,其中最耗时的就是无线路由器的身份验证时间了,这个一般情况下大约需要1秒至2秒左右的时间,所以即使破解试遍11,000的全部组合,也不会超过3小时。

在上述的实验环境下,实际模拟一个开启WPS的无线网络环境,破解笔记本上安装了最新BT4下的reaver1.4工具,几次测试都在60分钟以内。考虑到实际环境下信号不会这么理想,一般也不会超过3小时。

·····下转第240页

3.2.2 数据加密技术

信息加密技术通过密码技术对数据进行编码和解码的一种算法，根据不同的算法有对称加密体制、非对称加密体制和不可逆加密体制三种。对网络中传输的数据先进行加密，到达目的地后再解密还原为原始数据，目的是防止非法用户截获后盗用信息。

3.2.3 漏洞扫描技术

漏洞扫描就是通过对系统本身安全脆弱点的自检，找到安全漏洞，并及时给予修复，防范病毒或黑客的攻击。根据扫描对象不同，可以把漏洞扫描分Internet网扫描技术、系统扫描技术和数据库扫描技术等几种。

3.2.4 入侵检测技术

入侵检测技术是通过对计算机网络中的恶意使用行为进行实时识别和响应的一种安全技术。它可以在系统被破坏前自主地中断并响应安全漏洞和误操作，可以用来实时监听流动在网上的数据包，还可实时监控主机内用户的活动。因此入侵检测技术不仅可以检测来自外部的入侵行为，也可检测出内部的越轨行为，及时防黑客攻击和内部人员的道德风险。

3.2.5 访问控制技术

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它是保证网络安全最重要的核心策略之一。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。通过对用户访问网络资源的权限进行严格的认证和控制，可以在很大程度阻止未经允许的用户有意或无意地获取数据的技术。

3.2.6 病毒检测和杀毒技术

计算机病毒主要通过计算机及存储设备和网络传播病毒，要防治病毒最有效的手段就是切断计算机病毒的传播途径。一旦在使用过程中感染了病毒，就必须及时使用正版杀毒软进行查毒和杀毒。

随着计算机病毒在网络上的传播日益广泛，其相应的反病毒技术也随之日益更新。针对不同用户采取相应的检测方法是反病毒工作中不可或缺的环节。正确合理使用计算机病毒检测和杀毒技术有利于更好的防止计算机病毒的感染破坏，有利于更好的维护计算机网络安全，使得计算机网络真正发挥其积极的作用。

3.3 不断加强计算机及网络系统安全管理

为加强计算机安全管理，保障计算机级网络系统的正常运行，保证工作正常实施，确保涉密信息安全，结合计算机及网络使用实际情况，制定相应的计算机系统以及网络安全管理制度，是保障计算机系统和网安全的重要方面。

4、结语

在计算机网络日益普及的信息化时代，网络安全显得尤为重要。虽然现在用于网络安全防护的产品有很多，但是病毒、黑客、木马还有人为破坏仍然无孔不入，对计算机及网络的使用安全造成严重的危害。根本原因是网络自身的安全隐患无法根除，这就使得黑客进行入侵有机可乘。因此随着网络安全技术日趋完善，降低黑客入侵的可能性，使网络信息安全得到保障。如何把握网络技术给人们带来方便的同时，又能使信息安全得到保证，这要求不断的提高计算机系统及网络系统安全技术，不断的创新和发展保障计算机安全的各项技术，并制定出规范科学的计算机及网络安全使用各项制度。

参考文献

[1]简明.计算机网络信息安全及其防护策略的研究[J].科技资讯,2006.

[2]张民,徐跃进.网络安全实验教程[M].清华大学出版社.2007-6.

[3]武新华,翟长森等编着.黑客攻防秘技大曝光[M].清华大学出版社,2006.

[4](译)吴世忠,马芳,网络信息安全的真相[M].机械工业出版社,2001-9-1.

……上接第238页

4、对WiFi安全的影响

WiFi的发展一直伴随着安全的问题，无线局域网的安全也是随着各种对安全技术的破解而不断地发展提高。在无线局域网的早期发展阶段，主要使用物理地址（MAC）过滤和服务区标识符(SSID)匹配这两项主要的安全技术。物理地址过滤和服务区标识符匹配只能解决有限的安全问题。为了进一步解决安全问题，IEEE802.11推出了有线等效保密WEP（Wired Equivalent Privacy）协议，用于在无线局域网中保护链路层数据。WEP使用40位和104位密钥，采用RC4对称加密算法，在链路层加密数据和访问控制。不过，WEP的密钥机制存在被破译的安全隐患，需要新的安全技术来解决。2004年6月，802.11工作组正式发布了IEEE 802.11i，以加强无线网络的安全性和保证不同无线安全技术之间的兼容性，802.11i标准包括WPA和RSN两部分。而于IEEE完成并公布IEEE 802.11i无线局域网安全标准后，Wi-Fi 联盟也随即公布了第二代WPA标准WPA2。

WPA/WPA2是目前主流的无线安全认证协议，目前该协议本身还没有被发现存在明显的漏洞，目前的攻击手段还只能是暴力破解。但由于WPA/WPA2设置的复杂性，导致了WPS的出现，而WPS PIN码漏洞就会导致WPA/WPA2密码的泄漏。这就了WPA/WPA2的一个破解隐患。

现在市面上的无线路由器或AP，很多产品出厂时便将 WPS设置为默认开启。据US-CERT 统计，Belkin、Buffalo、D-Link、Linksys(Cisco)、Netgear、Technicolor、TP-Link和ZyXEL的产品都默认开启了WPS功能，这些产品都是市场的主要品牌，很多设备不但用于家用，还广泛地在商务领域使用。这些设备都面临被PIN码漏洞暴力破解的危险。

5、解决办法

针对WPS的漏洞，可以有以下几种办法解决：

(1)仍然需要使用WPS功能的用户，可以选择具有身份识别锁死功能的无线产品，或者等待厂家升级相关的固件。具有身份识别锁死功能的无线路由器或者AP，在某些次数的身份识别(3次或则5次)失败之后将临时锁死接入（锁定验证设备并延后60秒），虽然这不能彻底解决这一问题，但它确实会增加PIN码暴力破解耗费的时间，可能从几个小时增加到几天。

(2)不需要WPS功能或者要彻底避免PIN码暴力攻击的用户，目前的方法就是在你的使用WPS的无线网络还没被攻破之前马上关闭WPS服务并且使用WPA2等更安全的加密方法并手动设置密码。

参考文献

[1]Wi-Fi 联盟.Wi-Fi Protected Setup.规格说明书,V1.0h 2006.12.

[2]Cisco 安全响应.《Wi-Fi Protected Setup PIN Brute Force Vulnerability》.

[3]Stefan .《Brute forcing Wi-Fi Protected Setup》http://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability.

[4] US-CERT WPS PIN 漏洞警告. Vulnerability Note VU#723755,《WiFi Protected Setup (WPS) PIN brute force vulnerability》.