WPS，破解无线 WPA/WPA2 密钥的捷径

图/文：**杨 哲**/Longas 【ZerOne Security Team】

（注：本文已发表在《黑客防线》杂志 2010 年第 3 期上，引用时请注明出处，谢谢）

前言：其实很多时候破解无线 WPA/WPA2 加密并没有所想的那么复杂，有这样一些技巧可以帮助无线黑客们绕过 WPA/WPA2 的加密体系，本文讲述的就是其中一个比较取巧的方法即通过 WPS 破解。

需要特别强调一下：本文内容适合目前市面上 99%的支持 802.11N 系列无线路由器以及 70%的 802.11G 无线路由器，也许有的设备仍需要一些攻击手段的配合，但是有具备 WPS 功能的无线路由器的朋友们，还是要多加注意。

1．关于 WPS

1．1 WPS 和所谓“一键加密”

考虑到普通用户对无线安全设置的困惑，Wi-Fi 联盟推出了名为 Wi-Fi Protected Setup（Wi-Fi 保护设置，简称 WPS）的认证程序。Wi-Fi 联盟宣称，WPS 可以将设置安全网络的步骤减少一半。目前，新一代 11n 无线路由器及网卡均支持 WPS 功能，这对用户来说绝对是个好消息，当然，对黑客们来说也是。

图 1

具体来说，WPS（Wi-Fi Protected Setup，Wi-Fi 保护设置）是由 Wi-Fi 联盟（http://www.wi-fi.org/）组织实施的认证项目，主要致力于简化无线网络的安全加密设置。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）和安全密钥，然后在客户端验证密钥以阻止“不速之客”的闯入。Wi-Fi Protected Setup 能帮助用户自动设置网络名（SSID）、配置最高级别的 WPA2 安全密钥，具备这一功能的无线产品往往在机身上设计有一个功能键，称为 WPS 按钮，用户只需轻轻按下该按钮或输入 PIN 码，再经过两三步简单操作即可完成无线加密设置，同时在客户端和路由器之间建立起一个安全的连接。

值得注意的是，利用 WPS 简化网络安全配置要求接入点和客户端设备均须通过 WPS 认证，用户可在产品包装上寻找 Wi-Fi Protected Setup 的标志（如上图 1 所示），以确保所购产品具备 WPS 功能。不过要强调的是，在市场上并不是所有具备 WPS 功能的无线产品都会在包装贴上如上图 1 所示的标志。所以请特别注意如下图 2 所示的描述，当在外包装上产品简述中出现所谓“一键加密”功能描述的，即为具备 WPS 功能。

Blog：http://bigpack.blogbus.com
Email：longaslast@126.com
欢迎拍砖、交流、合作及其它事宜，

新书《无线网络安全攻防进阶》筹备中，更多内容，即将推出！感谢一直以来的支持！！

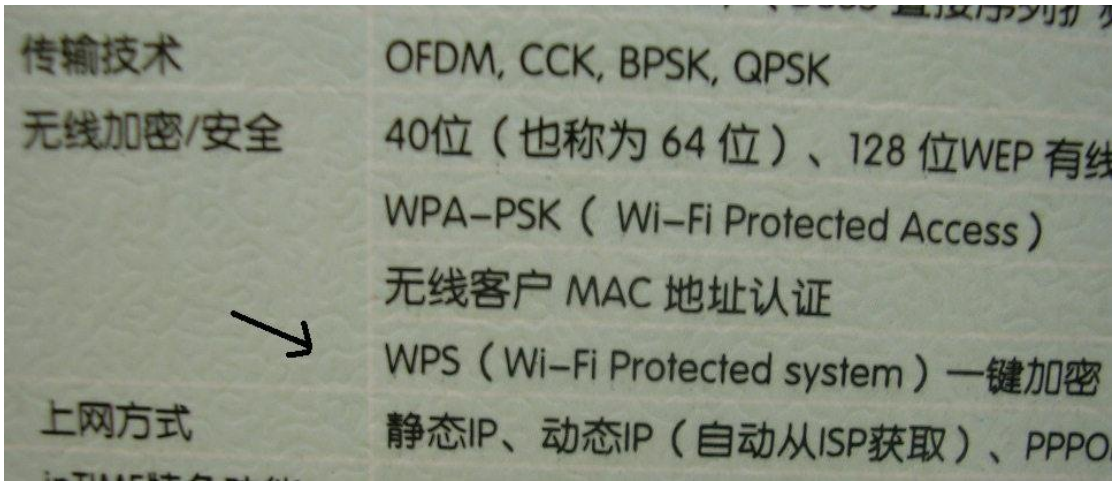

图 2

1．2　WPS 的基本设置

关于 WPS 的基本设置很简单，不过由于无线路由器的品牌和型号不同，配置时将稍有偏差。以下配置步骤仅供大家参考，同时也可看出 WPS 的便捷性以及厂商为何如此推崇 WPS 功能。

步骤 1：在无线客户端上运行无线网卡配置工具，选择“连接到带有 WPS 的无线网络”；

步骤 2：有些无线路由器是自动开启 WPS 功能的，比如 TPLINK，但还有些无线设备需要使用计算机登陆到路由器页面（如下图 3 所示），在有关页面选择连接无线设备，或者按住路由器上的 WPS 按钮（如下图 4 所示）。

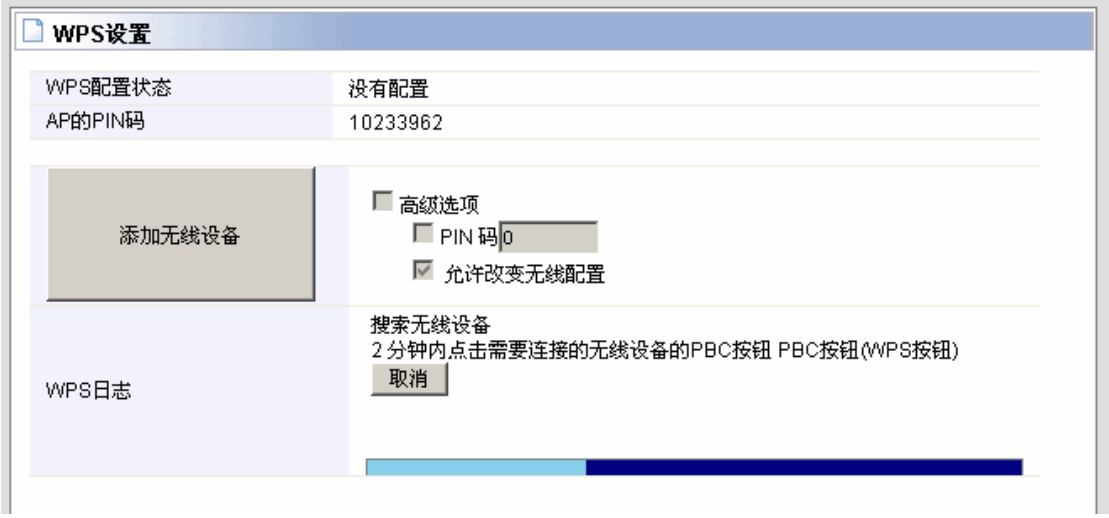

图 3

步骤 3：在无线网卡配置工具上选择 PBC 连接形式，或者在无线网卡上点选下图 5 中的 WPS 按键。

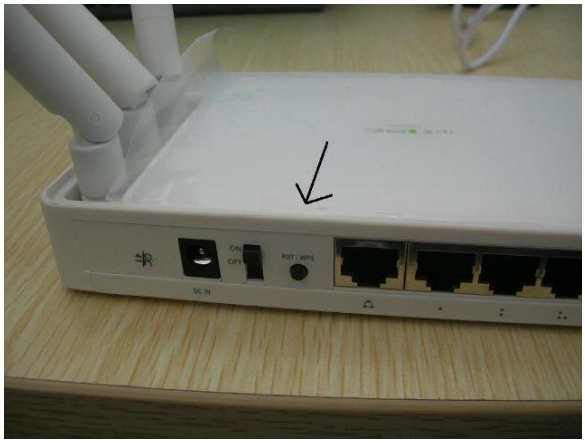

图 4

图 5

步骤 4：等待数秒钟，连接成功。

整个流程与 TCP/IP 的三次握手协议类似，看起来只有一呼一应两个联系，但是因为配置了 120 秒超时的限定，所以实际上也是一个三次握手的流程。WPS 完成的工作只是一个输入超长密钥的流程，但因为操作的便利以及人工介入管控，使得其过程不太容易被运用攻击。不过话说回来，也只是“不太容易被攻击”而已。

对于市面上的绝大多数 802.11N 系列无线路由器来说，都能非常便利的运用 WPS 功能，并且建立连接的时间不超过 20 秒。对一个初级用户来说，甚至最多仅仅只要按两次按键就可以建立超长位数的 WPA2 加密，无疑是一项非常有吸引力的功能。不过需要特别注意的是，使用 WPS 的前提是使用无线网卡自带的管理配置程序，不能使用 Windows 自带的无线管理配置服务。

2．扫描开启 WPS 的无线设备

对于无线黑客而言，关键在与如何检测有哪些无线设备开启 WPS，以及有哪些无线设备的 WPS 正处于搜寻状态等等，这些都是关系到利用 WPS 进行攻击的可能性。

2、1　扫描工具介绍

目前专门支持 WPS 扫描的工具并不多，不过由于 WPS 相关标准的公开，各大厂商在各自的无线网卡产品配套工具中，都内置了 WPS 扫描及总动配置功能。这里介绍两款工作在 Linux 下使用 python 编写的小工具，分别为 wpscan.py 和 wpspy.py。其中，wpscan.py 用于扫描开启 WPS 功能的无线网络设备，wpspy.py 则用来确认无线网络设备当前 WPS 状态。

2、2　扫描开启 WPS 功能的无线设备

关于无线网卡的载入等基本操作本文就不再浪费篇幅讲述了，具体的 WPS 扫描步骤如下。

步骤 1：扫描开启 WPS 功能的无线设备

扫描开启 WPS 功能的无线路由器，具体命令如下：

```
./wpscan.py  -i  mon0
```

回车后稍等片刻后，wpscan.py 可以将周围能够搜索到的开启 WPS 的无线路由器全部列举出来。如下图 6 所示，扫描出一款开启 WPS 的无线路由器，其 SSID 为“ZerOne_Lab”，其具体型号未能显示，但其芯片组为 Ralink。

图 6

没有显示出产品具体型号也是正常的，因为并不是所有的厂商都会在 WPS 中加入厂商的详细信息，这也是出于安全的考虑。不过一些大的厂商都会在 WPS 中加入一些信息，比如下图 7 中，在“ Model Name ”处，就识别出为 Belkin 的型号为 F5D7230-4 的无线路由器，甚至可以显示出具体的型号为 v9。这也就导致了信息的暴露，所以针对 WPS 的扫描也是有效探测无线设备的方法之一。呵呵，这个是我在 2010 年第一期黑防上《无线网络设备攻防白皮书》中没有提及的。

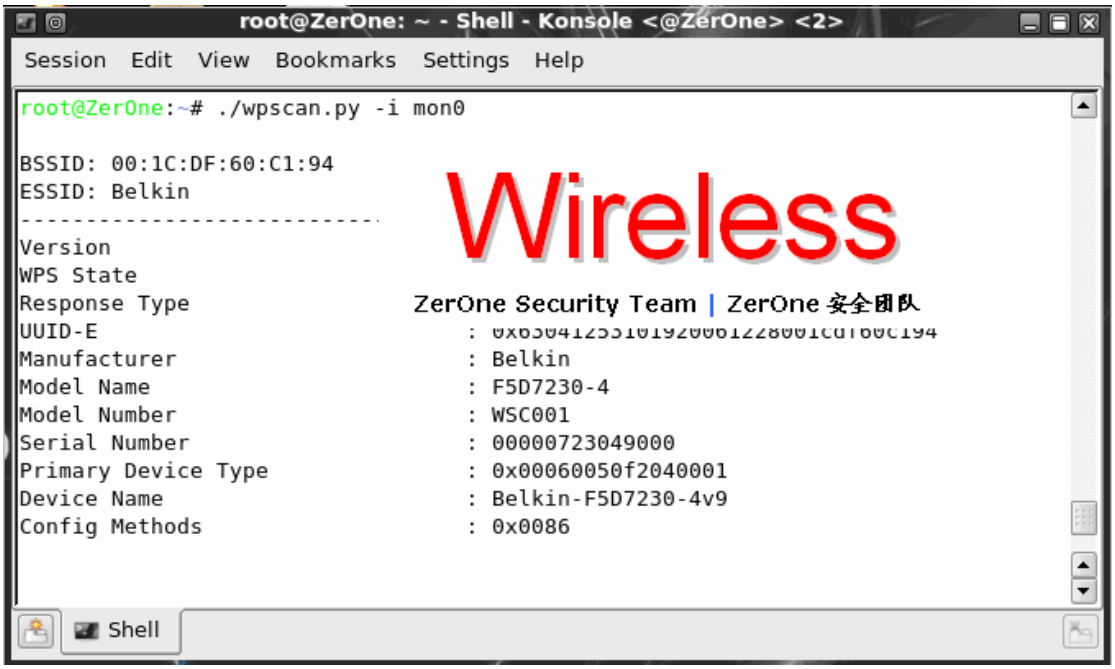

图 7

步骤 2：监测 WPS 状态。

在获知了存在开启 WPS 功能的无线设备后，即可对

```
wpspy.py -i mon0 -e AP's SSID
```

回车后即可看到如下图 8 所示内容，监测到 SSID 为“ZerOne_Lab”的无线路由器。当前 WPS 功能状态为已配置，即 WPSState 处显示为 Configured。而在 WPSStatePasswordID 处显示的“PushButton”，即要求客户端点击无线网卡上的 PBC 按键进行连接。

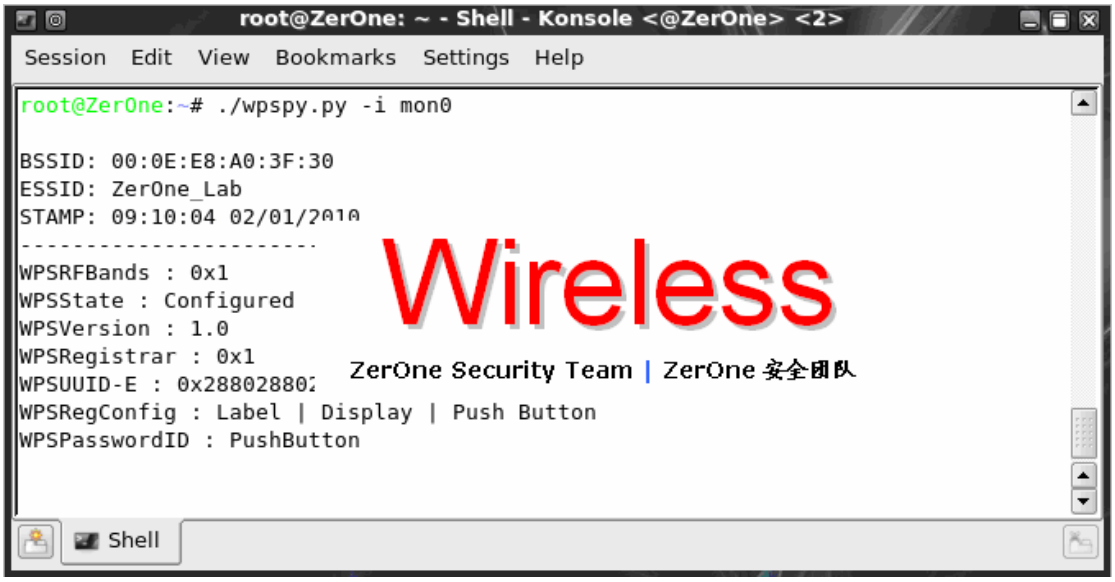

图 8

若 WPS 功能未被配置，则会出现如下图 9 所示内容，在 WPSState 处显示为 Not Configured。

```
------------------------
WPSRFBands : 0x1
WPSState : Not Configured
WPSVersion : 1.0
WPSRegistrar : 0x1
```

图 9

在 WPS 的状态改变过程中，使用 wpspy.py 监测的显示也在不断变化，这将有助于黑客们掌握当前的 WPS 部署情况。如下图 10 所示，两个不同的提示表示当前 WPS 正处于调试配置过程当中，当出现“ WPSPasswordID：PushButton ”时，将是最利于后续连接的时刻。

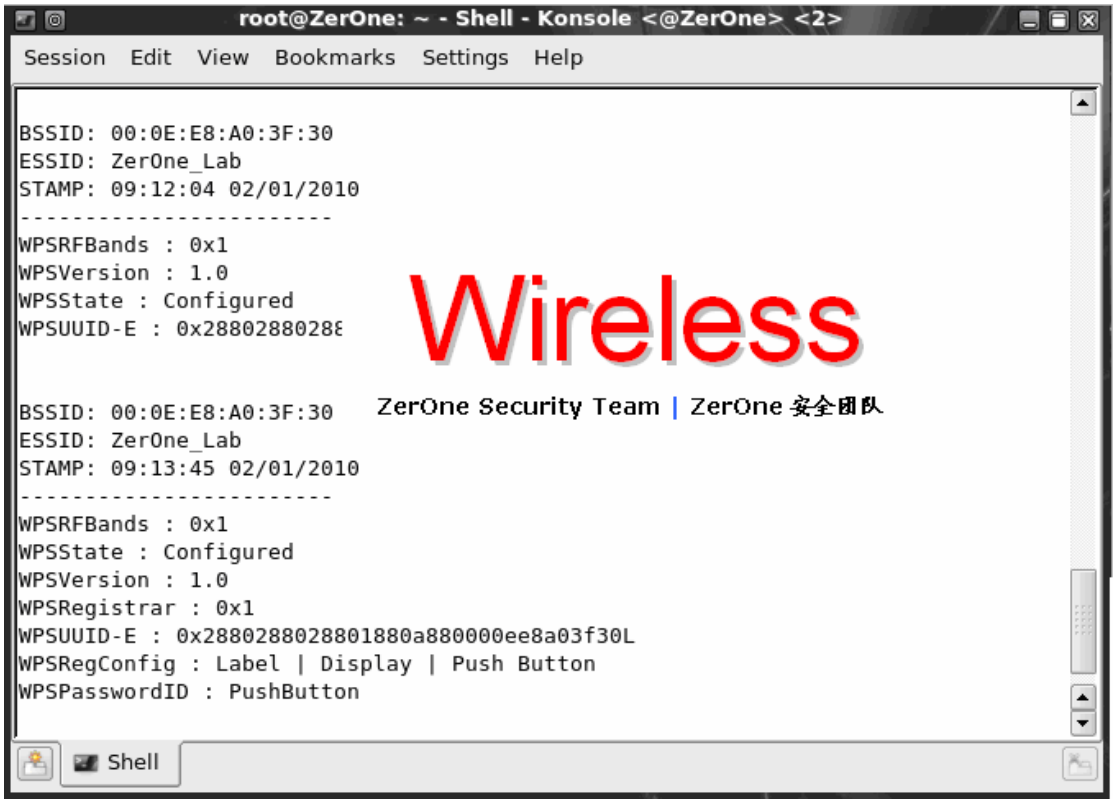

图 10

3．利用 WPS 破解 WPA/WPA2 密钥

直接进入正题，开始演示如何利用 WPS 破解 WPA/WPA2 密钥，看完之后相信很多朋友会大吃一惊地说：原来这么简单？！嘿嘿，具体步骤如下。

步骤 1：先确认当前网络中是否存在开启 WPS 功能的无线设备。

具体参考本文上面所述的工具，这里不再重复。

步骤 2：打开无线网卡配置工具。

此时打开无线网卡自带配置工具，扫描当前存在的无线网络。如下图 11 所示，可以看到，之前扫描发现的 SSID 名为“ ZerOne_Lab ”的无线网络信号充足，当前无线网卡处于其信号范围内。

需要注意的是，若此时无法接收到之前扫描的目标 AP 信号，应采用为无线网卡加装高

增益的天线、增大网卡功率、改变当前接收位置等多种方法来改善。此外，需要额外注意的是，不要使用 Windows 系统自带的无线网络配置工具 !! 否则将无法进行下一步无线网卡上的 WPS 功能配置。

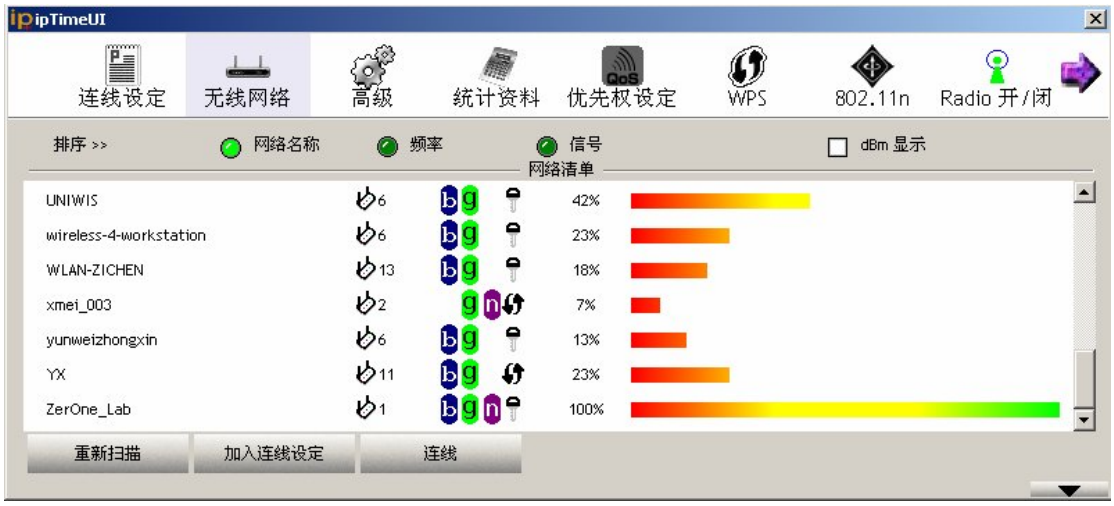

图 11

步骤 3：连接开启 WPS 功能无线设备

打开无线网卡配置工具中 WPS 配置页面。如下图 12 所示，选择“ 重新扫描 ”来确认当前开启 WPS 功能的无线网络，可以看到在下图中“ WPS AP 列表 ”中，出现了“ ZerOne_Lab ”的无线网络设备。

接下来，点击下方的“ PBC ”按键，开始尝试与该 AP 进行 WPS 自动连接。此时，在“ PBC ”按键右侧的状态栏中会出现“ PBC-Scanning AP ”的提示，表示当前处于扫描 WPS 设备当中。

图 12

稍等 10~~20 秒左右，会出现“ PBC-Get WPS profile successfully ”，即配置成功的提示，如下图 13 所示。此时，该无线网卡已经和 SSID 名为“ ZerOne_Lab ”的无线网络设备的 WPS 匹配成功，并成功连接至该无线网络。

图 13

此时若登录无线路由器，在其上对应的 WPS 设置中将能看到出现“ 添加无线设备成功 ”。如下图 14 所示。

图 14

步骤 4：查看无线连接加密配置内容

在客户端的无线网卡配置工具的 WPS 页面下点击打开内容项，可以看到具体的配置内容。如下图 15 所示，当前已连接网络名称为“ ZerOne_Lab ”，认证方法为 WPA2-PSK，加密方法为 TKIP，密钥为一系列星号显示。

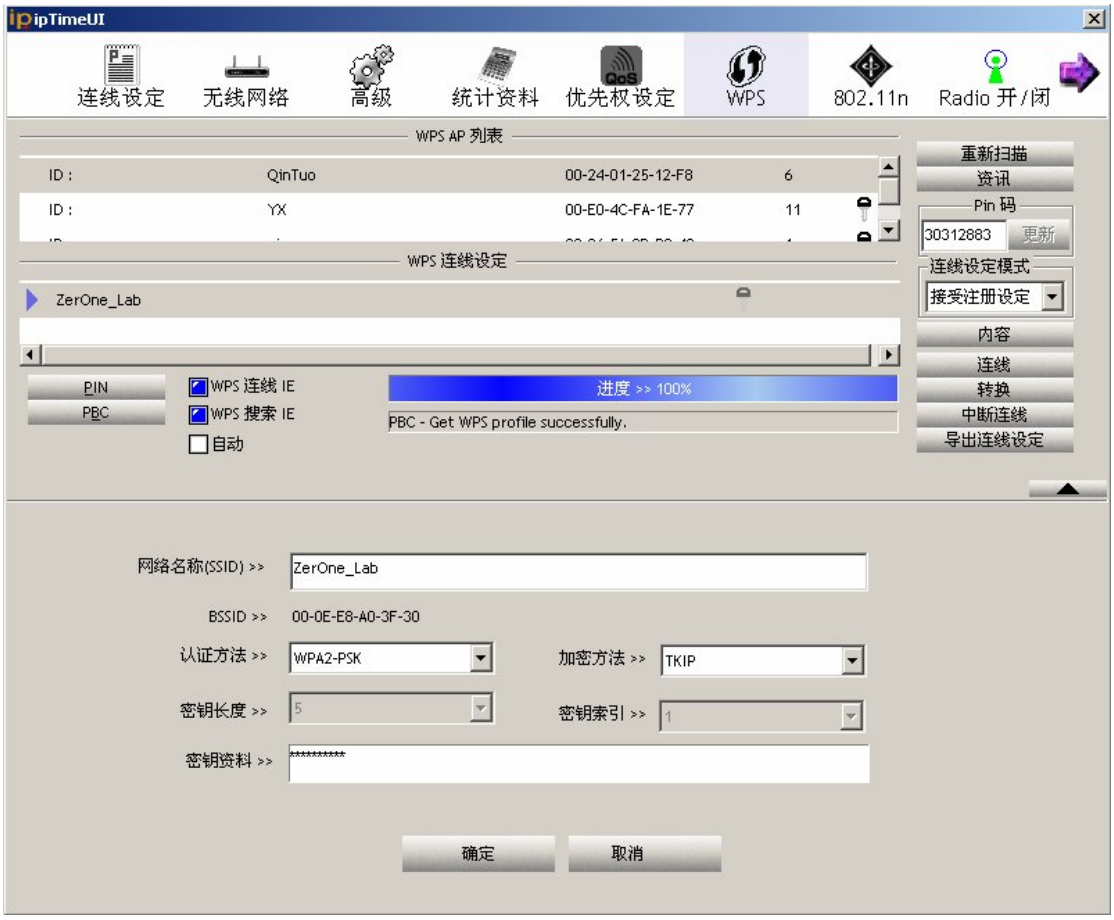

图 15

步骤 5：破解 WPA-PSK 或 WPA2-PSK 加密

既然是星号显示，那么使用星号查看器查看，即可显示出星号背后真实的密钥内容。如下图所示，打开星号密码查看工具，把鼠标光标移至密钥显示星号的位置，即可在下图 16 右上角密码查看工具中看到密码为 longaslast。

也就是说，当前 SSID 名为“ ZerOne_Lab ”的无线路由器，启用的 WPA2-PSK 密钥为：longaslast。至此，该无线网络的 WPA2-PSK 加密认证已被彻底攻破。

图 16

对于一些使用长字符串密码的 WPA-PSK 或者 WPA2-PSK 加密，此方法依然有效。如下图 17 所示，当前无线网络采用 WPA-PSK/WPA2-PSK 混合加密方式，具体密钥采用加密关键字为无规律长字符串。

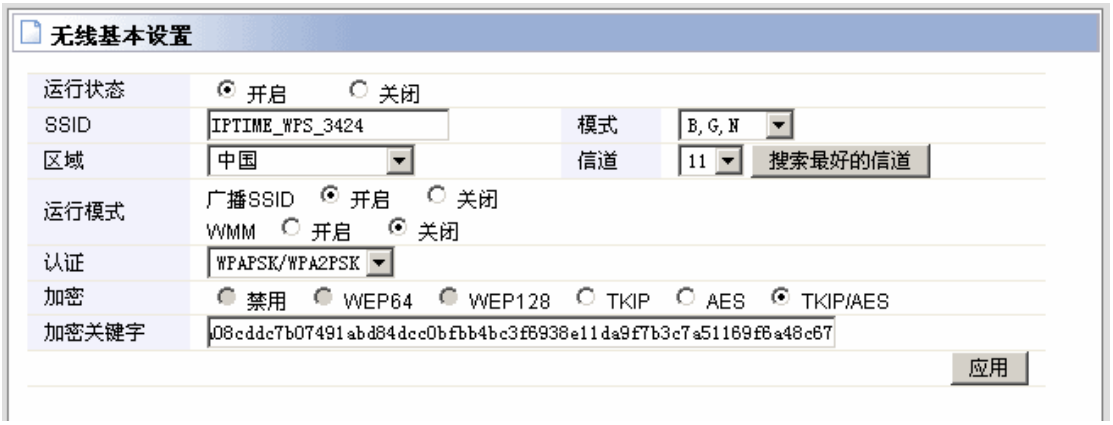

图 17

使用星号查看器查看，即可显示出星号背后真实的密钥内容。如下图 18 所示，当前 SSID 名为“ IPTIME_WPS_3424 ”的无线路由器，启用的密钥为：

35a08cddc7b07491abd8

即虽然之前设置时输入长达 60 多位的加密密钥，但在实际使用时只有前 20 位起作用。

Blog：http://bigpack.blogbus.com
Email：longaslast@126.com
欢迎拍砖、交流、合作及其它事宜，
新书《无线网络安全攻防进阶》筹备中，更多内容，即将推出！感谢一直以来的支持！！

这个原因除了 WPA-PSK 本身要求密钥在 8~~64 位之间的定义外，还可能因产品不同有所差异所导致。是不是很简单？

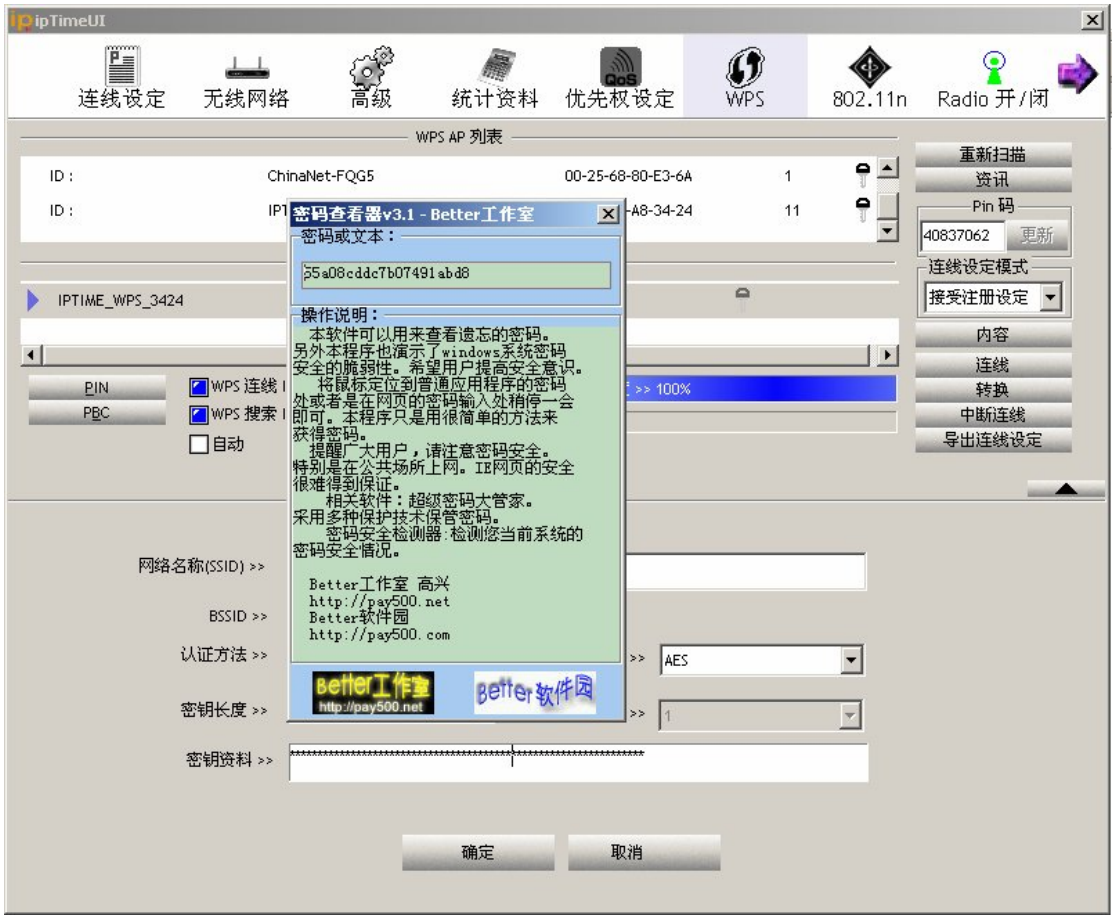

图 18

4．延伸攻击

既然 WPS 可以如此方便地使得无线客户端与无线网络设备之间建立认证关系，那么，是不是说具备 WPS 功能的无线设备就一定很不安全了呢？也不一定，因为有些设备默认是不开启 WPS 的，还有些设备甚至限制了 WPS 的搜索超时等，这些设定确实限制了攻击的效果，这就是为什么我说适合于市面上 99%的支持 802.11N 系列无线路由器以及 70%的 802.11G 无线路由器，注意是“适合”，并不是说就一定能搞定。不过，国内外的无线黑客们也想出了诸多新的方法来加强 WPS 攻击效果，下面给出几个比较有效的方式。

4．1　打造永久的 WPS 无线跳板后门

由于有些无线设备需要按住路由器上的 WPS 按钮才可以提供这个 WPS 功能。不过有些聪明的无线黑客发现只需要创建一个电路，来‘按下’无线路由器上的 WPS 按钮就可以了。对于某些品牌的无线路由器，比如 Linksys，甚至只需将无线设备上的 WPS 按钮上的引脚重新焊接，就可以使 WPS 功能保持永久开启，如下图 19 所示。

这样，这台无线设备就成为了内部网络中永远的无线后门。无论管理员修改成什么加密内容，黑客们都可以从外界快速地连接至该无线设备，并快速地获取到内部无线网络的加密密钥明文，而这样的后门可能很久都不会被发现！！

而这一切的一切并不难做到，只需要找个借口维修一下无线设备即可，甚至对于 Dlink

的某些品牌无线路由器而言，更是可以很容易地使用废弃的口香糖来将 WPS 按键包裹即可达到“ 按下 ”键位的效果，如下图所示。

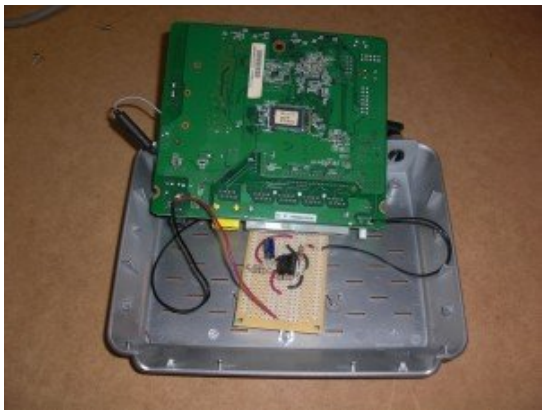

图 19

图 20

对于 Linksys 等品牌的无线网卡配置工具中，一旦通过 WPS 功能连接到无线网络后，黑客们甚至都不需要使用什么星号查看工具，直接打开就能看到 WPA-PSK/WPA2-PSK 加密的明文……恩，看看下图 21，这是不是可以说是个恶梦呢？

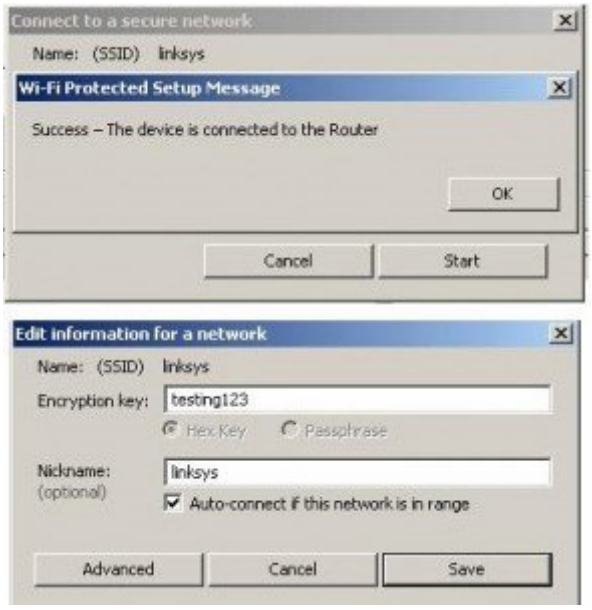

图 21

4． 2 使用 CSRF 攻击配合实现 WPS 攻击

还有一种情况，就是对于个别无线设备，其 WPS 功能无法主动配对，仍需要使用计算机登陆到无线路由器页面，然后在 WPS 选项中手动点选搜索。这个问题肯定会遇到，此时无线黑客们会考虑结合其它方式进行配合攻击，比如针对无线设备的 CSRF 攻击。

CSRF 的英文全称是 Cross Site Request Forgery，字面上的意思是跨站点伪造请求。以韩国 IPTime 无线路由器为例，将下述路径伪造后发送至具备管理员权限的用户，将会导致需要手动启动的 WPS 功能在后台悄悄启动，此时攻击者即可使用本节讲述的方法与 WPS 关联。

```
http://192.168.0.1/cgi-bin/wps_wizard.cgi?wps_pin=0
```

当然，使用一些脚本或者构造几个看不到的页面对于很多朋友来说并不困难，关于

CSRF 攻击更是有很多朋友都很擅长，各种黑客类期刊、网站以及论坛上也有很多高手已经发表了诸多文章，所以这里我就不再班门弄斧了，给出一个思路即可。关于针对无线设备的 CSRF 攻击有机会我们再来细细讨论，在《无线网络安全攻防进阶》里已经有专门的章节进行讲述，敬请期待。

5．后记

什么叫渗透？就是天马行空、物尽其用，无线渗透也是如此。也许本文的技术有些朋友会觉得很简单，但是渗透本就是如此的，除了较为复杂的技术，也有很多便捷的技巧，毕竟，有很多高级别的加密及防护技术都遭受过“ 马其诺防线 ”的结局。更多的方法我会在**《无线网络安全攻防实战》**后续的无线安全著作**《无线网络安全攻防进阶》**中给出实例和讲解。

欢迎大家与我联系：longaslast@126.com 或者直接到我的博客 http://bigpack.blogbus.com 做客。最后，对那些正使用无线 WPS 功能不亦乐乎的朋友们提个忠告：

有些技术方便的不光是我们，还有些不请自来之人。