

十大安全策略加固无线局域网安全 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/460/2021_2022__E5_8D_81_E5_A4_A7_E5_AE_89_E5_c100_460856.htm 移动鼠标点击电脑右下方的wifi（无线局域网）图标。你将发现你的无线局域网的名称。如果你像其它80%的wifi用户一样，很不幸你所连接的无线局域网可以说是不安全的。不安全的无线局域网实际上是邀请黑客访问你的电脑，盗取你的机密信息，上传软件最后对你发动攻击。幸运的是，只需要采取下述10条简单步骤，你就可以将你的无线局域网变得像纳克斯堡（美国国家黄金储藏地）一样牢不可破。修改管理员密码和用户名在你将路由器拆封，开始设置的时候，这时会弹出一个网页要求你输入网络地址和帐号信息。理论上来说，这一wifi设置是受注册屏保护的（用户名和密码）。问题：虽然用户名和密码的初衷是保证只有你才能进入wifi的设置程序以及你输入的个人信 息，实际上每个人都可以利用同样的路由器都是使用厂商提供的一样的注册。绝大多数人对此并没有对此做出任何改变，这样黑客就轻易侵入了，可以说是不费吹灰之力。解决方案：在第一次注册之后马上修改wifi设置中的用户名和密码。如果你打算这样做的话，尽量设置复杂的密码。黑客可能会使用一些简单的信息来猜测，譬如你的姓名，生日，纪念日，孩子或配偶的的姓名，或是宠物的，名字。一些黑客经常使用一种叫做“字典劫持”的方法（使用一种程序猜测常用的名字密码），因此你得保证你的密码的复杂性最好是字母与数字并存。升级wifi加密如果你在使用无线网络接受和发送信息的时候并没有采用充分的加密，黑客就可以轻易

的进入网络监控你的行为。如果你不幸正输入你的个人或是银行信息，黑客就可以借机盗取你的身份认证。传统的加密标准是有线等效保密（WEP）协议，然而黑客在30秒之内就可以将其破解，不管你使用多么复杂的密句。不幸的是，数以百万计的wifi用户使用的正是这种落后的WEP协议加密信息，我们本该选择更加先进的WPA2加密技术。

（Wi-Fi Protected Access，Wi-Fi保护访问，“WPA2”支持“AES”加密方式。老的“WEP”加密方式，在安全上存在着若被第三者恶意截获信号密码容易被破解的问题）。问题：尽管WPA2在加密保护方面有时明显，但是很多用户由于缺乏认识而没有采取升级措施，或是对升级所达到的效果不满意。所以，放着好的东西不用，他们宁愿选择WEP这种鸡肋似的老掉牙的加密技术。解决方案：解决之道当然是升级wifi加密到WPA2协议。但是你还是略作一些调整为升级铺平道路。第一步就是下载安装Windows XP版的WPA2 hotfix. 还有就是升级无线网卡驱动。这些升级在微软的Windows升级的“硬件选项”中找得到。既然你准备将你的电脑和网卡升级，你需要通过网页浏览器打开路由器注册界面（这就是你第一次设置wifi时的页面，你可以在说明书中找到这一URL地址）。注册成功之后，将安全设置改为“个人WPA2协议”并且勾选“TKIP AES”运算法则。最后在“共享密”中输入密码，保存修改。修改默认系统ID 当你买回Linksys 或D-Link路由器的时候并且安装的时候，它们都会有一个默认的系统ID叫做SSID或是ESSID。（SSID便是你给自己的无线网络所取的名字）。问题：一般来说，生产商都会在他们的设备上分配同样的SSID，80%的用户使用的是系统默认设置。

也就是说，80%的用户的wifi网络的名称就是出厂的默认设置。默认设置的一个问题就是黑客藉此可以了解一个wifi无线网络附近的所有网络，只需要使用默认的名称即可。尽管知晓SSID不会让所有的人进入我们的网络，但是却意味着这些网络缺乏有效的保护，因此这些网络往往成为羔羊。解决方案：在你配置你的局域网的时候马上改变默认的SSID.虽然这并不意味着你的网络访问会受到完全的控制，但是配置你的SSID将会使你区别于其它的未受保护的网路，黑客可能会知难而退。还有一个好处就是你的家人或是你不会因此链接到其它的网络之中，从而就不会将你暴露于黑客的枪口之下。

MAC地址过滤 如果你当初设置了不安全的wifi，很可能至少有不只一个网络邻居通过你联入网络。我们喜欢友好的邻居，但是这却给信息偷盗敞开大门，这时我们就不得不考虑了，更可怕的是还会伤害到你的电脑。想找出使用你的网络的人，你需要检查MAC地址。每一个wifi网络都被分配一个独一无二的物理地址或是MAC地址。你的wifi系统会自动记录下所有链接到你的设备的MAC地址。虽然找出这些MAC地址并不是完全有效，但是对保护无线局域网还是大有裨益的。

100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com