 大约在上世纪90年代初，借助于无线网络产品来扩展一个网络的灵活性的现象开始出现，从此以后，无线技术和无线设备开始逐渐流行起来。随着这些新的无线产品或技术的到来，安全似乎成了对无线网络如影随形的最大弱点。 在一个传统的有线网络中，攻击者要么必须从有线网络内部物理的连接你的网络中，要么需要想办法攻破边界防火墙或路由器的阻挡。而对于一个无线网络来说，一个潜在的攻击者所需要做的全部事情就是舒服的坐在他(她)的车里，手里具有一个支持无线功能的笔记本电脑和一个无线嗅探工具。 加固无线网络的安全性的方法有很多，本文的目的就是简单的描述一下其中比较常见的方法，以便你可以决定哪一个最适合让你来加固你的无线网络。 WEP(有线等效加密) 尽管从名字上看似乎是一个针对有线网络的安全选项，其实不是。WEP标准在无线网络的早期已经创建，目标是成为无线局域网WLAN的必要的安全防护层，但是WEP的表现无疑令人非常失望。它的根源在于设计上存在缺陷。 在使用WEP的系统中，在无线网络中传输的数据是使用一个随机产生的密钥来加密的。但是，WEP用来产生这些密钥的方法很快就被发现具有可预测性，这样对于潜在的入侵者来说，就可以很容易的截取和破解这些密钥。即使是一个中等技术水平的无线黑客也可以在两到三分钟内迅速的破解WEP加密。WEP破解过程如下图所示。 破解WEB是一个比较容易的过程 1、攻击者发送一个虚假的数据包给合

法的移动用户。 2、移动工作站使用WEP加密数据包，并将其转发给无线访问点(AP或路由器) 3、攻击者截获这个加密后的数据包，并将其与最初的数据包进行对比，以得到加密密钥。 尽管WEP已经被证明是过时且低效的，但是今天在许多现代的无线访问点和路由器中，它依然被支持。不仅如此，它依然是被个人或公司所使用的最多的加密方法之一。如果你正在使用WEP加密，我请你读完本篇文章的其余部分，并在以后尽可能的不要再使用WEP，如果你对你的网络的安全性非常重视的话。 