应用与技巧：消除无线网络安全风险 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E5_BA_94_E7_94_A8_E4_B8_8E_E6_c104_252302.htm 人们从来没有停止过对便利生活的追求，而为满足这种需要各种技术也不断被推动向前发展着。就在人们刚刚学会享受网络技术所带来的巨大便利之时，信息技术厂商已经在为我们描绘另一个更加宏大、美丽的场景，那就是无线网络。“ 网络能做什么 ”的浪潮已经过去，“ 如何使用网络 ”又将成为新一轮的竞争焦点。而这新一轮的网络发展正在力争让无线信号覆盖到全球的各个角落，试图让人们能够在任何时间、任何地点，通过任何设备都能联入全球网络。然而，当更多的线缆被肉眼看不见的无线信号取代以后，用户是否能够获得足够的安全保障将成为必须回答的问题之一。这就好似将所有的鸡蛋放在同一个篮子里。覆盖在地球表层的巨大信号体系既能够让我们的生活变得更加美好，也可能在转瞬之间夺走我们所有的安全感。 Wi-Fi Wi-Fi主要的安全问题 安全功能的隐患 从设计上来讲，Wi-Fi在安全方面所依仗的主要力量是WEP（有线对等保密）加密，然而这种保护手段已经被证明是不够强健的。更重要的是，WEP加密本身存在一些问题。WEP定义了一个24位的字段做为初始化向量（IV），而该向量会出现重用的情况。 设计与使用问题 大多数厂商的产品为了能够被快速配置和应用，并没有使用高安全系数的出厂设置。而很多用户并不了解如何配置，也往往不会对无线网络设备进行安全配置。 如何使Wi-Fi更安全 注意SSID SSID是一个无线网络的标识，在可能的情况下不应使用设备缺省的SSID。 另外，设

置为封闭的Wi-Fi网络不响应那些将SSID设置为Any的无线设备，而且不在无线网络内进行SSID广播，这样能够减少无线网络被发现的可能。 加固WEP 有限的WEP加密至少比不使用WEP的情况要好得多，所以一个基本的原则就是设置尽可能高强度的WEP密钥。 定期更换密钥 并不一定所有的环境都需要每周变更密钥，但是应该考虑至少每个季度更换一次密钥。随着时间的发展，一个从不更换密钥的无线网络其安全性会大幅度下降。 过滤计算机 通过指定一个特定的地址集，可以尽量保证只有得到授权的计算机才能访问无线网络。 企业应用的安全建议 新的往往更好 如果企业正在搭建无线网络，应该尽量购买使用较新的标准和协议的产品。而对于仍在使用旧标准设备的企业来说，应该紧密的关注厂商发布的升级信息。 利用已有的安全资源 对于安装了硬件防火墙的企业来说，尽量将无线访问点置于防火墙之外，这样将无线流量视为不受信任可以将防火墙应用于无线连接的过滤，从而提高安全起点。 将无线纳入整体安全策略 由于无线访问方式相对随意，所以将其进行监管显得尤其重要。不应该允许员工任意的在网络内部署无线设备，并应该定期的对公司的无线网络进行检查。 蓝牙（BlueTooth） 蓝牙的主要安全问题 蓝牙技术正以极快的速度渗透到人们的生活当中，根据很多市场调研机构的预测，在2008年蓝牙产品的市场需求量将达到目前的三倍。IDC预计在2008年将有超过半数的手机在出厂是内置蓝牙。 首要问题是产品漏洞 尽管蓝牙规范在推出伊始就针对安全性进行了较好的考虑，但是由于厂商实现和用户习惯等方方面面因素的影响，蓝牙应用的安全性仍然未臻完美。 目前在蓝牙领域发现的安全问题主要集中于信息盗取、设

备控制和拒绝服务攻击等，其大部分的原因都是由厂商设计上的缺陷造成的。 蓝牙受攻击的基本方式 目前已经发掘出一些方法可以突破蓝牙设备的安全机制。理论上被设置为不可见的蓝牙设备是不能够被发现的，然而事实并非如此。利用包括redfang（红獠牙，一种黑客工具）在内的一些软件工具可以发现处于不可见模式的蓝牙设备。 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