网络技术辅导:解析无线网络安全弊病威胁计算机等级考试
 伴随着低档次无线网络设备的价格不断走低，以及操作上的越来越简便，低档次无线局域网网络在最近几年得到了快速普及。为了方便进行资源共享、无线打印、移动办公操作，我们只要耗费几百元钱购买一台普通的无线路由器和一块无线网卡设备，就可以快速地搭建好一个简易的无线局域网网络了。不过，低档次无线局域网网络的不断普及，也容易给单位的信息安全带来不小的威胁。在这种情形下，我们该如何才能化解低档次无线网络的安全威胁，享受组网的快捷、便利呢? 低档次网络的安全弊病 以无线方式连接到小区宽带网络，并通过宽带网络进行共享访问Internet的组网环境下，我们往往只要先通过普通双绞线将低档无线路由器的WAN端口与小区宽带网络的交换端口连接在一起，然后参照说明书对无线路由器的连接端口参数进行合适的设置，就能上网访问了。由于在默认状态下，低档无线路由器会自动启用DHCP服务功能，当我们将无线网卡设备正确地安装到普通计算机上后，不需要进行任何参数设置就能自动连接到无线局域网网络中了。然而在享受组网便利的同时，低档次无线路由器的信号覆盖范围最远可达到300米左右，要是不采取安全措施进行防范的话，那么处于300米范围之内安装了无线网卡设备的普通计算机都能自动加入本地无线局域网网络中，那样一来本地无线局域网就容易遭遇非法攻击。 从目前来看，组建方便的低档次无线局域网存在下面一些安全弊病： 1、安全机制不太健全 低档次

无线局域网大部分都采用了安全防范性能一般的WEP协议，来对无线上网信号进行加密传输，而没有选用安全性能较高的WAP协议来保护无线信号的传输。普通上网用户即使采用了WEP加密协议、进行了WEP密钥设置，非法攻击者仍然能通过一些专业的攻击工具轻松破解加密信号，从而非常容易地截取客户上网地址、网络标识名称、无线频道信息、WEP密钥内容等信息，有了这些信息在手，非法攻击者就能方便地对本地无线局域网网络进行偷窃隐私或其他非法入侵操作了。 此外，低档次无线局域网几乎都不支持系统日志管理、入侵安全检测等功能，可以这么说低档次无线局域网目前的安全机制还不太健全。 2、无法进行物理隔离 低档次无线局域网从组建成功的那一刻，就直接暴露在外界，无线网络访问也无法进行任何有效的物理隔离，各种有意的、无意的非法攻击随时存在，那么无线局域网中的各种隐私信息也会随时被偷偷窃取、访问。 3、用户安全意识不够 低档次无线局域网往往只支持简单的地址绑定、地址过滤以及加密传输功能，这些基本安全功能在非法攻击者面前几乎没有多大防范作用。不过，一些不太熟悉无线网络知识的用户为了能够快速地实现移动办公、资源共享等目的，往往会毫不犹豫地选用组网成本低廉、管理维护操作简便的低档次无线局域网，至于无线局域网的安全性能究竟如何，相信这些初级上网用户几乎不会进行任何考虑。再加上这些不太熟悉无线网络知识的初级用户，对网络安全知识了解得更少了，这些用户在使用无线网络的过程中很少有意识去进行一些安全设置操作。 4、抗外界干扰能力差 无线局域网在工作的过程中，往往会选用一个特定的工作频段，在相同的工作频段内无线网络

过多时，信号覆盖范围会互相重叠，这样会严重影响有效信号的强弱，最终可能会影响无线局域网的信号传输稳定性.此外，无线上网信号在传输过程中，特别容易受到墙体之类的建筑物的阻挡或干扰，这样也会对无线局域网的稳定性造成一定的影响。对于那些低档次的无线局域网来说，它的抗外界干扰能力就更差了，显然这样的无线局域网是无法满足高质量网络访问应用要求的。 组网便利下的安全威胁 既然低档次无线局域网存在上述一些安全弊病，这些弊病要是突然发作起来或被非法攻击者利用的话，那么就可能给我们带来不小的安全威胁：1、造成隐私信息外泄 有的时候，不少无线局域网上网用户为了方便工作，往往会在不经意间将单位的重要隐私信息或核心工作信息，甚至将一些属于绝密范畴的信息通过移动设备挂上无线局域网网络中，这样无形之中就容易发生重要隐私信息外泄的危险，严重的时候能够给单位或个人造成巨大的经济损失。 2、降低内网安全能力 单位无线局域网附近有时还会存在一些家用无线局域网或者其他单位的无线局域网，这些无线局域网常常会用于移动办公或共享访问Internet网络的，这些无线网络的使用者大多没有足够的安全防范意识，并且他们应用无线网络的要求不是很高，也用不着对无线上网进行一些安全设置操作。在这种情形下，单位中任何一台安装了无线网卡设备的笔记本电脑都又可能自动连接到其他单位的无线局域网中，如此一来就容易发生这个单位的无线局域网与其他单位的无线局域网直接互联的现象，甚至可能出现单位无线局域网直接与Internet网络互联的现象，这些现象明显会降低单位内网安全防范能力，容易给单位造成严重的安全后果。 3、危及信息系统安全 考虑

到低档次无线局域网组网成本低廉，不需要进行复杂布线，管理维护也很方便，要是安全意识不到位，那么一些规模较小的单位很可能出于技术、成本等因素，来选用一些价格低廉、质量低劣的无线网络设备进行组网升级、信息点的延伸，由这些网络设备搭建而成的网络将会天然暴露在外界，无线网络访问无法做到有效的物理隔离，那样一来单位的信息系统安全将会随时受到危及。 化解无线网络安全威胁 虽然低档次无线局域网容易给我们带来各种意想不到的安全威胁，会给单位的信息系统造成不小的安全隐患，不过对于那些对安全性要求不是很高的小规模单位来说，仍然可以选用低档次的无线局域网，毕竟这种类型的组网成本非常低廉，更为重要的是通过制定有效的措施完全可以将低档次无线局域网的安全威胁降到最低限度，让规模不大的单位用户也能尽情地享受组网便利。 1、向检查要安全 为了随时了解单位无线网络的安全状态，我们应该定期对单位的内网、外网使用情况以及核心网络设备的工作状态进行详细检查，并做好详细的检查记录。与此同时，我们还应该加大力度对单位无线局域网附近区域的无线网络工作环境进行动态监测，一定的时候还需要对单位的网络系统安全进行评估以及审计.此外，对于涉及到处于单位核心隐私信息以及进行重要网络应用的工作场所，应该及时采取电磁屏蔽等手段，来阻止非法网络入侵或攻击。 2、向宣传要安全 由于低档次无线局域网很容易影响到单位内部网络的使用安全性，为此单位负责人必须准备好丰富齐全的网络安全资料，在单位上、下定期开展无线上网安全知识的宣传、培训，以便强化每一位无线上网用户的安全防范意识，同时有必要针对性地进行网络安全专项整

治工作，保证单位所有员工都能在思想上高度重视无线网络安全工作。 3、向管理要安全 俗话说“ 没有规矩，不成方圆 ”，为了保证无线局域网的使用安全性，我们同样要对无线网络设备的使用做出合理的规定，对无线上网用户进行合理地管理，统一规范无线网络设备的工作模式以及安全设置，明确上网用户的使用范围和访问权限.例如，禁止保存有重要单位信息的笔记本电脑连接到无线局域网中，禁止随意在无线局域网中进行共享访问，禁止移动设备随意挂上无线局域网中，对于存储、加工核心信息的工作场所必须进行屏蔽保护等。 相信在清醒地认识到低档次无线局域网存在的种种安全威胁后，我们只要采取有效的安全措施进行防范，还是能够享受到无线组网的便利，让低档次无线局域网也能很好地为我们提供“ 服务 ”。 特别推荐： 2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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