无线局域网的安全风险分析和解决方案 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__E6_97_A0_E7_BA_BF_E5_B1_80_E5_c98_460923.htm 我们基本上可以从下面几个方面考虑解决WLAN存在的安全问题。 1.首先确定安全策略，定位WLAN在整个工作中的主要用途，涉及传输数据和人员、设备。然后具体规划AP的物理位置、客户端的访问权限和控制模式等。 2.从网络结构着手。限制WLAN信号的范围，并将WLAN和重要的内部网络之间明确区分开来，在AP和内部网络之间采用防火墙进行安全隔离，必要时采用物理隔离手段。这样即使WLAN出现了安全问题也不会立即导致内部网络的严重危机。 3.避免Ad Hoc网络的产生。这需要管理员对员工的培训，以及对网络的不断监控。 4.禁用用户计算机的某些操作系统和应用程序对WLAN的自动连接功能，避免这些用户无意识地连接到未知WLAN中。 5.充分利用WLAN本身提供的安全特性进行安全保障。比如对于AP可以做以下工作： a)更改缺省的口令。一般设备出厂时的口令都非常简单，必须要更改； b)采用加密手段。尽管WEP已经被证明是比较脆弱的，但是采用加密方式比明文传播还是要安全一些； c)设置采用MAC地址的方式对客户端验证。在没有实施更加强壮的身份验证措施之前，这种防范措施还是必要的； d)更改SSID，并且配置AP不广播SSID。 e)更改SNMP设置。这种防范措施是和有线网络设备相同的。 6.在WLAN本身传输的数据重要性较高，或者连接到一个密级较高的网络的情况下，可以考虑采用进一步的安全防范措施： a)采用802.1x进行高级别的网络访问控制。尽管802.1x标准最初是

为有线以太网设计制定的，但它可以用于WLAN。802.1x导入了认证服务器，可以对WLAN中的主客体进行高级别的认证，认证方式可以选择采用传统的RADIUS服务器进行。 b)采用TKIP技术替代现有的简单WEP加密技术。这种方式的优势在于不需要全部更换硬件设备，仅仅通过更新驱动程序和软件就可以实现。另外，目前正在制订中的802.11i提供了进行了加密强化的WEP2（基于AES），以及强化的认证协议EAP。但是802.11i的成熟和推广尚且需要一段时间。 c)在WLAN之上采用VPN技术，进一步增强关键数据的安全性。VPN技术同样不是专门为WLAN设计的，但是可以作为关键性WLAN的增强保护。 7.采用WLAN 专用入侵检测系统对网络进行监控，及时发现非法接入的AP以及假冒的客户端，并且对WLAN的安全状况进行实时的分析和监控。 8.在WLAN的客户端采用个人防火墙、防病毒软件等措施保障不受到针对客户端攻击行为的损害。 正如上文所述，WLAN的安全既可以依靠WLAN本身具有的安全保障措施提供，也需要借助一些专用的安全产品来实现，同时需要有一套合理的WLAN专用安全管理规范和制度。下面介绍一些可以用于WLAN的安全产品。 WLAN安全产品 冠群金辰公司是一家专业的信息安全方案和服务提供商，提供防火墙、入侵检测、主机核心防护、防病毒、VPN、漏洞扫描、内容过滤网关等一系列安全产品，并具有强大的安全服务能力和研发能力。下面主要介绍三种产品：WLAN入侵检测系统、VPN和掌上设备的防病毒系统。 WLAN入侵检测系统 WLAN入侵检测系统是冠群金辰研发中的一种基于网络的入侵检测系统，除了能够对普通有线网络的入侵模式进行识别和响应，主要是针对采

用802.11b协议的WLAN进行网络安全状态的判断和分析
，WLAN入侵检测系统采用了分布式的结构，将进行数据采集的Sensor分布在WLAN的边缘和关键地点，并且通过有线的方式将收集到的信息统一传输到一个集中的信息处理平台。信息处理平台通过对802.11b协议的解码和分析，判断有无异常现象，比如非法接入的AP和终端设备、中间人攻击、有无违反规定传输数据的情况，以及通过对无线网络进行的性能和状态分析，识别拒绝服务攻击现象。它能够自动发现网络中存在的Ad Hoc网络，并且通过通知管理员来及时阻止可能造成的进一步损害。基于Web界面的安全管理界面让管理员可以进行策略的集中配置和分发，以及观察网络状况、产生报表。 WLAN入侵检测系统通过结合协议分析、特征比对以及异常状况检测三种技术，对WLAN网络流量进行深入分析，并且能够实时阻断非法连接。 