 安全问题始终是无线局域网的软肋，一直制约着无线局域网技术的进一步推广。从无线局域网技术的发展来看，人们一直都致力于解决无线局域网的安全问题。了解无线网络的安全进程，有助于用户采取有效的安全措施。 在无线局域网的早期发展阶段，物理地址(MAC)过滤和服务区标识符(SSID)匹配是两项主要的安全技术。物理地址过滤技术可以在无线访问点AP中维护一组允许访问的MAC地址列表，实现物理地址过滤。服务区标识符匹配则要求无线工作站出示正确的SSID，才能访问AP，通过提供口令认证机制，实现一定的无线安全。 物理地址过滤和服务区标识符匹配只能解决有限的安全问题。为了进一步解决安全问题，有线等效保密(Wired Equivalent Privacy，WEP)协议被推到台前。WEP用于在无线局域网中保护链路层数据。WEP使用40位、64位和128位钥匙，采用RC4对称加密算法，在链路层加密数据和访问控制。WEP具有很好的互操作性，所有通过Wi-Fi组织认证的产品都可以实现WEP互操作。 不过，WEP的密钥机制存在被破译的安全隐患，势必要被趋于完善的其他安全技术所取代。端口访问控制技术(Port Based Network Access Control，IEEE 802.1x)和可扩展认证协议(Extensible Authentication Protocol，EAP)可以看成是完善的安全技术出现之前的过渡方案。IEEE 802.1x标准定义了基于端口的网络访问控制，可以提供经过身份验证的网络访问。基于端口的网络访问控制使用交换局域网基础结构的物理特

征来对连接到交换机端口的设备进行身份验证。如果身份验证失败，使用以太网交换机端口来发送和接收帧的行为就会被拒绝。虽然这个标准是为有线以太网络设计的，但是经过改编后可以在IEEE 802.11无线局域网上应用。EAP不专属于某一厂商，它能够弥补WEP的弱点，并且同时能够解决在接入点之间的移动性问题。EAP还解决了VPN瓶颈问题，使用户能够以有线网络的速度进行工作。不过，配置EAP不是一件容易的事情，这也就是为什么PEAP受到欢迎的原因。PEAP是由微软，思科和 RSA Security共同开发，致力于简化客户端、服务器端以及目录的端到端整合。 Wi-Fi保护接入(Wi-Fi Protected Access，WPA)是作为通向802.11i道路的不可缺失的一环而出现，并成为在IEEE 802.11i 标准确定之前代替WEP的无线安全标准协议。 WPA是IEEE 802.11i的一个子集，其核心就是IEEE 802.1x和暂时密钥完整协议(Temporal Key Integrity Protocol，TKIP)。 WPA使包括802.11b、802.11a和802.11g在内的无线装置的安全性得到保证。这是因为WPA采用新的加密算法以及用户认证机制，满足 WLAN的安全需求。WPA沿用了WEP的基本原理同时又克服了WEP缺点。由于加强了生成加密密钥的算法，即使黑客收集到分组信息并对其进行解析，也几乎无法计算出通用密钥，解决了WEP倍受指责的缺点。不过，WPA不能向后兼容某些遗留设备和操作系统。此外，除非无线局域网具有运行WPA和加快该协议处理速度的硬件，否则WPA将降低网络性能。 WPA2是Wi-Fi联盟发布的第二代WPA标准。WPA2与后来发布的802.11i具有类似的特性，它们最重要的共性是预验证，即在用户对延迟毫无察觉的情况下实现安全快速漫游，同时采用CCMP加密包来替

代TKIP。 2004 年6月，802.11工作组正式发布了IEEE 802.11i，以加强无线网络的安全性和保证不同无线安全技术之间的兼容性，802.11i标准包括WPA和RSN两部分。WPA在文章前面已经提过。 RSN是接入点与移动设备之间的动态协商认证和加密算法。802.11i的认证方案是基于802.1x 和EAP，加密算法是AES。动态协商认证和加密算法使RSN可以与最新的安全水平保持同步，不断提供保护无线局域网传输信息所需要的安全性。与WEP和 WPA相比，RSN更可靠，但是RSN不能很好地在遗留设备上运行。 在Wi-Fi推出的初期，专家也建议用户通过VPN进行无线连接。 VPN采用DES、3DES等技术来保障数据传输的安全。IPSec VPN和SSL VPN是目前两种具有代表意义的VPN技术。IPSec VPN运行在网络层，保护在站点之间的数据传输安全，要求远程接入者必须正确地安装和配置客户端软件或接入设备，将访问限制在特定的接入设备、客户端程序、用户认证机制和预定义的安全关系上，提供了较高水平的安全性。SSL被预先安装在主机的浏览器中，是一种无客户机的解决方案，可以节省安装和维护成本。 对于安全性要求高的用户，将VPN安全技术与其他无线安全技术结合起来，是目前较为理想的无线局域网安全解决方案。 面对形形色色的无线安全方案，用户需要保持清醒：即使最新的802.11i也存在缺陷，没有一种方案就能解决所有安全问题。例如，许多Wi-Fi解决方案当前所提供的128位加密技术，不可能阻止黑客蓄意发起的攻击活动。许多用户也常常会犯一些简单错误，如忘记启动WEP功能，从而使无线连接成为不设防的连接，用户没有在企业防火墙的外部设置AP，结果使攻击者利用无线连接避开防火墙，入侵局域网。对于用户

来说，与其依赖一种安全技术，不如选择适合实际情况的无线安全方案，建立多层的安全保护机制，这样才能有助于避免无线技术带来的安全风险。