WPA2与思科LEAP安全协议有何不同？ PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022_WPA2_E4_B8_8E_E6_80_9D_c101_142528.htm 您能帮助我理解WPA2和思科LEAP安全协议的区别吗?哪一个更好、更方便或者更安全?思科的LEAP(轻型可扩展身份验证协议)是一个专有的、IEEE 802.1X端口访问协议标准批准之前的变体。802.1X是一个框架，让一台身份识别服务器在批准无线用户进入接入点的分布式网络(也就是接入点连接的有线网络)之前验证那个无线用户的证书。802.1X能够与许多不同的证书一起使用，如口令、令牌和证书等。这是通过让802.1X的请求和回答携带任何种类的EAP(可扩展身份验证协议)来完成的。 思科LEAP是这些种类的EAP之一，旨在提供口令身份识别。当使用LEAP的时候，接入点查验这个客户机的用户名，在客户机和身份识别服务器转发RADIUS(远程认证拨入用户服务)信息。这台身份认证服务器使用MS-CHAP(微软质询握手身份验证协议)查验客户机的口令。这台客户机不发送其口令，它使用这个口令和盘问生成一个hash(哈希)。这台服务器生成自己的hash，并且将这个hash与客户机发来的hash值进行比较。如果相匹配，这个客户机就被接受了。然后，另一个MS-CHAP交换让客户机识别服务器的身份。当双方都满意时，客户机和服务器就交换加密的密钥，这样，在这个过程中发送的数据就可以受到WEP的保护。 遗憾的是，LEAP容易受到字典攻击。首先，用户名是在没有加密的情况下发送的，每一个人都可以发现它。第二，使用字典中的词汇生成的hash值比较客户机发出的hash就能够破解(或者猜出)口令。还有一些共享的软件工

具能够自动进行破解。这些软件工具包括Anwrap、Asleap和THC-LEAPcracker。使用非常长的、随机的口令有助于阻止字典攻击。但是，这种绕过漏洞的方法是不实际的，因为许多WLAN与现有的用户名(如Windows域名)和口令一起使用LEAP。事实上，这就是LEAP为什么容易部署的原因。 还有许多能够与802.1X一起使用的其它陌生的EAP类型。例如，EAP-TLS支持基于数字证书的双向认证。PEAP(保护的EAP)支持在加密的TLS通道上的MS-CHAPv2口令认证，从而防止偷窥和字典攻击。事实上，有40多种定义的EAP类型。有些比LEAP弱一些(如EAP-MD5)，有些功能更强大一些(如EAP-TLS和PEAP)。当然，有一些类型的EAP比LEAP更难使用。例如，要使用EAP-TLS，你的客户机必须要有证书。没有一种EAP类型能够满足每一个人的需求。 与WPA2有关的协议如何呢?WPA协议第二版是Wi-Fi联盟管理的一个认证计划。正确采用符合IEEE 802.11i增强安全标准的部件的产品都可以通过WPA2测试。当你购买支持WPA2的无线产品时，这种产品将采用802.1X身份识别和AES加密。这种产品可能与EAP-TLS一起支持802.1X，也可能支持其它的EAP类型。因此，WPA2提供了比LEAP功能更强大的身份识别，以及更强大的数据加密。 但是，选择一个EAP类型的协议与WPA2协议一起使用要留给消费者做出决定。因此，安全最终与配置有关，如何做出决定取决于你的WLAN。但是，大多数使用WPA2协议的WLAN都使用功能更强大的EAP类型的协议，而不是使用LEAP。部署WPA2是很复杂的，特别是在拥有多种客户卡和操作系统的网络中。但是，在一家厂商的WLAN中与PEAP一起使用WPA2协议大约同部署思科LEAP一样费力

。 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