关于无线局域网应用中的安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_85_B3_E4_BA_8E_E6_97_A0_E7_c101_461772.htm 即使无线局域网络的系统管理者使用了内置的安全通讯协议：WEP(Wired Equivalent Privacy)，无线局域网的安全防护仍然不够。在伦敦一项长达7个月的调查显示，94%的无线局域网都没有正确设定，无法遏止黑客的入侵。隶属于国际商会(International Chamber of Commerce)的网络犯罪部门(Cybercrime Unit)就发现，即使无线网络很安全，也会因为种种原因而大打折扣。现在非常盛行「路过式的入侵(drive-by hacking)」，黑客开车进入商业办公区，在信号所及的地方，直接在车里渗透企业的无线局域网。 University of California at Berkeley(美国加州柏克莱大学)的三名研究人员，Nikita Borisov、Ian Goldberg、以及Dabid Wagner，在去年发现WEP编码的重大漏洞.除此之外，在2001年8月，密码学家Scott Fluhrer、Itsik Mantin、以及Adi Shamir在一篇论文中，指出了RC4编码的缺点，而RC4正是WEP的基础。就在几天后，2001年8月底，Rice University(美国莱斯大学)的学生与两名AT&amp.T(美国电报电话公司)实验室的员工(Adam Stubblefield与John Joannidis、Aviel D. Rubin)，将这两篇论文的内容化为实际的程序代码。令人惊讶的是，其中完全没有牵扯到任何特殊装置，你只要有一台可以连上无线网络的个人计算机，从网络上下载更新过的驱动程序，接下来就可以开始记录网络上来往的所有封包，再加以译码即可。 WEP的运作方式 在许多无线局域网中，WEP键值(key)被描述成一个字或位串，用来给整个网络做认证。

目前WEP使用2种编码大小，分别是64与128位，其中包含了24位的初始向量(IV，Initialization Vector)与实际的秘密键值(40与104位)。大家耳熟能详的40位编码模式，其实相当于64位编码。这标准中完全没有考虑到键值的管理问题.唯一的要求是，无线网卡与基地台必须使用同样的算法则。通常局域网的每一个用户都会使用同样的加密键值.然而，局域网用户会使用不同的IV，以避免封包总是使用同样WEP键值所「随机」产生的RC4内容。 在封包送出之前，会经过一个「忠诚检查(IC，Integrity Check)」，并产生一个验证码，其作用是避免数据在传输过程中，遭到黑客窜改。RC4接下来会从秘密键值与IV处，产生一个keystream，再用这个keystream对数据与IC做互斥运算(XOR，Exclusive-Or)。首先IV会以一般文字方式传送出去，然后才是加密后的数据。只要将IV、已知的键值、以及RC4的keystream再做一次互斥运算，我们就可以将数据还原。 弱点：初始向量(IV，Initialization Vector) 40或64位编码可以填入4组键值.然而我们只使用了第一组。 WEP编码的弱点在于IV实作的基础过于薄弱。例如说，如果黑客将两个使用同样IV的封包记录起来，再施以互斥运算，就可以得到IV的值，然后算出RC4的值，最后得到整组数据。 如果我们使用的初始向量为24位，那我们就可以在繁忙的网络点上(例如以11Mbps的频宽，不断传送1500字节的封包)，以不到5小时的时间算出结果。以这样的例子来说，总数据量为24GB。因此，要在几小时的时间内，记录所有传输的封包，并以笔记本计算机算出其结果，是绝对可行的事情。 由于该标准并没有规定IV所产生的相关事宜，所以并不是每家厂商都用到IV的24个位，并在短时间内就重复用到相

同的IV，好让整个程序快一点。所以黑客所要记录的封包就更少了。以Lucent(朗讯)的无线网卡来说，每次激活时它就会将IV的初始值设为0，然后再往上递增。黑客只要记录无线网络上几个用户的数据内容，马上就可以找到使用同样IV的封包。 Fluhrer、Martin、Shamir三人也发现，设计不良的IV有可能会泄漏键值的内容(信心水准为5%)，所以说只要记录400～600万个封包(顶多8.5 GB的数据量)，就有可能以IV来算出所有的WEP键值。 更进一步探讨，如果WEP键值的组合不是从16进位表，而是从ASCII表而来，那么因为可用的字符数变少，组合也会变少。那么被黑客猜中的机率就会大增，只要一两百万个封包，就可以决定WEP的值。 网络上可找到的入侵工具 Adam Stubblefield在其论文中详尽的描述了整个过程，却仅限于理论.但现在网络上四处可见这些免费的入侵工具程序。与Stubblefield所提的类似，所有程序支持的几乎清一色是Prism-2芯片。使用这芯片的包括了Compaq(康柏)WL100、友讯(D-Link)DWL-650、Linksys WPC11、以及SMC 2632W等，都是市面上常见的产品。会选用这芯片的原因是因为其Linux驱动程序(WLAN-NG)不需要登入网络，即可监听封包。这程序会先搜寻设计不良、有漏洞的IV，然后记录500～1,000万不等的封包，最后在那间将WEP键值算出来。 黑客可以采取主动式攻击 由于以上所说的被动式攻击(单纯的纪录封包)十分可靠、有效，所以主动式攻击反而失去了其重要性。不过毫无疑问的，黑客也可以主动的侵入网络，窃取数据。我们假设黑客知道了原始数据及加密后的数据，收讯方会将这些信息视为正确无误。接下来黑客就可以在不需要知道键值的情形下，将数据偷天换日，而收讯方仍然会将这些数

据当成正确的结果 有效的解决方法 RSA Security(RC4编码的发明机构)与Hifn(位于加州，专精于网络 安全的公司，www.hifn.com)正努力加强WEP的安全，并发展新的运算法则。两家机构为RC4发展的解决方案为「快速封包加密(Fast Packet Keying)」，每个封包送出时，都会快速的产生不同的RC4键值。传送与接收双方都使用了128位的RC4键值，称为暂时键值(TK，Temporal Key)。当双方利用TK连结时，会使用不同的keystream，其中会加入16位的IV，再一次的产生128位的RC4键值。用户可以通过软硬件与驱动程序更新，在现有无线局域网中使用RC4快速封包加密。 思科自行其道网络大厂Cisco(思科)则大幅改进其Aironet系列产品，不过这系列只能搭配自家产品使用。无线局域网安全的第一步应该是双方面，而非单方面的。为了搭配其Radius Server(Access Control Server 2000 V2.6)，思科还发展了LEAP通讯协议(Lightweight Extensible Authentication Protocol，轻量可延伸授权通讯协议)。 思科使用的是分享键值(shared-key)方法，以响应双方的通讯要求。不可逆、单方向的杂凑键(hash key)可以有效阻隔复制密码式的攻击。 至于WEP键值，思科采取了动态的、每个用户、每次通讯只用一次的WEP键值，由系统自行产生，系统管理者完全不需介入。每个通讯过程中，用户都会收到独一无二的WEP，而且不会跟其它人共享。在将WEP广播送出之前，还会以LEAP加密一次，只有拥有相对应键值的人，才能存取信息。 与Access Control Server 2000 2.6结合以后，就可以建立重复的认证模式。用户会每隔一段时间为自己做认证，并在每次登录时获得一个新的键值。每次通讯时，IV都会被更改，黑客就无法使用这些信息，建立密

码表。 最后，这些方法都不能提供万无一失的防护，因为背后用的都还是IV与WEP加密机制.不过不断变换的键值，的确能有效的遏止黑客攻击，让使用密码表的作法失败。如果键值更换的速度够频繁，黑客所记录的封包就无法提供足够的破解信息，你的无线局域网就会比较安全。 IEEE正在发展新的WEP标准(www.ieee.org)。在这项标准中，RC4将会以更新的编码通讯协议所取代，预计会使用AES(Advanced Encryption Standard，高级加密标准)。 