户端服务器，连接数据库对输入的信息进行判断，正确，直接登入到主界面中，错误，进行重新登入。

2）浏览查询商品功能：输入信息，将输入内容发送至服务器端，服务器处理逻辑请求、将搜索结果列表造型、发送信息之客户端，客户端将所得到的的结果在界面显示出来，在客户端选择具体的商品，显示商品详细信息，选择数量、加入购物车并购买。

购物车：点击购物车，客户端本地请求响应、读取本地文件、造型为对象，将列表中元素在客户端显示，点击提交订单、将数据写成字节流发送至服务器，服务器读取数据写入数据库。

订单查询功能：点击订单查询，请求发送至客户端服务器，服务器响应请求、将搜索结果列表造型发送信息至客户端显示。

5）缺物登记功能：点击缺书登记，转到缺书登记输入页面、输入相应信息，将请求发送至服务器，服务器响应请求将读取数据写入数据库。

6）网站留言聊天功能：点击网上聊天室，跳出登陆页面，成功登陆后即可跳出对话框进行群聊，群聊内容还可存入到数据库中。点击留言，跳出留言框，输入相应信息提交即可将数据插入数据库中，还可点击查看留言即可看到所有客户的留言信息。

后台：

1）管理员登入管理：输入账号密码到数据库进行验证，正确，直接登入到主界面中，错误，进行重新登入。

2）商品管理：成功登陆后，点击图书新增，页面显示新增页面，即可按规定输入相应图书信息，保存到数据库中；点击图书查询，页面将显示所有图书信息，以便修改或者删除；点击缺书查看，页面将显示所有所缺图书，也可定向查询，以便将已经增添的图书（现已经不缺）给删除。

3）订单管理：点击订单查看，页面显示出所有客户的订单，而管理员此时可以在搜索框中按条件输入，查询相应订单；点击订单处理，页面显示所有为完成订单，用户可对订单状态进行修改，同时也可定向查询符合条件的订单，以便修改。

4、系统实现及总计

开发人员在进行了系统的分析和设计后，开发人员通过基于Android 平台的程序编程后实现了基于 Android 移动设备的 B2C 电子商务系统，该系统经过测试运行后准确无误，并切实有效。

（苏州大学计算机科学与技术学院）

作者简介：孙慈嘉，女，本科生，苏州大学计算机科学与技术学院，研究方向：移动系统开发。周小科，男，博士生，讲师，苏州大学计算机科学与技术学院，研究方向：数据挖掘，地理信息系统，智能信息处理。

WPA/WPA2 协议安全性研究

马 迅

WPA/WPA2 是目前无线网络加密使用的主要协议，本文详细分析了该协议的原理和加密过程，深入分析了802.11i 的四步握手协议，并从中分析和探求了存在的安全性问题。

引言

无线局域网，因组网方式灵活，备受人们的喜爱。近来，即插即用的无线 AP 设备的推出，使无线局域网受到了更多人的关注。越来越多的人，开始通过无线网络，来使用终端和移动设备，在此，我们不禁要问，无线网络安全吗？

WEP

1. WEP 介绍

早期版本的 IEEE802.11 采用有线等效加密（wired equivalent privacy，wep）协议进行加密，WEP 协议是用在两台设备间无线传输的数据进行加密的方式，防止非法用户窃听或侵入无线网络。WEP 的设计较为简单，使用一个基于挑战与应答的认证协议和加密协议，用相同的密钥和加密算法来对数据进行加密盒解密。采用的是对称加密原理。使用 RC4 作为加密算法，密码长度分为 64bit 和 128bit 两种类型，其中包含 24bit 的初始向量（initial vector，IV）和 40bit 或 104bit 的密钥。另外，为了保护信息在传输过程中不会被修改，WEP 还包括一个使用 32 位 CRC 的校验机制（integrity check value，ICV）。

2. WEP 加密的过程

首先，计算校验和，得到明文。通过把输入的数据和计算得到的校验和组合起来得到新的加密数据，即明文，明文是下一步加密过程的输入。然后，将 24 位初始化向量 IV 和 40 位的密钥 PASSWORD 通过 RC4 算法产生一个 64 位的密码 KSA = RC4（IV+PASSWORD）。将这个 KSA 输入到虚拟随机数产生器中，它对初始化向量和密钥的校验和计算值进行加密计算。然后，利用校验和算出明文 DATA 的 CHECK SUM，将它附加于明文 DATA 后，并与之前产生的密码 KSA

按位异或运算，得到的 ENCRYPTED DATA 为加密后的密文。最后，将 IV 附加于 ENCRYPTED DATA 之后一起发送出去。

3. WEP 加密的缺陷

1）因为 RC4 是 stream cipher 的一种，同一个钥匙绝不能使用二次，所以使用 IV 的目的就是要避免重复。然而由于 24BIT 的 IV 空间太小，很容易造成 IV 重复使用。而且这个初始化向量是以明文传送的，攻击者可以通过抓包轻易获得。许多 WEP 系统要求密钥得用十六进制格式指定，有些用户会选择在有限的 0-9 A-F 的十六进制字符集中可以拼成英文词的密钥，如 C0DE C0DE C0DE C0DE，这种密钥很容易被猜出来。

2）CRC-32 校验问题。该算法是用来检验数据完整性的，本身并没有防止恶意攻击的能力。所以对网络上的恶意攻击毫无办法。

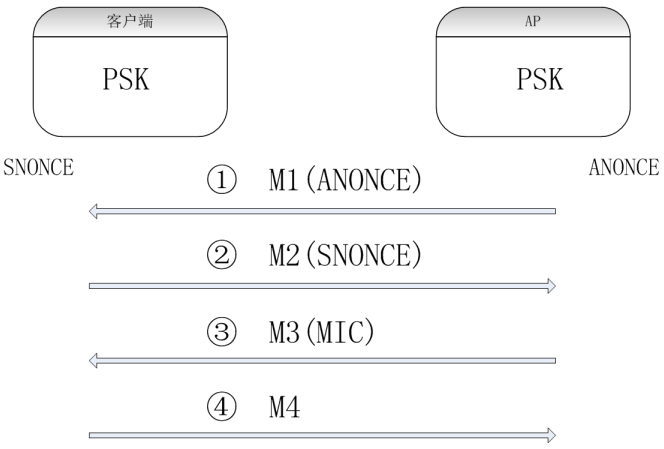
WPA/WPA2

1. WPA/WPA2 介绍

WEP 的重大缺陷，使得硬件厂商和实验室迫切需要开发一种新的安全协议，来保障无线网络的安全，由于 802.11 协议非常复杂，标准的制定又非常的耗费时间，Wi-Fi 联盟联合制定了 WPA 协议。后来，WPA 协议又经过 802.11i 修订和完善，就有了 WPA2 协议。WPA 协议有企业版和个人版两种模式。企业版需要架设专门的服务器来做客户端的认证，成本高投入大，但是安全性比较高，一般很少成为攻击的对象。所以本文主要针对个人版进行讲述。

2.WPA/WPA2 认证方式和认证过程

WPA 使用预共享密钥（Pre-shared key，PSK）模式，通过四次握手，完成认证过程。预共享密钥是一组 ASCII 码，长度可以是 8-63。在认证开始前，由认证双方协商获得。WPA 加密算法使用预共享密钥和 SSID 计算出成对主密钥（pairwise master key，PMK）。四次握手的具体过程和分析如下：



1）认证者向申请者发送消息 M1，M1 中包含用于产生 PTK（pairwise transient key，成对临时密钥）的一个随机数（由 AP 提供，称为 ANONCE）。

2）申请者利用事先共享的 PMK、ANONCE 和另一个随机数（由客户端提供，称为 SNONCE）计算 PTK。发送 EAPOL-KEY 消息 M2，M2 中包含 SNONCE，并且用刚计算出的 PTK 中的 KCK（EAPOL-KEY 完整性密钥）部分对 M2 进行 MIC（message integrity code，消息完整性校验值）认证

3）认证者得到 SNONCE 并利用事先共享的 PMK 计算出 PTK，利用 PTK 中 KCK 部分对 M2 进行 MIC 校验，如果校验失败就丢弃该 M2，正确则向申请者发送 M3，M3 中包含一个 MIC 校验，使申请者能够核实认证方拥有一个匹配的 PMK。

4）申请者收到 M3，校验正确后即装入 PTK，并发送 M4 给认证者，表示已经装入 PTK。认证者在收到 M4 并校验正确后也装入 PTK，至此四次握手过程完成，PTK 产生并完成装载。

3. WPA/WPA2 安全性分析

第一种情况：四次握手第二步客户端发送 M2 后，攻击者冒充 AP 向客户端发送伪造的 M1*，客户端收到伪造的 M1* 后，用攻击者的 ANONCE* 和本身产生的新的 SNONCE* 计算出新的 PTK*，新的 PTK* 和 PTK 显然是不一致的。AP 再将 PTK 验证后的 MIC 通过 M3 发回给客户端，客户端无法正确校验，导致四次握手过程被终止，造成 DOS 攻击。

第二种情况：基于 WPA 的四步握手认证从根本上是认证 MIC。用密码（passphrase）加密 AP 的 SSID 得到 PMK，由 PMK 分别结合 AP 的临时随机数 ANONCE，客户端的临时随机数 SNONCE、客户端的 MAC 地址、无线接入点 AP 的 MAC 地址得到 PTK，最后由 PTK 生成 MIC。在四次握手中，M1 和 M2 没有经过加密，是明文传送 ANONCE 和 SNONCE 的。假如已知 passphrase，那么只要获得第一和第二次握手的信息，就有计算出 MIC 的值的可能。攻击者利用这些已知的数据，通过假设再验证的方法，试探得到 passphrase，这种破解方式称为字典破解。破解步骤如下：

①从字典中取一个密码 passphrase，假设为已知用户的密码，配合 AP 的 SSID 得到 PMK.

从截获客户端的 MAC 地址、无线接入点的 MAC 地址、AP 的随机数 ANONCE、客户端的随机数 SNONCE，上一步得到的 PMK，计算生成 PTK。

②用 PTK 的前 16bit 计算出 MIC 值，用该值与四步握手第二步中客户端发往 AP 的 MIC 值进行比较，两者如果一致，假设密码 passphrase 即为 WPA 的真实密码。如果不一致，从字典中取出另一个密码，重新进行上述过程。

基于上述的原理，目前已经有多款黑客软件，可以对 WPA 协议进行破解。但是破解的关键在于字典的大小，如何找到足够大、信息合理的字典，是难题所在。同时，如果用户使用的是比较复杂的密码，也是比较难破解的。

结语

WPA/WPA2 协议作为无线安全协议，协议本身比较完整，算法方面漏洞很少。虽然有被

破解的可能，但是如果用户采用的是复杂的密码，破解的时间会很长，难度会很大。所以 WPA/WPA2 协议是安全的协议。

（洛阳理工学院现代教育技术中心）