无线网络中信息安全加密技术的研究

李成严[1]，张大珂[2]，李慧慧[1]

（1. 哈尔滨理工大学计算机与控制学院，哈尔滨 150080；2. 黑龙江省医院南岗分院计算机中心，哈尔滨 150001）

摘 要：首先分析了静态 WEP 加密机制的工作原理以及这种加密方式所存在的缺陷。在提出这些缺陷的基础上引出了当前的 WPA 加密方式，并对该加密方式进行了分析。然后，分别从认证和数据加密的角度对无线网络中的安全保护措施进行了一定的改进。

关键词：有线等价安全；Wi－Fi 保护接入；认证；临时密钥完整性协议

中图分类号：TN915.08 **文献标识码**：A **文章编号**：1009－2552(2004)04－0064－03

Study of information security and encrypt on wireless network

LI Cheng-yan[1], ZHANG Da-ke[2], LI Hui-hui[1]

(1. Computer & Control College, Harbin University of Science and Technology, Harbin 150080, China;
2. Computer Center, Nangang Branch, Heilongjiang Provincial Hospital, Harbin 150001, China)

Abstract: This paper analyzes the principle of static WEP key and it's flaw, then educes the current WPA key and analyzes it on the base of these flaws. Lastly, It improves the safety precautions of wireless network in the view of user authentication and DDA.

Key words: WEP; WPA; authentication; TKIP

0 引言

无线通讯的发展为组织和个人带来了很多方便，它具有轻便灵活、工作效率高、安装成本低廉等优点。然而，人们对 WLAN 自身安全难以保证的恐惧使许多企业不敢轻易部署 WLAN。虽然，早期确保安全的措施 SSID 和 ACL 以及 WEP 在一定程度上保证了无线网络的安全，但这些安全措施仍然存在许多漏洞。随着无线网络的进一步发展，一种新的安全保护 WPA 加密机制逐步形成，WPA 在一定程度上确保了无线网络的安全。

1 静态 WEP 和 WPA 加密机制

1.1 静态 WEP 加密

WEP 密钥由基本密钥和它的初始向量 IV 两部分组成。初始向量 IV 的长度为 24 位，基本密钥的长度为 40 或 104 位。所以，24 位的 IV 加上 40 或 104 位的基本密钥称为 64 位 WEP 或 128 位 WEP。

(1)静态 WEP 加密的过程

为了形成 WEP 数据帧，首先是传输消息 M 除去它的校验和 c(M)形成 M－c(M)，即明文 P 由两部分组成：消息 M 和消息的校验和 c(M)：

$P=\langle M, c(M)\rangle$ 其中 c(M)和 P 与密钥无关

接着初始向量 IV 和共享密钥 k(基本密钥)形成 WEP 密钥 IV－k。然后，利用这个 WEP 密钥进行初始化产生字节码，字节码与带校验和的明文进行异或操作产生密文 C：

$C=(M-c(M))\oplus RC4(IV-k)$

简单的，WEP 加密过程可表示为：

①选择初始向量(IV)为 v；

②利用 RC4 算法，RC4(v,k)生成伪随机的长密钥流；

③把密钥流和明文进行异或操作产生密文。

$C=P\oplus RC4(v,k)$

RC4 包括两部分，密钥调度算法和结果生成器。

收稿日期：2003－12－16

作者简介：李成严(1972－)，男，哈尔滨理工大学讲师。

在 WEP 中，密钥调度算法使用 64 位或 128 位 WEP 密钥来建立 RC4 状态矩阵 S，S 是{0，…… ，255}的置换矩阵；结果生成器使用状态矩阵 S 来产生伪随机序列。

(2)静态 WEP 密钥的破解

在 RC4 算法中，IV 生成算法所生成的 IV 是基于基本密钥的，而这一算法本身存在着缺陷[1]。具体说，初始向量 IV 是以明文形式在空中传送，它位于 802.11 报文的头部，很容易被窃听者捕获。攻击者会通过对截获大量 IV 的分析得出基本密钥。因初始向量 IV 的长度为 24 为，它共有 16777216 种可能值。因此，通过对明文和 IV 的统计分析可以计算出密钥。

若从 A 向 B 传输数据，在无线链路层传输的有初始向量 IV(v)和密文 C：

$A => B:v,(P \oplus RC4(v,k))$

其中 $P = <M, c(M)>$ 使用相同的初始向量 IV 和密钥对两条消息加密后对比就可以获得它们的有关信息。设：

$C1 = P1 \oplus RC4(v,k)$

$C2 = P2 \oplus RC4(v,k)$

则：

$C1 \oplus C2 = (P1 \oplus RC4(v,k)) \oplus (P2 \oplus RC4(v,k)) = P1 \oplus P2$

如果其中有一条明文是已知的，就可以推断出另一个来。由此可见 WEP 密钥的安全性差。

1.2 WPA 加密方式

WPA 使用一个叫“暂时密钥整体性协议”，此协议和算法改进了使用 WEP 密钥的安全性。它改变得到密钥的方法和不停地旋转密钥，并且为了防止包的伪造，它还增加了消息的整体性检查功能，使得无线网络的安全性大幅度增加。

WPA 这个标准包含两个方面重要的机制，分别为针对于数据加密的 Temporal Key Integrity Protocol (TKIP)临时完整性消息检查协议和针对于用户认证的 802.1x 机制。这两个机制的结合提供了动态密钥进而加密数据。

在使用 WPA 时，每位用户都拥有自己的加密密钥，密钥可以被设置为定期更换。在企业中，用户认证可由认证服务器处理；而家庭网络则可使用不需要认证服务器的“预先分配密钥”模式，在这种模式下，如果用户系统上的预先分配密钥与无线接入点上的密钥相匹配，用户就可登录到网络上。图(1)说明了使用 WPA 的运行流程。

2 认证方法

2.1 WPA 的认证

WPA 的加密机制使用了开放式系统认证和 802.1x 认证。

(1)开放式系统认证

开放式系统认证的过程是：首先，客户端发送探测帧给 AP，当 AP 收到该探测帧后，AP 给客户发送响应帧；其次，客户端再根据各个 AP 的回应帧，选择出一个信号较好的 AP；最后，客户端给选择好的 AP 发送请求认证帧，AP 再确认该认证帧，并返回给客户。

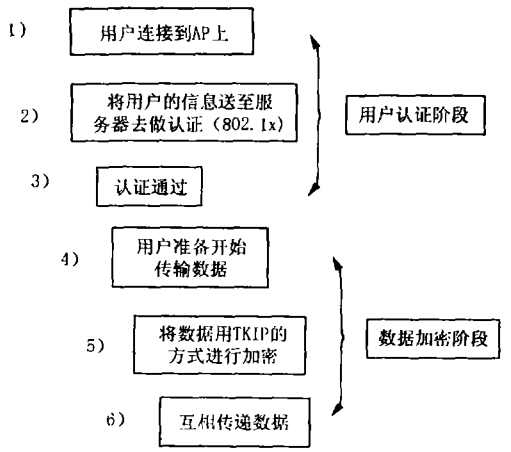

图 1 WPA 的运用流程图

(2)802.1x 认证[2]

对于大型运营商所建立的网络，由于设置了专门认证服务器如 Radius，则可以采用 802.1x 认证方式。802.1x 不是无线专有的认证方式，它是以前有线网络所采用的一种认证方式。IEEE 802.1x 称为基于端口的访问控制协议(Port based network access control protocol)。基于端口的访问控制能够在利用 IEEE 802 LAN 的优势基础上提供一种对连接到局域网设备或用户进行认证和授权的手段。802.1x 认证结构如图 2 所示。

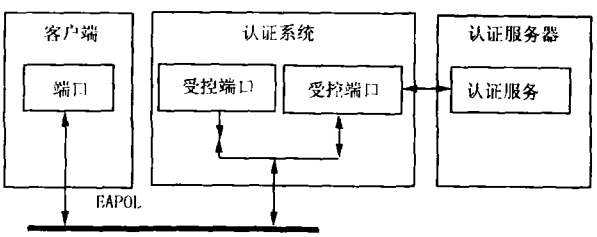

图 2 802.1x 认证

802.1x 认证主要由三部分组成：客户端系统、认证系统、认证服务器系统，其中最为关注的是认证

系统。认证系统[3]通常为支持 802.1x 协议的网络设备,该设备对应于不同用户的端口(可以是物理端口,也可以是用户设备的 MAC 地址)。对于基于物理端口的控制方式,每个物理端口包含两个逻辑端口:受控(Controlled Port)端口和不受控端口(Uncontrolled Port)。不受控端口始终处于双向连通状态,主要用来传递 EAPOL 协议帧,可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开,用于传递网络资源和服务。802.1x 协议仅仅关注端口的打开与关闭,对于合法用户接入时,该端口打开,而对于非法用户接入或没有用户接入时,则该端口处于关闭状态。认证的结果在于端口状态的改变,而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题,是各种认证技术中最简化的实现方案。

在 802.1x 认证中,认证系统通过不受控端口与客户端进行通信,二者之间运行 EAPOL 协议;认证系统与认证服务器之间运行 EAP 协议。

认证系统和认证服务器之间的通信可以通过网络进行,也可以使用其他的通信通道。例如当认证系统和认证服务器集成在一起时,两个实体之间的通信就可以不采用 EAP 协议。

认证服务器通常为 Radius 服务器,该服务器可以存储有关用户的信息,比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后,认证服务器会把用户相关信息传递给认证系统,由认证系统构建动态的访问控制列表,用户的后续流量将接受上述参数的监管。

2.2 EEAP 认证

EEAP 认证是对 IEEE 802.1x 认证的改进,它具有以下特点:

①提供了集中的、可升级的、基于用户的认证;

②认证算法要求用户和网络的相互认证;

③使用了 802.11x 认证;

④使用了动态 WEP。

EEAP 认证过程的描述如下:

①用户首先向无线接入点 AP 发送一开始的 EAP 信号帧;

②AP 将阻塞所有用户请求,直到认证完成。AP 回应一要求用户出示身份的请求 EAP 帧;

③用户通过接入点 AP 向认证服务器(一般为 Radius 服务器)发送一含有自己身份的 EAP 应答帧;

④认证服务器使用特定的认证算法或查询数据库来验证用户身份的合法性(其间认证服务器可与用户多次交换信息);

⑤认证服务器向 AP 发送接受或拒绝用户的信息;

⑥若用户被认证服务器认证接受,则用户对认证服务器(Radius 服务器)进行反向认证,防止伪冒认证者;

⑦如果认证服务器和用户相互认证成功,则 AP 向用户发送经会话密钥加密的用户广播密钥和密钥长度;

⑧用户和无线网络进行正常的业务数据交流。

3 数据加密与传输措施

对于 WEP 而言,它在发射数据以前采用了美国 RSA 实验室提供的 RC4 流密码来加密帧体和每个 802.11 帧体的校验。实际上,我们所说 WEP 不安全和 RC4 的加密算法无关,WEP 脆弱之处和密钥的产生和怎样进行加密有关。TKIP 采用与 WEP 同样的加密算法,但以不同的方式构造密钥。

WEP 编码弱点在于 IV 实现的基础过于薄弱,它之所以不安全,主要在于两方面:

(1)初始化向量 IV 的限制

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。

(2)由于使用静态 WEP 密钥而冲突的几率很高

当这两个问题结合在一起,并且在多个数据帧上同时使用带有相同 WEP 密钥的相同 IV 时,IV 冲突就产生了所谓"弱"WEP 密钥。当黑客将两个使用同样 IV 的封包记录下来,再进行互斥运算,就可以得到 IV 的值,然后算出 RC4 的值,最后得到整组数据。可见分析众多此类弱密钥时,就可以攻击 WEP 从而暴露共享秘密。下面让我们来看看 TKIP 相对于 WEP 都作了那些改变。

(1)48 比特初始向量

在 TKIP 中,将初始化向量由 24 位增加到 48 位,使冲突概率降低,大大增加了安全性。

(2)每一个包密钥的产生和分配

WPA 对于每个客户端周期性的产生一个新的独立密钥,用这个密钥来加密 802.11 的每一个帧体,这样避免了使用 WEP 时几个星期,甚至几个月都不更换密钥的情况。

(3)信息完整性代码

使用 MIC 来防止黑客攻击, (下转第 69 页)

否收到信号

```
        prev - > state = TASK_RUNNING;
        break;}
    default: /* 当前运行进程处于非 TASK_RUNNING 状态
        del_from_runqueue(prev);
    case TASK_RUNNING;
}
    prev - > need_resched = 0; /* 撤消当前进程的调度标志
```

当前运行进程的状态发生改变时，如果它是 TASK_INTERRUPTIBLE 状态，核心将改变它的运行状态，改变为运行态。否则，将当前进程从运行队列中删除。

当前运行进程参与调度时，在权值相同的情况下，它的优先级最高，将首先被调用；队列前面的进程优于其后面的进程被调用；当新的进程产生或可运行队列中的某个进程的优先级被改变时，将引起重新调度，如果它们的优先级高于当前进程，则当前进程被剥夺。

权值最大的进程是下一个被调度的进程，对于实时或非实时进程都一样。但是，由于衡量权值大小依据的内容不同，调度方式也不同。SCHED_YIELD 标志的进程权值是除了 0 进程之外，权值最小的进程，只要还有其它进程，它将让出中央处理器。SCHED_YIELD 标志的实时进程采取先进先出(FIFO)的调度策略。这种调度不考虑进程时间片是否用完，进程的权值始终不变，一旦获得运行，仅仅在等待同步事件或明确睡眠、可运行队列中出现权值比它更高的进程情况下，进程才会释放 CPU，确保实时进程始终按照它在可运行队列中的顺序运行先进先出。

找到权值最大的进程之后，核心判断最大的权值是否等于 0。这种情况只有 SCHED_OTHER 标志的非实时进程在时间片用完时才会发生。如果是，向可运行队列中所有的进程分配时间片，再从 repeat_schedule 出运行。可见，只有当所有非实时进程的时间片用完时，才同时向所有非实时进程重新分配时间片。这样，当单个非实时进程时间片完时，CPU 被剥夺，给予其它非实时进程运行的机会。

选定下一个调度的进程之后，判断当前运行进程是否继续拥有 CPU，如果是，继续运行；否则，核心进行相应的上下文切换，开始新的进程运行。

Linux 进程调度以时间片轮转为基础，同时兼顾实时性。非实时进程根据时间片进行轮转调度。实时进程的调度策略根据用户的需求来选择。实时性要求高时，采用先进先出的调度策略，用最快的响应速度，占有的时间最长；实时性要求低时，采用循环调度，使得多个实时进程同时获得较快的响应。

参 考 文 献：

[1] 周巍松. LINUX 系统分析与高级编程技术[M]. 北京：机械工业出版社，1999.

[2] Scott Maxwell. Linux 内核源代码分析[M]. 冯锐，等译. 北京：机械工业出版社，2000.

[3] (美)博伟特，等. 深入理解 LINUX 内核[M]. 陈莉君，等译. 北京：中国电力出版社，2001.

[4] 李善平，等. LINUX 内核 2.4 版源代码分析大全[M]. 北京：机械工业出版社，2002.1.

责任编辑：张棣

(上接第 66 页)

在帧体里附加了一个 4bit 的检查码，发送端根据帧体来确定 MIC，并把这个 MIC 填入帧体；接收端根据 MIC 来确定这一帧是否被接受，它首先检查信息和 MIC 是否匹配，然后再进行信息完整性检查。如果匹配，则说明信息传送完整，数据正常接受，图 3 为一个 TKIP 的帧结构。

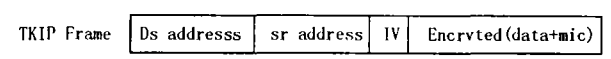

图 3 TKIP 的帧结构

4 结论

无线网络安全是一个不断改善和升级的过程，特别是无线技术迅猛发展的今天，一项认为完美的安全技术在实际应用中却漏洞百出，这就需要通过人们不断的努力来完善它。当然，WPA 还要走很长的路才能够完全克服 WEP 的缺点，而且并不是所有的用户都能够利用它。看来，只有将用户认证和传输数据加密等多种措施结合起来，才能构筑安全的无线局域网，这些都需要我们不断的学习和探索。

参 考 文 献：

[1] Scott Fluhrer, Itsik Mantin, Adi Shamir. Weaknesses in the Key Schedling Algorithm of RC4 [DB/OL]. URL: http//www. drizzle. com/aboba/IEEE/rc4_ksaproc. pdf, 2001 - 07 - 25.

[2] http://www. 80211 - planet. com/tutorials/article. php/1041171 [DB/OL].

[3] http://www - 90. ibm. com/deceloperworks/cn/security/wi - sec1/index. shtml[DB/OL].

责任编辑：张荣香