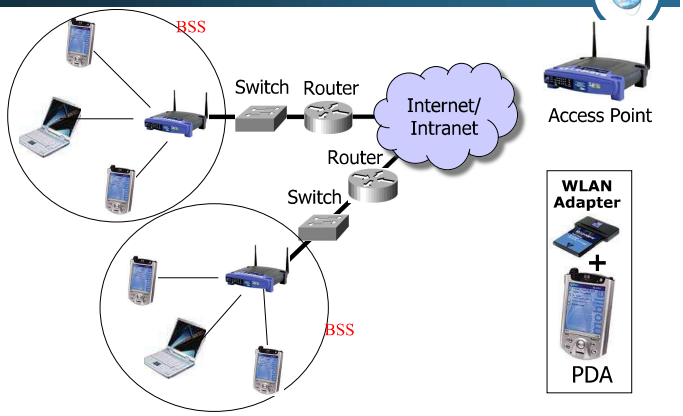
移动通信和无线网络安全

第六讲 无线局域网安全

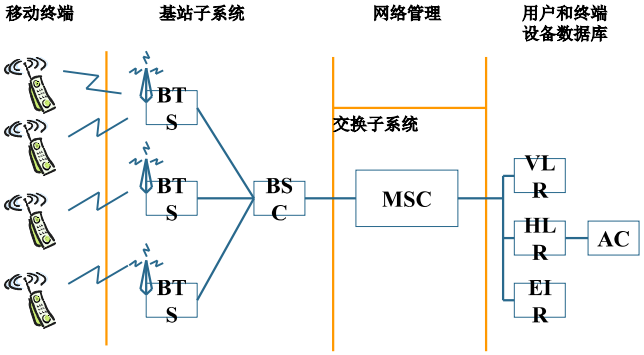
宋宇波
songyubo@seu.edu.cn

一、简介

Typical Wireless LAN Configuration



移动通信网络结构



无线局域网结构

Wireless LAN (WLAN)

是有线网络的延伸

局域安全性

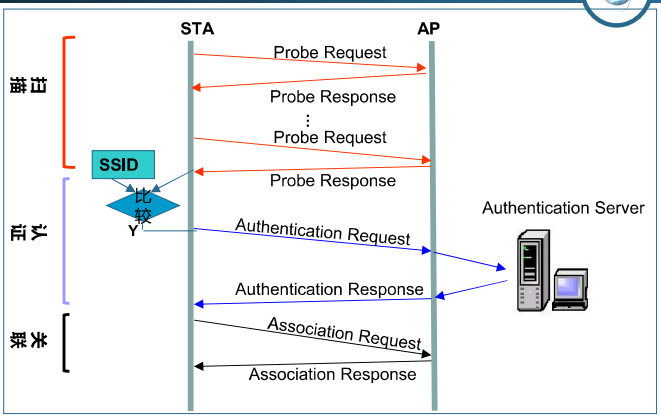
802.11

有线网络

Access Point

无线网络
用户端

无线接入过程示意图



- 认证
- 访问控制
- 保密
- 数据完整性
- 不可否认
- 密钥管理

- IEEE802.11
  - 认证：提供相当于有线媒介物理连接的功能。
    - 链路层上的认证
    - 不提供端到端或用户到用户的认证。
  - 保密：提供相当于有线物理封闭媒介的保密

二、密钥协商

- Problem
  - 通常采用手动配置密钥
    - 易出错
    - 字典攻击
  - 密钥不是一对一的
    - 一个BSS下的AP和所有STA都使用相同的密钥
    - 在ESS下，为了漫游方便，用户会把所有的AP都设为相同的密钥
  - 密钥没有生命周期

三、802.11的匿名性

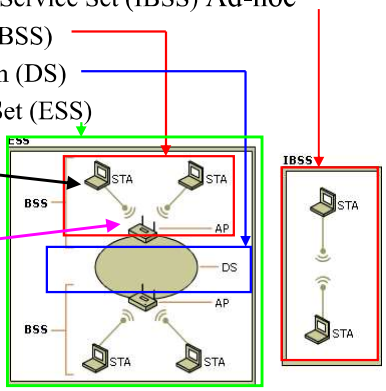
- 传统网络利用IMSI进行呼叫路由
- IP网络使用IP地址进行路由

- IMSI与用户一一对应
- IP与用户没有一一对应关系
  - DHCP
  - 用户可自行修改IP地址
  - NAT

四、802.11的认证

WLAN的架构

- Independent Basic Service Set (IBSS) Ad-hoc
- Basic Service Set (BSS)
- Distribution System (DS)
- Extended Service Set (ESS)
- Station (STA)
  - 无线用户端
- Access Point (AP)
  - 无线接入点



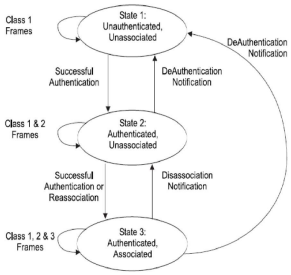
❖**SSID(Service Set Identifier): network name,唯一标示一个ESS**

状态图

❖**状态1： 未认证、未关联**

❖**状态2： 已认证、未关联**

❖**状态3： 已认证、已关联**



无线接入过程

第一阶段：扫描（SCAN）阶段

❖ 若无线站点 STA 设成 Ad-hoc 模式：
STA先寻找是否已有 IBSS（与STA所属相同的SSID）存在，如有，则参加（join）；若无，则会自己创建一个IBSS，等其他站来 join。

❖ 若无线站点 STA 设成 Infrastructure 模式：
1、主动扫描方式（特点：能迅速找到）
STA 依次在11个信道发出 Probe Request 帧，寻找与STA所属有相同SSID的AP，若找不到有相同 SSID 的 AP，则一直扫描下去…
2、被动扫描方式（特点：找到时间较长，但STA节电）
STA被动等待AP 每隔一段时间定时送出的 Beacon 信标帧，该帧提供了AP及所在BSS相关信息：“我在这里”…

无线接入过程

第二阶段：认证（Authentication）阶段

当 STA 找到与其有相同 SSID 的 AP，在 SSID 匹配的 AP 中，根据收到的 AP 信号强度，选择一个信号最强的 AP，然后进入认证阶段。只有身份认证通过的站点才能进行无线接入访问。802.11提供几种认证方法，有简单有复杂，如采用802.1x/EAP认证方法时大致为：

1. STA向AP发送认证请求
2. AP向认证服务器发送请求信息要求验证STA的身份
3. 认证服务器认证完毕后向AP返回相应信息
4. 如果STA身份不符，AP向STA返回错误信息
   如果STA身份相符，AP向STA返回认证响应信息

第三阶段：关联（Association）阶段

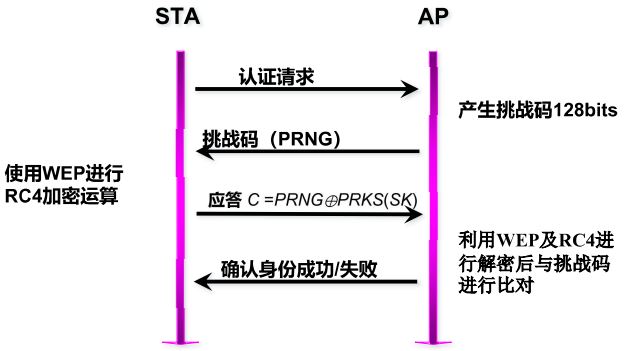
当 AP 向 STA 返回认证响应信息、身份认证获得通过后，进入关联阶段。

1. STA 向 AP 发送关联请求
2. AP 向 STA 返回关联响应

至此，接入过程才完成，STA 初始化完毕，可以开始向 AP 传送数据帧。

- **开放系统(Open System)认证**
- **共享密钥(Shared Key)认证**

共享密钥认证



认证与切换

- **认证时间大，影响了实时应用**

共享密钥认证方式漏洞

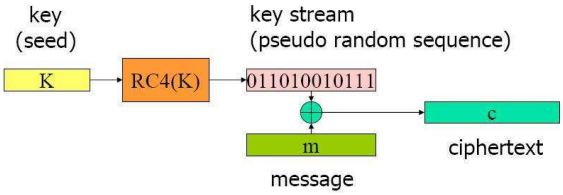
- **攻击者可以得到：**
  - **PRNG（第2步）**
  - **C（第3步），C=P⊕PRKS(K)**
- **P⊕C=?**
  - **= PRKS(K)**
- **接下去：？**

五、802.11的加密

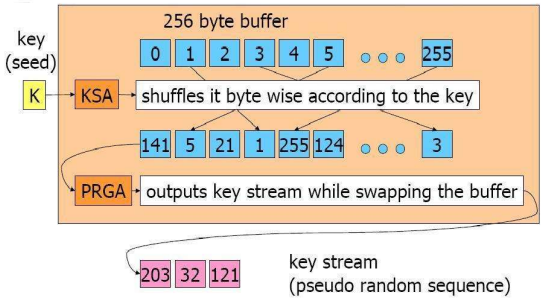
WEP(Wired Equivalent Privacy)加密

- **安全服务：**
  - **数据机密性**
  - **访问控制**
  - **数据完整性**
- **类型：**
  - **WEP-40**
  - **WEP-104**
- **采用RC4流加密算法**

RC4算法



RC4



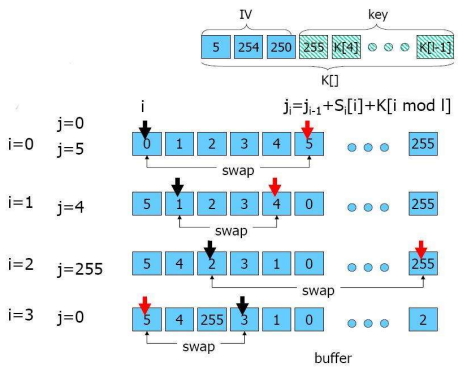
RC4

KSA(K)
Initialization:
For $i = 0 \ldots N-1$
$S[i] = i$
$j = 0$
Scrambling:
For $i = 0 \ldots N-1$
$j = j + S[i] + K[i \bmod \ell]$
$Swap(S[i], S[j])$

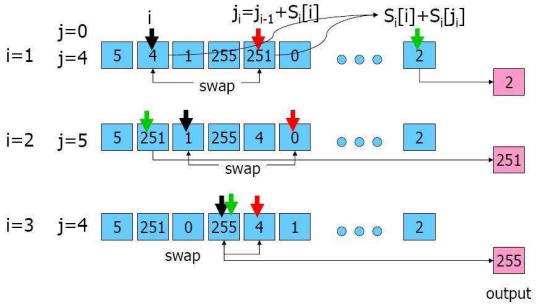
PRGA(K)
Initialization:
$i = 0$
$j = 0$
Generation loop:
$i = i + 1$
$j = j + S[i]$
$\text{Swap}(S[i], S[j])$
Output $z = S[S[i] + S[j]]$

$N = 256 \quad l : keylength \quad K[l] : IV[3] \,||\, SK[l-3]$

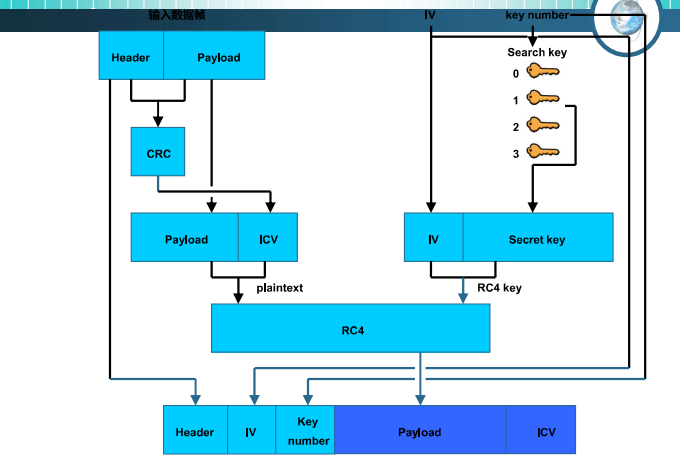
KSA



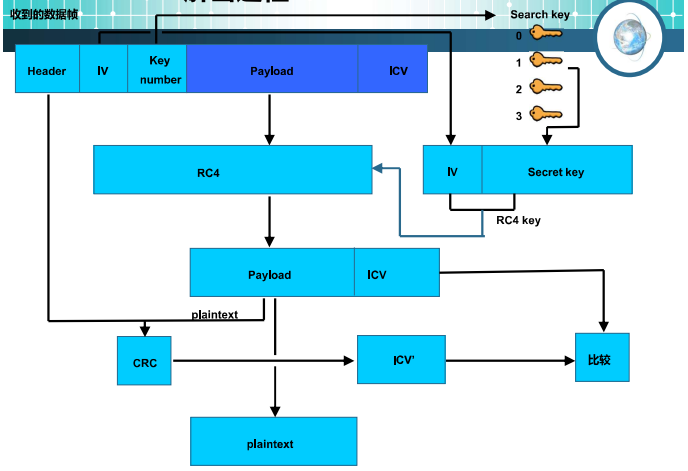
PRGA



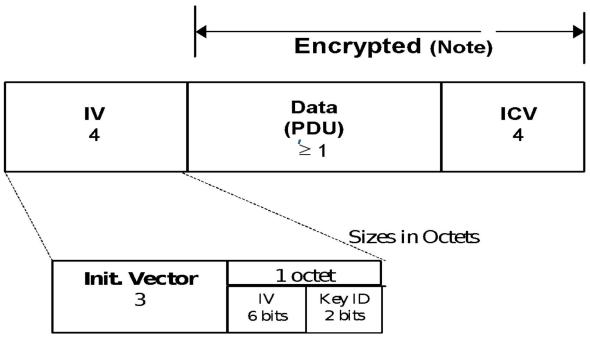
WEP加密过程



WEP解密过程



WEP数据帧格式



其他保护措施

- **跳频通信**
- **SSID**（Service Set Identifier, a 32-character 的唯一标识）
  - Probe request/probe response /beacon帧中包含SSID
- **MAC地址过滤**
  - AP上具有可接入的MAC地址列表

六、安全分析

WEP安全分析

1. **WEP加密是可选功能，在大多数的实际产品中默认为关闭，因此将用户数据完全暴露于攻击者面前。**

WEP安全分析

2. 密钥产生问题：
   1. 直接由用户写入40或108比特的密钥；
   2. 由用户输入一个口令，根据该口令通过某个密钥生成函数产生密钥。

WEP安全分析

3. 密钥分发问题：
   1. 密钥为无线局域网所有用户共享，且很少变动，因而容易泄漏。

WEP安全分析

4. 初始向量（Initialization vector，IV）空间太小。

$$C2 \oplus C1 = \{P1 \oplus RC4(iv \| SK)\} \oplus \{P2 \oplus RC4(iv \| SK)\} = P1 \oplus P2$$

*iv*空间: 24bits，
IV的生成方法：用计数器递增实现

WEP安全分析

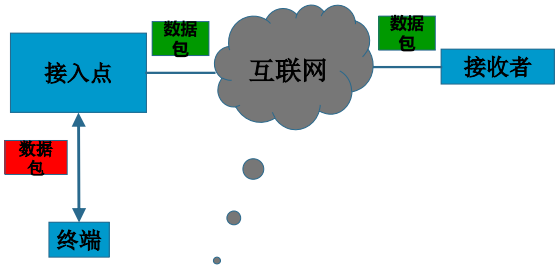
5.数据篡改攻击：

- RC4,CRC32算法:线性校验算法
  - 线性算法特征： $c(x \oplus y) = c(x) \oplus c(y)$
- 攻击方法
  - 已知：初始向量iv,密文C。
  - 未知：明文M，密钥K
  - C=RC4(iv,K)⊕{M,crc32(M)}
  - 随意伪造新明文M’，令M’=M+Δ
  - C’= C⊕<Δ,crc32(Δ)>

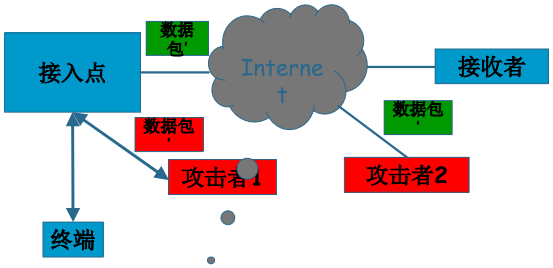
WEP安全分析

6. IP重定向
   - 攻击者可以将目标地址改为自己的地址
   - 需确保校验正确。
     - $x' = x + D'_H + D'_L - D_H - D_L$

数据包正常的操作



重定向攻击

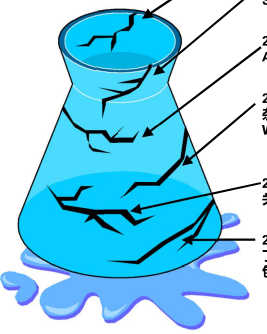


WEP安全分析

7. WEP没有重放保护机制

WEP 密钥破解

IEEE组织承认WEP无法提供任何安全保护，推荐用户升级到WPA, WPA2



2001 - The insecurity of 802.11, Mobicom, July 2001
N. Borisov, I. Goldberg and D. Wagner.

2001 - Weaknesses in the key scheduling algorithm of RC4.
S. Fluhrer, I. Mantin, A. Shamir. Aug 2001.

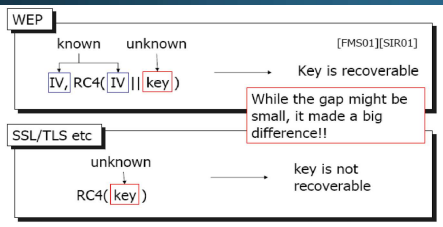
2002 - Using the Fluhrer, Mantin, and Shamir Attack to Break WEP
A. Stubblefield, J. Ioannidis, A. Rubin.

2004 – KoreK, 改进了上述攻击方法并简化了WEP攻击的复杂度，现在我们只需要大约500,000 个数据包就可以恢复WEP的密钥。

2005 – Adreas Klein 发现了RC4密钥流和密钥之间的更多相关性。

2007 – 一种称为PTW算法采用了Andreas的方法进一步简化了WEP的攻击。我们现在只需要大约 60,000 – 90,000个数据包就可以恢复WEP密钥。

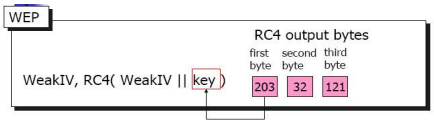
WEP算法的缺陷



•IV是明文。

•被加密的数据的第一个字节的明文是固定的。
  •0xAA

FMS攻击



❖通过收集特定IV格式(weak IV)的数据包来反向推导密钥。
- Weak IV
  - (B+3,N-1,X)形式的IV，称Weak IV
    - B : 欲破解的secret key byte
    - N : 256
    - X : 为任意值

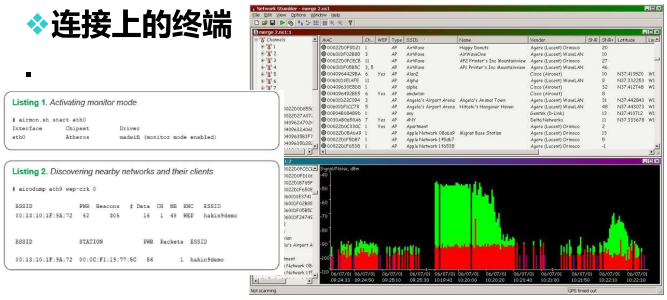
Fluhrer, Mantin, Shamir Attack

802.11网络攻击

1. 监听攻击：截取空中信号，进行分析，获取相关信息。
2. 插入攻击：通过监听获取的相关信息，假冒合法用户，通过无线信道接入信息系统，获取系统控制权。
3. 未授权信息服务：用户在未经授权的情况下享用系统信息资源。
4. 拒绝服务攻击：发送大量的无用数据报坏正常的无线通信。
5. 伪造AP(Fake AP)：伪装成合法AP，诱使用户登录

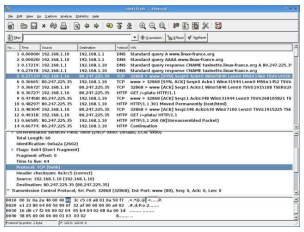
扫描

- 无线接入点MAC地址
- 运行的安全协议
- 加密密钥长度
- 连接上的终端



收集数据

- 利用Ethereal, Kismet等数据截获软件进行数据截获.
- 获得足够多的数据后即可以破解WEP（大概需要500M-1G的数据
  - 可以利用arp replay攻击缩短数据收集时间



破解WEP密钥

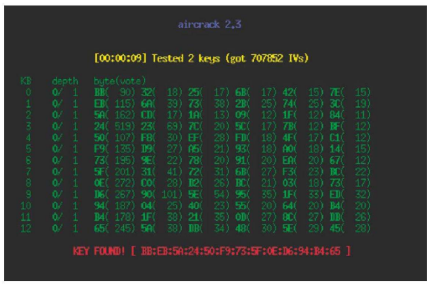


Figure 2. Aicrack results after a few minutes

跟RC4无关的攻击

- Packet Injection
  - 攻击者捕获一个WEP加密的数据包后，可以重放该数据包，网络仍会接受该报。
    - 如果发送的站点离开了网络，我们可以将MAC地址改为其他留在网络里的终端。这是可行的，因为MAC地址不受ICV保护
- Fake Authentication
  - Open System
  - Shared Key

Chopchop attack

- Let O_{crc} be an oracle, which takes an arbitrary encrypted packet and returns true, if the checksum in the encrypted packet was correct, false otherwise. If an attacker has a single encrypted packet of length l and access to such an oracle O_{crc}, he can decrypt the last m bytes of the packet and recover the last m bytes of the key stream used to encrypt the packet, with in average 128*m queries to the oracle and negligible computational effort.

CRC校验

$$P \bmod R_{CRC} = R_{ONE}$$

$$R_{CRC} = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$$

$$R_{ONE} = \sum_{i=0}^{31} X^i$$

❖将明文*P*表达为

$$P = Q \cdot X^8 + P_7$$

$$Q \cdot X^8 = P_{ONE} + P_7 \bmod R_{CRC}$$

$$\begin{aligned}(X^8)^{-1} &= X^{31} + X^{29} + X^{27} + X^{24} + X^{23} + X^{22} + X^{20} + X^{17} + \\ &\quad X^{16} + X^{15} + X^{14} + X^{13} + X^{10} + X^9 + X^7 + X^5 + X^2 + X \\ &= R_{INV}\end{aligned}$$

$$Q = R_{INV}(P_{ONE} + P_7) \bmod R_{CRC}$$

❖我们想构造一个新的*Q'*,使得

- $Q' = P_{ONE} \bmod R_{CRC}$

❖令 $P_{COR} = P_{ONE} + R_{INV}(P_{ONE} + P_7)$

❖则$Q' = Q + P_{COR} = P_{ONE} \bmod R_{CRC}$

❖P_{ONE}, R_{INV}都是常量

❖举例：

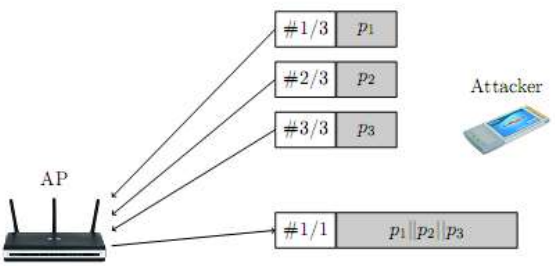
- 10000100100001011111011101101001110011001101
- $P_{PLAIN} = X^{39}+X^{34}+X^{31}+X^{26}+X^{24}+X^{23}+X^{22}+X^{21}+X^{20}+X^{18}+X^{17}+X^{16}+X^{14}+X^{13}+X^{11}+X^8+X^7+X^6+X^3+X^2+1$

$$\begin{aligned}P_{PLAIN} &= X^8 \cdot (X^{31} + X^{26} + X^{23} + X^{18} + X^{16} + X^{15} + \\ &\quad X^{14} + X^{13} + X^{12} + X^{10} + X^9 + X^8 + X^6 + \\ &\quad X^5 + X^3 + 1) + \\ &\quad (X^7 + X^6 + X^3 + X^2 + 1)\end{aligned}$$

$$P_7 = X^7 + X^6 + X^3 + X^2 + 1$$

$$\begin{aligned}Q &= X^{31} + X^{26} + X^{23} + X^{18} + X^{16} + X^{15} + X^{14} + X^{13} + \\ &\quad X^{12} + X^{10} + X^9 + X^8 + X^6 + X^5 + X^3 + 1\end{aligned}$$

$$\begin{aligned}P_{COR} &= X^{30} + X^{29} + X^{28} + X^{27} + X^{25} + X^{24} + X^{22} + X^{21} \\ &\quad X^{20} + X^{19} + X^{17} + X^{11} + X^7 + X^4 + X^2 + X\end{aligned}$$



WEP教训：需要公开讨论

❖IEEE使用“公开设计”

- 任何人都可以参加会议
- 相关标准资料可以免费获得

❖不足；

- 只有大公司才有时间和精力参加会议
- 没有来自密码界的讨论

❖许多缺陷早已存在

- 例如：CRC攻击，重定向攻击
- 如果设计正确，FMS等攻击都可以抵御

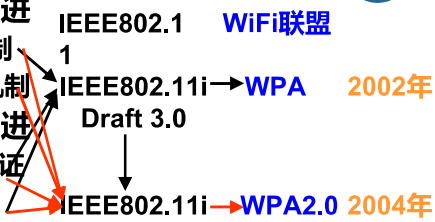
WEP教训：数据完整性保护的重要性

- 在无线局域网设计中，数据完整性保护只是次要目标。
- 但是简陋的完整性保护会破坏消息安全保护：
  - IP重定向攻击
  - TCP回应攻击
  - 数据包注入攻击
- 需要基于密码学的消息认证算法
  - "Encryption without integrity checking is all but useless" [Bellovin'96]

六、WPA/WPA2.0

15.4 WPA/WPA2.0标准

- 加密算法的改进
  - TKIP加密机制
  - CCMP加密机制
- 认证机制的改进
  - WPA-PSK认证
  - 802.1X认证

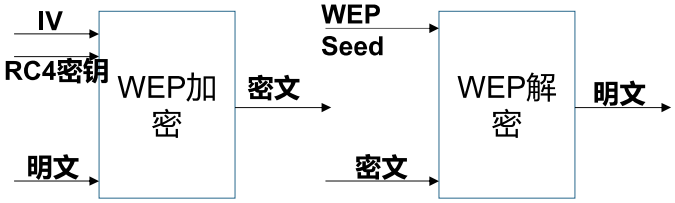


如何改进WEP

- 在现有的WEP基础上进行修改
  - TKIP加密机制
- 重新设计新的安全机制
  - CCMP加密机制

15.4.1 TKIP加密机制

- 设计者面临的限制
  - 限制1：只能通过软件升级的方式进行改进
  - 限制2：计算资源有限
  - 限制3：为了减少资源消耗，WEP算法固化在硬件模块中，无法修改



- TKIP：Temporal Key Integrity Protocol
  - 被设计为WEP算法外的一个壳(Wrapper)
    - 可以以软件方式实现
    - 重用现有的WEP算法
    - 将WEP作为新机制的一个组件

WEP的安全问题

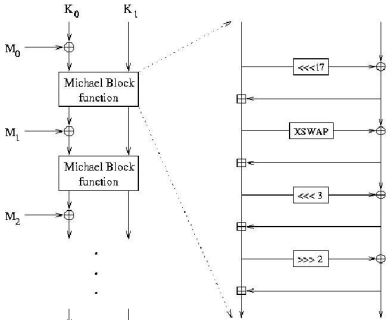
1	无法检测消息是否被篡改
2	没有提供重放攻击保护
3	IV长度太短，容易造成重复使用
4	存在Weak IV,容易遭受FMS攻击
5	直接使用主密钥，没有提供密钥更新机制

TKIP针对WEP的该进

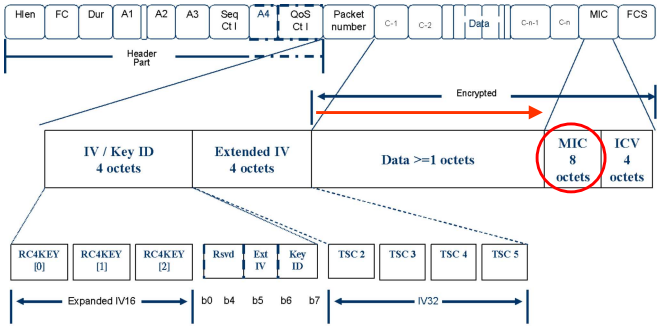
目的	改进	针对的安全问题
数据完整性保护	添加基于密码学的消息完整性校验码(MIC)， Michael函数	(1)
IV选择和使用	添加IV序列计号(48位)，TSC计数器，改变IV生成方式和功能	(2)，(3)
密钥混合	添加分组密钥混合函数，使得每次加密使用的密钥都不同	(4)
密钥管理	添加Re-keying机制，进行密钥分发、更新和生成临时密钥	(5)

Michael函数

Michael密钥为64位

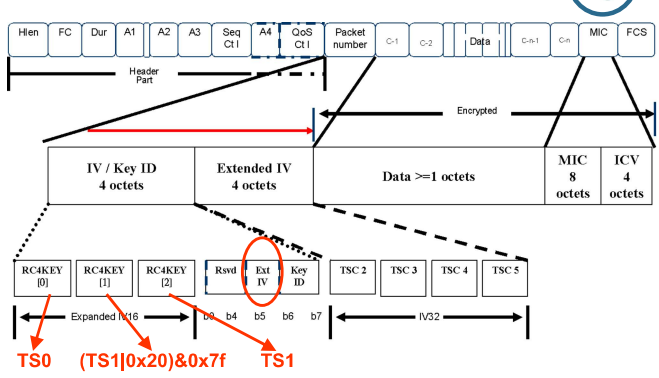


(L,R) ← (K0,K1)
do i from 1 to n
L ← L⊕Mi
(L,R) ← b(L,R)
return (L,R)



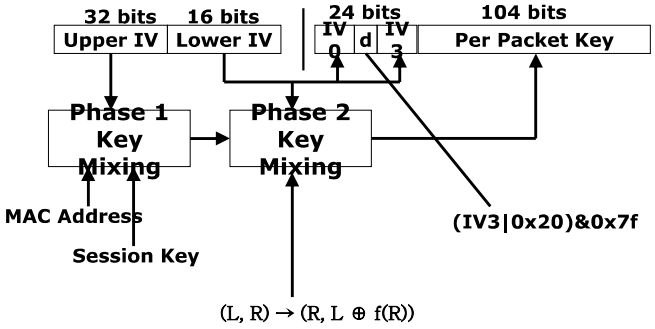
IV序列号

- **IV大小:**
  - 24bit ->48bit
- **IV作为数据包序列号：TSC**
  - 防止重发攻击
- **重新构造避免出现Weak IV**



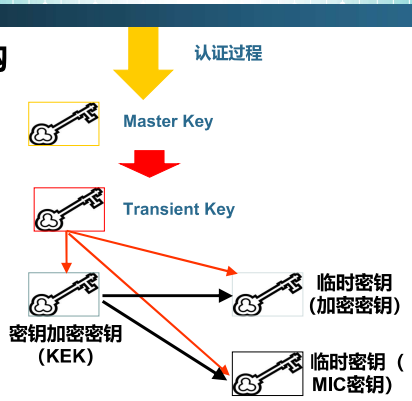
密钥混合函数

- 密钥混合函数：弥补WEP缺陷
  - 用临时密钥替代原有的WEP密钥和IV。
  - 临时密钥周期短，经常更换。
- 结构：
  - 阶段1：解决每个链路都使用相同密钥的问题
  - 阶段2：去除分组密钥和IV之间的相关性

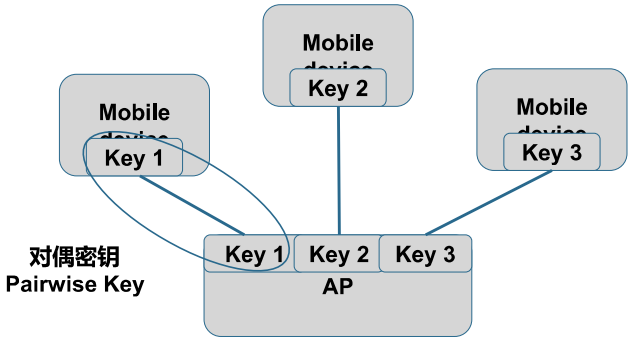


密钥更新

- 分级架构

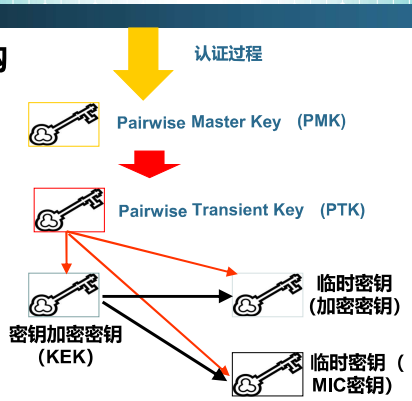


对偶密钥（Pairwise Keys）

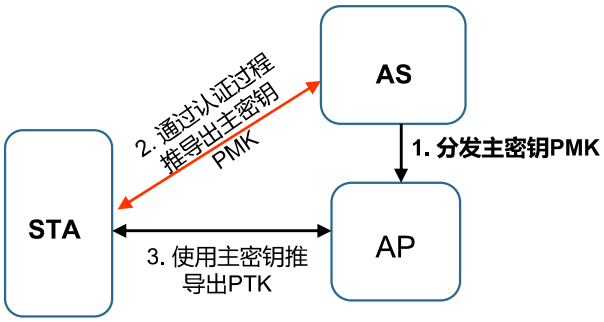


密钥更新

- 分级架构



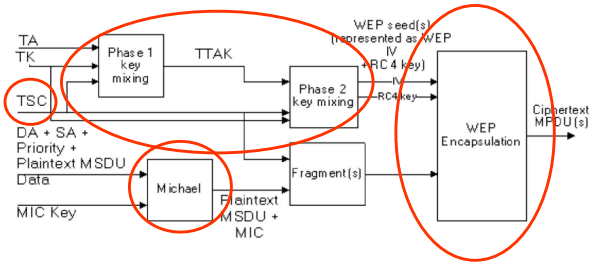
密钥更新过程



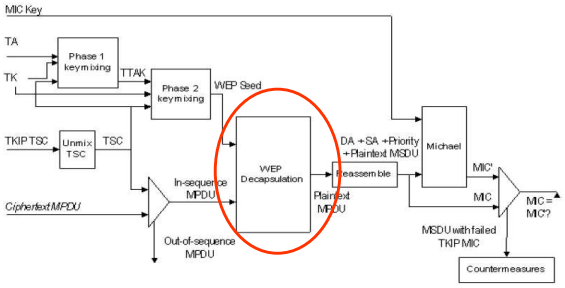
PTK = PRF-512(PMK, “Pair-wise key expansion”, AP_MAC || STA_MAC || ANonce || SNonce)

ANonce = PRF-256(Random Number, “Init Counter”, AP_MAC || Time)
SNonce = PRF-256(Random Number, “Init Counter”, STA_MAC || Time)

TKIP加密过程



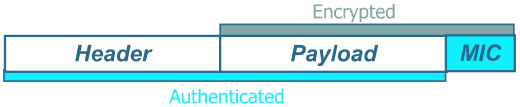
TKIP解密过程



15.4.2 CCMP加密机制

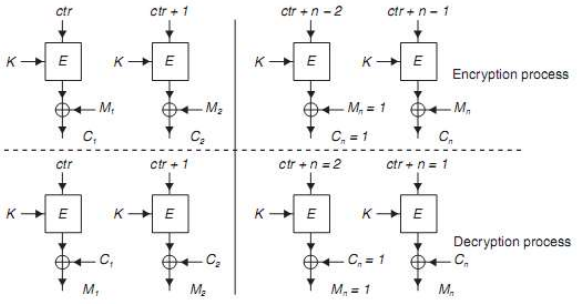
- 设计要求：
  1. 被正确加密
     a) 密钥不能重复使用
     b) Nonce和IV不能重复使用
  2. 防止数据被篡改
     a) 防止发送地址和接收地址被篡改
  3. 抗重发攻击
  4. 降低成本
     a) 尽可能减少加密函数使用数量
     b) 尽可能减少软件开销
     c) 尽量借鉴已有的安全机制

AES-CCM



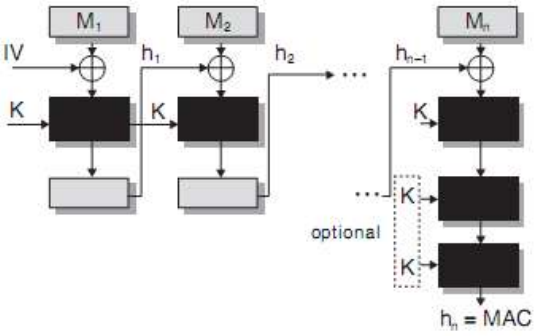
- CBC-MAC模式用于计算MIC码
- CTR模式用于进行加密

CTR模式

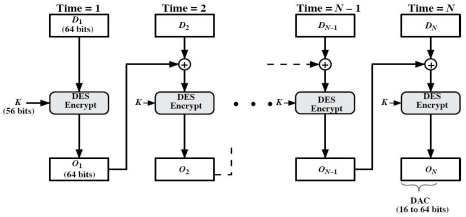


1. It allows a block cipher to be operated as a stream cipher.
2. The use of counter mode makes the generated key stream independent of the message, thus allowing the key stream to be generated before the message arrives.
3. Since the protocol by itself does not create any interdependency between the encryption of the various blocks in a message, the various blocks of the message can be encrypted in parallel if the hardware has a bank of AES encryption engines.
4. Since the decryption process is exactly the same as encryption, 30 each device only needs to implement the AES encryption block.
5. Since the counter mode does not require that the message be broken up into an exact number of blocks, the length of the encrypted text can be exactly the same as the length of the plain text message.

CBC-MAC



- MAC码为DES算法CBC模式下的最后一个输出，IV = 0
- 称为数据认证算法(Data Authentication Algorithm)
- 其输出称为(DAC: Data Authentication Code)，是O_N最左边的16位-64位。



- CBC-MAC在政府和工业界广泛采用
- CBC-MAC的限制：
  - 长度限制
  - MAC(X)=MAC(X||(X⊕T))
- CMAC：使用三个密钥来克服，这些密钥可以通过一个密钥导出。
- CMAC被NIST SP800-38B标准采用

- C1= E(K,M1)
- C2= E(K,[M2⊕C1])
- C3= E(K,[M3⊕C2])
- .
- .
- .
- Cn= E(K,[Mn ⊕ Cn-1 ⊕ K1])
- T= MSB_{Tlen}(Cn)

- T= 消息认证码
- Tlen=T的比特长度
- MSBs(X)= 比特串X的最左边的s位