WIFI

EN | ZH

WIFI

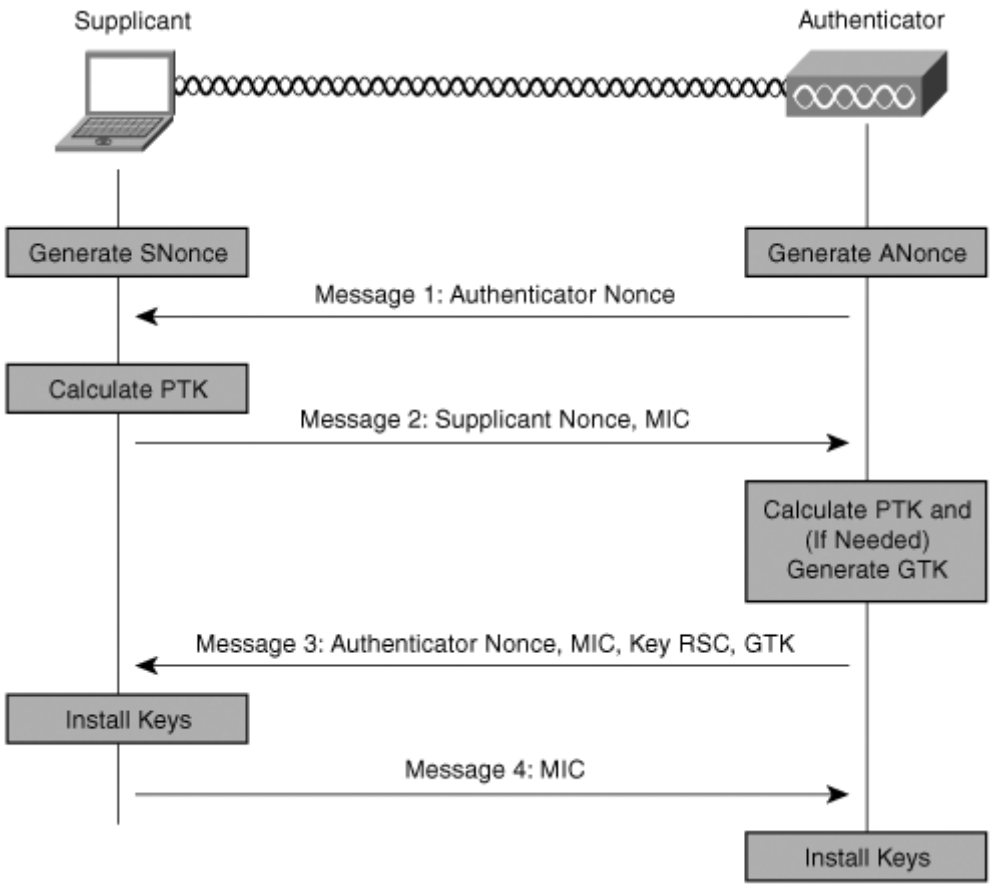
> `802.11` 是现今无线局域网通用的标准, 常见认证方式
>
> - 不启用安全
> - `WEP`
> - `WPA/WPA2-PSK`（预共享密钥）
> - `PA/WPA2 802.1X`（`radius` 认证）

WPA-PSK

认证大致过程如下图


AP定期广播beacon
在每个信道广播Probe Request
Probe Response
Authentication
Authentication
association request
association response
EAPOL四次握手

其中四次握手过程



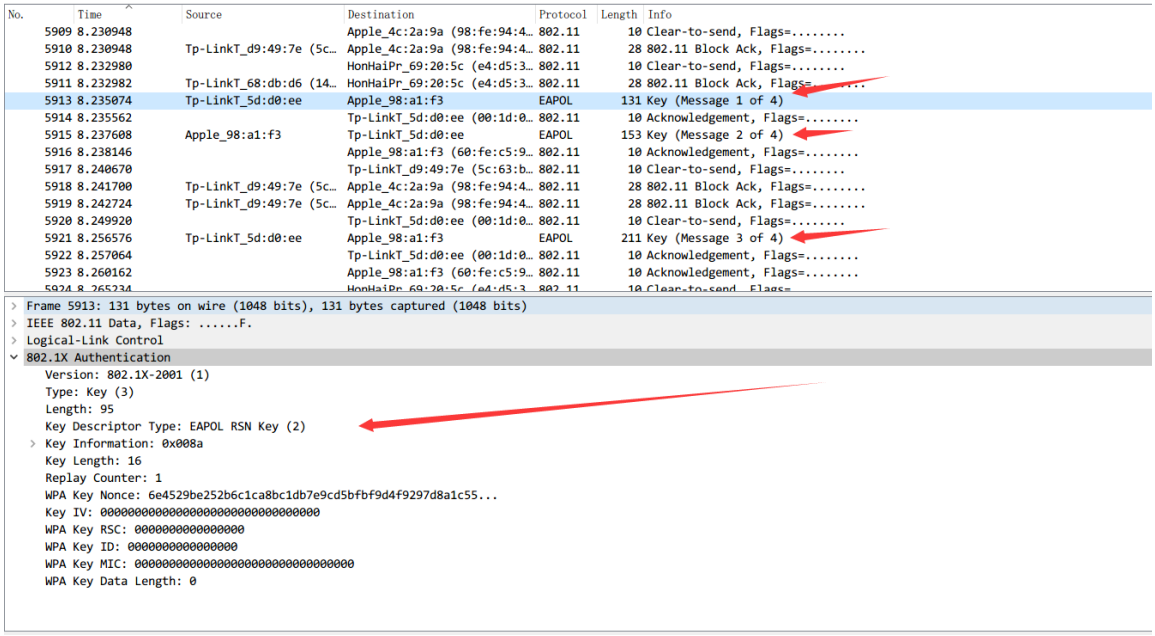
1. 4 次握手开始于验证器 (AP)，它产生一个随机的值(ANonce) 发送给请求者
2. 请求者也产生了它自己的随机 SNonce，然后用这两个 Nonces 以及 PMK 生成了 PTK。请求者回复消息 2 给验证器, 还有一个 MIC（message integrity code，消息验证码）作为 PMK 的验证
3. 它先要验证请求者在消息 2 中发来的 MIC 等信息，验证成功后，如果需要就生成 GTK。然后发送消息 3
4. 请求者收到消息 3，验证 MIC，安装密钥，发送消息 4，一个确认信息。验证器收到消息 4，验证 MIC，安装相同的密钥

例题

> 实验吧：`shipin.cap`

从大量的`Deauth`攻击基本可以判断是一个破解`wifi`时的流量攻击

同时也成功发现了握手包信息



接下来跑密码

- `linux` ： `aircrack` 套件
- `windows` ： `wifipr` ，速度比 `esaw` 快， `GTX850` 能将近 `10w\s` :)

得到密码 `88888888` 在 `wireshark` 中 `Edit -> Preferences -> Protocols -> IEEE802.11 -> Edit` 以 `key:SSID` 形式填入即可解密 `wifi` 包看到明文流量

> KCARCK 相关: https://www.krackattacks.com/

参考文献

- http://www.freebuf.com/articles/wireless/58342.html
- http://blog.csdn.net/keekjkj/article/details/46753883

评论