

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

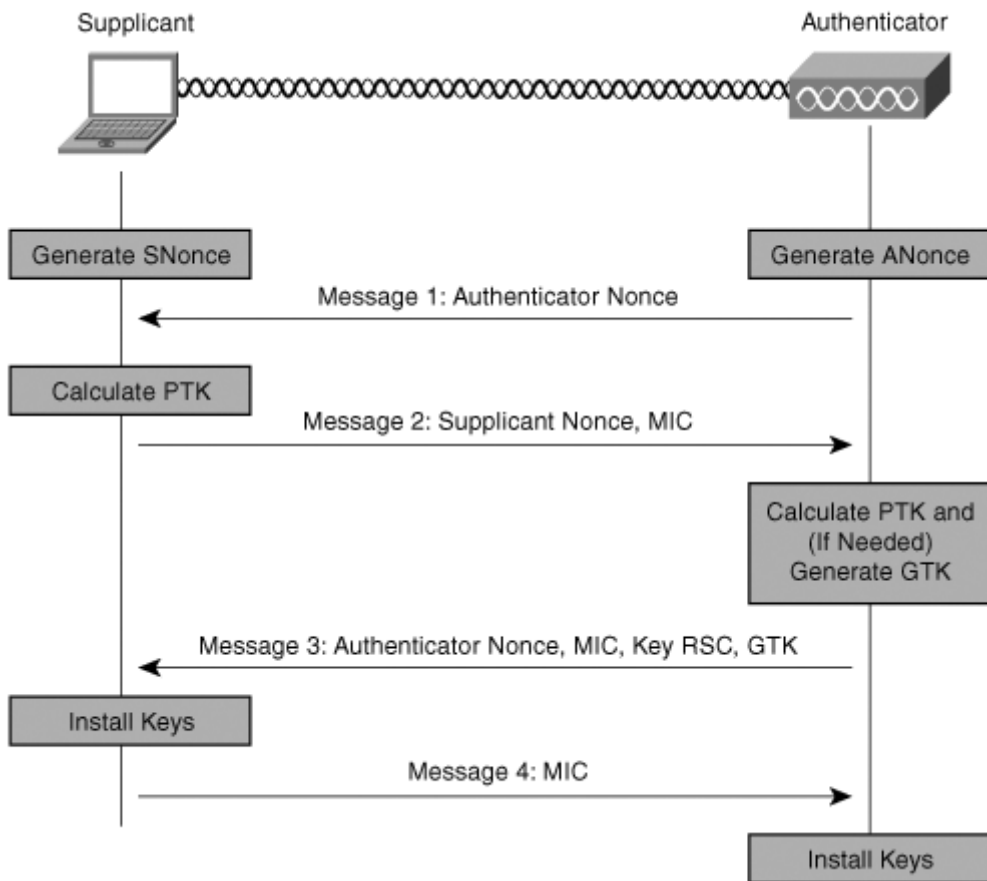
- 不启用安全
- WEP
- WPA/WPA2-PSK (预共享密钥)
- PA/WPA2 802.1X (radius 认证)

WPA-PSK

认证大致过程如下图



其中四次握手过程



1. 4 次握手始于验证器 (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

No.	Time	Source	Destination	Protocol	Length	Info
5909	8.230948		Apple_4c:2a:9a (98:fe:94:4...	802.11	10	Clear-to-send, Flags=.....
5910	8.230948	Tp-LinkT_d9:49:7e (5c...	Apple_4c:2a:9a (98:fe:94:4...	802.11	28	802.11 Block Ack, Flags=.....
5912	8.232980		HonHaiPr_69:20:5c (e4:d5:3...	802.11	10	Clear-to-send, Flags=.....
5911	8.232982	Tp-LinkT_68:db:d6 (14...	HonHaiPr_69:20:5c (e4:d5:3...	802.11	28	802.11 Block Ack, Flags=.....
5913	8.235074	Tp-LinkT_5d:d0:ee	Apple_98:a1:f3	EAPOL	131	Key (Message 1 of 4)
5914	8.235562		Tp-LinkT_5d:d0:ee (00:1d:0...	802.11	10	Acknowledgement, Flags=.....
5915	8.237608	Apple_98:a1:f3	Tp-LinkT_5d:d0:ee	EAPOL	153	Key (Message 2 of 4)
5916	8.238146		Apple_98:a1:f3 (60:fe:c5:9...	802.11	10	Acknowledgement, Flags=.....
5917	8.240670		Tp-LinkT_d9:49:7e (5c:63:b...	802.11	10	Clear-to-send, Flags=.....
5918	8.241700	Tp-LinkT_d9:49:7e (5c...	Apple_4c:2a:9a (98:fe:94:4...	802.11	28	802.11 Block Ack, Flags=.....
5919	8.242724	Tp-LinkT_d9:49:7e (5c...	Apple_4c:2a:9a (98:fe:94:4...	802.11	28	802.11 Block Ack, Flags=.....
5920	8.249920		Tp-LinkT_5d:d0:ee (00:1d:0...	802.11	10	Clear-to-send, Flags=.....
5921	8.256576	Tp-LinkT_5d:d0:ee	Apple_98:a1:f3	EAPOL	211	Key (Message 3 of 4)
5922	8.257064		Tp-LinkT_5d:d0:ee (00:1d:0...	802.11	10	Acknowledgement, Flags=.....
5923	8.260162		Apple_98:a1:f3 (60:fe:c5:9...	802.11	10	Acknowledgement, Flags=.....
5924	8.265234		HonHaiPr_69:20:5c (e4:d5:3...	802.11	10	Clear-to-send, Flags=.....

> Frame 5913: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)

> IEEE 802.11 Data, Flags:F.

> Logical-Link Control

> 802.1X Authentication

Version: 802.1X-2001 (1)
 Type: Key (3)
 Length: 95
 Key Descriptor Type: EAPOL RSN Key (2)
 Key Information: 0x008a
 Key Length: 16
 Replay Counter: 1
 WPA Key Nonce: 6e4529be252b6c1ca8bc1db7e9cd5bfbf9d4f9297d8a1c55...
 Key IV: 00000000000000000000000000000000
 WPA Key RSC: 0000000000000000
 WPA Key ID: 0000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 0

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