

Identifying and Responding to Wireless Attacks

Chris Hurley (roamer)
roamer@securitytribe.com



Black Hat Japan 2005

Contents

- A brief history of wireless security and attacks
- Attacks against WEP
- Attacks against WPA
- Attacks against VPN
- Man in the Middle Attacks
- Identifying and responding to these attacks



A brief history of wireless security and attacks

- Wired Equivalent Privacy (WEP) was the original security mechanism for 802.11 networks.
- Scott Fluhrer, Itsik Mantin, and Adi Shamir discovered that WEP was flawed in their paper “Weaknesses in the Key Scheduling Algorithm of RC4”



A brief history of wireless security and attacks

- Attacks based on Fluhrer, Mantin, and Shamir's paper have come to be known as "FMS Attacks"
- Shortly after the FMS paper was released tools to automate WEP cracking were developed
 - WEPCrack
 - AirSnort



A brief history of wireless security and attacks

- In response to the weaknesses in WEP new security mechanisms were developed.
 - Cisco developed the Lightweight Extensible Authentication Protocol (LEAP)
 - WiFi Protected Access (WPA) was developed to replace WEP
 - WPA-PSK (Pre-Shared Key)
 - WPA-RADIUS



A brief history of wireless security and attacks

- In March, 2003, Joshua Wright disclosed that LEAP was vulnerable to a dictionary attack
- A short time later Wright released ASLEAP, a tool to automate attacks against LEAP.
- Cisco released EAP-FAST as a replacement for LEAP about a year after Wright's initial disclosure to them.



A brief history of wireless security and attacks

- In November 2003 Robert Moskowitz of ISCA Labs detailed potential problems with WPA when deployed using a Pre-Shared Key in his paper “Weakness in Passphrase Choice in WPA Interface”



A brief history of wireless security and attacks

- In November 2004 Joshua Wright released CoWPAtty.
- CoWPAtty automated the dictionary attack process against WPA-PSK networks.



A brief history of wireless security and attacks

- Despite excessive cries to the contrary, WEP was still relatively safe to use in some environments.
- Cracking a WEP key was so time consuming that it was often not feasible.
- Regular rotation of WEP keys could render FMS attacks ineffective on most networks.



A brief history of wireless security and attacks

- After the release of the FMS paper, h1kari of Dachboden Labs released a paper detailing ways to more effectively crack WEP.
- In 2004 new tools based on a Chopping attack were released



A brief history of wireless security and attacks

- Chopping attacks take a WEP packet and “chop” off the last byte.
- This breaks the CRC/ICV.
- If the last byte was 0, xor last the last 4 bytes with a certain value to make a valid CRC.
- Retransmit the packet.



A brief history of wireless security and attacks

- This attack methodology significantly reduced the amount of time required to crack WEP keys.
- Made a largely theoretical attack (FMS) realistic
- Tools
 - Aircrack
 - weplab



A brief history of wireless security and attacks

- Where are we now?
 - Can wireless networks be deployed in a corporate environment securely?
 - Is wireless intrusion detection viable?
 - Can attacks against wireless networks be observed and reacted to in real time?



Attacks Against WEP

- Even with chopping attacks, a large number of packets still need to be captured by an attacker
- The easiest way to do this is by reinjecting packets back into the network to generate unique initialization vectors.



Attacks Against WEP

Normal-WEP.dump - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3508	178.393875	Cisco-Li_le:64:b2	Broadcast	IEEE 8	Beacon frame, SSID: "<no ssid>"
3510	178.496434	Cisco-Li_le:64:b2	Broadcast	IEEE 8	Beacon frame, SSID: "<no ssid>"
3512	178.598762	Cisco-Li_le:64:b2	Broadcast	IEEE 8	Beacon frame, SSID: "<no ssid>"
3514	178.701059	Cisco-Li_le:64:b2	Broadcast	IEEE 8	Beacon frame, SSID: "<no ssid>"
3516	178.803448	Cisco-Li_le:64:b2	Broadcast	IEEE 8	Beacon frame, SSID: "<no ssid>"
3518	178.905858	Cisco-Li_le:64:b2	Broadcast	IEEE 8	Beacon frame, SSID: "<no ssid>"

▶ Frame 1 (128 bytes on wire, 128 bytes captured)

- IEEE 802.11
 - Type/Subtype: Beacon frame (8)
 - ▶ Frame Control: 0x0080 (Normal)
 - Duration: 0
 - Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
 - Source address: 00:11:21:e0:98:00 (Cisco_e0:98:00)
 - BSS Id: 00:11:21:e0:98:00 (Cisco_e0:98:00)
 - Fragment number: 0
 - Sequence number: 1347

0000 00 11 21 e0 98 00 30 54 90 b1 c0 34 00 00 00 00 ..!...OT...4...
0020 64 00 31 00 00 06 72 6f 61 6d 65 72 01 08 82 84 d.l...ro amer...
0030 8b 0c 12 96 18 24 03 01 03 05 04 01 02 00 00 2a\$. *
0040 01 07 32 04 30 48 60 6c 85 1e 00 00 81 12 07 00 ..2.OH'l
0050 ff 03 11 00 61 70 00 00 00 00 00 00 00 00 00 00ap.....
0060 00 00 00 00 02 00 00 25 dd 16 00 40 96 04 00 0d%...@...
0070 06 a5 00 00 22 a3 00 00 41 54 00 00 61 43 00 00 " ... AT..aC..

Interpretation of tag (wlan_mgt.tag.interpretation), 6 bytes P: 8284 D: 8284 M: 0



Attacks Against WEP

The screenshot shows the Wireshark interface with a list of captured packets. The list contains several IEEE 802.11 Deauthentication frames. The detailed view of frame 4078 shows the following information:

- Frame 4078 (26 bytes on wire, 26 bytes captured)
- IEEE 802.11
- Type/Subtype: Deauthentication (12)
- Frame Control: 0x02C0 (Normal)
- Duration: 0
- Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
- Source address: 00:11:21:e0:98:00 (Cisco_e0:98:00)
- BSS Id: 00:11:21:e0:98:00 (Cisco_e0:98:00)
- Fragment number: 0
- Sequence number: 29
- IEEE 802.11 wireless LAN management frame

The packet bytes are displayed in hexadecimal and ASCII:

```
0000  02 00 00 ff ff ff ff ff ff 00 11 21 e0 98 00  ..!.....!...
0010  00 11 21 e0 98 00 d0 01 02 00  ..!.....
```

At the bottom of the window, it says: Type and subtype combined (wlan.fc.type_subtype), 1 byte P: 6864 D: 6864 M: 0

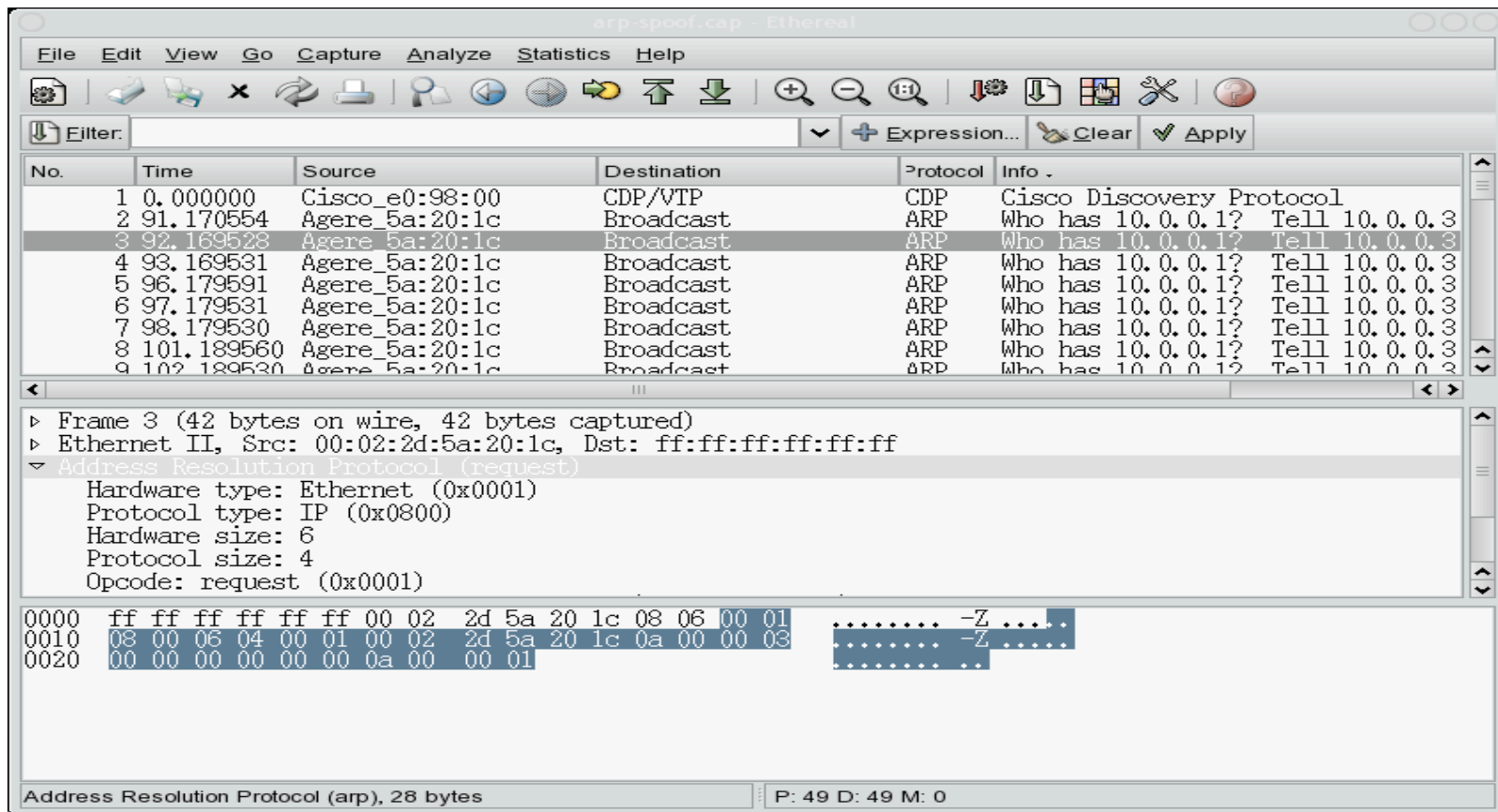


Attacks Against WEP

#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen
0	3	<no ssid>	00:13:10:1E:64:B2	WPA	managed	19	19	43	15537	8.12MiB	2005-09-26 02:37:54 -0400
1	3	roamer	00:11:21:E0:98:00	WEP	managed	39	34	49	14986	1.63MiB	2005-09-26 02:37:54 -0400
2	3	<any ssid>	00:02:2D:5A:20:1C		probe	0	16	39	856	31.67KiB	2005-09-26 02:31:10 -0400
3	3	<no ssid>	00:13:04:00:18:02	WEP	managed	0	14	14	1	24B	2005-09-26 02:28:15 -0400



Attacks Against WEP



The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of captured packets. Packet 3 is selected, and the details pane shows the structure of an ARP request. The packet bytes pane shows the raw hex and ASCII data of the ARP request.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_e0:98:00	CDP/VTP	CDP	Cisco Discovery Protocol
2	91.170554	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
3	92.169528	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
4	93.169531	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
5	96.179591	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
6	97.179531	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
7	98.179530	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
8	101.189560	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3
9	102.189530	Agere_5a:20:1c	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.3

Frame 3 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:02:2d:5a:20:1c, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)

```
0000  ff ff ff ff ff ff 00 02 2d 5a 20 1c 08 06 00 01  .....-Z...
0010  08 00 06 04 00 01 00 02 2d 5a 20 1c 0a 00 00 03  .....-Z...
0020  00 00 00 00 00 00 0a 00 00 01
```

Address Resolution Protocol (arp), 28 bytes | P: 49 D: 49 M: 0



Responding to Attacks Against WEP

- An attack against WEP is in progress
 - Deauthentication block
 - ARP Injection block
 - ARP Injection is easy to identify
 - Understand the approximate number of ‘normal’ ARP packets seen on your network
 - Rotate WEP keys
 - LAST RESORT: Shut down the WLAN



Attacks Against WPA

- WPA Pre Shared Keys with passphrases shorter than 21 characters are vulnerable to dictionary attacks
- This is an offline attack and not as easy to identify in real time as attacks against WEP



Attacks Against WPA

The screenshot shows the Wireshark interface with a capture of several deauthentication frames. The packet list pane shows frames 4078 through 4093, all of which are IEEE 802.11 Deauthentication frames from source Cisco_e0:98:00 to destination Broadcast. The packet details pane for frame 4078 shows the following structure:

- Frame 4078 (26 bytes on wire, 26 bytes captured)
- IEEE 802.11
 - Type/Subtype: Deauthentication (12)
 - Frame Control: 0x02C0 (Normal)
 - Duration: 0
 - Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
 - Source address: 00:11:21:e0:98:00 (Cisco_e0:98:00)
 - BSS Id: 00:11:21:e0:98:00 (Cisco_e0:98:00)
 - Fragment number: 0
 - Sequence number: 29
- IEEE 802.11 wireless LAN management frame

The packet bytes pane shows the raw hex and ASCII data:

```
0000  02 00 00 ff ff ff ff ff ff 00 11 21 e0 98 00  !.....!...
0010  00 11 21 e0 98 00 d0 01 02 00                ..!.....:
```



Attacks Against WPA

The screenshot shows a Wireshark interface with a list of captured packets. The selected packet is frame 64, which is an 802.1X Authentication frame. The detailed view shows the Ethernet II header and the 802.1X Authentication payload. The payload is displayed in hexadecimal and ASCII. The ASCII column shows a mix of printable characters and non-printable characters, including a null byte (00) and a carriage return (0d).

No.	Time	Source	Destination	Protocol	Info
56	87.230142	00:02:2d:5a:20:1c	00:13:10:1e:64:b2	EAPOL	Key
57	88.489126	00:13:10:1e:64:b2	00:02:2d:5a:20:1c	EAPOL	Key
58	88.498135	00:02:2d:5a:20:1c	00:13:10:1e:64:b2	EAPOL	Key
59	88.558558	00:13:10:1e:64:b2	00:02:2d:5a:20:1c	EAPOL	Key
60	88.558948	00:02:2d:5a:20:1c	00:13:10:1e:64:b2	EAPOL	Key
61	89.768545	00:13:10:1e:64:b2	00:02:2d:5a:20:1c	EAPOL	Key
62	89.769463	00:02:2d:5a:20:1c	00:13:10:1e:64:b2	EAPOL	Key
63	90.969571	00:13:10:1e:64:b2	00:02:2d:5a:20:1c	EAPOL	Key

Frame 64 (137 bytes on wire, 137 bytes captured)
Ethernet II, Src: 00:02:2d:5a:20:1c, Dst: 00:13:10:1e:64:b2
Destination: 00:13:10:1e:64:b2 (00:13:10:1e:64:b2)
Source: 00:02:2d:5a:20:1c (00:02:2d:5a:20:1c)
Type: 802.1X Authentication (0x888e)

802.1X Authentication

Offset	Hex	ASCII
0000	00 13 10 1e 64 b2 00 02 2d 5a 20 1c 88 8e 01 03d...-Z....
0010	00 77 fe 01 09 00 20 00 00 00 00 00 00 00 10 c4	w.....Uh]kL.Qc.
0020	89 77 e8 ba 87 90 55 68 7c 5d 6b 4c eb 51 63 84	w.....%...->.U..
0030	db ee a3 c6 25 e5 8f c5 10 2d 3e 1d 55 e1 c6 00P.....!{H.
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00P.....P.....
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 d6P.....P.....
0060	1c 3b a4 cd a2 c8 d4 a7 f6 d8 21 9f 7b 48 b6 00P.....P.....
0070	18 dd 16 00 50 f2 01 01 00 00 50 f2 02 01 00 00P.....P.....
0080	50 f2 02 01 00 00 50 f2 02P.....P.....

802.1X Authentication (eapol), 123 bytes | P: 193 D: 193 M: 0



Responding to Attacks Against WPA

- Unlike WEP attacks by the time you can take action, it is likely too late
- If your WPA passphrase is more than 21 characters, no action is necessary
- If it is shorter than 21 characters, immediately change to a passphrase longer than 21 characters
- Use WPA with RADIUS or some other form of secondary authentication. Preferably two factor authentication



Man in the Middle Attacks

- Attempt to have clients authenticate to an access point that is not a legitimate AP.
- Capture cleartext traffic to glean usernames, passwords, and other sensitive information



Man in the Middle Attacks

- Client based MITM attack
 - Use a client card configured in HOSTAP mode to act as an access point
 - Use a client card configured in HOSTAP mode to spoof a legitimate access point
- Access Point based MITM attack
 - Use an access point with custom firmware to spoof a legitimate access point



Man in the Middle Attacks

ethereal-mitm.cap - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
162	15.505102	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
165	15.645390	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
176	16.515048	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
179	16.634109	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
190	17.524990	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
193	17.613449	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
215	19.558756	00:02:2d:5a:20:1c	00:13:10:1e:64:b0	IEEE 802	Data
445	43.022189	00:02:2d:5a:20:1c	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "MITM" [Malformed Pa
447	43.124787	00:02:2d:5a:20:1c	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "MITM" [Malformed Pa

Frame 215 (166 bytes on wire, 166 bytes captured)

- AVS WLAN Monitoring Header
- IEEE 802.11 Data (70 bytes)

```
0000  80 21 10 01 00 00 00 40 00 00 00 00 9c cf bf aa  .!.....@ .....
0010  00 00 00 00 00 70 4b 40 00 00 00 04 00 00 00 03  .....pk@ .....
0020  00 00 00 6e 00 00 00 00 00 00 00 00 00 00 00 03  ....n.....
0030  00 00 00 3d 00 00 00 0b 00 00 00 00 00 00 00 01  ...=.....
0040  08 41 d5 00 00 13 10 1e 64 b2 00 02 2d 5a 20 1c  .A.....d...-Z.
0050  00 13 10 1e 64 b0 b0 bd 06 26 6e 20 00 00 00 00  ...d...&n...
0060  7e 75 bb c8 40 e9 c2 a0 28 5a 9f 83 e9 5a 2a 53  -u..@... (Z...Z+S
0070  9a ef ad 92 8e c3 52 bc 77 df f3 be f3 30 e0 3a  ....R. w...0.:
0080  b1 db ed 66 82 3a 2a b2 ac 44 70 45 5f a0 93 f8  ...f.:*. .DpE...
0090  61 2a 63 60 62 0e 75 af 7d 6a 74 8d 68 34 b7 04  a*c`b.u. }jt.h4..
00a0  26 02 66 66 66 66 66 66 66 66 66 66 66 66 66 66  f.....f.....f.....
```

File: ethereal-mitm.cap 283 KB 00:01:52 P: 1653 D: 1653 M: 0



Man in the Middle Attacks

The screenshot shows the Wireshark interface with a capture file named 'spool.cap'. The main packet list contains several IEEE 802 Beacon frames, all with SSID 'TEST'. The selected frame (No. 19035) is expanded to show the Prism Monitoring Header and a hex dump of the frame data.

No.	Time	Source	Destination	Protocol	Info
19035	1035.516151	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19036	1035.598520	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19037	1035.618538	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19038	1035.700915	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19039	1035.720938	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19040	1035.803315	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19041	1035.823332	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19042	1035.925731	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19043	1036.028124	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"

Frame 19035 (225 bytes on wire, 225 bytes captured)
Prism Monitoring Header
Message Code: 65
Message Length: 144
Device: eth1
Host Time: 0xcd54b (DID 0x1041, Status 0x0, Length 0x4)
MAC Time: 0x41e90edc (DID 0x2041, Status 0x0, Length 0x4)
RSSI: 0x0 (DID 0x4041, Status 0x1, Length 0x4)
Signal: 0x48 (DID 0x6041, Status 0x0, Length 0x4)

```
0000 41 00 00 00 90 00 00 00 65 74 68 31 00 00 00 00  A.....eth1....
0010 01 00 00 00 45 00 07 00 41 10 00 00 00 00 04 00  ..E...A.....
0020 4b d5 0c 00 41 20 00 00 00 00 04 00 dc 0e e9 41  K...A.....A
0030 41 30 00 00 01 00 04 00 00 00 00 00 41 40 00 00  A0.....Ae..
0040 01 00 04 00 00 00 00 00 41 50 00 00 01 00 04 00  .....AP.....
0050 00 00 00 00 41 60 00 00 00 00 04 00 48 00 00 00  .....A.....H...
0060 41 70 00 00 00 00 04 00 31 00 00 00 41 80 00 00  Ap.....1...A...
0070 00 00 04 00 02 00 00 00 41 90 00 00 00 00 04 00  .....A.....
0080 00 00 00 00 41 a0 00 00 00 00 04 00 51 00 00 00  .....A.....Q...
0090 80 00 00 00 ff ff ff ff ff ff 00 13 10 77 82 16  .....w.....
00a0 00 13 10 77 82 16 a0 10 8d 91 20 63 00 00 00 00  .....w.....c...
00b0 64 00 01 04 00 04 54 45 53 54 01 08 82 84 8b 96  d.....TE ST....
00c0 24 30 48 6c 03 01 06 05 04 00 01 00 00 2a 01 00  $0HL.....+...
00d0 2f 01 00 32 04 0c 12 18 60 dd 06 00 10 18 02 00  /...2.....
00e0 04
```

File: spool.cap 5044 KB 00:19:11 P: 21173 D: 21173 M: 0



Man in the Middle Attacks

spoofer.cap - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19042	1035.925731	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19043	1036.028124	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19044	1036.130518	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19045	1036.232933	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19046	1036.335306	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19047	1036.437698	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19048	1036.540104	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19049	1036.642488	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19050	1036.744887	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"

Frame 19049 (225 bytes on wire, 225 bytes captured)

Prism Monitoring Header

- Message Code: 65
- Message Length: 144
- Device: eth1
- Host Time: 0xcd5bc (DID 0x1041, Status 0x0, Length 0x4)
- MAC Time: 0x41fa3ec3 (DID 0x2041, Status 0x0, Length 0x4)
- RSSI: 0x0 (DID 0x4041, Status 0x1, Length 0x4)
- Signal: 0x48 (DID 0x6041, Status 0x0, Length 0x4)

```
0000 41 00 00 00 90 00 00 00 65 74 68 31 00 00 00 00 A.....eth1....
0010 01 00 00 00 45 00 07 00 41 10 00 00 00 00 04 00 ....E...A.....
0020 bc d5 0c 00 41 20 00 00 00 00 04 00 c3 3e fa 41 ....A.....>.A
0030 41 30 00 00 01 00 04 00 00 00 00 00 41 40 00 00 A0.....@e.
0040 01 00 04 00 00 00 00 00 41 50 00 00 01 00 04 00 .....AP.....
0050 00 00 00 00 41 60 00 00 00 00 04 00 48 00 00 00 .....A.....H...
0060 41 70 00 00 00 00 04 00 1e 00 00 00 41 80 00 00 Ap.....A...
0070 00 00 04 00 02 00 00 00 41 90 00 00 00 00 04 00 .....A.....
0080 00 00 00 00 41 a0 00 00 00 00 04 00 51 00 00 00 .....A.....Q...
0090 80 00 00 00 ff ff ff ff ff ff 00 13 10 77 82 16 .....w.P...lc...
00a0 00 13 10 77 82 16 50 11 86 c1 31 63 00 00 00 00 ....w.P...lc...
00b0 64 00 01 04 00 04 54 45 53 54 01 08 82 84 8b 96 d.....TE ST....
00c0 24 30 48 6c 03 01 06 05 04 00 01 00 00 2a 01 00 $0HL.....*...
00d0 2f 01 00 32 04 0c 12 18 60 dd 06 00 10 18 02 00 /.2.....
00e0 04
```

File: spoofer.cap 5044 KB 00:19:11 P: 21173 D: 21173 M: 0



Man in the Middle Attacks

The screenshot shows the Wireshark interface with a capture file named 'spoofedAP.png'. The main display area shows a list of captured frames. Frame 19042 is highlighted, showing a beacon frame from source 00:13:10:77:82:16 to destination ff:ff:ff:ff:ff:ff. The details pane shows the Prism Monitoring Header for this frame, including fields like Message Code, Device, Host Time, MAC Time, RSSI, and Signal. The packet bytes pane shows the raw hex and ASCII data of the frame.

No.	Time	Source	Destination	Protocol	Info
19034	1035.496127	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19035	1035.516151	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19036	1035.598520	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19037	1035.618538	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19038	1035.700915	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19039	1035.720938	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19040	1035.803315	00:13:10:85:81:e0	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19041	1035.823332	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19042	1035.925731	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"

Frame 19042 (225 bytes on wire, 225 bytes captured)
Prism Monitoring Header
Message Code: 65
Message Length: 144
Device: eth1
Host Time: 0xcd574 (DID 0x1041, Status 0x0, Length 0x4)
MAC Time: 0x41ef4ed5 (DID 0x2041, Status 0x0, Length 0x4)
RSSI: 0x0 (DID 0x4041, Status 0x1, Length 0x4)
Signal: 0x49 (DID 0x6041, Status 0x0, Length 0x4)

```
0000 41 00 00 00 90 00 00 00 65 74 68 31 00 00 00 00  A.....eth1....
0010 01 00 00 00 45 00 07 00 41 10 00 00 00 00 04 00  ....E...A.....
0020 74 d5 0c 00 41 20 00 00 00 00 04 00 d5 4e ef 41  t...A...N.A
0030 41 30 00 00 01 00 04 00 00 00 00 00 41 40 00 00  A0.....Ae...
0040 01 00 04 00 00 00 00 00 41 50 00 00 01 00 04 00  ....AP.....
0050 00 00 00 00 41 60 00 00 00 00 04 00 49 00 00 00  ....A'.....I...
0060 41 70 00 00 00 00 04 00 2e 00 00 00 41 80 00 00  Ap.....A...
0070 00 00 04 00 02 00 00 00 41 90 00 00 00 00 04 00  ....A.....A...
0080 00 00 00 00 41 a0 00 00 00 00 04 00 51 00 00 00  ....A.....Q...
0090 80 00 00 00 ff ff ff ff ff ff 00 13 10 77 82 16  ....w.....w...
00a0 00 13 10 77 82 16 e0 10 8d d1 26 63 00 00 00 00  ....w.....&c...
00b0 64 00 01 04 00 04 54 45 53 54 01 08 82 84 8b 96  d.....TE ST....
00c0 24 30 48 6c 03 01 06 05 04 00 01 00 00 2a 01 00  $0H1.....+...
00d0 2f 01 00 32 04 0c 12 18 60 dd 06 00 10 18 02 00  /...2.....
00e0 04
```



Man in the Middle Attacks

spoofedAP.png - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19276	1056.715315	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19277	1056.814292	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19278	1056.817762	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19279	1056.823363	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xa4f5ab
19280	1056.823819	00:50:da:1e:f0:51	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.0.36? Tell 192.168.0.1
19281	1056.829491	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xa4f5ab
19282	1056.916692	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19283	1056.920156	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"
19284	1057.019084	00:13:10:77:82:16	ff:ff:ff:ff:ff:ff	IEEE 802	Beacon frame, SSID: "TEST"

Frame 19278 (225 bytes on wire, 225 bytes captured)

Prism Monitoring Header

- Message Code: 65
- Message Length: 144
- Device: eth1
- Host Time: 0xcdd9d (DID 0x1041, Status 0x0, Length 0x4)
- MAC Time: 0x432e1b0f (DID 0x2041, Status 0x0, Length 0x4)
- RSSI: 0x0 (DID 0x4041, Status 0x1, Length 0x4)
- Signal: 0x5b (DID 0x6041, Status 0x0, Length 0x4)

```
0000 41 00 00 00 90 00 00 00 65 74 68 31 00 00 00 00  A.....eth1....
0010 01 00 00 00 45 00 07 00 41 10 00 00 00 00 04 00  ....E...A.....
0020 9d dd 0c 00 41 20 00 00 00 00 04 00 0f 1b 2e 43  ....A.....C
0030 41 30 00 00 01 00 04 00 00 00 00 00 41 40 00 00  A0.....@e..
0040 01 00 04 00 00 00 00 00 41 50 00 00 01 00 04 00  ....AP.....
0050 00 00 00 00 41 60 00 00 00 00 04 00 5b 00 00 00  ....A.....[...
0060 41 70 00 00 00 00 04 00 34 00 00 00 41 80 00 00  Ap.....4...A...
0070 00 00 04 00 02 00 00 00 41 90 00 00 00 00 04 00  ....A.....
0080 00 00 00 00 41 a0 00 00 00 00 04 00 51 00 00 00  ....A.....Q...
0090 80 00 00 00 ff ff ff ff ff ff 00 13 10 77 82 16  .....w.....
00a0 00 13 10 77 82 16 50 01 88 d1 20 00 00 00 00 00  ....w...P.....
00b0 64 00 01 04 00 04 54 45 53 54 01 08 82 84 8b 96  d.....TE ST....
00c0 24 30 48 6c 03 01 06 05 04 00 01 01 00 2a 01 00  $0Hl.....*..
00d0 2f 01 00 32 04 0c 12 18 60 dd 06 00 10 18 02 00  /..2.....
00e0 04
```

File: spoofedAP.png 5044 KB 00:19:11 P: 21173 D: 21173 M: 0



Responding to Man in the Middle Attacks

- Real time response to Man in the Middle Attacks is difficult.
- Preventative measures should be in place prior to a Man in the Middle attack commencing.



Responding to Man in the Middle Attacks

- Always require authentication to the network over an encrypted channel
- Use two factor authentication
- Treat the WLAN as a DMZ host with no network privileges without authentication
- Utilize wireless network equipment that actively responds to these type of events



Conclusion

- Wireless attacks have evolved significantly over the years
- As attacks have evolved, so have the tools available to administrators to respond to attacks
- No tool is a substitute for well trained, vigilant Administrators



Questions?

- roamer@securitytribe.com
- chris@goons.org

