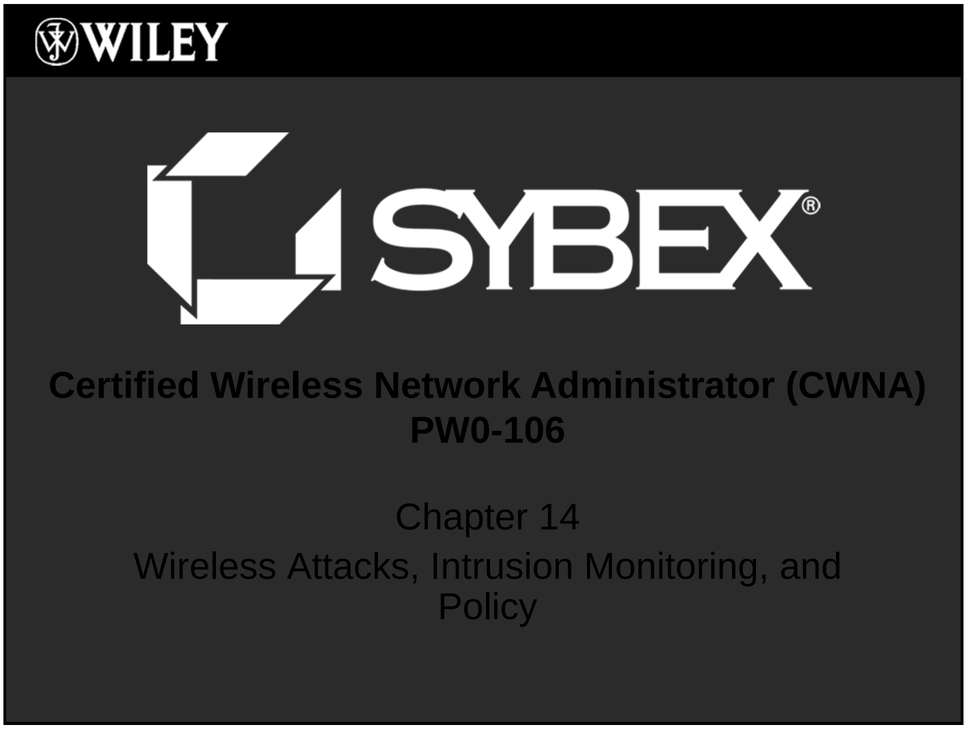
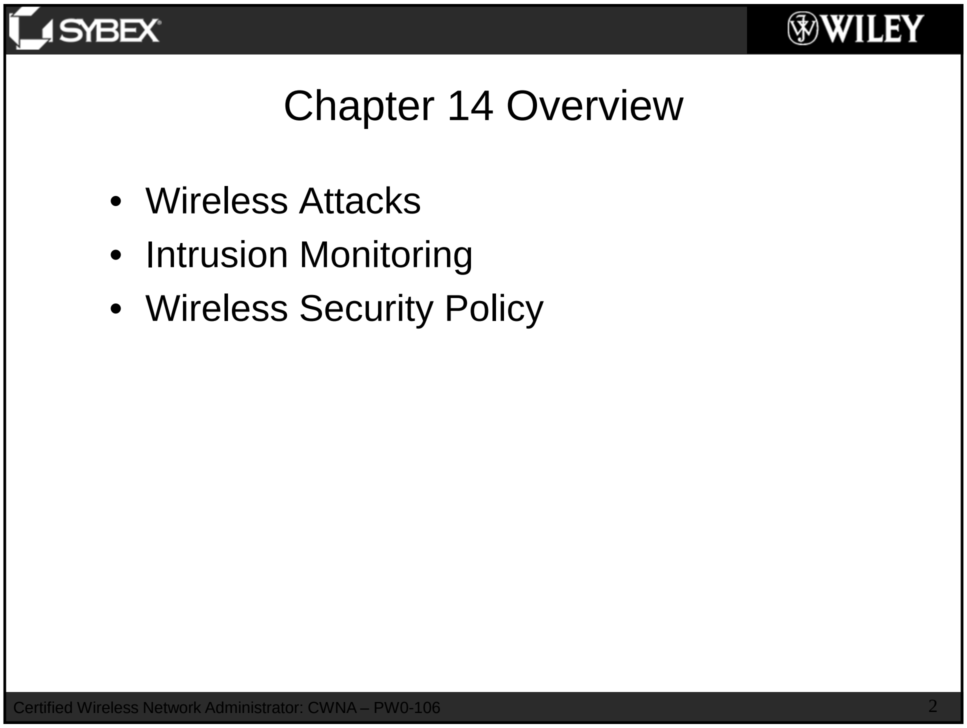


Certified Wireless Network Administrator (CWNA) PW0-106

Chapter 14

Wireless Attacks, Intrusion Monitoring, and Policy

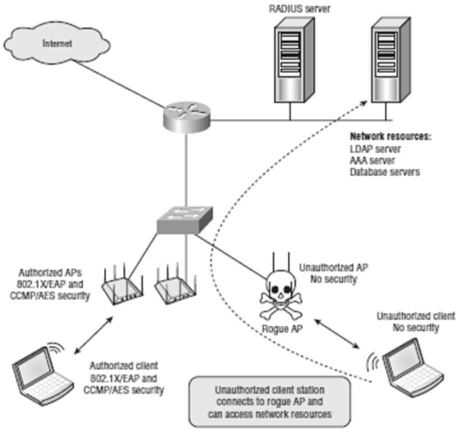


Chapter 14 Overview

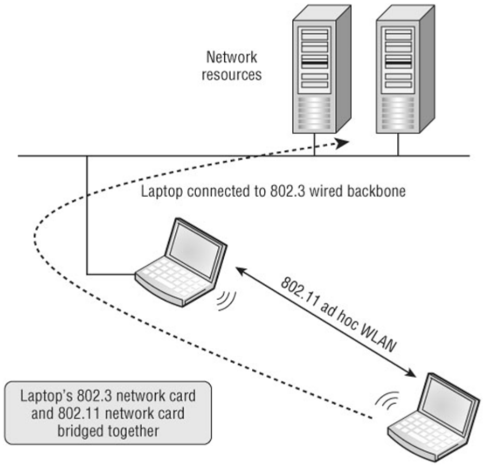
- Wireless Attacks
- Intrusion Monitoring
- Wireless Security Policy

Rogue Wireless Devices

- IEEE 802.1AE Media Access Control Security standard, often referred to as MACsec, specifies a set of protocols to meet the security requirements for protecting data traversing Ethernet LANs
- Makes this good way to not only utilize existing resources but also provide better security foryour wired network by protecting against rogue APs

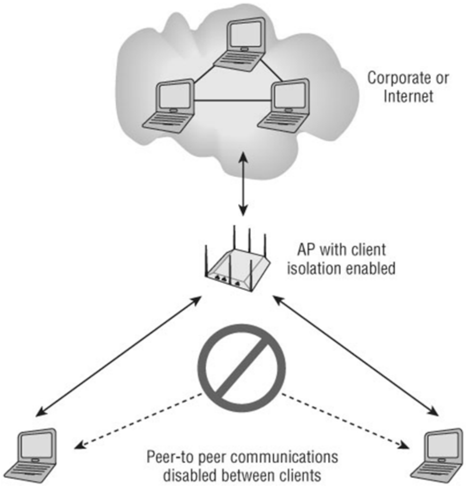


Bridged Ad Hoc WLAN



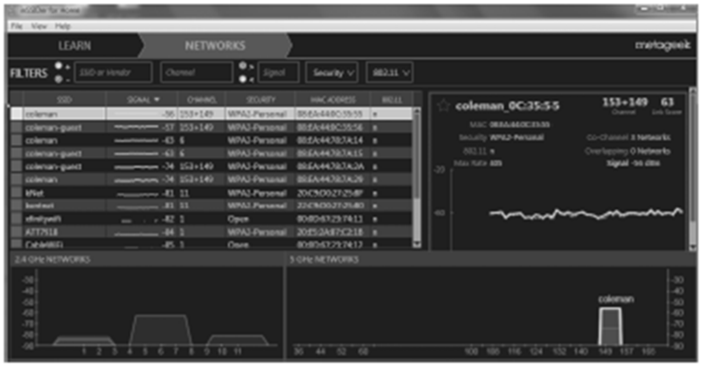
SYBEX WILEY

Client Isolation (Peer-to-Peer Attacks)


Corporate or Internet
AP with client isolation enabled
Peer-to peer communications disabled between clients

SYBEX WILEY

Casual Eavesdropping (WiFi Discovery)



SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	802.11
coleman	-56	153+149	WPA2-Personal	88:EA:44:0C:35:55	n
coleman-guest	-57	153+149	WPA2-Personal	88:EA:44:0C:35:56	n
coleman	-63	6	WPA2-Personal	88:EA:44:7B:7A:14	n
coleman-guest	-63	6	WPA2-Personal	88:EA:44:7B:7A:15	n
coleman-guest	-74	153+149	WPA2-Personal	88:EA:44:7B:7A:2A	n
coleman	-74	153+149	WPA2-Personal	88:EA:44:7B:7A:29	n
kNet	-81	11	WPA2-Personal	20:C9:D0:27:25:8F	n
[illegible]	-81	11	WPA2-Personal	22:C9:D0:27:25:80	n
xfinitywifi	-82	1	Open	80:80:67:29:74:11	n
ATT7918	-84	1	WPA2-Personal	20:E5:2A:87:C2:18	n
CableWiFi	-85	1	Open	80:80:67:29:74:12	n

coleman_0C:35:55 153+149 Channel 63 Link Score

MAC 88:EA:44:0C:35:55

Security WPA2-Personal Co-Channel 3 Networks

802.11 n Overlapping 0 Networks

Max Rate 300 Signal -56 dBm

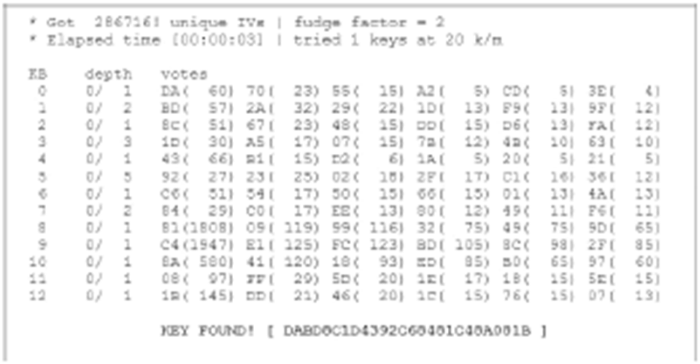
SYBEX WILEY

WiFiFoFum WLAN discovery tool

SYBEX WILEY

Encryption Cracking

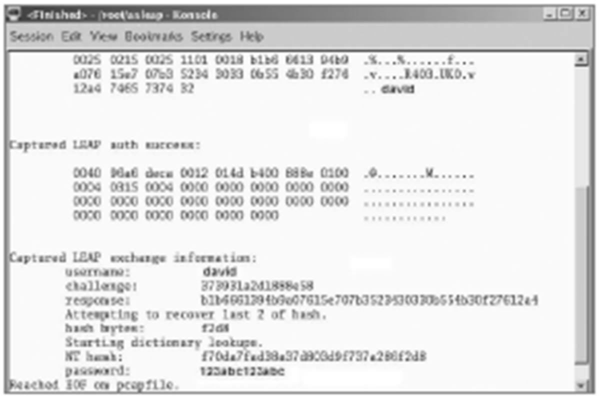
- WEP cracking tool



```
* Got  286716! unique IVs | fudge factor = 2
* Elapsed time [00:00:03] | tried 1 keys at 20 k/m

KB    depth   votes
 0     0/  1   DA(  60) 70(  23) 55(  15) A2(   5) CD(   5) 3E(   4)
 1     0/  2   BD(  57) 2A(  32) 29(  22) 1D(  13) F9(  13) 9F(  12)
 2     0/  1   8C(  51) 67(  23) 48(  15) DD(  15) D6(  13) FA(  12)
 3     0/  3   1D(  30) A5(  17) 07(  15) 7B(  12) 4B(  10) 63(  10)
 4     0/  1   43(  66) B1(  15) D2(   6) 1A(   5) 20(   5) 21(   5)
 5     0/  5   92(  27) 23(  25) 02(  18) 2F(  17) C1(  16) 36(  12)
 6     0/  1   C6(  51) 54(  17) 50(  15) 66(  15) 01(  13) 4A(  13)
 7     0/  2   84(  29) C0(  17) EE(  13) 80(  12) 49(  11) F6(  11)
 8     0/  1   81(1808) 09( 119) 99( 116) 32(  75) 49(  75) 9D(  65)
 9     0/  1   C4(1947) E1( 125) FC( 123) BD( 105) 8C(  98) 2F(  85)
10     0/  1   8A( 580) 41( 120) 18(  93) ED(  85) B0(  65) 97(  60)
11     0/  1   08(  97) FF(  29) 5D(  20) 1E(  17) 18(  15) 5E(  15)
12     0/  1   1B( 145) DD(  21) 46(  20) 1C(  15) 76(  15) 07(  13)

               KEY FOUND! [ DABD8C1D4392C68481C48A081B ]
```

Authentication Attacks

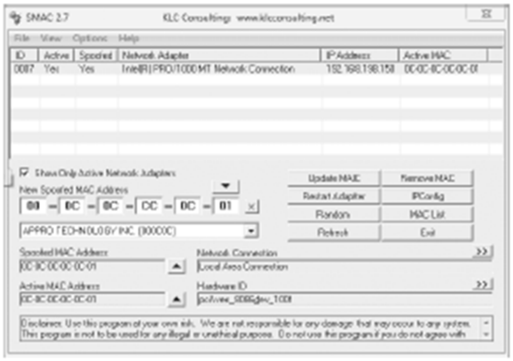
- Offline Dictionary Attack
- A policy mandating very strong passphrases of 20 characters or more should always be in place whenever a WPA/WPA2-Personal solution is deployed.


<Finished> - /root/asleap - Konsole
Session Edit View Bookmarks Settings Help

```
        0025 0215 0025 1101 0018 b1b6 6613 94b9  .%...%......f...
        a076 15e7 07b3 5234 3033 0655 4b30 f274  .v....R403.UK0.v
        12a4 7465 7374 32                        .. david


Captured LEAP auth success:

        0040 90a6 deca 0012 014d b400 888e 0100  .@.......M......
        0004 0815 0004 0000 0000 0000 0000 0000  ................
        0000 0000 0000 0000 0000 0000 0000 0000  ................
        0000 0000 0000 0000 0000 0000            ............

Captured LEAP exchange information:
       username:          david
       challenge:         373931a2d1888a58
       response:          b1b4661294b9a07615e707b3523430330b554b30f27612a4
       Attempting to recover last 2 of hash.
       hash bytes:        f2d8
       Starting dictionary lookups.
       NT hash:           f70da7fad38a37d903d9f737a280f2d8
       password:          123abc123abc
Reached EOF on pcapfile.
```

MAC Spoofing

- MAC spoofing software utility



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0087	Yes	Yes	Intel(R) PRO/1000 MT Network Connection	192.168.198.158	0C-0C-0C-0C-0C-01

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 – 0C – 0C – CC – 0C – 01

APPRO TECHNOLOGY INC. (00000C)

Spoofed MAC Address: 0C-0C-0C-0C-0C-01

Network Connection: Local Area Connection

Active MAC Address: 0C-0C-0C-0C-0C-01

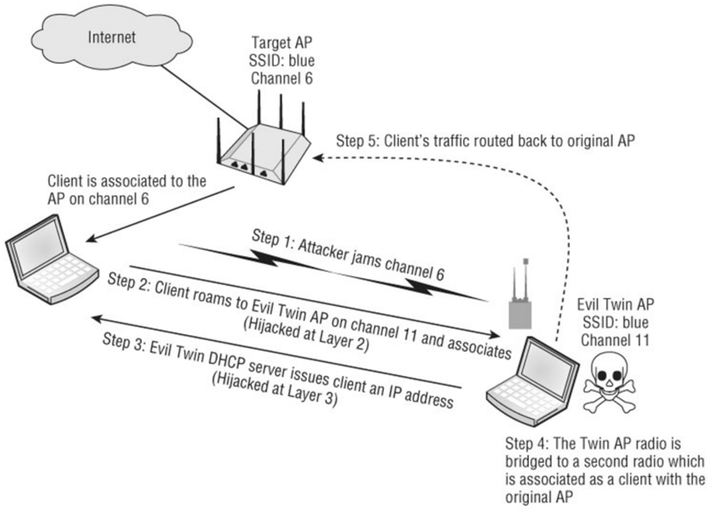
Hardware ID: pci\ven_8086&dev_1001

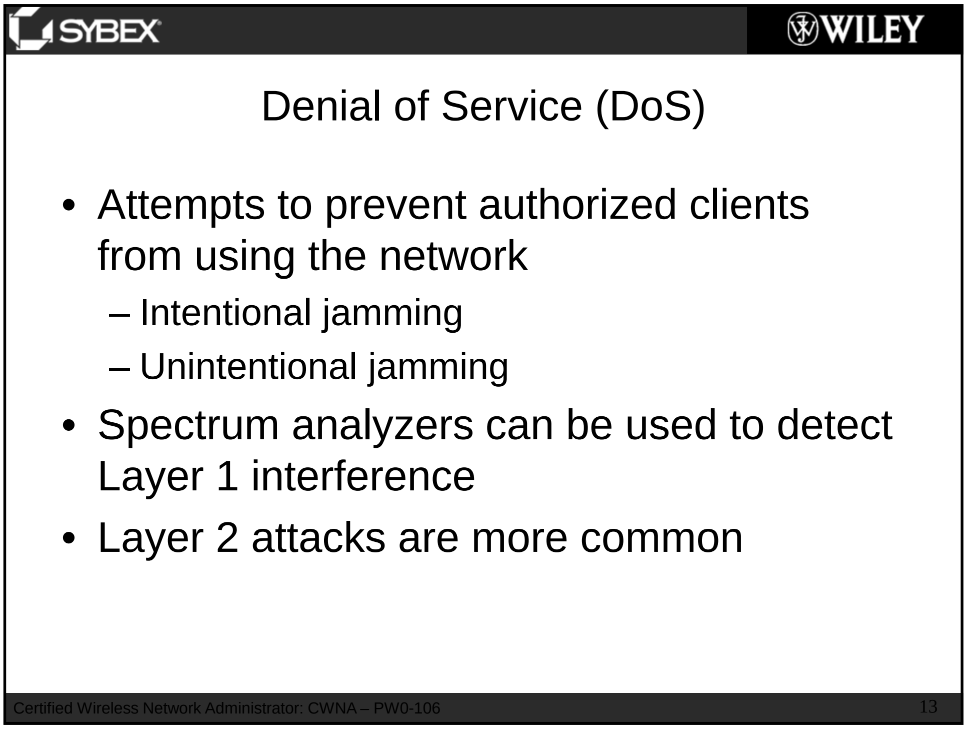
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Management Interface Exploits

- Take advantage of management tools
  - Web based
  - Client based
  - CLI
- Must use HTTPS for web-based management
- Must require authentication
  - Change from defaults

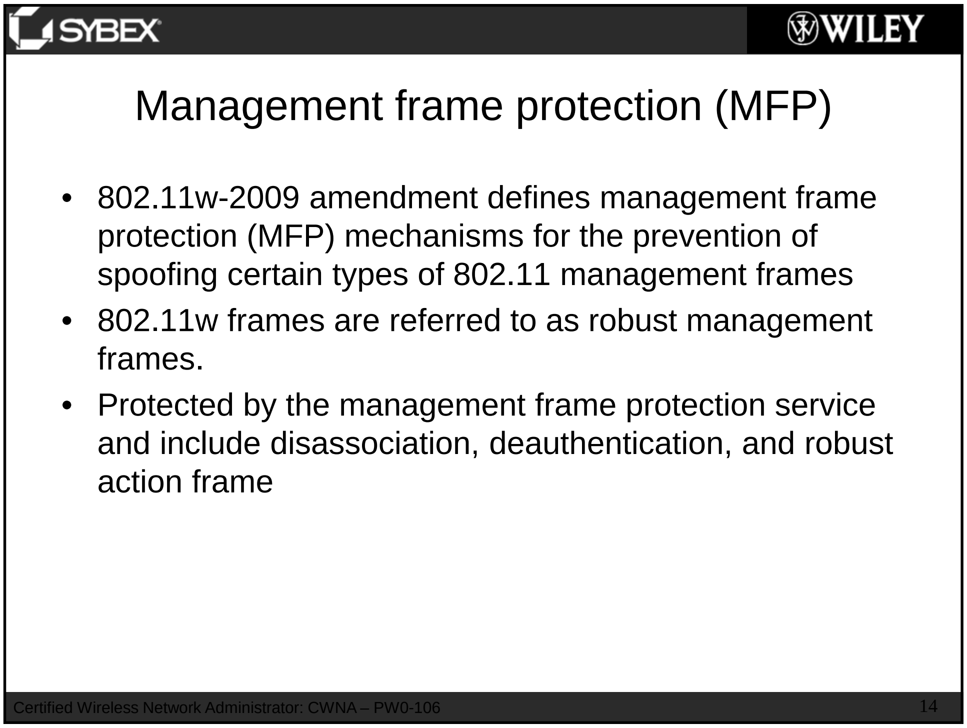
Wireless Hijacking


Internet
Target AP
SSID: blue
Channel 6
Step 5: Client's traffic routed back to original AP
Client is associated to the AP on channel 6
Step 1: Attacker jams channel 6
Step 2: Client roams to Evil Twin AP on channel 11 and associates (Hijacked at Layer 2)
Step 3: Evil Twin DHCP server issues client an IP address (Hijacked at Layer 3)
Evil Twin AP
SSID: blue
Channel 11
Step 4: The Twin AP radio is bridged to a second radio which is associated as a client with the original AP



Denial of Service (DoS)

- Attempts to prevent authorized clients from using the network
  - Intentional jamming
  - Unintentional jamming
- Spectrum analyzers can be used to detect Layer 1 interference
- Layer 2 attacks are more common



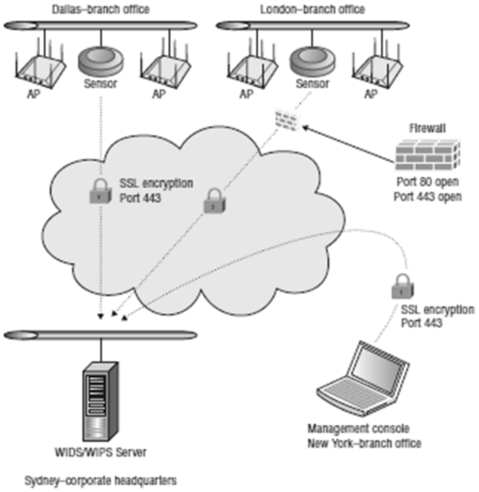
Management frame protection (MFP)

- 802.11w-2009 amendment defines management frame protection (MFP) mechanisms for the prevention of spoofing certain types of 802.11 management frames
- 802.11w frames are referred to as robust management frames.
- Protected by the management frame protection service and include disassociation, deauthentication, and robust action frame

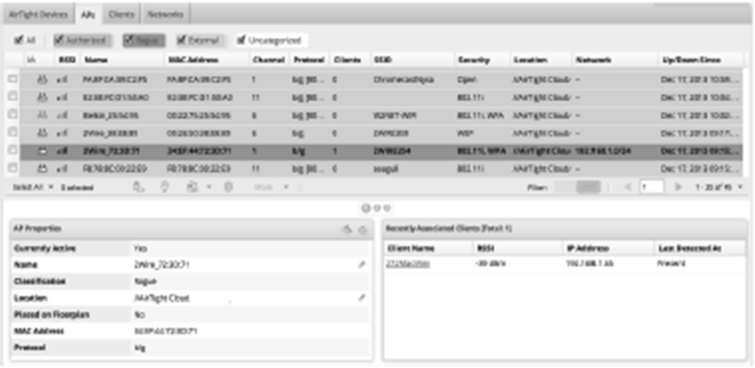
Intrusion Monitoring

- Wireless Intrusion *Detection* System (WIDS)
  - WIDS Server
  - Management Consoles
  - Sensors
- Wireless Intrusion *Prevention* System (WIPS)
  - Infrastructure device
  - Unknown device
  - Known device
  - Rogue device

WIDS



WIDS Management Console



	RSSI	Name	MAC Address	Channel	Protocol	Clients	SSID	Security	Location	Network	Up/Down Since
□	[illegible]	FA:8F:CA:39:C2:F5	FA:8F:CA:39:C2:F5	1	b/g [80...	0	[illegible]	Open	//AirTight Cloud/	–	Dec 17, 2013 10:38...
□	[illegible]	[illegible]	[illegible]	11	b/g [80...	0		802.11i	//AirTight Cloud/	–	Dec 17, 2013 10:0...
□	[illegible]	Belkin_[illegible]	[illegible]	6	b/g [80...	0	[illegible]	802.11i, WPA	//AirTight Cloud/	–	Dec 17, 2013 10:0...
□	[illegible]	2Wire_[illegible]	[illegible]	6	b/g	0	[illegible]	WEP	//AirTight Cloud/	–	Dec 17, 2013 09:...
□	[illegible]	2Wire_72:30:71	[illegible]:72:30:71	1	b/g	1	[illegible]	802.11i, WPA	//AirTight Clou	192.168.1.0/24	Dec 17, 2013 09:...
□	[illegible]	FB:78:8C:00:22:69	FB:78:8C:00:22:69	11	b/g [80...	0	seagull	802.11i	//AirTight Cloud/	–	Dec 17, 2013 09:...

AP Properties

Currently Active	Yes
Name	2Wire_72:30:71
Classification	Rogue
Location	//AirTight Cloud
Placed on Floorplan	No
MAC Address	[illegible]:72:30:71
Protocol	b/g

Recently Associated Clients (Total: 1)

Client Name	RSSI	IP Address	Last Detected At
[illegible]	-39 dBm	192.168.1.65	Present

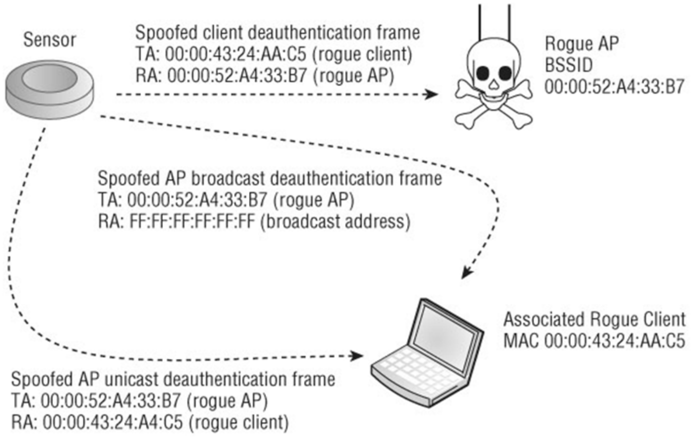
WIDS design models

- Overlay- most secure model is an overlay WIDS that is deployed on top of the existing wireless network
- Integrated- centralized WLAN controller or a centralized network management server (NMS) functions as the IDS server.
- Integration Enabled - Wi-Fi vendor’s APs integrate software code that can be used to turn the APs into sensors that will communicate with the third-party WIDS server.

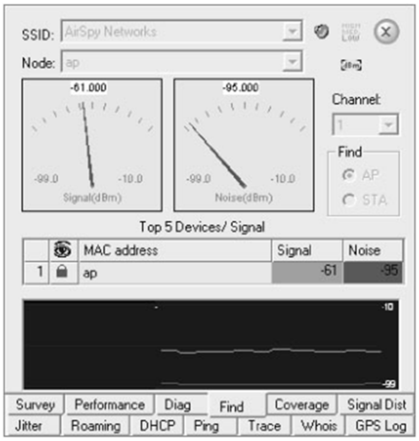
Wireless Intrusion Prevention System (WIPS)

- Locates, identifies and classifies devices
  - – Infrastructure Device
  - – Unknown Device
  - – Known Device
  - – Rogue Device

Wireless Rogue Containment


Sensor
Spoofed client deauthentication frame
TA: 00:00:43:24:AA:C5 (rogue client)
RA: 00:00:52:A4:33:B7 (rogue AP)
Rogue AP
BSSID
00:00:52:A4:33:B7
Spoofed AP broadcast deauthentication frame
TA: 00:00:52:A4:33:B7 (rogue AP)
RA: FF:FF:FF:FF:FF:FF (broadcast address)
Associated Rogue Client
MAC 00:00:43:24:AA:C5
Spoofed AP unicast deauthentication frame
TA: 00:00:52:A4:33:B7 (rogue AP)
RA: 00:00:43:24:A4:C5 (rogue client)

Mobile WIDS Locator



SSID: AirSpy Networks

Node: ap

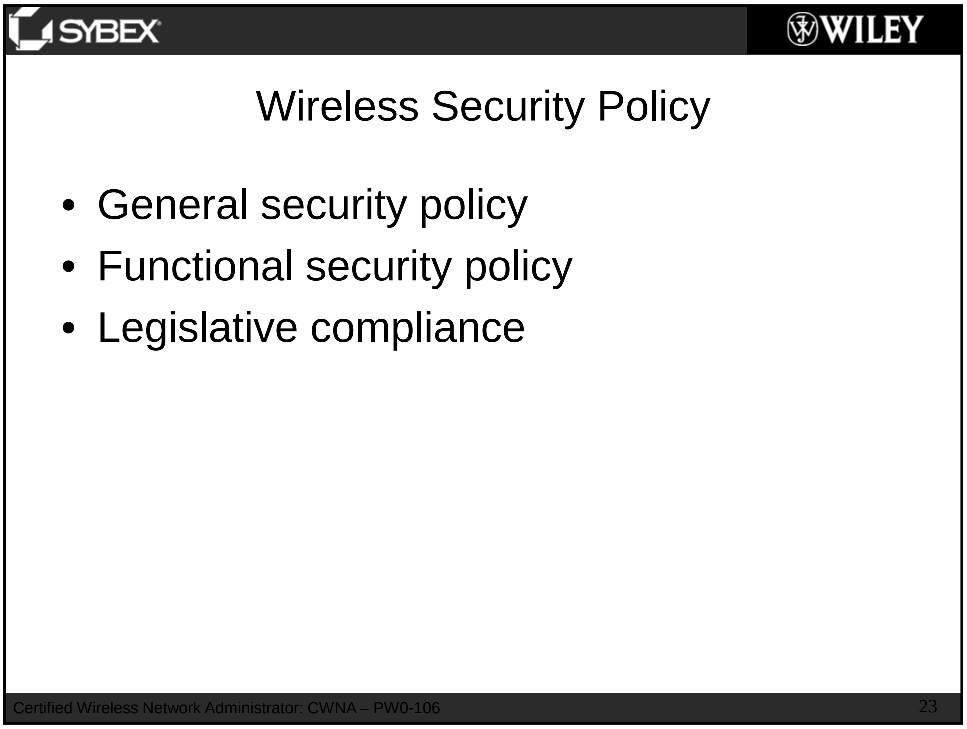
Channel: 1

Top 5 Devices/ Signal

		MAC address	Signal	Noise
1	🔒	ap	-61	-95

Spectrum Analyzer

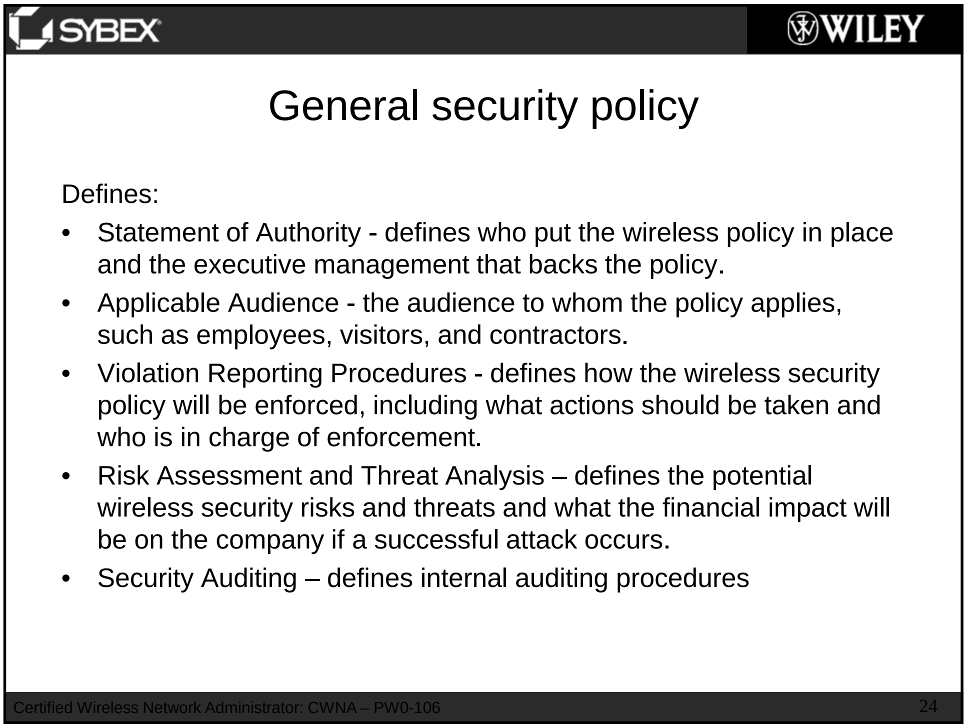
- Frequency domain tool that can detect any RF signal in the frequency range that is being scanned.
  - Mobile
  - Distributed



SYBEX WILEY

Wireless Security Policy

- General security policy
- Functional security policy
- Legislative compliance

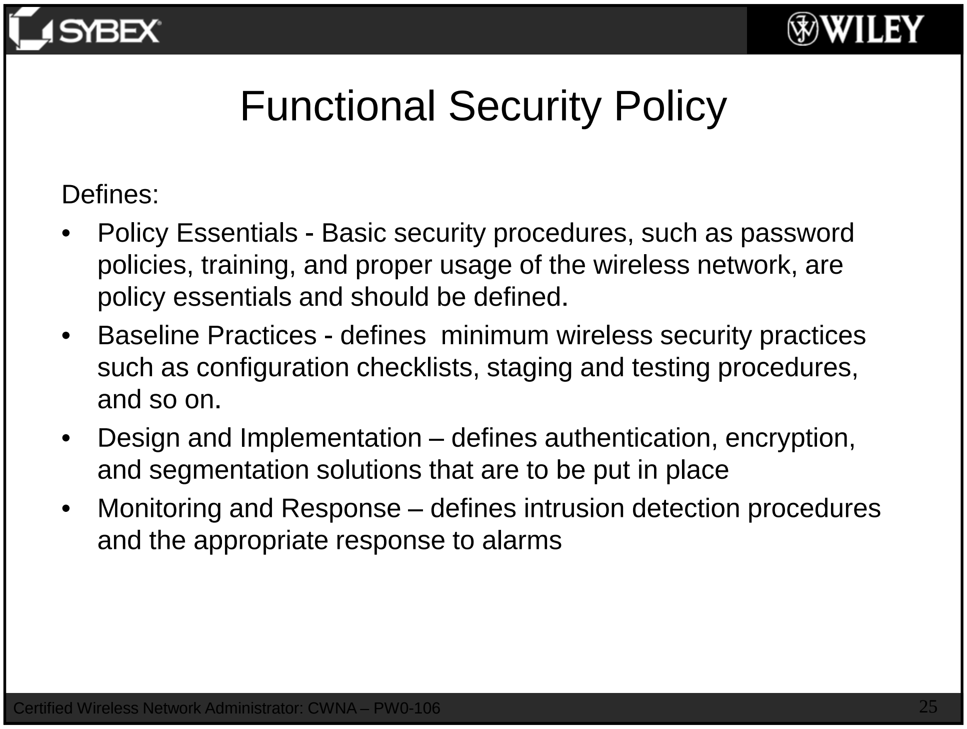


SYBEX WILEY

General security policy

Defines:

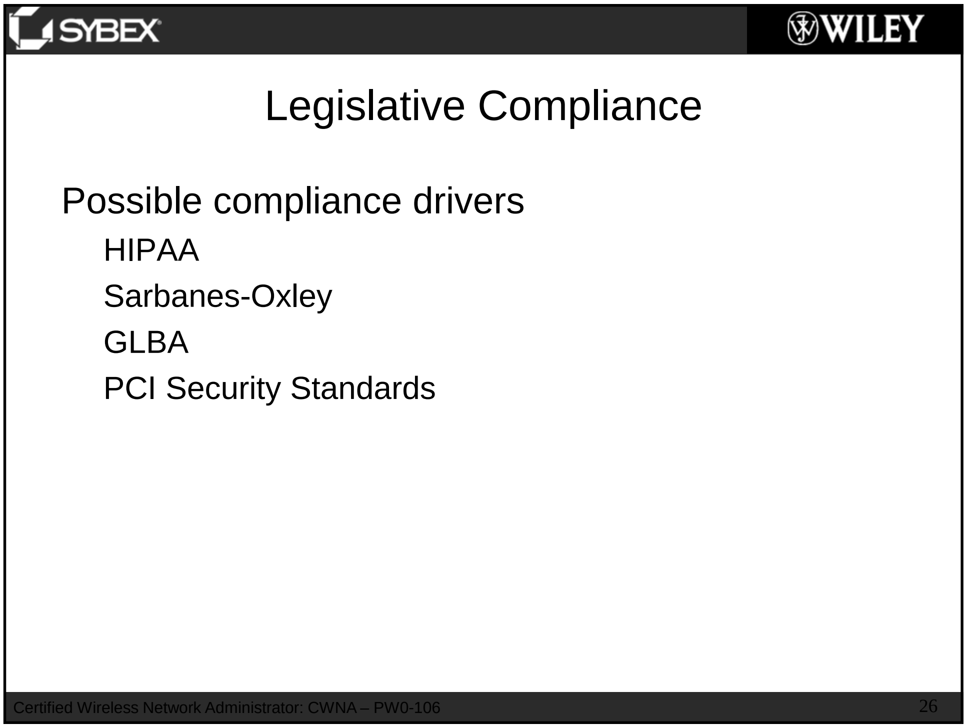
- Statement of Authority - defines who put the wireless policy in place and the executive management that backs the policy.
- Applicable Audience - the audience to whom the policy applies, such as employees, visitors, and contractors.
- Violation Reporting Procedures - defines how the wireless security policy will be enforced, including what actions should be taken and who is in charge of enforcement.
- Risk Assessment and Threat Analysis – defines the potential wireless security risks and threats and what the financial impact will be on the company if a successful attack occurs.
- Security Auditing – defines internal auditing procedures



Functional Security Policy

Defines:

- Policy Essentials - Basic security procedures, such as password policies, training, and proper usage of the wireless network, are policy essentials and should be defined.
- Baseline Practices - defines minimum wireless security practices such as configuration checklists, staging and testing procedures, and so on.
- Design and Implementation – defines authentication, encryption, and segmentation solutions that are to be put in place
- Monitoring and Response – defines intrusion detection procedures and the appropriate response to alarms



Legislative Compliance

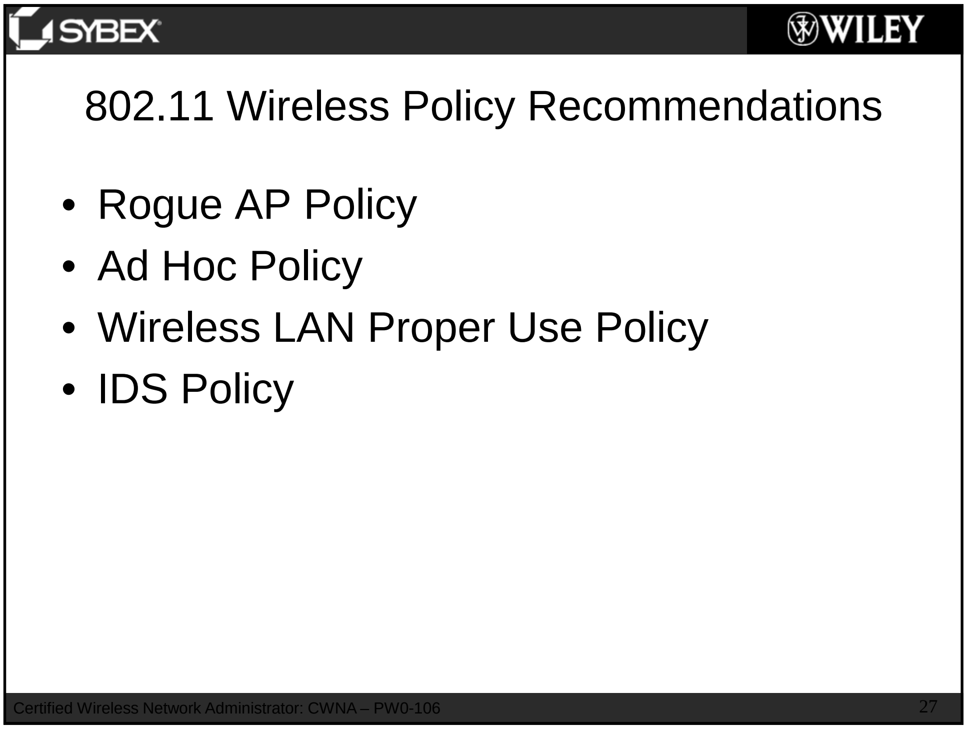
Possible compliance drivers

HIPAA

Sarbanes-Oxley

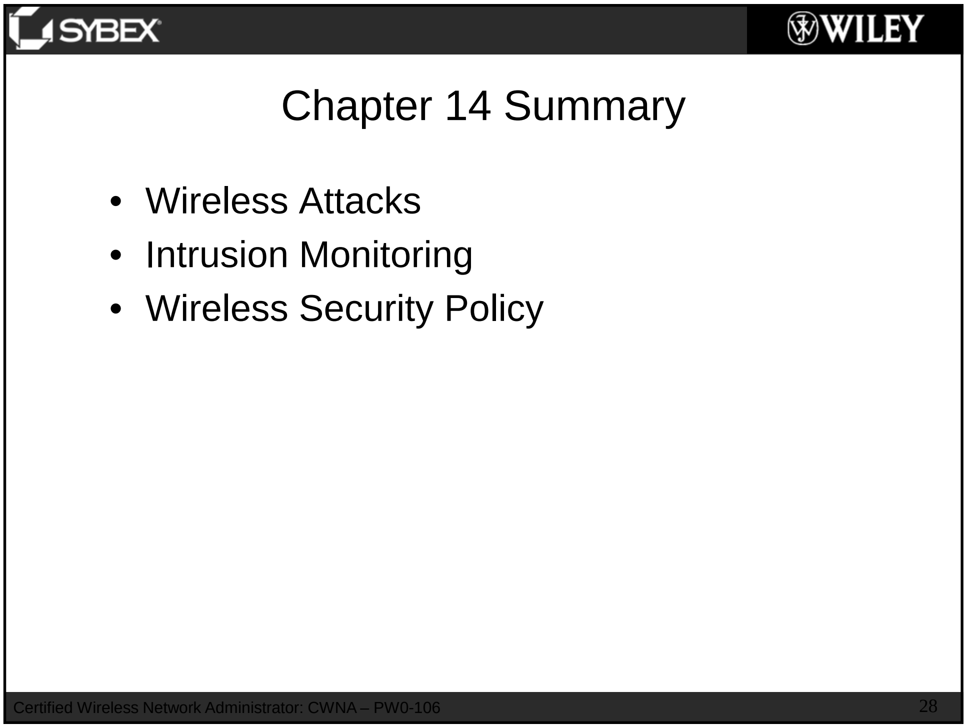
GLBA

PCI Security Standards



802.11 Wireless Policy Recommendations

- Rogue AP Policy
- Ad Hoc Policy
- Wireless LAN Proper Use Policy
- IDS Policy



Chapter 14 Summary

- Wireless Attacks
- Intrusion Monitoring
- Wireless Security Policy