Five components of WLAN Security

1. Data Privacy
    1. Privacy is important because transmission occurs over the air in freely licensed bands. The Data can be sniffed by anyone within range.
    2. **Eavesdropping** – Also referred to *war driving.* Many free utilities exist to find WLAN's (Such NetStumbler and InSSIDer) These programs broadcast null probe request across all channels forcing the AP's to respond. (With the SSID, Channel, Encryption Type, etc). Casual eavesdropping is considered harmless. However this can be performed with a protocol analyzer and legitimate data can be captured. This is also known as a passive attack
2. AAA
    1. Authentication - Verification of credentials
    2. Authorization - Granting access to resources.
    3. Accounting - Audit of what was accessed by who.(This is important for HIPAA compliance)
3. Segmentation
    1. Access/Role segmentation via RBAC.
        1. RBAC provides restricted access to authorized users. May restrict bandwidth usage and port access.
    2. Network segmentation via Firewalls or VLANs.
        1. VLANs provide different networks for different SSID's depicting different security or QoS rules.
4. Monitoring
    1. Provided by a WIPS or WIDS, that watches for Layer 1/2 attacks.
    2. Spectrum Analysis can be performed to find sources of interference at layer 1.
5. Security Policy

Legacy Security

Open System - No/Null authentication, anyone is able to join. Performed as a two way handshake.

WEP - Wired Equivalent Privacy, a Shared key authentication to prevent casual eavesdropping. The key is configured on the both the access point and the client. This WEP key is used to encrypt all 802.11 data frames. Can keys can either be ASCII or Hex characters. RADIUS can use dynamic WEP keys on a per-packets basis, enhancing security WEP however is still weak.

WEP Shared Key Authentication

This process is illustrated below.

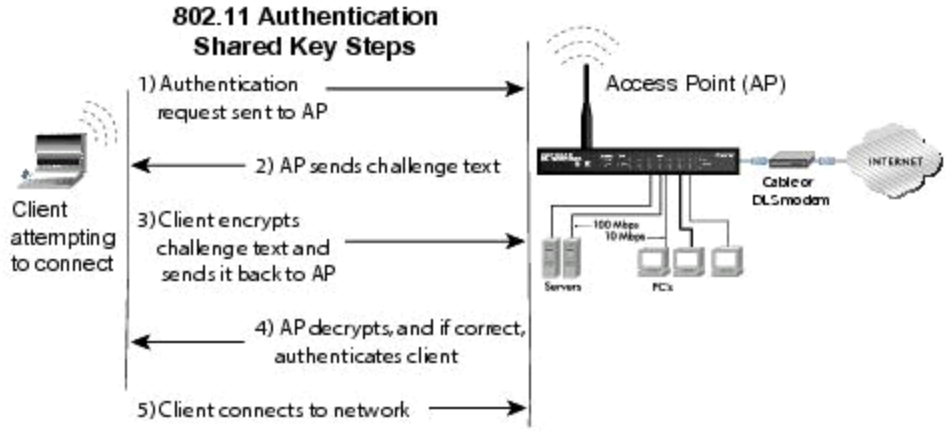

Image: WEP Authentication process

Integrity Check Value ICV is ran against the data prior to encryption and is used to prevent the data from being altered.
64-Bit WEP uses a 40-Bit static key and a 24-bit Initialization Vector (IV) The IV is sent in clear text and changes every frame. However their are only 16,777,216 different combinations.
Key Length 10 Hex or 5 ASCII
128-Bit WEP used a 104-Bit static key and 24-Bit IV.
Key Length 26 Hex or 13 ASCII

WEP Weaknesses:

IV Collision Attacks - Since their are only 16 Million different IVs they will repeat and the attacker will be able to recover the key.
Weak key Attack - Weak keys are created due to the RC4's key scheduling algorithm.
Reinjection Attack - An attacker using a packet injector (such as AirPCap Nx or Scapy) to inject packets forcing the use of addition IV's. This allows the IV's to be used sooner.
Bit Flipping Attack - Data Integrity is weak and the data can be altered.

Note: Current Free tools can crack WEP in as little as 5 minutes such airodump or aircrack.

MAC Filtering - Only allows specific MAC address access to the WLAN. MAC Address can be easily spoofed by various open source and free tools, and sometimes this can be changed within the device properties.

SSID Cloaking - Also called closed network. The SSID field in a beacon frame is simply empty/Null. This can be easily found by Layer 2 analyzers and sniffers such as NetStumbler/AirPCap/Omnipeek. This can also cause addition overhead to IT staff since the SSID needs to be configured on WLAN client. This feature may also cause issues with legacy WLAN cards.

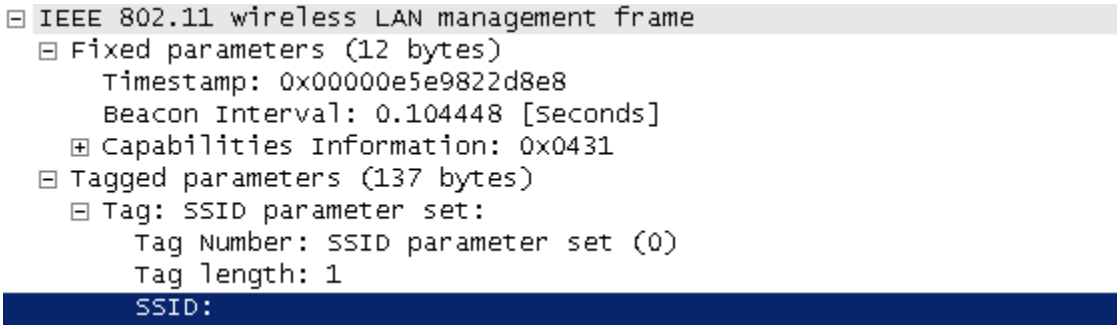

Image: Beacon Frame with no SSID information

Modern Security

4 Way handshake - The creation of dynamic encryption keys 5 separate keys are created in this process two master keys Group master keys (GMK) and the Pairwise Master Key (PMK). The keys are seeding to form the dynamic keys for encrypting the data. The final two keys are the pairwise transient key (PTK) and group temportal key (GTK) which are used to encrypt/decrypt unicast traffic.

RSN Robust Security Network - States 2 STA's must generate dynamic encryption keys through a *4-way handshake* this is referred to as an RSNA Robust Security Network Association. This generated encryption key is specific to the 2 WLAN radios.
RSN is also identified by a the *Information Element IE* field found within the beacon frame.

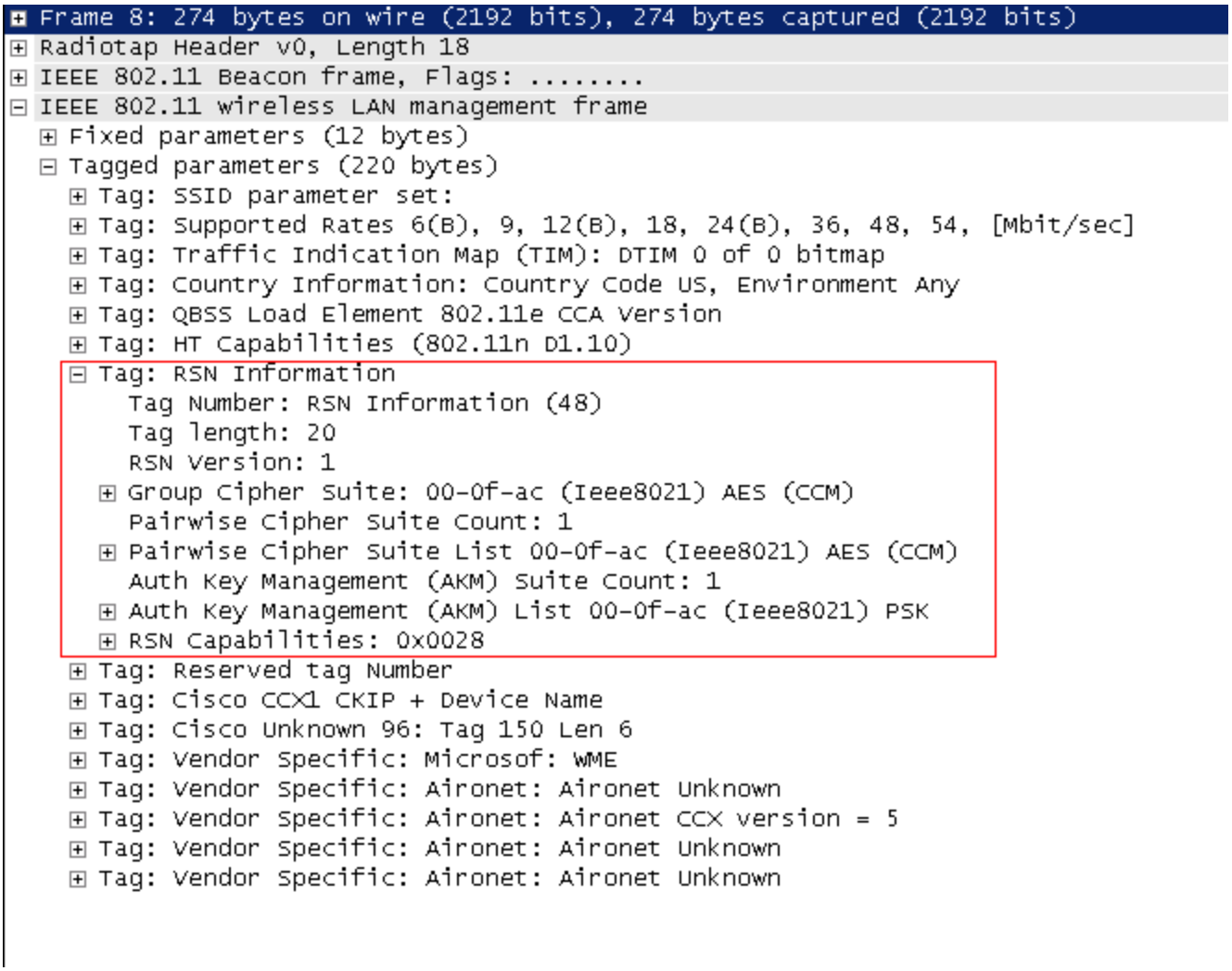

Image: RSN Information within a beacon frame

4865	35.395471	149 HonHaiPr_7d:7a:bd	Cisco_08:ec:30	EAPOL	149 Key
4863	35.393050	175 Cisco_08:ec:30	HonHaiPr_7d:7a:bd	EAPOL	175 Key
4861	35.391762	175 HonHaiPr_7d:7a:bd	Cisco_08:ec:30	EAPOL	175 Key
4859	35.354034	149 Cisco_08:ec:30	HonHaiPr_7d:7a:bd	EAPOL	149 Key

Image: You can see the client initiating the EAPOL (EAP Over LAN) transaction with the Cisco AP.

Passphrase based security

- Creates a 256 bit PSK to communicate with WLAN
- 8-53 ASCII characters can be used for the key or 64 Hex
- Longer the passphrase the more secure it is
- weak pass phrases can be easily compromised.

TKIP Temporal Key Integrity Protocol - Designed as a software upgrade from WEP. This was the foundation for the WPA certification from the Wi-Fi Alliance. EoL with 802.11i, however 802.11i is backward compatible with WPA
Enhancements in TKIP:

1. Use of RC4 stream cipher for backward compatibility with WEP.
2. RC4 is used with WEP Encryption, RC4 is not a weak algorithm it was just implemented poorly.
3. RC4 uses key strengths of 64 or 128 Bits. RC4 is also used in SSL connections.
4. Dynamic re-keying mechanism to change encryption and integrity keys. IV is mixed with the secret root key then sent to RC4
5. Per packet key mixing of the IV to separate weak keys.
6. Uses a 48 bit IV compared to the 24 bit used by WEP
7. 64 Bit MIC Message Integrity Check
8. Message Integrity Check/MIC Prevents data from being tampered with
    1. If MIC's do not match the data is assumed to have been altered and all clients will be DeAuthenticated and stopping new associations for 1 minute.
9. Sequence Counters to protect from replay attacks

The **802.11i** standard, now part of the 802.11-2007 standard, requires 802.1X/EAP in the enterprise and PSK (Pre-Shared Keys) for SOHO deployments. CCMP/AES is the required encryption method. TKIP/RC4 is optional. EAP is also a layer 2 protocol.

CCMP Counter mode with Cipher block Chaining Message authentication code Protocol - Mandatory in the 802.11i amendment, also part of WPA2, uses the AES algorithm. Wi-Fi uses 128 bit blocks.

1. AES has been cracked but requires extreme measures. Side Channel attacks.
2. AES/CCMP - requires more processor power and typically requires a hardware upgrade compared to a typical software upgrade for TKIP
3. AES Meets FIPS140-2 Complaint

802.11 Frames and Encryption

- Management frames are **not** encrypted.
- Control frames do not have a body and are **not** encrypted.
- Data frames - The MSDU inside the body is encrypted. This is a layer 2 encryption that protects information through layer 3 - 7.

```
⊞ Frame 724: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
⊞ Radiotap Header v0, Length 18
⊟ IEEE 802.11 Data, Flags: .p.....T
    Type/Subtype: Data (0x20)
  ⊞ Frame Control: 0x4108 (Normal)
    Duration: 44

    Source address: Aironet_
    Destination address: Cisco_ab
    Fragment number: 0
    Sequence number: 1478
  ⊞ TKIP parameters
⊟ Data (60 bytes)
    Data: bc3f2e8b8b3683f222fa3120596a20f4e0a80ddb9a9c3568...
    [Length: 60]
```

Image: You can see the TKIP Parameters, and the data is in cipher text.

802.1X Authentication (framework) - Initially used for wired port based authentication, also now used with WLANs.
Involves

- Supplicant - Client device trying to connect
- Authenticator - middle man devices (AP/Switch/WLC) that passes on authentication information to authentication serve. This device does not allow network access until the the authentication is successful.
- Authentication Server - Receives information from authenticator and verifies credentials using a user DB (internal or external)

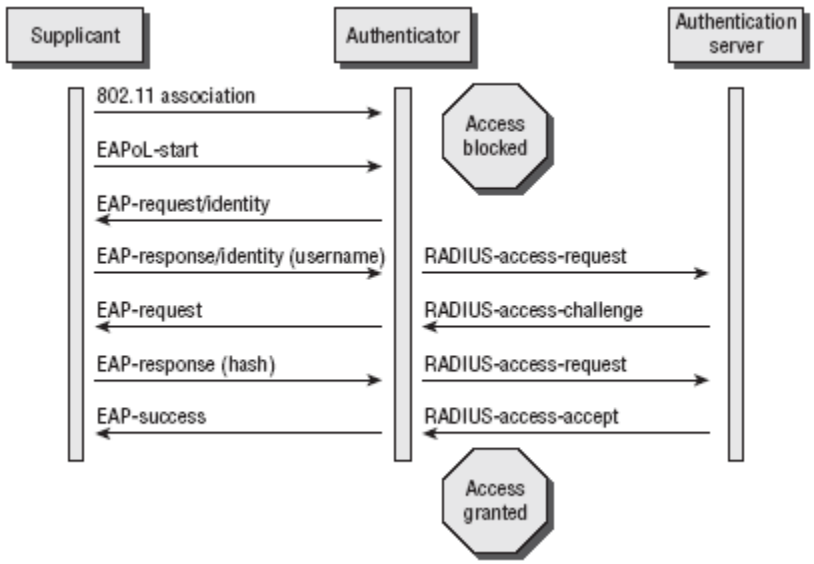

Image: 802.1X authentication process.

EAP Extensible Authentication Protocol - Authentication process used with 802.1X
Common EAP types:

- EAP-TLS - Requires PKI on client and server. Most secure.
- EAP-TTLS - TLS Tunnel, Requires server side certificate.
- PEAP - Protected EAP. Microsoft Supported by MS-CHAP Only server side certificate.
- EAP-FAST - From Cisco uses PAC Protected Access Control no PKI required. Uses MS-CHAPv2
- LEAP - Uses with MS-CHAPv2 supported with MS passwords and certificates.

More information can be found
here: http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

Wi-Fi Protected Setup WPS - Another *standard* created by the Wi-Fi Alliance for simple secure SOHO WLAN deployments. This may not be supported on older harder since this standard has only been around since 2007.

- Pin Method - A pin number stamped on the AP needs to be entered on the client when trying to associated to the access point.
- PBC - Push Button Connection involves pressing a physical button when connecting the access point

RBAC - Provides restricted access to authorized users. May restrict bandwidth usage and port access, or even administrative access to IT personnel.

Secure Device Management - It is important to remember to manage and configure devices using a secure protocols, this ensures the actual network devices cannot be tampered with.
http://itnetworkingpros.wordpress.com/2011/03/10/secure-cisco-device-management/

Virtual Private Network /VPN - Private communication from a device over the internet to a home/central office. Operate at Layer 3 (the network layer), still used for secure connectivity through public hotspots.
Before 802.11i when Layer2 WLAN security was weak VPN was the primary way of securing data over the WLAN. VPN's consist of 2 part Tunneling and Encryption (DES, 3DES, AES, RC4, MD5, SHA1), a VPN will encapsulate one IP frame within another IP frame
2 Two common VPN protocols PPTP & IPSec - Provide user authentication, data encryption, and integrity.

1. PPTP Point-to-Point Tunneling Protocol - Created by Microsoft, Built into windows and was easy to configuration, encryption was provided by MPPE/RC4 Microsoft Point-to-Point Encryption. Utilizes MS-CHAPv2, which is susceptible to dictionary attacks.

2. L2TP Layer 2 Tunneling Protocol - Based off Cisco L2F (Layer 2 Forwarding) and Microsoft's PPTP.Requires IPSec (utilizing IKE) for encryption and is more secure then PPTP
3. WebVPN - SSL/TLS Connections via web browsers.

Network Security Analysis, Performance Analysis, and troubleshooting

Common threats to WLAN's

- Eavesdropping
- RF DoS
- MAC Spoofing
- Hijacking
- Man in the middle attacks
- P2P attacks
- Encryption cracking

Wi-Fi Alliance certification:

WPA-Personal	Passphrase	TKIP/RC4
WPA-Enterprise	802.1X/EAP	TKIP/RC4
WPA2-Personal	Passhprase	CCMP/AES or TKIP/RC4
WPA2-Enterprise	802.1X/EAP	CCMP/AES or TKIP/RC4

Wireless Intrusion Detection Systems WIDS - Works at layers 1 and 2 to watch for possible attacks (such as DoS and Wi-Fi Hijacking). A typical WIDS deployment involves a server, management console, and sensors. The sensors do not provide WLAN access to clients but instead just watch the RF medium.

Signatures

Precedence	Name	Frame Type	Action	State	Description
1	Bcast deauth	Managemen	Report	Enabled	Broadcast Deauthentication Frame
2	NULL probe resp 1	Managemen	Report	Enabled	NULL Probe Response - Zero length SSID element
3	NULL probe resp 2	Managemen	Report	Enabled	NULL Probe Response - No SSID element
4	Assoc flood	Managemen	Report	Enabled	Association Request flood
5	Reassoc flood	Managemen	Report	Enabled	Reassociation Request flood
6	Broadcast Probe floo	Managemen	Report	Enabled	Broadcast Probe Request flood
7	Disassoc flood	Managemen	Report	Enabled	Disassociation flood
8	Deauth flood	Managemen	Report	Enabled	Deauthentication flood
9	Res mgmt 6 & 7	Managemen	Report	Enabled	Reserved management sub-types 6 and 7
10	Res mgmt D	Managemen	Report	Enabled	Reserved management sub-type D
11	Res mgmt E & F	Managemen	Report	Enabled	Reserved management sub-types E and F
12	EAPOL flood	Data	Report	Enabled	EAPOL Flood Attack
13	NetStumbler 3.2.0	Data	Report	Enabled	NetStumbler 3.2.0
14	NetStumbler 3.2.3	Data	Report	Enabled	NetStumbler 3.2.3
15	NetStumbler 3.3.0	Data	Report	Enabled	NetStumbler 3.3.0
16	NetStumbler generic	Data	Report	Enabled	NetStumbler
17	Wellenreiter	Managemen	Report	Enabled	Wellenreiter

Image: Common attacks a WIPS can protect from.

Deployment Methods:

1. Overlay - Deployed over existing WLAN
2. Integrated - Part of the WLC/LWAP Model. The LWAPs are able to act like sensors.
3. Integration Enabled - The Existing hardware is capable of being integrated with the management interface of WIDS server software.

Wireless Intrusion Prevention Systems WIPS - Similar to a WIDS except the WIPS is capable of mitigating attacks. WIPS classifies APs in one of four ways:

1. Infrastructure - A legitimate network device.
2. Unknown - A detected device that has not yet been classified.
3. Known - A detected device that has been classified.
4. Rouge - A device that is not authorized or is seen to interfere with the WLAN

Many WIPS mitigate attacks differently, most commonly the AP will spoof the MAC address of the rouge AP and send out DeAuth frames. Some vendors offer a mobile WIPS, which is simply a laptop program that can find rouge devices and perform protocol analysis.

```
⊞ Frame 3979: 44 bytes on wire (352 bits), 44 bytes captured (352 bits)
⊞ Radiotap Header v0, Length 18
⊟ IEEE 802.11 Deauthentication, Flags: ....R...
    Type/Subtype: Deauthentication (0x0c)
  ⊞ Frame Control: 0x08C0 (Normal)
    Duration: 127
    Destination address: HewlettP_3b:25:d6 (d4:85:64:3b:25:d6)
    Source address: 56:54:9b:ba:d9:d4 (56:54:9b:ba:d9:d4)
    BSS Id: 56:54:9b:ba:d9:d4 (56:54:9b:ba:d9:d4)
    Fragment number: 0
    Sequence number: 1983
⊞ IEEE 802.11 wireless LAN management frame
```

Image: DeAuth frame sent spoofed from a Cisco AP to an Ad Hoc connection.

Rouge Access Points - These devices can be setup by anyone (typically by an end user). What makes these devices dangerous is the fact they can provide unauthorized access to the wired network (and network resources).

Ad Hoc Networks - Known as an IBSS Independent Basic Service Set. Ad Hoc networks allow computers to connect directly to each other without the use of an access point allowing users to transfer and share files on the fly. Most WLANs have the ability to block peer to peer connects using a technology called *Public Secure Packet Forwarding* (PSPF)

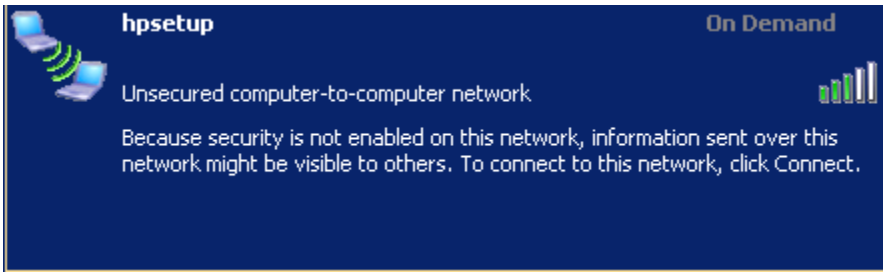

Image: An Ad Hoc network from Windows Zero Config

Wireless Hijacking - Malicious users can install access point software to imitate an access point that will allow unsuspecting users to connect to the malicious user allow all the client to be capture and possibly tampered with.

DoS Attacks - Intentional attacks can be performed with Wi-Fi jamming devices. Nothing can be done against these kind of attacks. These can also be unintentional (by BlueTooth devices, cordless phones, microwaves

Spectrum Analysis:
Protocol Analysis:

Network Security Policies

Recommendations:
Remote Access Policy - For users that travel to remote off-site locations with laptops. Typically mandate the use of a IPSec VPN, AV, and Firewall.
Rouge AP Policy - States End-users should not use their own type of WLAN AP/Router devices
Ad Hoc Policy - Prevent users from initiating peer to peer wireless connections
WLAN Proper Use Policy - Outline how the WLAN should used by the end users
IDS Policy - States how to respond to WIDS/WIPS events.

General Security Policy - Define how to deal with rouge devices.
Statement of authority - Defines the policy and that it is backed by management
Application audience - Defines who must abide by the policy.
Violation reporting procedures - Defines how the policy will be enforced.
Risk Assessment and threat analysis - What may happen if a successful compromise occurs.
Security Auditing - Define auditing procedures.

Functional Security Policy - Defines the technical aspects of WLAN security. Defines the following:
Policy Essentials - Password policies, training, and proper WLAN usage.
Baseline practices - Configuration checklists.
Design and implementation - Defines the Encryption, encryption, segmentation policies.
Monitor and response - Defines IDS procedures and appropriate responses.

Captive Portal - SSL Web page that can require users to sign in and acknowledge a UAP. Once authenticated to captive Internet traffic flows. Found at Hot spots, hotels, airports, etc.

Legislative Compliances

HIPPA - Found in the health care field to protect the medical records of patients.

1. HIPAA Title I - Protects health insurance of someone who loses/changes job
2. HIPAA Title II - Establishes mandatory regulations for health care providers for securing computer data/information.

Sarbanes-Oxley - For financial institutes, dictates accounting and auditing.

Graham-Leach-Bhiley - Also for financial institutes to protect credit card, social security numbers, names, addresses and so forth. (Personal information)

PCI Compliance - Payment Card Industry for protecting credit card information
6 Requirements:

1. Build and maintain and secure network/Firewall.
2. Protect card holder data/Encryption
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitors and test networks
6. Maintain an information security policy