A Brief Survey On Wi-Fi Security

What do we have in this article?

INTRODUCTION

Contradict to the wired network, to make a wireless network secure is more difficult task. As will be discussed in the following sections, wireless technologies that bound to the standards which obsolete very fast and this also applies to the new rapid technology adoption. Another issue is the technology, standard and protocol development direction. Several wireless technologies developed independently with their own working group. In the co-exist environment, wireless security will complement and/or utilize the wired security technologies. In this case, vulnerabilities that exist in the wireless network, of course will jeopardize the established wired network. In this paper we will try to survey main implementation adopted by the wireless communication in order to make it secure. The strength and weakness will also be discussed in order to find the good balance in the real deployment. Finally the most secure scheme will be revealed.

2.1 CURRENT WIRELESS TECHNOLOGY

In the smallest range, we have a Bluetooth [2] example. It is a wireless network technology that has its own development direction other than the 802.11 family. Bluetooth supports a very short range in the region of 10 meters and relatively low bandwidth roughly around 1-3 Mbps. It is designed for low-power network devices like portable or handheld gadgets. Nowadays it is a normal feature for handheld devices which include notebook to have a built-in Bluetooth support.
In the medium range, the popularity of the wireless Fidelity (Wi-Fi) has developed the market for unregulated band or unlicensed client-access radios in a wide variety of applications. This technology is one of the last-mile wireless broadband and narrowband services. However, the current main type of the last-mile deployment is the large-area coverage normally called hot-spots. Wireless last-mile coverage is based on IEEE 802.11 standard [1] which uses the high-gain antennas, while hot spots use the modified version of the IEEE 802.11 apparatus which is called a mesh operation. Wi-Fi resembles the wireless local area network.
In 2005, for a wider range, the Worldwide Interoperability for Microwave Access (WiMAX) certified the IEEE 802.16-2004 standard [3] for fixed-position radios. WiMAX will provide the point-to-multi-point and point-to-point wireless broadband devices in both the regulated and unregulated bands. Then, the IEEE 802.16e standard [4] for portable devices has been approved in 2006, regulating the client radio frequencies in licensed and unlicensed bands. This promising technology will provide service providers an additional layer of services benefits.
WiMAX actually resembles a wireless metropolitan-area network segment which provides broadband wireless connectivity to portable, fixed and roaming users. Its designed target is for long-range networking as opposed to local area wireless networking and the research in this field still continues. It is developed independently from Wi-Fi, providing additional distance up to 50 kilometers with total data rates can be up to 75 Mbps, providing sufficient bandwidth to support hundreds concurrent users using a single radio base station. WiMAX has been said to

provide many wireless access advantageous to the remote and isolated area.

2.2 WIRELESS DEPLOYMENTS

The current trends show that the price of the wireless gadgets keep decreasing with the every advent of new technologies. The affordability makes wireless as a popular and practical alternative. Wireless deployment can be as simple as connecting two adjacent computers wirelessly. More complicated deployment will have hundreds or thousands of devices with centralized servers and distributed APs. Basically, wireless network can be structured into two different modes, based on the coverage size needed. These two modes are [5]:

1. **Ad-hoc mode**: This mode is a temporary, as is basis type. There is no AP in this mode and the devices are directly sharing their resources when in the range. The shared resources available as long as the devices are running. Bluetooth is one of the examples.
2. **Infrastructure**: This mode resembles the wired network. In this mode the AP is used for the wireless devices to communicate each other and it is dominant mode that can be found in residential, corporate building, university campus and plants. The wireless devices can keep connecting as long as they are directly connected to and within the wireless network coverage. Wireless security elements could be enforced on all the wireless devices and users such as through policies, authentication, encryption and many more.

Currently the wireless deployment still dominated in the last mile coverage. This is because of the unregulated frequency availability which lowered the cost of deployment and maintenance. Furthermore, the mass introduction of the cheaper consumer wireless devices makes it an attractive offer. Other than providing an alternative mode of communication medium, the main reason of the adoption is based on the mobility nature of the devices. However, in term of deployments, we can categorize them into four main segments of utilization as listed below.

1. The Wireless Personal area networks (WPAN – 802.16).
2. The Wireless Local area networks (WLAN).
3. The Wireless Metropolitan area networks (WMAN).
4. The Wireless Wide area networks (WWAN).

2.2.1 WIRELESS PERSONAL AREA NETWORK

WPAN can cover a range up to 30 feet or around 10m. Although this seems absurdly small, but this range allows wireless devices to be connected wirelessly to other nearby wireless devices [6]. WPAN provides a very short distant and for small group or community that can share resources wirelessly. Bluetooth which based on the IEEE 802.15.1 standard [7] for example, is mostly used for short range computing and communication peripherals, such as a PDA to a computer or a hand phones. It is normal that the new Bluetooth version can provide data rate performance up to 1Mbps. Another example is the ultra-wide band (UWB) which is designed for multimedia services transmission. The related standard for UWB is IEEE 802.15.3 which can support a data rate up to 400Mbps which equivalent to the DVD video quality standard. In this case the WPAN becomes a high-speed personnel area network. Other usage includes the ad-hoc network where a local area network in which computers and network devices are in close proximity to others in similar subnet. These devices are connected temporarily and as is basis. The receiver and transmitter used are built-in type devices.
However there is no independent pre-existing network for WPAN. All the devices in WPAN communicate based on the ad-hoc network, can be connected when within the range and disconnected when out of range. Better built-in devices can be designed in the future to provide non ad-hoc network. Other similar scenario can be found when using the Infrared (IR) to exchange data between laptops. The nature of wireless devices discovering each other and in many situation it is automatic, is a very big issue in wireless security field.

2.2.2 WIRELESS LOCAL AREA NETWORK

Similar to its counterpart, LAN in fixed line, WLANs can provide coverage larger than WPAN but still limited. Typical coverage areas can be found in a campus, a corporate building, a hospital, or a manufacturing plant [8]. Take note that, the traditional wired LAN can be expanded using wireless through the wireless Access Points (APs) for example, creating a heterogeneous network. The standards-based WLAN typically serve more users and applications compared to WPAN and can serve a distance up to 10 meters or more although this depend on the physical environment such as walls and frequency reflectors. The legacy and new wireless standards that have been released associated with WLAN are included the following three major revisions.

1. 802.11n - bandwidth speeds up to 600 Mbps (2009).
2. 802.11g - bandwidth speeds up to 54 Mbps.
3. 802.11b - bandwidth speeds up to 11 Mbps.
4. 802.11a - bandwidth speeds up to 54 Mbps.

On the service provider part which normally called Wireless Internet Service Providers (WISPs) usually use the existing Wi-Fi mesh topologies or the directional antennas for better signal and larger coverage. For example those deployments can increase the performance beyond the 54Mbps with 10 kilometers in range while still obeying the 802.11 standard. The increased range creates the WLAN and WMAN segments as shown in Figure 1. However there are many more variables such as the APs to user's distance, the number of users and topologies which actually define the WLAN and WWAN.

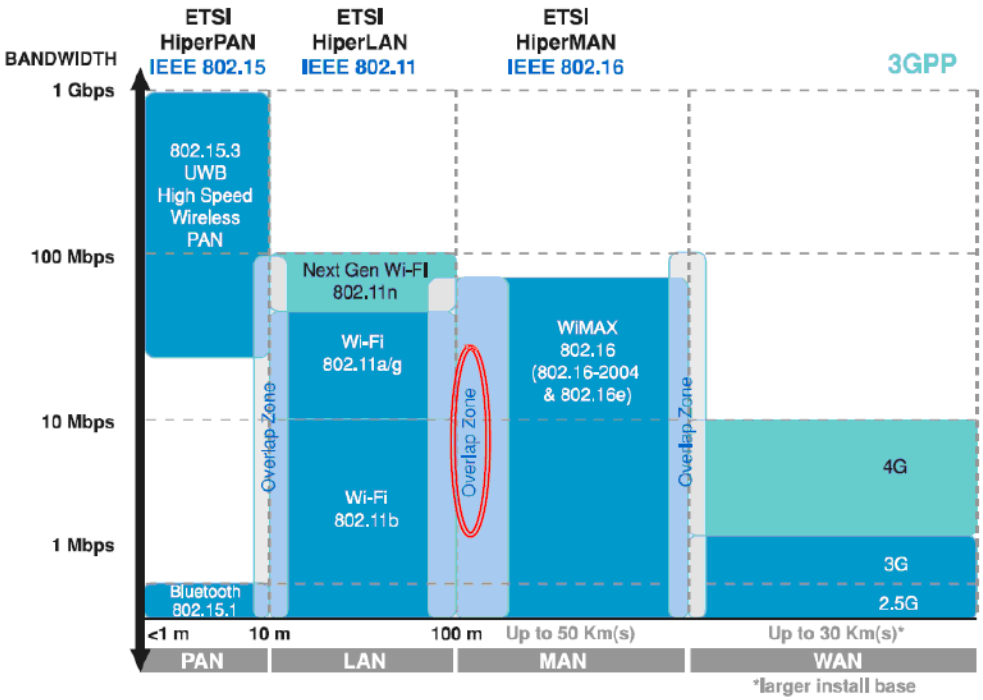

Figure 1: Wireless technologies target segments [12]

2.2.3 WIRELESS METROPOLITAN AREA NETWORK AND WIRELESS WIDE AREA NETWORK

The WMAN is the third usage segment shown in Figure 2. The WLANs collection makes the WMAN and the range can be up to 50 km. The implementation examples in this segment include the WiMAX, DSL/ADSL and DOCSIS legacy coppered wired technologies.

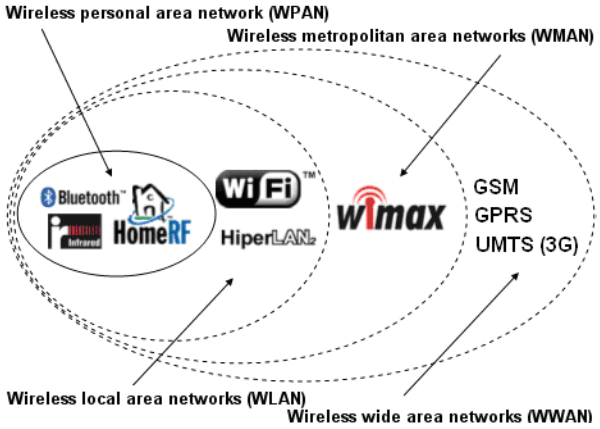

Figure 2: Wireless networks categories

The fourth usage segment shown in Figure 2 is the WWAN. WWAN aggregates WMANs and the range can cover the area up to 50 km. Compared to the previous wireless technology, this is a large area coverage which makes the backhaul or core network possible. In order to cater for the big amount of traffic, WWAN still utilizes various type of existing technology such as fiber optic links and terrestrial microwaves as a complement which normally acts as the backhaul for inter-WWAN connections. Depending on the type of traffic (data, voice or video), the performance can goes up to 10Gbps.

There must be very compelling reasons for deploying wireless communication in all the segment usage because the traditional wired communication already existed long time ago. In the WPAN and WLAN, the main reason of deployment is the mobility while in the WMAN and WWAN it is more on the cost per user, for example, deployment in remote area with less user population. In this case there should be no landline and Radio Base Station (RBS). However the real requirements for each segment are based on a variety of variables as listed below:

1. The distance and power of the signal.
2. The topology including the user location.
3. The bandwidth needs.
4. The services offered.
5. The security features.

Figure 1 also shows the wireless standards, standards bodies and their features such as distance and bandwidth which mapped to the four

usage segments previously explained. Regarding the standard, there are three main bodies involved in wireless technology as listed below:

1. European Telecommunications Standards Institute (ETSI) [9]
2. Institute of Electrical and Electronics Engineers (IEEE) [10]
3. Third-Generation Partnership Project (3GPP) [11]

The IEEE and ETSI standards are interoperable and concentrate mainly on wireless packet-based networking. However, ESTI is concentrated more on the technology and standard for the European countries. The 3GPP standard focuses on cellular and third-generation mobile systems and very apparent in the mobile sectors.

2.3 WIRELESS PROTOCOLS AND CHARACTERISTICS

This section describes the fundamental of the wireless technology protocols and the basic characteristics. It is beneficial to know the protocols and their respective features before discussing and understanding the security aspects. Table 1 summarizes the main protocols used in wireless communication. There are other standards such as recommendation and management in the 802.11 family and implementation guide, for example the 802.11i which is used for security [1].

Table 1: Established and obsolete IEEE 802.11 wireless protocol summary

Protocol	Release Year	Max. Data (Bit) Rate (Mbps)	Frequency (GHz)	Signal Modulation	Indoor Radius, (estimate) m
802.11n	2009 (expected)	600	2.4/5	OFDM	70
802.11y (US only)	2008	54	3.7	OFDM	50
802.11g	2003	54	2.4	OFDM	38
802.11b	1999	11	2.4	HR/DSSS	38
802.11a	1999	54	5	OFDM	35
802.11 legacy	1997	2	2.4	FHSS or DSSS	20

The OFDM technology utilizes the sub-carrier optimization, which users are assigned small sub-carriers based on radio frequency conditions. The orthogonal means the divided carrier's frequencies are chosen so that the peak of one frequency matches with the nulls of the bordering frequency. Table 2 provides the characteristics for the wireless protocols listed in the previous Table.

Table 2: IEEE 802.11 wireless protocol characteristics

Protocol	Description
802.11n	1. Designed to replace the older 802.11g, 802.11b and 802.11a. It is Wi-Fi standards for local area networking (LAN). 2. Builds on the previous 802.11 standards by adding multiple-input multiple-output (MIMO). 3. The OFDM version using Multiple-Input/Multiple-Output (MIMO) and Channel Bonding (CB). 4. Projected IEEE ratification in second quarter 2008; however, pre-11n Access Points (AP) and wireless adapters already available and implemented by vendors. 5. Almost 70 products in 2007 certified to comply with the Draft 2.0. 6. Data rates: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps with varying modulation types. 7. Contains 3 non-overlapping channels that used in Industrial, Scientific, Medical (ISM) frequency band at 2.4 GHz when CB is not being utilized and 2 when CB is employed. 8. While in 5 GHz frequency band with or without CB, contains 12 non-overlapping Unlicensed National Information Infrastructure (UNII) channels.
802.11g	1. Data rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps with varying modulation types and can be reverted to 1, 2, 5.5, and 11 Mbps using DSSS and CCK. 2. Fully backwards compatible with 802.11b hardware. 3. OFDM with 52 sub-carrier channels and backwards compatible with 802.11b using DSSS and CCK. 4. Contains 3 non-overlapping channels in ISM frequency band at 2.4 GHz. 5. However 802.11g suffers from the same interference as 802.11b.
802.11b	1. Data rates: 1, 2, 5.5 and 11 Mbps with varying modulation types. 2. It is a HR/DSSS and technically uses Complementary Code Keying (CCK) as its modulation technique. 3. Contains 3 non-overlapping channels in ISM frequency band at 2.4 GHz. 4. However devices suffer interference from other products operating in the 2.4 GHz band range such as Bluetooth devices, microwave ovens and cordless telephones.
802.11a	1. Uses the same core protocol as the original standard. 2. Data rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps with varying modulation types and based on the OFDM with 52 sub-carrier channels. 3. Contains 12 non-overlapping UNII channels in 5 GHz frequency band. 4. Not extensively used because the less-expensive 802.11b was already widely adopted. 5. Worse than but less expensive than 802.11g products and backwards-compatible with 802.11b, the 802.11a.
802.11 legacy	1. The original version of the standard IEEE 802.11. 2. Two raw data rates of 1 and 2 Mbps and based on the FHSS or DSSS.

	3. Contains 3 non-overlapping channels in ISM frequency band at 2.4 GHz. 4. Originally defined as Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) that used in Ethernet. 5. Currently superseded and popularized by 802.11b/g/n.
802.11i	1. Designed to provide secured communication of wireless LAN as defined by all the IEEE 802.11X specifications. 2. Not part of the 802.11 standard. 3. Enhances the WEP (refer to WEP section for details). 4. Based on the Wi-Fi Protected Access (WPA) (refer to WPA2 section for details).

The Table 3 summarizes the key characteristics of 802.11 wireless LANs in general.

Table 3: General characteristics of 802.11

Characteristic	Description
Data and Network Security	Using the RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited key management.
Operating Range Frequency Band	Estimated up to 150 feet indoors and 1500 feet outdoors. More feet using WiMAX. Utilize 2.4 GHz (ISM band) and 5 GHz.
Physical Layer Data Rates	Deploying DSSS, FHSS, OFDM, and Infrared. Starting from 1Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps (11b), 54 Mbps (11a and 11g) and 600 Mbps (11n).
Positive Aspects	Provide Ethernet speeds without wires; many different products from many different companies. Wireless devices keep decreasing from time to time.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

As an example, Table 4 summarizes the 802.11n wireless protocol operation modes and this protocol supposed to be the leading in the current and future wireless technology adoption. The Tx stands for the transmitter and Rx is receiver.

Table 4: 802.11 wireless protocol operation modes example

Mode	Max. Rate (Mbps)	Antenna Tx/Rx Arrangements
2x3 40MHz	300	2 Tx, 3 Rx
2x2 40MHz	270	2 Tx, 2 Rx
2x3 20MHz	144.44	2 Tx, 3 Rx
2x2 20MHz	130	2 Tx, 2 Rx
a/b/g legacy with Antenna Diversity and CB	121.5	1 Tx, 1 Rx

3.0 THE SECURITY ASPECTS

3.1 WIRELESS SECURITY ASPECT: AN OVERVIEW

This part will discuss the built-in 802.11 security features. It provides an overview of the typical security features to better illustrate its limitations and strength. By considering the current technology used in wireless, not much improvement has been done in the security aspect. The nature of 802.11 based wireless LANs which broadcast RF data for the client stations to receive is not like its counterpart in wired Ethernet. Without any security implementation, any client in the signal range can receive the signal. Of course the a/b/g/n of the 802.11 standard need to be revised or enhanced in order to resolve the wireless security complexity issues. The 802.11 family has been scrutinized for their flaws and exposed by researchers for example in the message-integrity mechanisms, authentication process and data-privacy that defined in the specification. The real exploit example and in what may be considered the biggest exploit that happened in the TJX Companies Inc.'s computer network that exposed at least 45.7 million credit and debit card holders to identity theft by exploiting the Wi-Fi weaknesses at a Marshalls clothing store [13].
The National Institute of Standards and Technology (NIST) prepared a report [14] that gives a recommendation to the US government not to use wireless LANs except in special cases. NIST also advises placing LAN access points in physically protected areas and suggests to use a virtual private network (VPN) for all the clients and gateways. Wi-Fi networks that are not encrypted can be sniffed or intercepted during the transmission over the network and the data can be read and collected for bad use. In the sections that follow, we will explore what has been done to and achieved in the wireless security in finding new method of protections. As general information, there are three basic general security goals defined by IEEE mainly for the WLAN environment use as listed below. This is normally known as CIA.

1. **Confidentiality** - Confidentiality or privacy services developed in order to provide privacy as in a wired network. The intention was to prevent data from eavesdropping activity. This service, in general, only allows authorized persons to view the data.
2. **Integrity** - This service developed to ensure that messages are not modified or tampered during the data transmission between the access point and wireless clients in an active attack. This service will ensure the data coming into or exiting the network is trustworthy.
3. **Authentication** - This service provide identity verification of the communicating client stations. The client stations that cannot authenticate themselves properly will be denied the access. In simple words, only the authorized persons are permitted to gain access to the network. The following Figure shows the authentication techniques used in 802.11 in general.

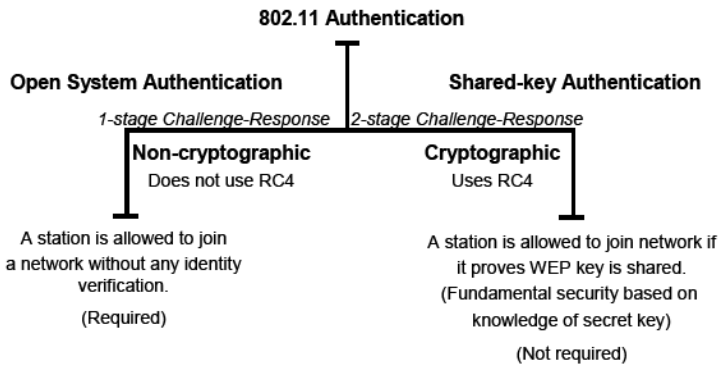

Figure 3: Taxonomy of 802.11 authentication techniques

3.1.1 MAC ADDRESS FILTERING

As implemented by a firewall and router for Access Control List (ACL), Media Access Control (MAC) address filtering is a way to protect the communication through the air, particularly beyond the 802.11b standards. Every network interface card (NIC) has a 12 digit hexadecimal address number that is uniquely assigned to every NIC in the world and it is called a MAC or physical address. An access policy of the AP which permitting only those MAC addresses of the authorized devices can be created because every NIC card has a unique MAC address. The unauthorized user can be easily blocked and authorized users can be forced to obey the refined access policies. However, MAC address filtering also has the following weaknesses:

1. MAC address can be changed or spoofed, so an attacker will use a wireless sniffer to fingerprint the MAC address range and use the MAC to 'impersonate' the original MAC.
2. There should be a database of the MAC address of every wireless device in the network and combining with the access level, this might be a problem when we have hundreds or thousands of MAC address in the network.

More information regarding WEP weakness can be found in [15], [16].

3.1.2 WIRED EQUIVALENT PRIVACY (WEP)

In order to provide a practical secure environment, IEEE 802.11 specification has identified and introduced several services that can be implemented. WEP originally designed to protect data at the link-level for the period of the wireless transmission between AP and clients. WEP is stand for Wired Equivalent Privacy and was originally designed as an equivalent protection to a wired network. However, there are many WEP misconceptions, for example, WEP is not an encryption algorithm, and it would never protect your data from attackers who wants to find out your data during the transmission. There is no end-to-end protection, but only for the wireless portion of the connection as depicted in the following Figure.

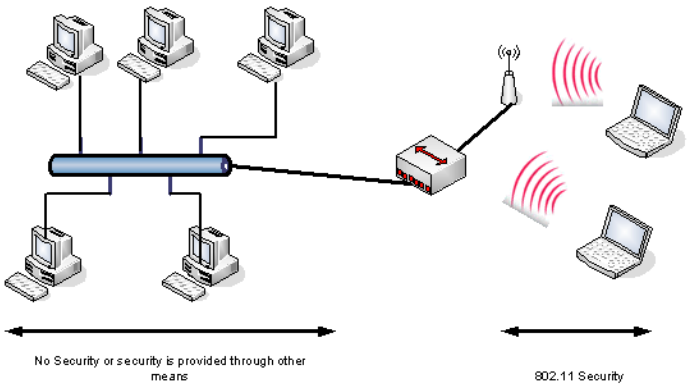

Figure 4: A typical 802.11 wireless network security

WEP is designed to create a natural security in the wireless transmission as existed in the wired transmission. It tries to make your data as secure as it would be on unencrypted, wired Ethernet network. WEP can be configured in the following 3 ways:

1. 128 bit encryption.
2. 40 bit encryption.
3. No encryption mode.

WEP is an optional, negotiated and agreed-upon encryptions standard that is must be pre-configured before a user connects to the wireless AP. After it was configured on both sides, all the communications through the air are encrypted, providing a secure transmission. User who

wants to connect to the AP using WEP, their PC must be WEP enabled and have a password or key which is shared among the end users. In a simple WEP operation, each packet is encrypted from one access point to a client device. Each packet's data and their respective secret 40-bit number are encrypted and then both will go through the RC4 encryption algorithm. The same 40 bit number will be used to decrypt the received data with the RC4 algorithm in the reverse manner, making the data transmission possible for the client device. The 128 encryption key bit is also supported and with known misconceptions and flaws with WEP, it is recommended to use the 128 bit encryption as a better solution.

3.1.3 WEP LIMITATION AND WEAKNESS

In order to provide the encryption services in protecting the wireless traffic, the WEP key is combined with the 24 bit number (Initialization Vector, or IV). The IV is randomly generated and is combined with either the 40 bit or 104 bit WEP key in order to give an encryption strength and protection of full 128 bits. However, there are many security vulnerabilities found as listed in the following Table:

Table 5: Known WEP vulnerabilities

Vulnerability	Description
A known plaintext attack (by Berkeley team , [17], [18])	1. A lots of known plaintext attacks in IP traffic such as ICMP, ARP and TCP ACK. 2. Can launch pings from Internet through AP to probing attacker. 3. Enables recovery of key stream of length x for a given IV. 4. Can forge packets of size y by reusing IV in absence of a keyed MIC.
The IV key re-use issue (by Berkeley team , [17], [18]) An authentication forging (by Berkeley team)	1. Key re-use is made possible by the small IV range and there is no protection for IV replay. 2. Enables statistical attack against cipher texts with replayed IVs. 1. WEP v1.0 encrypts challenge using IV chosen by client. 2. Recovery of key stream for a given IV enables the re-use of that IV for forging WEP v1.0 authentication. 3. Does not provide key, so can't join LAN.
A partial known plaintext (by Berkeley team , [17])	1. May only know a portion of the plaintext such as IP header. 2. Possible to recover X octets of the keystream, X < x. 3. Can lengthen keystream from X to x through repeated snooping. 4. Possible to spin bits in realtime by modifying the CRC32 and then divert traffic to attacker. Enabled by the linearity of CRC32 and there is no keyed MIC.
A dictionary brute force attack DoS attack	1. Possible where WEP keys derived from passwords. 1. There is no authentication for disassociate messages and reassociate messages.
A realtime decryption (by Berkeley team and [17])	1. Repeated IV re-use, probing enables building of a dictionary of IVs, key streams. 2. Enables decryption of traffic in realtime. 3. Possible to store dictionary due to the small IV size. Just need 1500 octets of key stream for each IV that is 2^{24} * 1500 octets = 24 GB.

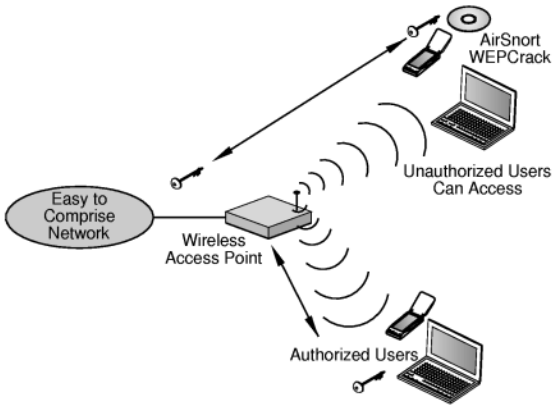

Figure 5: WEP standard for securing wireless networks

3.1.4 WEP2

The WEP version 2 increases the size of IV space to 128 bits. In addition, the key may be changed periodically via IEEE 802.11x re-authentication to avoid the staleness. WEP uses the Kerberos for authentication within IEEE 802.1X. However there are still no keyed message integrity and countermeasure (MIC), no authentication for re-associate and disassociate and no IV replay protection. Hence the WEP2 not considerably more secure than WEPv1.0 when considering the small IV size. Furthermore, without the keyed MIC, WEP2 still not efficient. In WEP2 the denial of service (DoS) attacks is still not addressed hence WEP2 should not be treated as a major security enhancement compared to WEP 1.0. The following Table summarizes the WEP2 vulnerabilities.

Table 6: Known WEP2 vulnerabilities

Vulnerability	Description
The authentication forging attack	1. Since intentional IV replay still possible, the larger IV does not affect.

The dictionary attack	1. New vulnerabilities introduced by mandatory KerberosV authentication. Newer Kerberos version should overcome this issue.
The realtime decryption	1. Should be greatly more difficult due to larger IV: 2^{128} * 1500 octets = 5.1E32 GB.
The IV key re-use issue	1. With larger IV, re-key support makes unintentional re-use much less likely however without IV replay protection, intentional reuse still possible.
The known/Partial plaintext attacks	1. The larger IV does not affect. 2. Probing the key stream extension still possible in absence of keyed MIC. 3. Still possible to recover key streams via ping from Internet. 4. Can still falsify packets by reusing IV and key stream. 5. Can still divert traffic in absence of non-linear, keyed MIC.
The KerberosV Dictionary Attack Vulnerabilities [19]	1. Password checkers not successful in considerably increasing the password entropy. 2. Structure of TGT (service name = krbtgt) enables verification of key guess by decrypting only 14 octets; similar issues with the PADATA. 3. The use of DES to encrypt TGT enables the use of parallel DES cracking techniques. 4. From 25,000 sample of TGTs, 2045 could be decrypted in two weeks using a cluster of 3 UltraSPARC-2 (200 MHz) and 5 UltraSPARC-1 (167 MHz) machines. 5. Today, less than 10 off-the-shelf PCs could accomplish the same thing in 1 day at lower cost.

3.1.5 Wi-Fi PROTECTED ACCESS (WPA)

In late 2002, a new standard called Wi-Fi Protected Access [20] has been created by Wi-Fi Alliance in the purpose to deal with the obvious flaws found in WEP. WPA combines two components:

1. The first component is called Temporal Key Integrity Protocol (TKIP). TKIP replaces WEP with a much stronger protocol. It provides data encryption improvements that include a key mixing function, a re-keying mechanism and a message integrity check. These components have been designed to rotate through keys fast enough before the encryption keys can be decoded by any sniffer program. Well, TKIP addresses all of WEP's known encryption vulnerabilities using these improvements. The IEEE new encryption standard called 802.11i (WPA2) is considered more vigorous and it is a replacement for TKIP.
2. The second component is the 802.1X security. This component addresses issue that related to the key management of the user authentication.

When 802.1X security and TKIP combined, a strong level of wireless security will be provided where a user must be authenticated before he is permitted an access to the network. In the deployment, WPA has two modes of operation:

1. Basic mode or WPA with pre-shared key (WPA-PSK)
2. WPA with centralized security management.

In the first mode normally setup for personal use such as for residential and Small Office Home Office (SOHO). The password used is shared. The second mode normally used for enterprise which suitable for medium to large environment. In this mode the 802.1X key and other back-end security infrastructure such as RADIUS server are needed. However WPA already has been analyzed for its known vulnerabilities [21], [22], [23]. In a simple situation, WPA not spared from DoS attack using forged IEEE 802.11 disassociation message and de-authentication message.

3.1.6 WPA2/802.11i/RSN

The WEP key could be derived by passively gathering particular frames from a WLAN as demonstrated by cryptanalysts Fluhrer, Mantin, and Shamir. This knowledge was found after WEP encryption was broken in August 2001. This idea generates the 802.11i. Until then, the working group began intensifying researches for more secure wireless encryption. The 802.11i is a two layer standard group which concentrates both on issues concerning 802.1x and network security, as well as a deeper look into a specific WEP security fix called Temporal Key Integrity (TKI). The 802.11i was approved in July, 2004, and uses the AES [24] encryption, instead of RC4 [25], which was used in WEP previously. However 802.11i also has security vulnerabilities, for example, can be found in [26], [27], [28]. The 802.11i contains a module called Robust Security Network (RSN), which the authentication and encryption algorithms will be dynamically negotiated for the communications between wireless and wireless clients AP. In this dynamic case, new algorithms can be added instantly if new attacks or threats are revealed.
RSN uses the 802.11x with AES and Extensible Authentication Protocol (EAP). A Counter Mode CBC MAC Protocol (CCMP) is term used to describe the security protocol that RSN builds on AES. Although 256 bits key length supported by AES, it is not compatible with the legacy hardware. However, Transitional Security Network or TSN was designed to solve this compatibility issue. Well, in order to enhance the wireless security, it look likes the implementation becomes more complex. Do the WPA2 secure enough? WPA2 (and WPA too) used with Pre Shared Key (PSK) mode have been tested vulnerable to brute force dictionary attack. The dictionary attack launched against the captured WPA2 traffic session to discover the PSK using for example, an open source tool [29]. The speed of recovery can be even faster using high processing power devices such as Field Programmable Gate Arrays (FPGAs) chip [30] and General Processor Units (GPUs) of the graphic board [31]. However, the operation mode that found vulnerable is the basic or WPA-PSK and not the enterprise.

3.1.7 EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

The 802.1X actually focusing on the security of the port level and this resolution was originally planned to standardize security on the wired network ports, but then found to be applicable to the wireless networking also. When using 802.1X, a device that requests access to the AP follow the below steps with the EAP:

1. Client will be requested an authentication information from APs.
2. The requested authentication then supplied by the user.
3. The supplied authentication information then forwarded by APs to RADIUS server for authentication and permission.
4. The client is allowed to connect and transmit data after got authorization from RADIUS server.

3.2 ENHANCING THE WIRELESS SECURITY

For the consumer domain, a recommended encryption is WPA2 (also called AES PreShared Key) meanwhile the WPA2 along with a radius server (RADIUS [32]) and the strongest EAP-TLS [33], should be used for enterprise. RADIUS stands for Remote Access Dialin User Service normally used in dial-up services, is a widely deployed protocol for network access that provides authentication, authorization and accounting (AAA or 3A). EAP [34] is the IETF standard for extensible authentication in network access. It is standardized for use within the Point-to-Point Protocol (PPP) (RFC 2284), wired IEEE 802 networks (IEEE 802.1X), and Virtual Private Networks (VPN) (L2TP/IPsec and a Pre-IKE Credential Provisioning Protocol – PIC). However, both EAP and RADIUS also have known vulnerabilities [35], [36]. Cisco produced its own EAP called LEAP (lightweight EAP) [37]. LEAP protocol is also vulnerable to dictionary attacks, and several LEAP cracking tools are now already available [38]. The four commonly used EAP methods in use today are:

1. The EAP–TLS
2. The EAP–TTLS
3. The EAP–MD5
4. The LEAP

There is some possible means of securing your wireless network beyond the previously discussed schemes. In many cases, the awareness of wireless network shortcomings has initiated the wireless LANs banning in some organizations. However, security aware institutions are strengthening their wireless network with a layered approach that may include the following items [39]:

1. Using 802.11X authentication and key management.
2. Choosing the available EAP and match it with your environment
3. The session to time out can be set periodically such as every 10 minutes or less.
4. The active SSID broadcasting can be stopped.
5. Implementing the physical and logical access point such as using biometric.
6. The broadcast keys can be rotated for every 10 minutes or less.
7. Implement the authentication and encryption.
8. Setup a virtual private network over wireless
9. Scanning the rogue access points for potential vulnerabilities.
10. The SSID may be changed and selecting a random SSID to avoid the fingerprinting the network structure.
11. Implement, enforce and monitor security policies.
12. Setting up proactive measures, real time system such as using Intrusion Detection System.
13. Making the wireless behind a protected zone such as behind the firewall and DMZ.
14. Adapt and adopt the latest software or firmware update.
15. Adapt and adopt new updated design and implementation.
16. Many more...

As shown in Figure 6 [40], those recommendations can be demonstrated by using a staged policy which start from identifying the vulnerabilities, do the assessment and then proceed from that point.

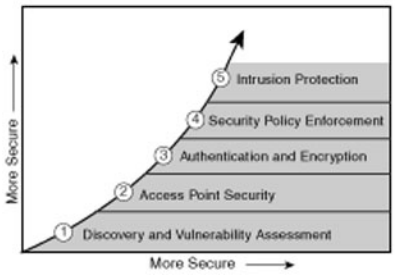

Figure 6: Securing a wireless network in stages

At the end only WPA2 is the winner though still not too resistant to the dictionary brute force attack particularly for WPA-PSK which will be even faster to be cracked by using custom made processor such as FGPA or GPU chips. The dictionary attack against WPA-PSK potential should be minimized by using relatively strong passwords and changing them periodically. The early schemes such as WEP, WEP2 and WPA 1.0 are no longer secure mainly if used by home user. Other better solution for the un-secure schemes is to combine them with the wired technologies such as DES/3DES and AES.
At the time this paper is written, WPA/WPA2 seems not vulnerable to the dictionary brute force attack at the enterprise level. Hence it should be suitable for enterprise deployment by combining with other wired technologies. Other existing wired technologies that have been adopted such as MAC filtering just acts as a complement to the wireless environment. It should be a normal situation for any current network system which consists of the wired and wireless portions with different schemes used for security purposes.

4.1 FUTURE WORK

The future work must be concentrated on improving the WPA2. Based on the weaknesses found in the earlier schemes such as WEP and WPA version 1. There should also be a new scheme designed from scratch which means it should be totally a new technology in Wi-Fi security. In addition, any new technology which will be introduced in the market must go though a more robust testing stage to make sure only 'maturely' tested scheme will be used commercially.

CONCLUSION

In many circumstances, the security in wireless tries to adopt and adapt the security implemented in the wired network. However, the rapid growth of the wireless market makes the solutions obsolete in the faster way. With the nature of broadcasted signal, wireless network makes security implementation harder. The current network infrastructure which consist a heterogeneous component, wired and wireless, makes it even more difficult to find best solution. In this case, the vulnerable wireless network will surely make the wired network opened to attacks. Furthermore, different standards with different directions and short technology life cycle contribute some of the problem in wireless security implementation.

Obviously reliable security answers to make wireless networks as secure as the wired counterpart are still not available. As a cost-effective solution, the 802.1X security may be deployed to refuse user access without proper credentials, possibly should provide strong security for wireless networks. For environments that require more robust security, to make wireless networks as secure as the wired counterpart, the current VPN tunnels technology (together with 3DES encryption etc.) can be layered on top of the existing 802.1X security for a more complete solution. While offering a practical solution to wireless security, this approach may resolve the main security problem to wireless deployment. However the implementation should becomes more complex and for sure suffers more overheads.

In order to overcome the flaws of the early WEP adoption, WPA was introduced. At the physical layer, WPA employs TKIP and 802.1X security for user authentication. This approach creates the basis for better wireless network security that similar to the wired network. The WPA is capable at certain point to prevent most difficult attacks on wireless networks and has been improved with the introduction of WPA2/802.11i.

Whatever security scheme used for the wireless, we still don't have a total secure wireless communication because all the technology used from WEP to WPA2 and the combination with the existing wired technologies have been analyzed and tested for known vulnerabilities. Hence, as in the wired, the best thing is not to totally depend on the security features that are known not secure. Other simple solutions such as education, security awareness and better understanding of the attacks and exploits should be adopted.

REFERENCES

1. [1] IEEE.org, "IEEE Std 802.11," June 2007. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11-2007.pdf. [Accessed: August 4, 2008].
2. [2] Bluetooth.org, "Bluetooth Special Interest Group" [Online]. Available: https://www.bluetooth.org/apps/content/. [Accessed: August 4, 2008].
3. [3] IEEE.org, "IEEE Standard 802.16-2004," October 2004. [Online]. Available: http://ieee802.org/16/pubs/80216-2004.html. [Accessed: August 4, 2008].
4. [4] IEEE.org, "IEEE Std 802.16e™-2005 and IEEE Std 802.16-2004/Cor1-2005," Februari 2006. [Online]. Available: http://www.ieee802.org/16/pubs/80216e.html. [Accessed: August 4, 2008].
5. [5] Ankush Karnik, Katia Passerini, "Wireless network security - A discussion from a business perspective," in *Wireless Telecommunications Symposium*, 2005, pp. 261 – 267.
6. [6] Kioskea, "Wireless networks," [Online]. Available: http://en.kioskea.net/wireless/wlan.php3. [Accessed: August 5, 2008].
7. [7] The IEEE802.org, "IEEE 802.15 Working Group for WPAN," [Online]. Available: http://www.ieee802.org/15/. Sept. 2008. [Accessed: August 5, 2008].
8. [8] Greyfriars Consulting Group, "Wireless Solutions Fast Start Course," [Online]. Available: http://www.greyfriars.net/gcg/greyweb.nsf /miam/article01. 2005. [Accessed: August 7, 2008].
9. [9] The ETSI web site, "European Telecommunications Standards Institute," [Online]. Available: http://www.etsi.org/WebSite /homepage.aspx. [Accessed: August 16, 2008].
10. [10] The IEEE.org, "The Institute of Electrical and Electronics Engineers, Inc.," 2008. [Online]. Available: http://www.ieee.org. [Accessed: August 13, 2008].
11. [11] The 3rd Generation Partnership Project (3GPP) web site, "Shaping the future of mobile communication standards," 2008. [Online]. Available: http://www.3gpp.org/. [Accessed August 21, 2008].
12. [12] Intel Corp. Wi-Fi (802.11) White Papers, "Understanding Wi-Fi and WiMAX as Metro-Access Solutions," October 2004. [Online]. Available: http://whitepapers.silicon.com/0,39024759,60107942p,00.htm. [Accessed: August 21, 2008].
13. [13] Bill Brenner, "TJX breach tied to Wi-Fi exploits," 07 May 2007, [Online]. Available: http://searchsecurity.techtarget.com /originalContent/0,289142,sid14_gci1254020,00.html. [Accessed: August 21, 2008].
14. [14] Tom Karygiannis, Les Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices," November 2002. [Online]. Available: http://csrc.nist.gov/. [Accessed: August 23, 2008].
15. [15] Nikita Borisov, Ian Goldberg, David Wagner, "Security of the WEP algorithm," 2001. [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html. [Accessed: August 24, 2008].
16. [16] Scot Fluhrer, Itsik Mantin, Adi Shamir, "Weakness in the Key Scheduling Algorithm of RC4, Preliminary Draft" July 25, 2001. [Online]. Available: http://www.crypto.com/papers/others/rc4_ksaproc.ps. [Accessed: August 24, 2008].
17. [17] Arbaugh, William; Mishra, Arunesh A. "An Initial Security Analysis of the 802.1X Standard." 6 February 2002. [Online]. Available: http://www.cs.umd.edu/%7Ewaa/1x.pdf. [Accessed: August 24, 2008].
18. [18] Walker, Jesse. "Unsafe at any Key Size: An analysis of the WEP encapsulation. November 2000." 4 September 2003. [Online]. Available: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip. [Accessed: August 24, 2008].
19. [19] Wu, T. "A Real-World Analysis of Kerberos Password Security," 1998. [Online]. Available: http://www.isoc.org/isoc/conferences /ndss/99/proceedings/papers/wu.pdf. [Accessed: Sept. 3, 2008].
20. [20] wi-fi.org, "WPA (Wi-Fi Protected Access) Knowledge Centre," 2007. [Online]. Available: http://www.wi-fi.org/knowledge_center/wpa/. [Accessed: Sept. 3, 2008].
21. [21] Robert Moskowitz, "Weakness in Passphrase Choice in WPA Interface," ICSA Labs, a division of TruSecure Corp., November 4, 2003. [Online]. Available: http://wifinetnews.com/archives/002452.html. [Accessed: Sept. 3, 2008].

22. [22] Vebjorn Moen, Havard Raddum, Kjell J. Hole, "Weaknesses in the Temporal Key Hash of WPA," Dept of Informatic, Univ. of Bergen, April 5, 2004. [Online]. Available: http://www.nowires.org/Papers-PDF/WPA_attack.pdf. [Accessed: Sept. 11, 2008].
23. [23] You Sung Kang, KyungHee Oh, ByungHo Chung, Kyoil Chung and DaeHun Nyang, *Analysis and Countermeasure on Vulnerability of WPA Key Exchange Mechanism*. Springer Berlin/Heidelberg: Berlin, 2004.
24. [24] Wikipedia.org, "Advanced Encryption Standard," [Online]. Available: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: Sept. 11, 2008].
25. [25] Wikipedia.org, "RC4," [Online]. Available: http://en.wikipedia.org/wiki/RC4. [Accessed: Sept. 15, 2008].
26. [26] Changhua He, John C Mitchell, "Analysis of the 802.11i 4-Way Handshake," in *Proceedings of the 3rd ACM workshop on Wireless security*, 2004, pp. 43 - 50.
27. [27] Changhua He and John C Mitchell, "Message Attack on the 4-Way Handshake," Electrical Engineering and Computer Science Departments Stanford University, Stanford, May 2004. [Online]. Available: http://www.drizzle.com/%7Eaboba/IEEE/11-04-0497-00-000i-1-message-attack-4-way-handshake.doc. [Accessed: Sept. 15, 2008].
28. [28] Magnus Falk, "Fast and Secure Roaming in WLAN," 22 Dec 2004. [Online]. Available: http://www.diva-portal.org /diva/getDocument?urn_nbn_se_liu_diva-2695-1__fulltext.pdf. [Accessed: Sept. 17, 2008].
29. [29] Josh W., "coWPAtty - Attacking WPA/WPA2-PSK Exchanges," March 20 2008. [Online]. Available: http://www.willhackforsushi.com /Cowpatty.html. [Accessed: Sept. 17, 2008].
30. [30] ElcomSoft Co. Ltd., "ElcomSoft Breaks Wi-Fi Encryption Faster with GPU Acceleration," October 9, 2008. [Online]. Available: http://www.prweb.com/releases/wi-fi/cracking/prweb1405954.htm. [Accessed: Sept. 17, 2008].
31. [31] Dhulton, "SHA1/PBKDF2 WPA Brute-Force," 2006. [Online]. Available: http://openciphers.sourceforge.net/oc/wpa.php. [Accessed: Sept. 17, 2008].
32. [32] IETF.org, "Remote Authentication Dial In User Service (RADIUS) RFC," 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2865.txt. [Accessed: Sept. 17, 2008].
33. [33] IETF.org, "The EAP-TLS Authentication Protocol," March 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5216.txt. [Accessed: Sept. 23, 2008].
34. [34] Wi-fi.org, "Extended EAP (Extensible Authentication Protocol) Knowledge Centre," 2007. [Online]. Available: http://www.wi-fi.org /knowledge_center/eap. [Accessed: Sept. 25, 2008].
35. [35] Thomas Wu., "A Real-World Analysis of Kerberos Password Security," Stanford University, 1999. In *Proceedings of the 1999 Network and Distributed System Security Symposium*, 1999.
36. [36] Joshua Hill, "An Analysis of the RADIUS Authentication Protocol," InfoGard Laboratories, 2001, [Online]. Available: http://www.untruth.org/%7Ejosh/security/radius/radius-auth.html. [Accessed: Sept. 25, 2008].
37. [37] Cameron Macnally, "Cisco LEAP Protocol Description," 6 Sep 2001, [Online]. Available: http://www.missl.cs.umd.edu/wireless /ethereal/leap.txt. [Accessed: Sept. 26, 2008].
38. [38] Cisco.com, "Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability," August, 2003, [Online]. Available: http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml. [Accessed: Sept. 29, 2008].
39. [39] Thomas M. Thomas, Tom Thomas, *Network Security First-Step*. Cisco Press: New York, 2004.
40. [40] Thomas M. Thomas, *Wireless Security*. Cisco Press: New York, 2004.

LIST OF ABBREVIATIONS

3A - Authentication, Authorization and Accounting
3DES - Triple Data Encryption System
3GPP - Third-Generation Partnership Project
AAA - Authentication, Authorization and Accounting
ACL - Access Control List
ADSL - Asymmetric Digital Subscriber Line
AES - Advanced Encryption Standard
AP - Access Points
CB - Channel Bonding
CCK - Complementary code keying
CCMP - Counter Mode CBC MAC Protocol
CSMA-CA - Carrier Sense Multiple Access with Collision Avoidance
DES - Data Encryption System
DOCSIS - Data Over Cable Service Interface Specification
DOS - Denial-of-Service
DMZ - De-militarized Zone
DSL - Digital subscriber line
DSSS - Direct-sequence Spread Spectrum
EAP - Extensible Authentication Protocol
ETSI - European Telecommunications Standards Institute
FHSS - Frequency-hopping spread spectrum
FPGA - Field-programmable Gate Array
GPU - General Processor Unit
HR/DSSS - High Rate / Direct Sequence Spread Spectrum Physical Layer
IEEE - Institute of Electrical and Electronics Engineers
IPsec - Internet Protocol Security
IETF - Internet Engineering Task Force
IV - Initialization Vector
LAN - Wireless Local area networks
LEAP - Lightweight EAP
L2TP - Layer 2 Tunneling Protocol
MAC - Media Access Control
MAN - Wireless Metropolitan area networks

MD5 - Message-Digest algorithm 5
MIC - Message Integrity and Countermeasure
MIMO - Multiple-input multiple-output
NIC - Network interface card
NIST - National Institute of Standards and Technology
OFDM - Orthogonal frequency-division multiplexing
PAN - Wireless Personal area networks
PDA - Personal Digital Assistant
PIC - Pre-IKE Credential Provisioning Protocol
PPP - Point to Point Protocol
RADIUS - Remote Access Dialin User Service
RSN - Robust Security Network
SSID - Service Set Identifier
TKI - Temporal Key Integrity
TKIP - Temporal Key Integrity Protocol
TLS - Transport Layer Security
TSN - Transitional Security Network
TTLS - Tunneled Transport Layer Security
UNII - Unlicensed National Information Infrastructure
UWB - Ultra-wide band
VPN - Virtual Private Network
WAN - Wireless Wide area networks
WEP - Wired Equivalent Privacy
WEP2 - WEP version 2
Wi-Fi - Wireless Fidelity
WiMAX - Worldwide Interoperability for Microwave Access
WISP - Wireless Internet Service Providers
WPA - Wi-Fi Protected Access
WPA2 - Wi-Fi Protected Access version 2
WPA-PSK - Wi-Fi Protected Access - Pre Shared Key

| Winsock |< Internet Protocol version 6 (ipV6) | Linux Sockets >| Site Index | Winsock In .NET |