802.11 KABLOSUZ YEREL ALAN AĞLARINDA WEP v3 WPA ANAHTARLARININ ELDE EDİLMESİ

Hayrettin Evirgen[a], Ahmet Sertol Köksal[b], Orhan Er[a], Hüseyin Ekiz[b]

[a]Sakarya Üniversitesi, Bilgisayar Mühendisliği Bölümü, 54187 Sakarya, TÜRKİYE
[b]Sakarya Üniversitesi, Elektronik ve Bilgisayar Eğitimi Bölümü, 54187 Sakarya, TÜRKİYE
evirgen@sakarya.edu.tr, askoksal@sakarya.edu.tr, orhaner@sakarya.edu.tr, ekiz@sakarya.edu.tr

ABSTRACT

WLAN is a wireless local area network that links two or more computers without using wires. WLAN utilizes spread-spectrum modulation technology based on radio waves to enable communication between devices in a limited area. This provides mobility for users and limit of the area is depending on characteristics of the WLAN system. However, some amount of security risk is associated with WLANs. WEP, WPA and WPA2 are techniques to provide security service for wireless computer networks. This study aims to determine different methods on 802.11 WLAN to achieve WEP and WPA keys using computer programs (Kismet, Airodump, Aircrack, Ethereal, Cowpatty), network tools and wireless network adaptors.

Key words*:* WPA, WEP, 802.11i, Wireless LAN, Wireless Security, Key Cracking

1. GİRİŞ

Kablosuz iletişim teknolojisi, en basit tanımıyla, noktadan noktaya veya bir ağ yapısı şeklinde bağlantı sağlayan bir teknolojidir. Kablosuz iletişim teknolojisini diğerlerinden ayıran nokta; iletim ortamı olarak havayı kullanmasıdır. Kablosuz yerel alan ağları, günümüzde en yaygın şekliyle WLAN (Wireless Local Area Network) olarak adlandırılmaktadır.

Bu çalışmanın temel amacı, güvenli bir kablosuz yerel alan ağı oluşturmak için izlenmesi gereken politikaları ve olası saldırılara karşı en güvenilir yöntemleri belirlemektir. Kablosuz ağlarda güvenliği sağlamak için aşağıdaki kriterlerin sağlanması gereklidir:

i. Asıllama (Authentication), kablosuz ağ düğümünün kimlik bilgilerinin geçerliliğinin denetlenmesidir.

ii. Şifreleme: Veri paketleri gönderilmeden önce, gizliliğin sağlanması için verilerin şifrelenmesidir.

iii. Veri bütünlüğü: Veri paketleri gönderilmeden önce, alıcı ve verici tarafında iletinin içeriğini kontrol eden ve sıralayan bir bilginin iletiye eklenmesidir.

Bu amaç doğrultusunda gerçekleştirilen uygulama iki farklı kablosuz ağ üzerinde yapılmıştır. Birincisi; Sakarya Üniversitesi bünyesinde kurulu olan kablosuz bir ağdır. Bu ağ bir güvenlik duvarı tarafından korunmaktadır. İkincisi ise orta ölçekli şirketler için örnek teşkil etmesi bakımından başka hiçbir kablosuz ağın olmadığı bir ortamda kurulmuştur.

2. ASILLAMA (AUTHENTICATION)

IEEE 802.11 iki tür asıllama tekniği tanımlamıştır. Bu teknikler; açık sistem asıllama ve ortak anahtarlı asıllamadır.

Açık sistem asıllamada kimlik denetimi yapılmaz. Kullanıcı erişim noktasından bağlantı isteminde bulunur, erişim noktası da isteği kabul eder. Bu yöntemde şifreleme kullanılmaz.

Ortak anahtar asıllama yönteminde, farklı olarak şifreleme kullanılır. İstemci AP'den istekte bulunur. AP rasgele bir mesajı istemciye gönderir. İstemci bu mesajı, kablosuz ağa kayıt olurken almış olduğu anahtar ile şifreler ve şifreli mesajı AP'ye gönderir. AP almış olduğu bu mesajı kontrol ederek doğruluğunu denetler. Mesaj doğru ise bağlantıya izin verir [2].

Bu teknikler birçok güvenlik açıkları içermektedir. Bu güvenlik açıklarını gidermek amacıyla 802.1x asıllama yöntemi geliştirilmiştir. 802.1x standardı IEEE tarafından geliştirilen port tabanlı güvenlik protokolüdür. Kablosuz ağda güvenliği temin etmek ve WEP'in zayıflıklarını gidermek için kablolu ağlarda kullanılan teknolojiden faydalanır. Bu standart ile ağ, kullanıcı, asıllayıcı ve asıllama sunucusu olmak üzere üçe ayrılır. 802.1x asıllama işlemi şu şekilde gerçekleşir:

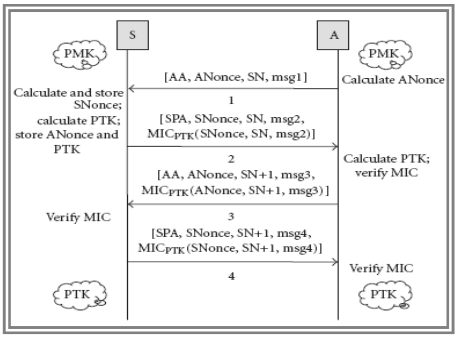
1. Kullanıcı kimlik bilgilerini göndererek AP'den erişim isteğinde bulunur.

2. AP, bu isteği kimlik kontrolü yapılmayan bir port üzerinden RADIUS sunucusuna iletir.
3. RADIUS sunucusu AP yolu ile kullanıcıdan talepte bulunur.
4. Kullanıcı, AP yoluyla RADIUS sunucusuna kimlik bilgilerini cevap olarak iletir.
5. Kimlik bilgileri doğru ise, RADIUS sunucusu AP'ye şifrelenmiş bir asıllama anahtarı gönderir.
6. AP, sadece o oturumda kullanılabilecek şifreli bir asıllama anahtarını kullanıcıya gönderir.

İstemci-AP-RADIUS arasındaki iletişimi tanımlayan 802.1x standardı mevcut diğer standartları da kullanmaktadır. Bu standartların en önemlisi olan EAP, RADIUS sunucu ve kullanıcı arasında AP yolu üzerinden, talep ettikleri asıllama işlemini gerçekleştirmek için kullanılır. EAP esasen modem yolu ile dial-up asıllama için tasarlanmıştır. EAP mesajlarının WLAN'a uyarlama işlemini 802.1x standardı EAP over LAN (EAPOL) ile tanımlamıştır. EAPOL çerçeveleri EAP mesajlarını sunucu ve kullanıcı arasında taşır [3,4].

2.1. OTURUM ANAHTARI ÜRETİMİ

802.1X/EAP asıllama mekanizması, dinamik bir oturum anahtarı üreterek güvenliği sağlamaya çalışır. Bu amaçla, kullanıcı, erişim noktası ve sunucu tarafından başlangıçta bilinen bir ana anahtardan (PMK – Pairwise Master Key) yararlanılır. PMK anahtarı 256 bit uzunluğundadır. Bu anahtar, kullanıcı ile asıllayıcının asıllama işlemi esnasında, veri iletişiminde kullanacakları geçici oturum anahtarını üretmelerinde kullanılır. Ancak, kablosuz ağda bir sunucu bulunmaması durumunda PMK yerine statik bir anahtar (PSK – Preshared Key) kullanılmaktadır. Geçici oturum anahtarı PTK (Pairwise Transient Key) olarak adlandırılır ve 512 bit uzunluğundadır. PTK anahtarının üretilmesi çok önemlidir. Çünkü bu işlem aynı zamanda asıllama işleminin tamamlanmasında da etkilidir. PTK anahtarının üretilmesi dörtlü anlaşma (handshake) adı verilen bir protokol ile gerçekleştirilir. Şekil 1, PTK anahtarının dörtlü anlaşma protokolü ile üretilmesini göstermektedir.



Şekil 1. Dörtlü anlaşma protokolü [7]

Dörtlü anlaşmada, sadece 4 tür mesaj tanımlanmıştır. Bu mesajlar:

Msg1 : [AA, ANonce, SN, Msg1], Msg2 : [SPA, SNonce, SN, Msg2, MIC(SNonce, SN, Msg2)]
Msg3 : [AA, ANonce, SN + 1, Msg3, MIC(ANonce, SN + 1, Msg3)], Msg4 : [SPA, SNonce, SN + 1, Msg4, MIC(SNonce, SN + 1, Msg4)]

S : Kullanıcı, A : Asıllayıcı, MIC : Mesaj bütünlük kodu, AA : Asıllayıcının MAC adresi, SPA : Kullanıcının MAC adresi, ANonce : Asıllayıcı (AP) tarafından üretilen rastgele bir değer, SNonce : Kullanıcı tarafından üretilen rastgele bir değer, SN : Mesajın sıra numarası, MsgX : Mesaj X'in tipini tanımlar.

Dörtlü anlaşma protokolü "Nonce" değerlerinin üretilmesiyle başlar. Bu değerler sadece bir kez üretilir. Asıllayıcı (A) ANonce değerini Msg1 içine koyarak kullanıcıya (S) iletir. Kullanıcı Msg1 mesajını aldıktan sonra, AA, SN ve ANonce değerlerini bilecektir. Bu aşamada, kullanıcı SNonce adında yeni bir rastgele değer üretir; ANonce, SNonce, AA, SPA, PMK veya PSK değerleri PRNG (pseudorandom) fonksiyonu ile şifrelenerek PTK değeri hesaplanır. Bu PTK değerinden de Msg2 mesajı ile birlikte gönderilecek MIC değeri hesaplanır.

PTK ve MIC değerleri hesaplandıktan sonra kullanıcı, ANonce, SNonce ve PTK değerlerini saklar ve Msg2 mesajını asıllayıcıya gönderir. Asıllayıcı Msg2 mesajını aldıktan sonra, SNonce değerini bileceği için, kullanıcı ile aynı prosedürü kullanarak PTK değerini hesaplayabilir. Asıllayıcı, hesapladığı bu PTK değerini kullanarak MIC değerini hesaplar ve bu değeri Msg2 mesajı içinde aldığı MIC değeri ile karşılaştırır. Her iki MIC değeri eşitse kullanıcı onaylanır ve asıllayıcı Msg3 mesajını kullanıcıya gönderir. Kullanıcı da aynı şekilde MIC değerini onayladıktan sonra Msg4 mesajını asıllayıcıya gönderir ve dörtlü anlaşma tamamlanır.
Dörtlü anlaşma protokolü bunların dışında, aşağıda sıralanmış güvenlik önlemlerini de içermektedir:

1. Kullanıcı ve asıllayıcı geçerli olmayan bir SN veya MIC değeri içeren mesaj alırlarsa, bu mesajı dikkate almayacaklardır. Bu yaklaşımla Man In The Middle (Ortadaki Adam) saldırılarından korunmak amaçlanmaktadır.
2. Kullanıcı, Msg1 mesajını bir zaman damgası ile birlikte almazsa, bu mesajı dikkate almayacak, asıllama yapmayacak ve asıllama prosedürü yeniden başlayacaktır.
3. Asıllayıcı, Msg2 veya Msg4 mesajını bir zaman damgası ile birlikte almazsa, Msg1 veya Msg3 mesajını tekrar göndermeyi deneyecektir ve belli

bir deneme sonunda kullanıcı ile bağlantısını kesecektir [7,8].

3. ŞİFRELEME ve VERİ BÜTÜNLÜĞÜ

3.1. WEP

Wired Equivalent Privacy (WEP), 802.11 standardıyla beraber geliştirilmiş olan temel güvenlik birimidir. Kablosuz düğümler arasındaki iletimde şifreleme ve veri bütünlüğünü sağlama işlemlerini gerçekleştirmeye çalışır. RC4 şifreleme algoritmasını kullanır. WEP şifreleme için kullanıcı ve erişim sağlayıcı tarafında 40 bitlik statik bir anahtar tanımlanır. Ayrıca WEP, akış şifresini elde etmek için 24 bitlik bir ilklendirme vektörü (Initialization Vector – IV) kullanılır. WEP'in çalışması şu şekildedir:

1. Veri bütünlüğünü sağlamak amacıyla, veri bir doğrulama algoritmasına (integrity check) tabi tutularak, doğrulama bitleri (ICV – Integrity Check Value) elde edilir.
2. Bu doğrulama bitleri verinin sonuna eklenir.
3. 24 bitlik IV statik anahtarın başına eklenir; 64 bitlik paket oluşturulur.
4. 64 bitlik bu paket RC4 (rastgele sayı üretici – PseudoRandom Number Generator-PRNG)) algoritması ile şifrelenir.
5. 2. adımda elde edilen veri ile 4. adımda elde edilen veri bir XOR işleminden geçer.
6. Elde edilen bu verinin başına tekrar IV eklenir ve iletilecek şifreli veri elde edilir. Elde edilen bu verinin başına, alıcı ve vericinin MAC adresi eklenerek kablosuz ortama gönderilir.
7. Şifreli veri, karşı tarafta aynı işlemler tersi yönde uygulanarak açılır [1,5].

3.2. WPA

Wi-Fi Protected Access (WPA), WEP'in zayıflıklarını gidermek amacıyla 2004'te Wi-Fi Alliance tarafından geliştirilmiştir. WEP'in güvenliğini tamamen yitirmesi üzerine IEEE, 802.11i adını verdiği yeni bir güvenlik mekanizması geliştirme çalışmalarına başlamıştır. Bu geçiş sürecinde güvenliğin sağlanması, geçici bir süreliğine olsa da WPA tarafından gerçeklenmektedir. Bunun nedeni ise; WPA'nın ek bir donanım gerektirmemesi, yazılım veya cihaz yazılım güncellemeleriyle geçişin sağlanabilmesidir.

WPA ile 802.1x tabanlı asıllama yapılması zorunludur. Ancak, bu yöntemde RADIUS sunucusu kullanımı isteğe bağlıdır. Bunun yerine ön-paylaşımlı anahtar (pre-shared key – PSK) kullanımı ile asıllama işlemi yapılabilmektedir. Bir RADIUS sunucusu kullanımı halinde ise WPA tüm 802.1x ve EAP protokollerini desteklemektedir. WPA, şifreleme mekanizması olarak, yine kendine has ve geçiş sürecindeki ihtiyaçları karşılamayı hedefleyen farklı bir protokolü kullanmaktadır. TKIP (Temporal Key Integrity Protocol) adı verilen bu protokol WEP'te olduğu gibi RC4 algoritmasını kullanır. Fakat geliştirdiği yeni yöntemlerle WEP'in zayıflıklarını çok büyük ölçüde gidermiştir [4,6].

Tablo 1. WEP ve WPA'nın karşılaştırılması

WEP	WPA
Ön paylaşımlı anahtar mekanizması ile güvenliği sağlar. Anahtar kullanıcılar arasında ortaktır.	802.1x asıllama ile kullanıcıya has anahtar üretilir.
Kullanılan senkron akış şifreleme ağ ortamları için uygun (güvenli) değildir.	WEP ile aynıdır.
Her paket için IV tarafından üretilen anahtar zayıf bir anahtardır ve saldırılara karşı açıktır.	Ortak anahtar kullanılarak üretilen geçici şifreleme anahtarı ve anahtar her paket için ayrı ayrı oluşturulur.
Statik anahtar + küçük boyutlu IV + her paket için anahtar üretim metodu = İstenilen güvenliği sağlamak için yeterli değildir.	48 bit IV + her oturum için yeniden anahtar üretilmesi = Daha güvenli bir sistemdir.
IV'lerin tekrarlanma olasılığı çok yüksektir.	IV'lerin tekrarlanma olasılığı çok düşüktür.
Veri bütünlüğü için doğrusal bir algoritma kullanır. Bu zayıf bir veri bütünlüğü korumasıdır.	Veri bütünlüğü için doğrusal olmayan Michael algoritması kullanır. Bu güçlü bir veri bütünlüğü korumasıdır.
Alıcı ve gönderici adresleri şifrelenmeden gönderildiği için veri farklı adreslere yönlendirilebilir.	Alıcı ve gönderici adresleri de şifrelenir.
Tekrar saldırılarına karşı korumasızdır.	Ardışık sayı üretici ile tekrar saldırılarına karşı koruma sağlar.
Kullanıcı AP'yi asıllamaz.	802.1x ile karşılıklı asıllama yapılır.

3. 3. IEEE 802.11i (WPA2)

IEEE 802.11i, RSN (Robust Security Network) adında yeni bir kablosuz ağ türü tanımlar. Bu bazı durumlarda WEP tabanlı ağlarla aynıdır fakat bununla birlikte RSN'e bağlanmak için kablosuz

cihazların RSN uyumlu olması gerekir. RSN uyumlu cihazlar yazılım güncellemesi ile elde edilememektedir. Ancak üretim aşamasında bu sağlanabilir. Bu yüzden yazılım güncellemesi ile kullanılabilen WPA teknolojisinden farklı olarak WPA2 olarak da adlandırılan 802.11i teknolojisini kullanabilmek için mevcut kablosuz cihazların RSN uyumlu cihazlarla değiştirilmesi şarttır. Bu da günümüzde oldukça yaygın olarak kullanılan kablosuz cihazların değiştirilmesinin yüksek maliyet gereksinimleri dolayısıyla 802.11i teknolojisinin genellikle kullanılmadığını göstermektedir. Bununla birlikte 802.11i ile kablosuz ağlarda tam bir güvenlik sağlanmaktadır.

WPA2'de kullanılan yöntemler genel hatlarıyla WPA'da kullanılanlarla aynıdır. RC4 şifreleme algoritmasından kaynaklanan zayıflıkları gidermek amacıyla, WPA2 farklı bir şifreleme algoritması kullanmaktadır. AES (Advanced Encryption Standard) adı verilen bu algoritma ile gerçekleştirilen şifreleme günümüzde tam bir güvenlik sunmaktadır. AES algoritmasında blok şifreleme tekniği kullanılmaktadır [5,8].

4. UYGULAMA

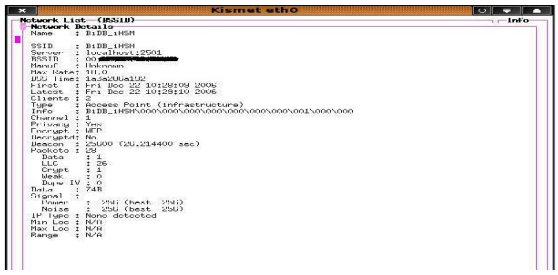
Gerçekleştirilen uygulama iki farklı ağda denenmiştir. Birinci ağ Cisco AiroNet 1100 AP kullanmaktadır ve kablolu ağa olan bağlantı güvenlik duvarı tarafından engellenmektedir. İkinci ağ ise USRobotics Maxg Router AP kullanmaktadır. Saldırı amaçlı kullanılan bilgisayar Intel pro2200 802.11b/g wireless adapter'e sahip dizüstü bilgisayardır. Uygulamalar sırasında Linux işletim sistemi kullanılmıştır.

4.1. WEP Anahtarının Elde Edilmesi

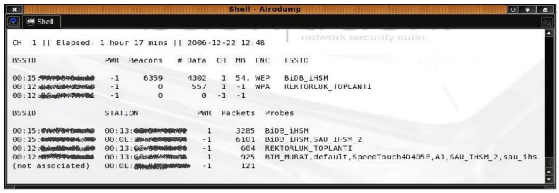
"Kismet" programı (Şekil 2) ile ağ ortamı hakkında bilgiler elde edildikten sonra, paket toplama işini daha iyi yapan "airodump" programı (Şekil 3) ile ağ trafiğinden paketler toplanmıştır.

Yeterli paket toplandıktan sonra "aircrack" programı (Şekil 4) kullanılarak WEP anahtarı elde edilmeye çalışılmıştır. Yapılan çalışmalarda, 64 ve 128 bit WEP anahtarlarının elde edilmesi için sırasıyla, yaklaşık olarak 150.000 ve 230.000 IV paketi toplanması gerekmiştir.

Her iki ağda yapılan çalışmalarda, en büyük sorun ağ trafiği hakkında olmuştur. Trafiğin yeterli yoğunlukta olmadığı durumlarda "aireplay" adlı program kullanılmıştır. "aireplay" ile STA-AP arasında iletilen paketler yakalanıp, tekrar tekrar ve farklı istasyonlardan gönderiliyormuş gibi simüle edilerek yoğun bir ağ trafiği oluşturulmuştur. Uygulama sonucu Tablo 2'de gösterilmektedir.

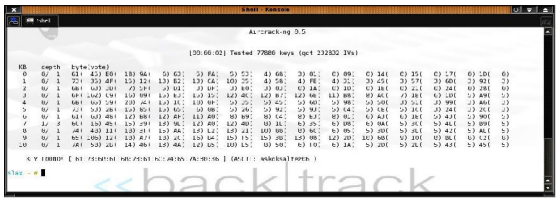


Şekil 2. "Kismet" programı



Şekil 3. "airodump" ekran görüntüsü

Bu çalışmada her iki ağ için, WEP anahtarı aynı yöntemle elde edilmiştir.



Şekil 4. **"**aircrack" ekran görüntüsü

Tablo 2. Uygulama sonuçları

SSID Yayını	MAC Filtreleme	Anahtar Uzunluğu	Şifreleme	Sonuç
Evet	Hayır	64 bit	WEP	Başarılı
Evet	Hayır	128 bit	WEP	Başarılı
Hayır	Evet	64 bit	WEP	Başarılı
Hayır	Evet	128 bit	WEP	Başarılı

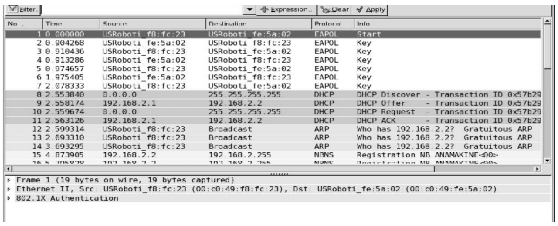
4.2. WPA Anahtarının Elde Edilmesi

WPA ile şifrelenmiş bir kablosuz ağın anahtarını elde etmek için öncelikle kullanılacak anahtar sözlüklerinin temin edilmesi gereklidir. Daha sonra; STA ve AP arasında bir asıllama (authentication) işleminin yapılması beklenmektedir. Asıllama işlemi sırasında "handshake" adı verilen EAPOL mesajlarının yakalanması gerekir. Yakalanan bu mesajlar ve sözlük dosyaları birlikte kullanılarak WPA anahtarı elde edilebilir.

EAPOL mesajlarının yakalanması için, "airodump" programından faydalanılmıştır Toplanan bu paketler içinde bir adet asıllama işlemi verisinin (handshake) olması yeterlidir. Eğer kablosuz ağda uzun süre bir

asıllama işlemi gerçekleşmezse, “aireplay” programı kullanılabilir. Bu program ile o an için asıllanmış olan bir kullanıcıya, bağlı olduğu AP taklit edilerek sahte mesajlar gönderilir. Bu sahte mesajlar doğal olarak yanlış anahtarla şifrelenmiş olacağından, kullanıcı AP’yi yeniden asıllama işlemine zorlayacaktır ve yeni bir asıllama işlemi yapılacaktır. Bu asıllama işlemi sırasında, WPA anahtarını elde etmek için kullanacak olduğumuz “handshake” paketini elde etmiş oluruz.

Ancak yapılan çalışmalarda görülmüştür ki; “airodump” her zaman EAPOL mesajlarını yakalayamamaktadır. Bu sorunun çözümü, “ethereal” programının kullanılmasıyla sağlanmıştır. Grafik arabirimli “ethereal” hem Linux hem de Windows’ta çalışabilmektedir ve WPA EAPOL paketlerini tam bir başarıyla yakalayıp kaydedebilmektedir. Şekil 5’te “ethereal” programı ile paketlerin yakalanması (capture işlemi) gösterilmiştir.



Şekil 5. “ethereal” ile paketlerin yakalanması

“airodump” ve/veya “etheral” programı ile istenen veri paketi elde edildikten sonraki aşama, bu paketi sözlük dosyaları ile harmanlayıp şifresini çözmektir. Bu işlem için iki farklı program kullanılmıştır. Birincisi, “aircrack”, ikincisi “cowpatty” (Şekil 6) programıdır.

Şekil 6. “cowpatty” ile WPA anahtarının elde edilişi

5. SONUÇLAR

Bu çalışma süresince 802.11 kablosuz ağlarında güvenlik konusu ele alınmış, geliştirilen güvenlik mekanizmaları incelenmiş, farklı güvenlik mekanizmaları üzerinde iki uygulama yapılmıştır. Yapılan uygulamalar sonucunda görülmüştür ki; WEP ve WPA-PSK şifreleme teknikleri kablosuz ağlarda güvenliği temin etmemektedir. Güvenli bir kablosuz ağ oluşturmak için 802.11i veya diğer adıyla WPA2 standardının kullanılması gerekmektedir.

Kablosuz bir ağ yapılandırmasında uygulanabilecek güvenlik mekanizmaları aşağıdaki gibidir:

1. Açık erişim
2. 64-128 bit WEP şifreleme (ortak anahtarlı asıllama ile),
3. WPA şifreleme (802.1x asıllama ile),
4. WPA şifreleme (802.1x asıllama ve RADIUS sunucu ile),
5. WPA2 şifreleme (802.1x asıllama ile)
6. WPA2 şifreleme (802.1x asıllama ve RADIUS sunucu ile),
7. VPN ve WPA2 şifreleme (802.1x asıllama ve RADIUS sunucu ile).

1,2,3 numaralı çözümler güvenli değildir. 4 numaralı çözüm günümüzde güvenlidir ancak gelecek için tam bir güvenlik vaat etmemektedir. 5,6,7 numaralı çözümler tam güvenlik sağlamaktadır.

Küçük ölçekli şirketler ve kişisel kullanım için 5; orta ölçekli şirketler, ticari kuruluşlar için 6; veri gizliliğinin çok önemli olduğu büyük kurumlar için 7 numaralı çözüm kullanılmalıdır.

KAYNAKLAR

1. YÜKSEL, E., SOYTÜRK, M., OVATMAN, T., ÖRENCİK, B., Telsiz Yerel Alan Ağlarında Güvenlik Sorunu. İTÜ & Deniz Harp Okulu Komutanlığı, İstanbul.
2. JOSEPH, D., Deploying Secure 802.11 Wireless Networks with Microsoft Windows. Microsoft Pres, 2004.
3. HURLEY, C., How to Cheat at Securing a Wireless Network. Syngress Publishing, Inc., 2006.
4. EDNEY, J., ARBAUGH, W.A., Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley, July 2003.
5. GAST, M., 802.11 Wireless Networks: The Definitive Guide. O’Reilly, April 2002.
6. CHANDRA, P., Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security. Elsevier Inc., 2005.
7. DE RANGO, F., LENTINI, D. C., MARANO, S., Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack inWi-Fi Protected Access and IEEE 802.11i. University of Calabria, Cosenza, Italy, June 2006.
8. HE, C., MITCHELL, J. C., 1 Message Attack on the 4-Way Handshake. Stanford University, May 2004.