KABLOSUZ AĞLARDA GÜVENLİĞİN ARTIRILMASI

[1]Berk Cengiz, [2]Murat Koyuncu ve [3]Tuncay Ercan
[1,2]Bilgisayar Müh.Böl., Atılım Üniversitesi, Ankara
[3]Bilgisayar Müh.Böl., Yaşar Üniversitesi, İzmir
berk.cengiz@deleeuw.com.tr, mkoyuncu@atilim.edu.tr, tuncay.ercan@yasar.edu.tr

ABSTRACT

The wireless networks are dominating the airwaves, with a very high penetration rate at our homes and offices due to decrease in hardware prices and simplicity of use. However, security concerns have emerged which requires users and network administrators to act accordingly.

There is a strong demand towards acquisition of wireless enabled networks and associated devices, therefore if the penetration rates for wireless devices keep their current pace, we are likely to face growing concerns for security and must take precautions before becoming a real target for the attackers.

By means of this paper; the reader will be able to revise his/her notion of security and will be aware of ever growing threats in the wireless world we are heading so fast, with concrete examples and possible solutions.

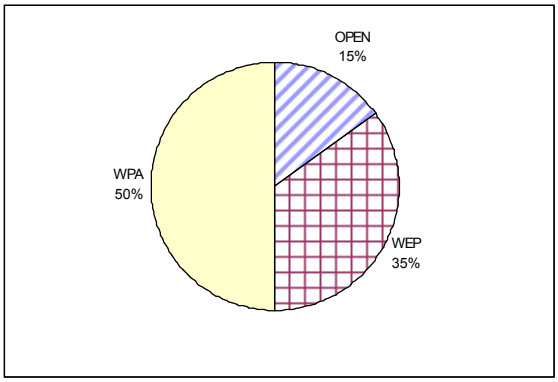
Keywords: wireless network security, attack schemes, protection scenarios, WEP, WPA.

1. GİRİŞ

Internet erişim hizmetlerindeki fiyat düşüşüyle birlikte, ev ve iş ortamında daha yaygın bir şekilde kullanılmaya başlanan kablosuz ağlar, tartışılmaz faydalarının yanı sıra, yaygın olarak çok da fazla bilinmeyen yeni riskleri beraberinde getirmektedir.

Kablosuz ağlarda kullanılan güvenlik yöntemleriyle ilgili olarak Ankara içerisinde yapılan taramanın sonucu Şekil-1'de verilmiştir. Şekilde toplam 1000 kablosuz ağda kullanılan güvenlik yöntemlerinin dağılımı görülmektedir. Yapılan çalışma gösteriyor ki kablosuz ağ kullanan kullanıcıların yaklaşık olarak yarısı OPEN (şifre gerektirmeyen bağlantı) ya da WEP (Wired Equivalent Privacy) şifreleme protokolü kullanmakta, diğer yarısı ise WPA (Wi-Fi Protected Access) ya da WPA2 şifrelemesi kullanmaktadır. WEP şifreleme sisteminin yapısal hatası sebebiyle, zaten güvenli olarak kabul edilmediği artık bilinen bir gerçektir. Bu durumda Şekil-1'de verilen OPEN ve WEP kullanıcılarının toplamını aldığımızda, kablosuz ağların %50'sinin aslında güvensiz olarak çalıştığını görüyoruz. Buna ilave olarak, WPA veya WPA2 kullananların önemli bir kısmı kullandıkları kablosuz ağ erişim noktalarının üretim sırasında atanan adını değiştirmediklerinden, Rainbow Table Attack (www.renderlab.net/projects/WPA-tables/) adlı saldırıya maruz kalmaları veya zayıf şifreler kullandıklarından kolay ele geçirilmeleri ihtimal dâhilindedir. Bu nedenle, kablosuz ağların aslında %50'den fazlasının yeterli güvenliğe sahip olmadığını söylemek yanlış olmayacaktır.

İstatistiksel çalışmaların yapılma sürecinde, ev kullanıcılarına sorulan "Neden WEP şifrelemesini kullanıyorsunuz?" sorusuna verilen cevaplarda "Bana karışık geliyor", "kimsenin bulabileceğini sanmıyorum" ya da "ADSL modemi aldığımız yer bu şekilde kurdu" ifadelerinin yer alması, aslında toplumun bu konuda yeterince bilgi sahibi olmadığını ve yeterince bilinçlenmediğini göstermektedir.



Şekil-1: Ankara'daki 1000 kablosuz ağ için şifreleme kullanım oranları

Kablosuz ağ şifrelerinin çalınması sonucunda yaşanabilecek bazı sorunlar aşağıda verilmiştir:

- Çocuk pornosu indirmek gibi suç teşkil eden faaliyetler sizin bağlantınız üzerinden yapılabilir.
- Şifreyi ele geçiren kişi, kablosuz ağ erişim cihazının şifresini değiştirebilir, sistemi kullanılamaz hale getirebilir ve sizi tüm konfigürasyonu sildirecek şekilde cihazı resetlemek zorunda bırakabilir.
- Ağ üzerinden geçen tüm trafiği kendine yönlendirebilir ve sizin bilgilerinizin bir kopyasını oluşturabilir.
- Erişim kotanızı doldurabilir.

- Trafiği, NAT kullanarak yönlendirebilir ve örneğin bir bankayı taklit edebilir.

Tabi ki WEP şifreleme sistemi, hiç bir güvenlik sağlamayan OPEN metoduna göre en azından bir seviyeye kadar koruma sağlamaktadır. Ancak ne yaptığını bilen bir saldırgan için ağ şifresini ele geçirmek günümüz teknolojisiyle maksimum 15 dakika sürmektedir [1].

İnternet üzerinden indirilebilen "AirCrack Suite" (www.aircrack-ng.org) ve benzeri yazılımlarla kablosuz ağlara yönelik saldırılar gerçekleştirmek mümkündür. Bununla birlikte, çok anlaşılır olmayan dokümantasyonu, grafiksel bir arabirimin bulunmaması ve sadece belirli çip setlerine sahip kablosuz adaptörler ile çalışıyor olması, bu tür yazılımların herkes tarafından kullanılmasını belirli oranda engellemektedir.

Bu çalışma kapsamında; yukarıda özeti verilen kablosuz ağlardaki güvenlik alternatiflerinin kullanım oranları tespit edilmiş, WEP ve WPA şifreleme yöntemlerinde şifrelerin kırılma durumları incelenmiş, bu amaçla Kablosuz Ağ Analizörü (Wireless Network Analyzer-WNA) olarak isimlendirilen bir araç oluşturulmuş ve kablosuz ağlarda güvenliğin artırılması için neler yapılması gerektiği ortaya konulmaya çalışılmıştır. Çalışmanın asıl amacı, kablosuz ağlarda güvenlik sorunlarına dikkat çekmek ve bu konuda İnternet kullanıcılarını bilinçlendirmektir [2].

Bu bildiri altı bölümden oluşmuştur. İkinci bölümde kablosuz ağların tarihçesi ve kablosuz ağlarda güvenlik konularıyla ilgili özet bilgi verilmiştir. Kablosuz ağlarda güvenlik testi yapmak üzere oluşturulan Kablosuz Ağ Analizörü üçüncü bölümde tanıtılmış, Kablosuz ağlara yapılabilecek saldırı senaryoları dördüncü bölümde açıklanmıştır. Beşinci bölümde kablosuz ağlarda güvenliğin artırılması için alınması gereken önlemler tartışılmış, altıncı bölümde ise çalışmayla ilgili sonuçlar sunulmuştur.

2. Kablosuz Ağların Tarihçesi ve Güvenlik

Kablosuz ağların ortaya çıkması aslında 19. Yüzyıla kadar geri gitmektedir. Guglielmo Marconi, "radyonun babası", 1890'lı yıllarda radyo dalgaları ile deneyler yaparken, işlerin bu noktaya gelebileceğini öngörmüş müydü acaba? Amerikan ordusunun hemen adapte ettiği radyo sinyalli ağlar, 2. Dünya Savaşı sırasında şifreleme sistemleriyle de desteklenerek bugün kullandığımız sistemlerin aslında temelini oluşturmuştur.

Bilgisayarlarda ilk kablosuz ağı, 1971 yılında Hawaii Üniversitesinde kurulan ALOHANET [3] adlı yıldız topolojili sistemde görmekteyiz. Dört ada üzerinde dağınık halde bulunan sistemleri 7 bilgisayar aracılığıyla buluşturmayı başaran yapı, kablosuz ağların bilgisayar dünyası açısından ilk büyük başarısı olarak değerlendirilebilir.

Kablosuz ağların yaygınlaşması rüyası aslında Bill Gates'e aittir [4]. 2001 yılında yaptığı bir konuşmada gelecek 10 yılın portresini çizen Gates, kablosuz ağların ev kullanıcıları seviyesine ineceğini öngörmüş olup, gelecekle ilgili vizyonunun ne kadar iyi olduğunu kanıtlamıştır.

802.11 protokolünün ilk sürümü 1997 yılında hazırlanmış ve 1999 da revize edilmiştir. Takip eden yıllarda 802.11a, b ve g protokolleri kullanıma sunulmuştur. 2008 yılında 802.11y, 2009 yılında ise 802.11n protokolüyle tanışacağız. Protokollerin gelişmesiyle birlikte kapsama alanının ve hızın neredeyse paralel bir artış gösterdiğini gözlemlemekteyiz. 2009 yılında karşımıza çıkacak olan 802.11n protokolünün varsayılan hızı 248 Mbit/s olup, kapsama alanı yaklaşık olarak 5000 metredir.

Kablosuz ağların gelişim süreci içerisinde ön plana çıkan bir konu da güvenliğin sağlanması olmuştur. Berkeley Üniversitesinde yapılan bir araştırmayı temel alan Fluhrer, Mantin, ve Shamir'in çalışması [5], WEP şifreleme sisteminin bir tasarım problemi yüzünden saldırılara açık olduğunu göstermiştir. 2005 yılında iki FBI ajanı, James C. Smith ve Geoff Bickers, bir güvenlik konferansında seyircilerin gözü önünde 128 bitlik WEP şifresini üç dakikadan daha kısa sürede kırarak güvenlikle ilgili kaygılara yenilerini eklemişlerdir.

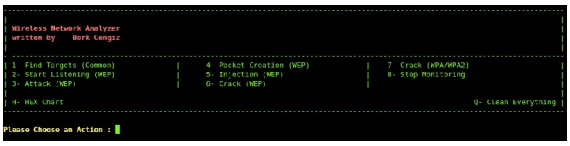
2003 yılında WiFi Alliance grubu, WPA algoritmasını kullanıma sokarak WEP'den kaynaklanan güvenlik sorununu aşmaya çalışmıştır. Bir sonraki adım olarak da, WiFi sertifikasyonuna sahip olduğunu göstermek isteyen her üretici 2006 yılından itibaren WPA2'yi desteklemek zorunda bırakılmıştır.

Yeni şifreleme yöntemleri, güvenlik açısından kullanıcıları rahatlatan çalışmalar olmakla beraber yüzde yüz bir koruma sağlayıp sağlamadıkları tartışması, bir sonraki bölümde de görüleceği üzere, hala devam etmektedir. Kablosuz ağların özelliğinden dolayı bugüne kadar olduğu gibi bundan sonra da güvenlik tartışmaları devam edecektir. Yukarıda bahsedilen, 5000 metre kapsama alanı sağlayacak yeni kablosuz ağ teknolojilerinde de bu kablosuz ağları kurcalamak için birçok saldırganın sırada olduğunu varsaymak çok da yanlış bir yaklaşım olmayacaktır.

3. WNA ile Güvenlik Analizi

Kablosuz Ağ Analizörü (WNA) aslında tamamen AirCrack Suite üzerinde çalışan bir sistem olarak oluşturulmuştur. Sanal bir makineye (Virtual Machine) kurulması sebebiyle hemen her türlü işletim sisteminde rahatça kullanılabilmektedir. Sanal makine olarak VMWare yazılımı kullanılmıştır. Sistemle ilgili en büyük kısıtlama, AirCrack Suite yazılımından kaynaklanan, belirli kablosuz ağ adaptörlerine olan bağımlılıktır ve bunu da aşmanın bir yolu şu anda bulunmamaktadır. Her ne kadar bu bir sorun gibi gözükse de, söz konusu adaptörlerin sadece 20 dolar gibi düşük maliyetlerle alınabiliyor olması bu dezavantajı önemli bir engel olmaktan çıkarmaktadır.

Ana ekranı Şekil-2'de görülen WNA, Linux shell script aracılığıyla, basit de olsa grafiksel bir çalışma ortamı sağlamakta ve kullanıcıya yapılacak işlemi menüden seçme imkânı vermektedir. Kullanıcıdan hedef kablosuz ağın adı gibi basit girdileri sisteme girmesi beklenmektedir. WNA, AirCrack Suite yazılımını arka planda bir kütüphane gibi kullanarak, sadece gerekli parametreleri kullanıcıdan almakta ve normalde kullanıcının girmesi gereken komutları kendisi çalıştırmaktadır. Bu işlemleri yaparken muhtemel hatalara karşı toleranslı olup, çökmemekte ve kullanıcının karşısına çözümü olmayan problemlerle gelmemektedir.



Şekil-2: WNA ana ekranı

WNA'nın aslında en büyük başarısı, AirCrack Suite yazılımı tarafından sunulan sayısız saldırı metodunu sadeleştirerek, kesin çözüme ulaşmayı sağlayan birkaç metodu, belirli bir mantık sırasına göre çalıştırmasıdır. Yapılan sayısız denemeler sonucunda, WNA kullanarak çözülemeyen WEP şifresi sayısı bir elin parmaklarını geçmemektedir.

WPA şifreleme yöntemi ise tamamen farklı bir mantıkla çalıştığından, WNA kullanarak şifre kırma başarı şansı oldukça değişkendir. Kaba kuvvet mantığı ile sözlük saldırı (dictionary attack) sisteminin bir arada kullanılmasını gerektiren WNA'nın WPA saldırısının, sonuca 5 dakika ile 24 ay süresinde gidebileceği hesaplanmıştır. Bu derece geniş bir zaman aralığının ortaya çıkmasındaki en büyük etken şifrelemede kullanılan karakter setinin zenginliğidir. Konulan şifrelere bir de muhtemel sembolleri eklediğinizde ortaya çıkan kombinasyon, günümüz teknolojisinde mantıklı zaman aralıklarında hedefe ulaşmayı imkansız kılabilmektedir.

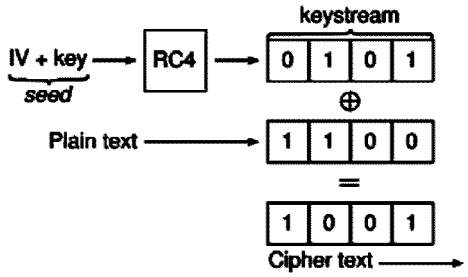
WNA bir kablosuz ağ saldırı aracı olarak geliştirilmemiştir. Kablosuz ağlardaki güvenlik sorununa dikkat çekmek ve bu konuda İnternet kullanıcılarını bilinçlendirmek adına yapılan bir akademik çalışmanın parçası olarak geliştirilmiştir. Böyle bir aracın, özellikle ağ yöneticileri tarafından, sorumlu oldukları ağları güvenlik açısından test etmeleri amacıyla kullanılabileceği değerlendirilmektedir. Bu kapsamda, geliştirilen aracın adı "Kablosuz Ağ Analizörü" olarak isimlendirilmiştir.

4. Muhtemel Saldırı Senaryoları

4.1 WEP Saldırısı

WNA kullanarak WEP şifreleme metodunu aşmak kesinlikle bir sorun teşkil etmemektedir. 64 bit ya da 128 bit şifreleme tekniği kullanılmasının da çok fazla etkisi olmamaktadır. İkisi arasında yaklaşık 5 dakikalık zaman farkı oluşmaktadır.

WEP şifreleme tekniğinin çalışma yöntemi Şekil-3'te verilmiştir [6]. RC4 şifreleme tekniği ile üretilen anahtar seti ile açık veri XOR'lanarak şifrelenmiş veri elde edilmektedir. WEP şifreleme tekniğinde aslında bir tasarım hatası mevcuttur. Şifrenin bir kısmı, paketin başlık kısmında açık bir şekilde havadan gönderilmektedir. Yeterince trafik yaratılırsa ya da sabırla trafiğin oluşması beklenirse, yakalanan açık ve şifreli veriler kullanılarak, şifre istatistiksel metotlarla kolayca elde edilebilmektedir [5], [7].



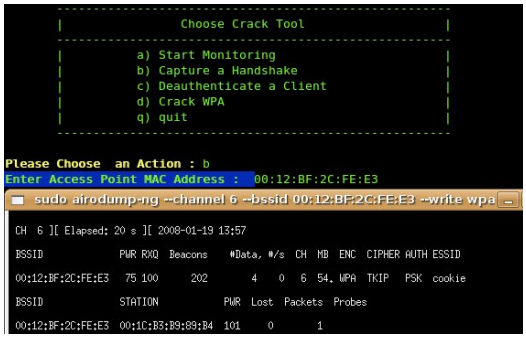
Şekil-3: WEP Şifreleme Yöntemi

WNA kullanarak sabırla bir kablosuz ağda trafik olmasını beklemeye gerek kalmamaktadır. WNA kablosuz erişim noktasına kendini sahtekarlıkla tanıtarak (fake authentication) kendi trafiğini kendisi yaratmakta, bu tip trafik internet erişimini yavaşlatan trafik olmadığı için de gerçek kullanıcılar tarafından tespit edilmesi pek kolay olmamaktadır. Sadece ARP paketlerini göndererek yeterli trafiği çok kısa bir sürede yaratmak mümkün olmaktadır. Bazen de bozuk paketler göndererek sonuca ulaşmak mümkündür. Ancak yapılan testlerde kablosuz ağ cihazlarının yarıya yakını bozuk paketlere tepki vermektedir. Yakın zamanda üretilen

cihazların çoğu, bu saldırı tipinde doğru karar vererek bozuk paketleri dikkate almamaktadır. Ancak, ARP paketleriyle yapılan saldırılarda kesinlikle sonuca ulaşılabilmektedir.

4.2 WPA Saldırısı

WPA şifreleme yönteminde ise, durum WEP'e göre oldukça farklıdır. WNA ile bir WPA şifresinin kırılabilmesi için 4 basamaklı bir işlemin uygulanması gerekmektedir. Uygulanan adımlar Şekil-4'de verilen WNA ekranında da görülmektedir. Bu basamaklar sırasıyla aşağıda açıklanmıştır.



Şekil-4: WNA ile WPA saldırısı

a) *Monitörü Açmak:* İlk olarak çevreyi dinleyerek hedef kanal belirlenmekte ve sisteme girilmektedir. Avrupa ve Asya ülkelerinde 1 ile 11 arasındaki kanallar, Amerika kıtasında ise 1 ile 13 arası kanallar kullanılmaktadır.

b) *4 Yollu El Sıkışmanın Yakalanması:* WPA şifresinin kırılabilmesi için mutlaka 4 yollu el sıkışmanın yakalanması gerekmektedir. Bir istemcinin kablosuz ağa bağlanmak isterken mutlaka bu el sıkışmasını gerçekleştirmek zorunda olmasından dolayı, aslında bu oldukça basit bir işlem olmaktadır. Bu noktada sorun teşkil eden tek şey, istemcinin bilgisayarını açıp kablosuz ağa bağlanma anını sabırla bekleyerek yakalayabilmektir.

c) *İstemciyi Zorla Düşürmek:* Bir önceki adımda beklemek sorun oluyorsa, işlemi bu aşamadaki yöntemle hızlandırmak mümkün olmaktadır. Bağlı bulunan bir istemciye çok sayıda paket göndererek kablosuz bağlantısı kesilmektedir. Bağlantısı kesilen istemci hemen kablosuz ağa yeniden bağlanmaya çalışacağından, 4 yollu el sıkışmayı tekrar etmek zorunda kalmaktadır. Yapılan testler gösteriyor ki bazı istemciler bu saldırıdan etkilenmemekte, bazı istemciler de kablosuz ağdan kopmalarına rağmen 4 yollu el sıkışmayı gerçekleştirmemektedir. Ancak, yine de %50 ihtimalle bu saldırı sonuç vermektedir.

d) *WPA Şifresini Bulmak:* WPA 4 yollu el sıkışma yakalandığında yapılacak işlem ise, bir sözlük kullanarak ihtimalleri denemektir. İşin ilginç tarafı WEP saldırılarından farklı olarak bu adıma gelindiğinde hedefe yakın olmak gibi bir sorun kalmamasıdır. Bu noktadan sonraki saldırı tamamen çevrimdışı olarak gerçekleşmektedir.

Bu yöntemle yapılan WPA saldırılarının etkili olabilmesi için iyi bir sözlük kullanmak şarttır. En garantili çözüm ise muhtemel tüm ASCII karakter birleşimlerinin bulunduğu bir sözlük kullanmaktır. Örneğin, Linux işletim sisteminde bu tür bir sözlüğü basit bir Perl script ile hazırlamak mümkündür. Ancak, boyut olarak 10 GB üzeri bir sözlüğün oluşacağını göz önünde bulundurmak gerekir. Şekil-5'te bu saldırı kullanılarak elde edilen bir şifre görüntülenmektedir.

Şekil 5. WPA saldırısı sonucu

WNA'da kullanılan yöntemle WPA şifrelerinin kırılmasının 5 dakika ile 24 ay arasındaki bir sürede gerçekleşeceği hesaplanmıştır. Güvenliği artırmak için, WPA şifreleme yönteminde kullanılan şifrenin uzunluğu ve karmaşıklığı büyük önem arz etmektedir. Bu nedenle, saldırılardan kurtulmanın en basit yönteminin, uzun ve harf/rakam haricindeki karakterlerle de desteklenmiş bir şifre kullanmak olduğunu söyleyebiliriz.

5. Korunma Yöntemleri

WEP algoritmasının kırılabileceği zaten bir süredir bilinen bir durumdu. Ancak WPA'nın da benzer saldırılarla, üstelik de çevrimdışı olarak kırılabilmesi fikri, güvenlikle ilgili önlemlerin artırılmasını gerektirmektedir.

Buradan hareketle sistem yöneticileri (SY) ya da ev kullanıcıları (EK) kablosuz ağlarında aşağıda verilen önlemleri alırlarsa, pratik olarak kablosuz ağ şifrelerinin kırılması çok zor hale gelecektir. Bazı önlemler her iki kullanıcı profili için de geçerliyken, bazı önlemler daha çok büyük organizasyonlardaki sistem yöneticileri tarafından yapılabilecek hususlardır.

- (SY, EK) Kesinlikle WEP şifreleme algoritması kullanılmamalıdır. Her ne kadar, bazı kablosuz erişim noktası kullanım kılavuzlarında söz konusu saldırılardan etkilenmediği iddia edilse de, yapılan testler sadece sürenin uzadığını göstermektedir.

- (SY, EK) MAC adresi değiştirilebilir olduğundan MAC filtreleme yöntemine güvenilmemelidir.

- (SY, EK) Kablosuz ağın adını saklamak yeterli bir çözüm değildir, tabi ki saldırganların işini zorlaştırmak için uygulanabilir, ancak şunu da unutmamak gerekir ki gizli ağlar bazen saldırganlarda ayrı bir heyecan da yaratmaktadır. Ayrıca kablosuz ağın adı kesinlikle fabrikadan çıkış halindeki isimden farklı olmalı ve şirket ya da kurum adı ile ilgili olmamalıdır.

- (SY, EK) WPA2 şifreleme algoritması kullanılmalıdır. Eğer erişim noktaları buna imkan vermiyorsa, yeni firmware sürümleri yüklenmeli ya da firmware yükseltmelerine izin verilen daha kaliteli kablosuz erişim noktaları kullanılmalıdır.

- (SY, EK) Belirli sürelerde WPA/WPA2 şifreleri değiştirilmelidir ve 12 karakterden uzun şifreler seçilmeli, hatta şifre "!" "@" gibi karakterlerle de desteklenmelidir.

- (SY) Mümkünse RADIUS ve WPA2 kombinasyonu kullanılmalıdır.

- (SY) Erişim kütükleri periyodik aralıklarla incelenmelidir. Bu aynı zamanda sistem yöneticisinin iş tanımında yer almalıdır. Eğer şüpheli hareketler gözleniyorsa şifre değiştirilmeli ve takibe devam edilmelidir.

- (SY) Sistem yöneticisi saldırganların bakış açısından düşünebilmelidir. Güvenlikle ilgili günlük olarak güncellenen sitelere üye olunmalı ve yeni bir açık keşfedildiğinde bunu saldırganla aynı zamanda öğrenmelidir.

6. SONUÇLAR

Kablosuz ağlardaki hızlı yaygınlaşma ve hız artışı, güvenlik önlemlerinin de daha fazla dikkate alınmasını mecburi kılmaktadır. Bu noktada, sistem yöneticilerinin ve ev kullanıcılarının konuyla ilgili olarak bilgi sahibi olmaları ve daha bilinçli davranmaları çok önemlidir. Sistem yöneticilerinin konuyla ilgili eğitimler almaları veya kendilerini yetiştirmeleri mümkündür. Ancak, bilişim teknolojilerine özel ilgisi olanlar hariç ev kullanıcılarının konuyla ilgili olarak bilinçlendirilmeleri oldukça zordur. Bu nedenle, ev kullanıcılarını ilk etapta koruma görevi, kablosuz ağ erişim noktası satan ve İnternet erişimi sağlayan firmalara düşmektedir.

Sistem yöneticisi ve ev kullanıcılarının beşinci bölümde açıklanan güvenlik artırıcı önlemleri almaları faydalı olacaktır. Bunun ötesinde, cihaz üreticisi firmalar tarafından yapılacak; WEP algoritmasını seçilemez duruma getirmek, 12 karakterden kısa WPA şifrelerini kabul etmemek, periyodik olarak kablosuz ağ geçidinin şifresini değiştirmeyi hatırlatmak ve hatta son kullanıcıyı buna zorlamak, basit ama etkili önlemler olacaktır.

Şu da unutulmamalıdır ki, kaba kuvvet saldırılarının en büyük dezavantajı, çözüm hızının saldırgan makinenin işlemci gücüyle sınırlı olmasıdır. Ancak paralel işleme yöntemleriyle bunu hızlandırmak teorik olarak mümkündür. Gelişen teknolojiyle şifre kırma sürelerinin çok aşağılara çekilmesi ihtimal dâhilindedir. Bu nedenle, RADIUS kullanımı gibi bir takım güvenlik önlemlerinin daha da yaygınlaştırılması ve hatta ev kullanıcıları seviyesine indirilmesi güvenlik önlemlerine katkı sağlayacaktır. Güvenlikle ilgili alınabilecek en önemli önlem ise kablosuz ağ kullanıcılarını bilinçlendirmek olacaktır.

KAYNAKLAR

[1] C. Hurley, F.Thornton, R.Rogers, D.Connelly and B. Baker. *Wardriving & Wireless Penetration Testing*, Syngress Publ.Inc., 2007.

[2] B. Cengiz, "*WNA, Wireless Network Analyzer"*, Tezsiz Yüksek Lisans Proje Raporu, Atılım Üniversitesi, Bilgisayar Müh.Böl.,2008.

[3] J. Hopkins School of Public Health, *"History of Wireless",* Archived at http://www.jhsph.edu/wireless/history.html.

[4] M. Frishberg, "*Gates Predicts a Wireless World",* Wired Magazine, Archived at http://www.wired.com/techbiz/media/news/2001/11/48775.

[5] S. Fluhrer, I. Mantin and A. Shamir, *"Weaknesses in the Key Scheduling Algorithm of RC4".* In LNCS Vol.2259, pp.1-24, Springer, 2001.

[6] Wikipedia, "Wired Equivalent Privacy", Archived at http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.

[7] E. Tews, R.-P. Weinmann, and A. Pyshkin, "*Breaking 104 bit WEP in less than 60 seconds",* WISA 2007, pp. 188-202, Jeju Island, Korea, 2007.