TELSİZ YEREL ALAN AĞLARINDA GÜVENLİK SORUNU

Ender YÜKSEL[1] Müjdat SOYTÜRK[2] Tolga OVATMAN[3] Bülent ÖRENCİK[4]

[1,3,4]Bilgisayar Mühendisliği Bölümü
Elektrik-Elektronik Fakültesi
İstanbul Teknik Üniversitesi, 80626, Maslak, İstanbul
[2] Deniz Harp Okulu Komutanlığı, 34942, Tuzla, İSTANBUL

[1]e-posta: ender@cs.itu.edu.tr [2] e-posta: msoyturk@dho.edu.tr
[3] e-posta: ovatman@cs.itu.edu.tr [4] e-posta: orencik@cs.itu.edu.tr

Anahtar sözcükler: Telsiz ağ, WEP, IEEE 802.11, WLAN Güvenliği

ABSTRACT

Wireless Local Area Networks (WLANs) provide cost-effectiveness and flexibility to the network and provide mobility to the network users. However, there are potential problems due to wireless communications and applied security protocols. In this paper, the security mechanisms and protocols for wireless local area networks; WEP and IEEE 802.11i are mentioned, and the security problems related to WLAN are discussed. WLAN attacking experiments has shown that unconscious WLAN management and unconscious usage of WLAN devices cause a great security hazard in the network. The new security protocol for WLANs, IEEE 802.11i protects the network from such security problems.

1 GİRİŞ

Telsiz ağlar, kullanıcılara sunduğu gezginlik imkanı, kablolama maliyetinin olmayışı gibi nedenlerle giderek yaygınlaşmaktadır. Telsiz ağların, gönderim ortamı olarak havayı kullanmasından dolayı, kendine özgü kısıtların yanında, güvenlik sorunu da bulunmaktadır [1, 2].

Telsiz ağlar için geliştirilen güvenlik mekanizması, IEEE 802.11'de sunulan WEP (Wired Equivalent Privacy)'tir [2, 4 - 12]. WEP ile, telli ağlardaki güvenlik seviyesine denk bir güvenlik hedeflenmiştir. Fakat, WEP, telsiz ağ güvenliğini sağlamada (veri bütünlüğü, gizlilik) başarısız olmuştur [5-12]. WEP'teki problemleri gidermek için geçici çözümler önerilmişse de bunlar da başarısız olmuşlardır. Bu sorunu gidermek için IEEE 802.11 Çalışma Grubu tarafından geliştirilen yeni standart, IEEE 802.11i standardıdır [13 - 17].

Bu bildiride, telsiz ağlar için geliştirilen güvenlik yöntemleri, karşılaşılan problemler ve güvenlik saldırıları ile önerilen / geliştirilen çözüm yöntemleri incelenmektedir. WEP'in kırılmasına yönelik saldırılar, uygulamalı olarak gösterilmiştir.

2 TELSİZ AĞ VE ÖZELLİKLERİ

Telsiz ağlar, duraklar (STA - Stations) ve erişim noktaları (AP - Access Points) olmak üzere 2 ana bileşenden oluşmaktadır. Bu mevcut bileşenlere göre telsiz ağlar 2 değişik kipte çalışabilirler. Bunlar, kullanıcının ağdaki bir diğer kullanıcı ile doğrudan iletişimde bulunduğu *tasarsız* (ad-hoc*) kip* ve her kullanıcının (STA) iletişimini erişim noktası (AP) ile / aracılığıyla yaptığı *altyapılı* (*infrastructure) kip*'tir [1-12].

Telsiz ağları oluşturan en küçük yapı bloğu Temel Servis Kümesi (Basic Service Set – BSS)'dir. BSS'ler aynı gönderim ortamını paylaşan ve aynı MAC protokolünü kullanan bir kaç duraktan (STA) oluşmaktadır. Bir BSS ayrı olabileceği gibi erişim noktaları (AP) aracılığıyla bir omurgaya (backbone) bağlanabilir. AP'ler telli ağlardaki köprü görevi gören anahtarlama ürünleri ile aynı görevi görmektedirler. BSS'ler, literatürde geçen hücre (cell) ile eşanlamlıdır. İki veya daha fazla BSS, bir dağıtık sistemle bağlanarak Genişletilmiş Servis Kümesini (Extended Service Set - ESS) oluştururlar. Buradaki dağıtık sistem genellikle bir telli omurga'dır [1].

Telsiz ağlar kullanıcılara birçok kolaylık sağlamasına ve telli sabit ağlara destek olmasına karşın, bu ağların gelişiminde ve kullanımında karşılaşılan bazı kısıtlar ve problemler de vardır.

Bu kısıtların en önemlileri bant genişliği ve enerji ile ilgilidir. İletişim ortamının hava olmasından kaynaklanan problemler de vardır. Yapılan gönderimler, gönderenin erimi içindeki diğer tüm düğümler tarafından alınabilmektedir. Bu özelliğinden dolayı paket çatışması (collision) oluşabilir [1].

Bir diğer problem de güvenlik sorunudur. Yapılan bir gönderimi istenmeyen kişiler de alabilecektir. Gönderimleri yetkisiz kişilerin almasına karşın, sadece adreslenen alıcının anlamlandırabilmesi için şifreleme ve asıllama protokolleri kullanılmaktadır. Fakat kullanılan mevcut protokoller ve yöntemler yetersiz kalmakta ve güvenlik sorunu devam etmektedir.

3 GÜVENLİK PROTOKOLLERİ VE PROBLEMLERİ

Telsiz ağlar için IEEE 802.11 ile tanımlanan standart güvenlik mekanizması WEP (Wired Equivalent Privacy)'dir. WEP ile 3 temel güvenlik hedefi olarak görülen ***gizlilik, erişim kontrolü ve veri bütünlüğü*** sağlanmak istenmiştir.

3.1 WEP

3.1.1 Asıllama

Kullanıcı (STA) veri iletişimine başlamadan önce erişim noktası (AP) ile arasında ilişkilendirilmelidir (association) [5-12]. Ancak ilişkilendirilmiş duraklar veri iletişimi yapabilirler. Bu nedenle ilişkilendirme işleminden önce asıllama (authentication) yapılmalıdır. IEEE 802.11 standardı 2 tip asıllama yöntemi sunmaktadır. Varsayılan ve daha basit olan açık sistem asıllama (Open System Authentication) yöntemidir. Diğer yöntem ise Ortak-Anahtar Asıllama (Shared-Key Authentication) yöntemidir. Bu yöntemde, kullanıcı (STA) ve erişim noktası (AP) arasında paylaşılan bir anahtara göre asıllama yapılır. Böylece, ağa ve ağ kaynaklarına erişim daha güvenli hale getirilmiştir. Fakat, bu asıllama yönteminin kullanılması için WEP'te bu mekanizmanın çalışır duruma getirilmesi gerekmektedir (varsayılan açık sistem asıllama) [5-12].

Asıllama şu şekilde yapılır [5]:

1. İlişkilendirilmek isteyen istemci durak, kimliğini öğrendiği erişim noktasına asıllama isteğini gönderir.

2. Erişim noktası, istemcinin isteğine bir soru mesajı göndererek cevap verir. Bu mesajda, istemcinin, erişim noktasının gönderdiği veriyi şifrelemesi istenir.

3. İstemci, sunucu erişim noktasının gönderdiği açık veriyi, ortak anahtar ile şifreler ve erişim noktasına gönderir.

4. Erişim noktası, simetrik anahtar olan ortak anahtar ile şifrelenmiş veriyi açar. Sorgu mesajında gönderdiği veri ile aynıysa, asıllama işlemini sona erdirmek için istemciye asıllandığını bildirir.

5. Asıllama işleminden sonra istemci ilişkilendirme istek mesajı gönderir. Sunucu erişim noktası, ilişkilendirme cevap mesajı göndererek, ilişkilendirmeyi sağlar [5, 7].

3.1.2 WEP'in elemanları

Anahtar: WEP, asıllama ve şifreleme işlemlerinde kullanmak için bir ortak anahtar kullanır. WEP'te standart anahtar uzunluğu 40 bit'tir. (Farklı üreticiler, 104-bit'lik anahtarlar kullanabilmektedir) [8].

CRC: Açık metin için CRC hesaplanarak, açık metnin sonuna eklenir.

Şifreleme Algoritması: WEP, RC4 akış şifreleme algoritmasını kullanır. RC4 algoritmasını ortak anahtar ile kullanarak, yeni bir tek kullanımlık dinamik akış anahtarı elde eder ve açık metini bu akış anahtarı ile XOR'layarak, CRC ekli şifreli metne ulaşır.

Şifre Çözme Algoritması: Şifre çözme algoritması, şifreleme algoritması ile aynıdır. RC4 algoritmasını ortak anahtar ile kullanarak, tek kullanımlık dinamik akış anahtarı elde eder ve şifreli metni bu anahtar ile XOR'layarak, CRC ekli açık metni bulur.

İlklendirme Vektörü (IV – Initialization Vector): Şifreleme işlemi için kullanılan tek kullanımlık akış şifresini elde ederken, RC4 algoritmasına ortak anahtar ile beraber ilklendirme vektörü de parametre olarak girer. Her gönderilecek paket için ayrı IV kullanılır. Böylece her paket ayrı tek kullanımlık anahtar ile şifrelenerek gönderilir.

3.1.3 Anahtar Dağıtımı

WEP'te anahtar yönetim mekanizması yoktur. Ortak anahtarın, bir şekilde kullanıcılar arasında önceden temin edildiği varsayılır. IEEE 802.11 standardı, anahtarın önceden paylaşıldığını kabul eder [5-12].

3.1.4 WEP Şifreleme Algoritmasının Çalışması

WEP şifreleme algoritması şu şekilde çalışmaktadır:

1. 24 bit'lik ilklendirme vektörü, 40 bit'lik gizli anahtara (ortak anahtar) eklenir. Oluşan bu yeni anahtar (64 bit), RC4 algoritmasına girdi olacaktır. Bu şekilde, her kullanımda, RC4 algoritmasına farklı bir anahtar girecektir [5-12].

2. Birinci adımdan gelen 64-bit anahtar RC4 algoritmasına girdi olarak aktarılır. RC4 algoritması, sahte rastgele sayı üreteci ile bir akış anahtarı elde eder. Bu anahtarın uzunluğu, girdi parametresi kadardır (64 bit).

3. Açık metin veri bütünlüğü sağlamak için veri bütünlüğü kontrol algoritmasına sokularak, sağlama bitleri (checksum - CRC) elde edilir. Bu sağlama bitleri, açık metnin sonuna eklenir.

4. Üçüncü adımdan gelen veri vektörü (veri + sağlama bitleri (CRC)), ikinci aşamadan elde edilen akış şifresi ile XOR'lanarak şifrelenir. Böylece şifreli metin elde edilir.

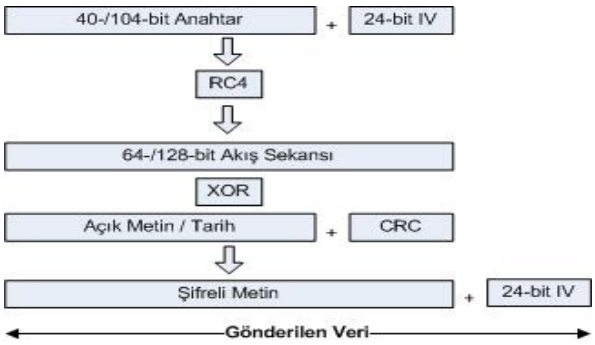
5. IV (ilklendirme vektörü), şifreli metnin başına eklenerek telsiz ortamdan gönderilir (Şekil 1).

3.1.5 WEP'in Zayıflıkları

WEP 'in açıkları ile ilgili birçok makale ve teknik rapor yayınlamıştır [5 –12]. IEEE 802.11 Çalışma grubu da, WEP'in zayıflıklarını kabul etmiş ve çözüm önerileri ile birlikte yeni bir protokol geliştirmiştir. WEP'in bu açıkları, saldırganlar için aktif veya pasif saldırılar düzenlemesine imkan vermektedir. Herbir saldırı, frekans bandını dinleme sonucu elde edilen bilgilere göre yapılır.

WEP'in kullanılması IEEE 802.11'de seçime bağlıdır. Varsayılan (default) açık sistem asıllamadan sonra

veri iletişimine geçilir. Eğer WEP opsiyonu seçilmemişse, şifreleme yapılmaz. Metinler açık olarak gönderilir.



Şekil 1 Açık metinin şifrelenmesi ve gönderilmesi

IV Çatışması

WEP, RC4 algoritmasına parametre olarak ortak anahtar ile beraber IV'ü geçirmektedir. IV değeri her paket için değişmektedir. Başlangıçta sıfır değerindedir ve her işleme girdiğinde değeri bir artar. 24 bit uzunluktaki IV, 2^{24} farklı değer alır. Böylece RC4 algoritmasından 2^{24} tane farklı akış şifresi elde edilmiş olunur.

RC4 algoritması bir Vernam şifrelemesidir. Bu algoritma ile üretilen anahtarlar tek kullanımlık anahtarlar olduğundan kırılması imkansızdır. Fakat WEP'te bu durum söz konusu değildir. WEP'te ortak anahtar ve IV ile 2^{24} farklı akış şifresi elde edilmektedir. Fakat, her bir paket farklı bir akış şifresi ile şifrelenir. 2^{24} paket sonra bütün IV değerleri, dolayısıyla bütün akış şifreleri kullanılmış olunacaktır. Ilk 2^{24} çalıştırmadan sonra RC4 algoritmasının her çalıştırılışında aynı akış şifreleri üretilecektir. Meşgul bir erişim noktası 11Mbps veri hızıyla sürekli olarak 1500-byte uzunlukta paketler gönderdiğinde, aynı akış şifresi ile şifrelenmiş mesajların oluşması için geçen süre 5 saattir. Her iterasyonda artan IV yerine, IV değerler kümesinden rastgele değerler alınması bu durumu engelleyemeyecek, "doğum günü" (birthday) saldırılarıyla, aynı şifre ile şifrelenmiş mesajlar elde edilebilecektir [5-12].

Aynı akış şifresi ile şifrelenen mesajlar elde edildiğinde, istatistiksel analiz yöntemleri kullanılarak açık metin elde edilebilir.

RC4 Algoritmasının Zayıf Anahtar Üretmesi

WEP'teki bir diğer açık da, RC4 algoritmasından kaynaklanmaktadır. İlk olarak Fluhrer, Mantin ve Shamir tarafından yayınlandığı için, bu açıklıktan faydalanarak gerçekleştirilen saldırılar bu kişilerin isimleriyle anılmaktadır.

RC4 algoritmasının anahtar üretim algoritması (key scheduling algorithm) zayıf akış anahtarları üretmektedir. Bu zayıf anahtarlar tespit edilerek, anahtarların ilk önce başlangıç bitleri ve daha sonra ardışık şekilde diğer kısımları çözülebilmektedir.

Yetkisiz Erişim Noktası (Rogue AP)

Bir yetkisiz erişim noktası (AP), hassas bilgilere erişmek isteyen kötü niyetli kişilerin kullandığı ya da yeterince güvenlik bilgisi olmayan yöneticilerin kendi veya şirket faydası için ofislerine kurdukları AP'lerdir. Her iki durumda da, bu yetkisiz AP'ler güvenliği tehdit etmektedir.

Yetkisiz AP'ler, karışıma (interference) neden olacaklar ve sistem başarımını düşüreceklerdir. Daha da kötüsü, yetkisiz kişilerin (saldırgan) ağa erişmesine neden olmaktadırlar. Telsiz ağ durakları, ilişkilendirildikleri (associated) AP'den ayrılıp, kendilerine daha yakın olan bir yetkisiz AP ile ilişkilenebilirler. Bu durum WEP'in etkin duruma getirilmemesinde oluşur. Yetkisiz AP'den faydalanan bir saldırgan, yetkisiz AP ile ilişkilenen diğer ağ duraklarına (PC) erişebilir. Yetkisiz AP'nin telli ağ tarafına da bağlı olması, saldırganların telli ağa da erişmesini sağlamaktadır.

ARP Yanıltması (ARP Spoofing)

Diğer bir ismi, ARP bozulması (ARP poisoning) olan ARP yanıltması (ARP spoofing), saldırganların, ağdaki paketleri ele geçirmek veya ağa zarar vermek için kullandıkları bir yöntemdir. Durakların geçici olarak tuttukları MAC ve IP adres çiftlerinin değiştirilmesi yöntemini kullanır.

Saldırganlar, ağda sahte ARP bildirim (notification) mesajları yayınlar. Birçok sahte ARP mesajının gönderilmesi, ağ elemanlarının yanlış adreslere veri göndermesine neden olmakta, böylece bu mesajların bir kısmı saldırganın eline geçmektedir. Bu sayede saldırgan, seçeceği bir kurban hakkında bilgiye sahip olur. Böylece, "ortadaki adam" (man-in-the-middle) saldırısı başta olmak üzere, farklı tipte saldırılar gerçekleştirilebilir. Saldırgan, ağa zarar verebileceği gibi, ağ trafiğini izleyebilir ve ağ kullanıcılarının şifrelerini ele geçirebilir.

3.1.6 Gerçekleştirilen Saldırılar

IEEE 802.11'deki yukarıda belirtilen zayıflıklardan faydalanarak, pasif ve aktif saldırılar düzenlenebilmektedir.

Pasif saldırılar

Pasif saldırılar, WEP'te IV çatışmasından faydalanarak, iki veya daha fazla şifreli metin ele geçirilmesi ve metinlerin içeriklerinin elde edilmesidir. Ayrıca, birçok şifreli metnin elde edilmesi ortak anahtarın saldırgan tarafından bulunmasına yardımcı olacaktır.

Aktif Saldırılar

Aktif saldırılar, tekrar saldırıları (replay attacks) ve mesajın içeriğini değiştirerek yapılan saldırılardır. WEP, mesaj bütünlüğünü korumak için CRC kullanır. Fakat, kullanılan CRC doğrusal bir yöntem olduğundan, metinde yapılan n bitteki değişiklik için CRC'de hangi bitin değişeceği hesaplanabilmektedir.

Bir diğer saldırı da, gönderilen mesajların başına eklenen 802.11 MAC başlığının açık olarak gönderilmesinden faydalanılarak gerçekleştirilir. Bu başlıkta, göndericinin ve alıcının adresleri açık bir şekilde bulunmaktadır. Saldırgan, iletişimde olan bir erişim noktası ile bir kullanıcı arasında girdiğinde elde ettiği mesajların 802.11 başlık kısmındaki adresleri istediği bir adresle değiştirebilir. Böylece, şifreli mesajlar istediği adrese gidecektir. Alıcı eğer telli bir ağdaysa, mesajların şifresi çözülerek açık olarak gönderilecektir. Saldırgan araya girdiğinde, mesajlara kendi sabit ağ adresini yazdığında mesajın hem açık halini, hem de şifreli halini elde etmiş olacaktır. ARP yanıltması, bu saldırıya örnektir.

3.1.7 WEP Zayıflıklarına Karşı Alınan Yöntemler

WEP2 : IEEE 802.11 tarafından WEP'in bir uyarlaması geliştirilmiştir. IV, 24 bit'ten 128 bit'e çıkarılmış ve Kerberos V desteği sağlanmıştır. Fakat, bunlar WEP'in zayıflıklarından kurtulmasına yetmemiştir.

Gelişmiş WEP anahtarı: Kullanılan ortak anahtar 40 bit'ten 104 bit'e çıkarılmış, fakat bu yaklaşım da WEP'in mevcut açıklarını gidememiştir.

Dinamik WEP anahtarı: Cisco ve Microsoft, sürekli olarak kullanılan ortak anahtar yerine dinamik anahtarlar kullanmışlardır. Dinamik anahtarlar, erişim noktalarına dağıtılarak, ağı dinleme yöntemi ile trafik analizi yapılması engellenmiştir. Fakat bu yaklaşım, sadece birkaç üreticinin kendilerinin kullandığı bir yaklaşımdır. Ayrıca, bir sistem yöneticisinin anahtar dağıtımına ihtiyaç duymaktadır. Bilinen bir saldırı görülmemiştir.

VPN Uygulamaları: VPN uygulamaları ile WEP güvenli hale getirilmeye çalışılmıştır.

IEEE 802.11i: WEP'e alternatif olarak ve WEP'teki problemleri gidermesi için geliştirilmiştir. Bu standart, WEP'ten her yönüyle farklıdır.

3.2 Yeni Güvenlik Protokolü: IEEE 802.11i

WEP'in açıklarını gidermek için IEEE 802.11 Çalışma Grubu tarafından yeni bir protokol geliştirilmiştir [6, 13-16]. Bu protokol ile;

- Kimlik asıllama (authentication)
- Şifreleme (encryption)
- Yetkilendirme (authorization)
- Anahtar Yönetimi (key management) hedeflenmiş ve
- korunmamış bilgilerin gönderilmemesi / alınmaması,
- mesajın kaynağının asıllanması (taklidi önler),
- mesajlara sıra no konması (replay saldırı tespiti),
- her paket için şifreleme yapılmaması (şifrelemeyi gereksiz yapmayı engeller),
- kaynak ve varış adreslerinin korunması,
- gizlilik ve mesaj bütünlüğü için bir güçlü şifreleme algoritması kullanılması,
- QoS gelişmelerine uyum sağlama (IEEE 802.11e ile) yoluna gidilmiştir.

IEEE 802.11i standardı, bu bağlamda veri güvenliği için yeni bir şifreleme algoritması kullanmakta, yetkisiz kullanıcıların ağa erişimini engellemek için asıllama sunucusu ile asıllama yapmakta ve anahtar yönetimini dinamik bir şekilde gerçeklemektedir. IEEE 802.11i, iki katmandan oluşmaktadır. Alt katmanda, gelişmiş şifreleme algoritmaları (TKIP ve CCMP) bulunmakta, üst katmanda ise kimlik asıllama ve anahtar dağıtımı için 802.1x yer almaktadır.

Kullanıcılar ağ kaynaklarına erişmeden önce asıllanmakta, asıllama işleminden sonra, üretilen oturum anahtarları dağıtılmakta ve bu anahtarlar kullanılarak üretilecek yeni anahtarlar ile güvenli veri transferi yapılmaktadır (Şekil 2).

Şekil 2 Kullanıcı asıllama ve anahtar yönetimi

3.2.1 Asıllama

IEEE 802.11i standardı, karşılıklı asıllama için 802.1x EAP tabanlı asıllamayı uygulamaktadır. 802.1x telli ağlar için geliştirilmesine karşın telsiz ağlar için de kullanılmaktadır. Bu standart, istemci ile erişim noktası arasında bir asıllama sunucusu (authentication server) kullanarak asıllama ve port-tabanlı erişim kontrolü sağlamaktadır. 802.1x standardı 3 elemandan oluşmaktadır.

- *Kullanıcı (supplicant):* asıllama isteğinde bulunandır.
- *Asıllama Sunucusu (authenticaton server):* RADIUS gibi asıllama hizmetleri için bir sunucudur.
- *Asıllayıcı (authenticator):* kullanıcı ile asıllama sunucusu arasındaki birimdir. Genellikle erişim noktasıdır (AP).

Asıllama işlemi birkaç adımdan oluşur (Şekil 3) [14]:

1. Kullanıcı, asıllayıcıya bağlantı talebinde bulunur. Asıllayıcı, bağlantı isteğini alınca, tüm portları kapalı tutar fakat kullanıcı ile arasında bir port açar.

2. Asıllayıcı, kullanıcıdan kimliğini (identity) ister.

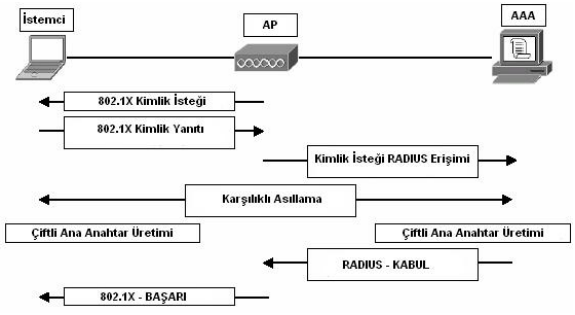
3. Kullanıcı kimliğini gönderir. Asıllayıcı kimlik bilgisini bir asıllama sunucusuna gönderir.

4. Asıllama sunucusu, kullanıcının kimliğini asıllar. Asıllandığında, KABUL (ACCEPT) mesajı

asıllayıcıya gönderilir. Asıllayıcı, kullanıcının portunu yetkilendirilmiş duruma getirir.

5. Kullanıcı, asıllama sunucusundan, onun kimliğini ister. Asıllama sunucusu, kimlik bilgisini kullanıcıya gönderir.

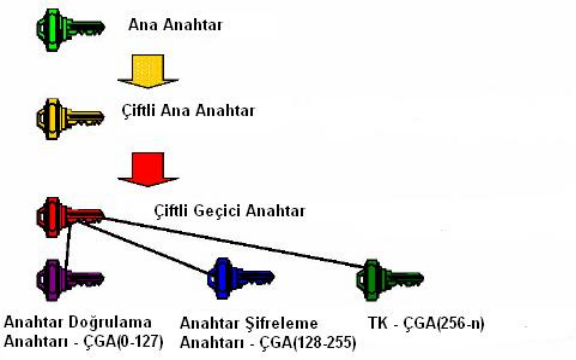
6. Kullanıcı, asıllama sunucusunun kimliğini asılladığında, veri trafiğe başlanır.



Şekil 3 IEEE 802.1x ile asıllama işlemi [14]

3.2.2 Anahtar Yönetimi

802.1x ile anahtar yönetimi de sağlanmaktadır [14]. Kullanıcı ve asıllama sunucularının Ana Anahtarı (Master Key - MK) vardır. Bu anahtar kullanılarak, diğer anahtarlar üretilir. Anahtar üretimi hiyerarşik bir şekilde yapılır. Anahtar üretimi, Şekil 4'te görülmektedir. Asıllama işlemi sonunda, hem kullanıcı tarafında hem de asıllama sunucusu tarafında MK'lerden Çiftli Ana Anahtar (Pairwise Master Key - PMK) üretilmektedir. PMK, alt seviyede şifrelemede kullanılacak anahtarları üretmede kullanılmaktadır. Asıllama işleminden sonra, asıllama sunucusu (AS) ürettiği PMK'yı asıllayıcıya (AP) gönderir. Böylece hem kullanıcı hem de asıllayıcı PMK'dan alt seviyede gerekli şifreleri üretebilirler.



Şekil 4 Anahtar üretimi.

Asıllama sunucusunun olmadığı durumlarda, yani ev kullanıcıları veya asıllama sunucusuna gerek olmayan küçük işyerlerinde yukarıdaki işlemler, asıllama sunucusu olmadan yapılacaktır. PMK ise kullanıcı ve erişim noktası (AP) tarafından elle girilir. Böylece alt seviyede kullanılacak anahtarlar üretilebilir. Asıllama sunucusu (AS) kullanmaktan tek farkı, önceden dağıtılan anahtar kullanımıdır.

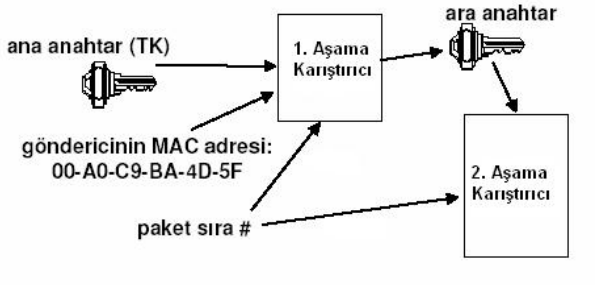
Bu anahtarlardan sadece TK (Temporal Key), şifrelemede dolaylı olarak yer almaktadır (TK'dan geçici tek kullanımlık anahtarlar üretilerek [14]).

3.2.3 Şifreleme

Anahtarların dağıtımından sonra güvenli veri transferi başlayabilir. 802.11i 'de üst katman asıllama ve anahtar dağıtımını, alt katman ise şifrelemeyi sağlamaktadır. Şifreleme için IEEE 802.11i'de AES şifreleme algoritması kullanılır. Bu algoritmayı kullanan şifreleme protokolü CCMP (Counter-Mode / CBC-MAC Protocol)'dir. CCMP'de AES'i kullanabilmesi için ek donanıma ihtiyaç vardır. Yeni çıkacak ürünlerde bu özelliği taşıyan donanım bulunacaktır. Fakat IEEE 802.11i protokolünü, kullanılan ve şu anda piyasada bulunan ürünlerin mevcut donanımında değişikliğe gerek duymadan, sadece yazılımsal değişiklik ile uygulamak için, bu katmanda ikinci bir şifreleme protokolü TKIP (Temporal Key Integrity Protocol) önerilmiştir [14].

TKIP (Temporal Key Integrity Protocol)

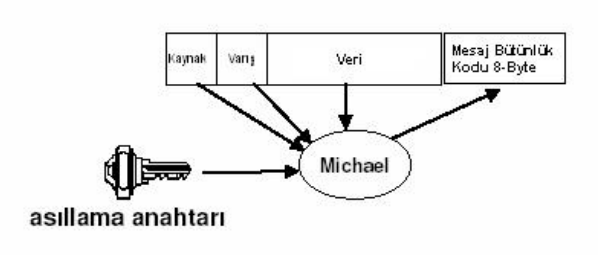
TKIP protokolü, mevcut ürünlerin donanımında herhangi bir değişiklik yapmadan, sadece yazılımsal değişiklik yaparak güvenli veri transferini sağlamak maksadıyla geliştirilmiştir. Bu nedenle, altta WEP'i kullanır. WEP'in açıklarını ve zayıflıklarını yok edecek şekilde güvenli veri transferini gerçekleştirmek için önlemler alınmıştır. Bu nedenle, WEP'in etrafında bir kabuk görevi görür. Bu nedenle de, CCMP'ye göre daha fazla işlem yaptığından, güvenlikten çok kullanıcılara zorluk çıkardığı görüşü hakimdir [14].



Şekil 5 TKIP'de anahtar üretimi

TKIP'de ilklendirme vektörü (IV) 48 bit'e çıkarılmıştır. IV, hem paketlere sıra numarası vermek, hem de her paket için tek kullanımlık anahtar üretmede kullanılmaktadır. Paketlere sıra numarası verilmesi tekrar (replay) saldırılarını önlemek içindir. Ayrıca sırasız gelen paketler de alıcı tarafından atılmaktadır. 48 bit IV ve aynı TK ile üretilecek tek kullanımlık anahtarlar ancak yaklaşık 100 yıl sonra tekrarlanmaktadır. Bu nedenle WEP'teki IV çatışmasından kaynaklanan saldırılar önlenmektedir. TKIP'de tek kullanımlık anahtar üretimi Şekil 5'de gösterilmiştir.

Her paket için kullanılan IV değeri TKIP'de değişmektedir. Bu yaklaşım da zayıf anahtar üretiminden faydalanan saldırıları önlemektedir.



Şekil 6 "Michael" algoritması

TKIP'de veri bütünlüğünü sağlamak için "Michael" algoritması kullanılmaktadır. Michael – Mesaj Bütünlük Kodu (Message Integrity Code – MIC), kaynak ve varış MAC adreslerini ve veriyi alarak sağlama bitleri (checksum) oluşturur. Bu sağlama bitleri, verinin sonuna şifrelenerek eklenir. Bu yöntem, mesaj içeriğinin değiştirilmesini önler. Ayrıca WEP'in tersine, alıcı ve göndericinin adresleri açık bir şekilde gönderilmez. Michael algoritması Şekil-6'dadır.

CCMP (Counter-Mode / CBC-MAC Protocol)

CCMP, IEEE 802.11i protokolunun yeni şifreleme yöntemidir. Gelişmiş ve güçlü bir şifreleme algoritması olan AES (Advanced Encryption Standard)'i kullanır. AES şifreleme birçok farklı kipte kullanılabilir. IEEE 802.11i standardı, AES 'iCBC-MAC ile sayaç (counter) kipini kullanır. Anahtar uzunluğu 128 bit'tir. CCMP protokolünü kullanmak, IEEE 802.11i'de zorunludur. IEEE 802.11i'de AES kullanılması, yeni çıkacak ürünlerde ek donanım gerektirmektedir.

CCMP'de de IV kullanılır ve uzunluğu 48 bit'tir. IV, paketlere sıra numarası vermek için kullanılır. Bu paket numarası daha sonra, diğer bilgilerle beraber hem mesaj bütünlük kodu (MIC) oluşturmak, hem de paketi şifrelemek için AES şifreleme algoritmasında parametre olarak kullanılır.

3.2.4 IEEE 802.11i'nin Sağladıkları

1. IEEE 802.11i standardı, WEP'te olmayan anahtar yönetimini sağlamıştır. Anahtar yönetimi hiyerarşik bir şekilde sağlanmaktadır.

2. Kullanıcılar, bir asıllama sunucusu tarafından asıllanmakta, aynı zamanda kullanıcılar da sunucuyu asıllamaktadır (karşılıklı asıllama – mutual authentication). Asıllama, IEEE 802.11i'de zorunludur.

3. Asıllama için kullanılan IEEE 802.1x protokolü, üst katman asıllama protokollerini de desteklemektedir. Asıllama sunucusu olarak en yaygın kullanılan RADIUS sunucusudur. Sunucu seçimi ve üst katmanlarda kullanılacak asıllama protokolleri IEEE 802.11i standardına dahil değildir.

4. Güçlü bir şifreleme algoritması olan AES'i kullanmaktadır. Böylece daha güvenilir şifreleme sağlanmıştır.

5. Veri bütünlüğü, WEP'e göre daha güvenilir hale getirilmiştir.

6. Ayrıca, dolaşımı (roaming) desteklemektedir.

4 UYGULAMA

Deneysel çalışmada 802.11 telsiz ağların önemli sorunlarından olan "Yetkisiz Erişim Noktası", "ARP Yanıltması" ve "WEP Anahtarı Kırma" problemleri incelenmiştir.

4.1 Çalışma Ortamı

Deneysel çalışmada gerçek bir telsiz ağ ortamından yararlanılmıştır. Çalışmanın yapıldığı İstanbul Teknik Üniversitesi Elektrik-Elektronik Fakültesi telsiz ağı, 18 adet 802.11b telsiz erişim noktası içermektedir. Kullanıcılar, taşınabilir bilgisayarları ile fakültenin erişim noktalarının eriminde bulunan herhangi bir noktadan internete girebilmektedirler. Deneysel çalışma için, birinde dahili Intel pro 2100 diğerinde pcmcia D-link airplus 802.11b telsiz ağ kartı bulunan Windows XP işletim sistemli iki taşınabilir bilgisayar, harici D-link dwl 120+ 802.11b telsiz ağ kartı bulunan Fedora Core 3 işletim sistemli bir masaüstü bilgisayar, bir D-link dwl 900AP+ 802.11b erişim noktası ve bir CentrCom dağıtıcı (hub) kullanılmıştır.

4.2 Yetkisiz Erişim Noktası Problemi

Şekil 7'de görülen yapıda, telsiz ağ A, WEP veya WPA kullanılmayan bir ağdır. Kullanıcılar bu ağa, gerekli telsiz ağ donanımına sahip herhangi bir bilgisayarla erişebilmektedirler. Telli ağ B ise, dışarıdan erişime kapalı, güvenli gözüken bir yerel alan ağıdır. Deneyin bu aşamasında, güvensiz bir telsiz ağın, güvenli bir telli ağ için nasıl bir tehlike yarattığı gözlenmiştir.

Bu çalışmada önce telsiz ağ kartına sahip taşınabilir bilgisayarlar ile farklı noktalardan A telsiz ağına girilerek ağın durumu ve yapısı hakkında bilgi toplanmıştır. Telsiz ağ ile ilgili bilgi almak için yardımcı yazılımlara gerek olmadan işletim sistemindeki araçların kullanımı yeterlidir. Yapılan ön çalışmalar sonucu DHCP (Dynamic Host Configuration Protocol) sunucusu adresi, erişim noktaları adresleri, istemci bilgisayarlara atanan ağ adresleri, erişim noktalarının SSID'leri (Service Set Identifier) ve erişim noktalarında uygulanan güvenlik önlemleri gibi ağ hakkındaki gerekli bilgiler elde edilmiştir. Benzer bir çok ortamda olduğu gibi WEP protokolünün etkinleştirilmediği ve hiçbir SSID'nin değiştirilmeyip, varsayılan değeriyle bırakıldığı anlaşılmıştır. Toplanan bu bilgiler, kurulacak olan yetkisiz erişim noktası için kullanılmıştır.

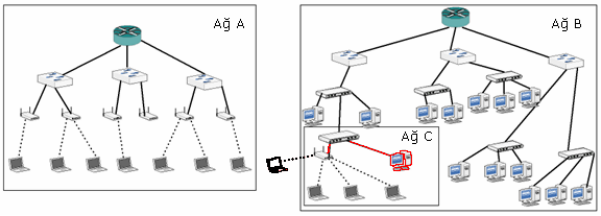
Telli ağ B'deki herhangi bir kullanıcının, herhangi bir amaçla, ancak ağ yöneticisinden habersiz olarak, telli ağa bir telsiz erişim noktası yerleştirmesi durumunda,

A telsiz ağındaki kötü niyetli bir kullanıcı için B telli ağına erişebilme şansı doğmaktadır.

Yetkisiz erişim noktası probleminin denenmesi için, B telli ağındaki bir noktaya dağıtıcı eklenerek, bu dağıtıcıya bir telsiz erişim noktası bağlanmıştır. Bu telsiz erişim noktası, yeni telsiz ağ kullanıcılarına hizmet verecek şekilde ayarlanmıştır.

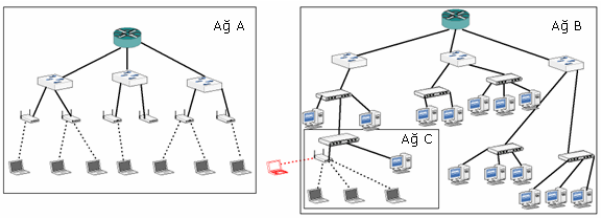
Telsiz erişim noktası aynı zamanda bir DHCP sunucusu olarak çalışmaktadır ve istemcilere atayabileceği ağ adresleri, erişim noktasının üzerinde tanımlanmıştır. Telsiz erişim noktasının, kendisine bağlanan istemcilere atayacağı IP adresleri, B telli ağına ayırılmış adreslerdendir.

Bu şekilde bir yapıda olabilecek iki ciddi açık, deney yoluyla gözlemlenmiştir.



Şekil 7 Yetkisiz Erişim Noktası ile paket yakalama

Bunlardan ilki, B ağına yetkisiz erişim noktası bağlayan kullanıcının kötü niyetli olmasıdır. Bu kullanıcının, yetkisiz erişim noktasına A ağındaki telsiz erişim noktalarıyla aynı veya benzer bir SSID vermesi durumunda, A ağına bağlandığını zanneden fakat gerçekte B ağındaki yetkisiz erişim noktasına bağlanan herhangi bir kullanıcının tüm trafiğini dağıtıcı üzerinden izlemesi ve bu trafiğe müdahale etmesi mümkündür. Deneyde bu yapı gerçek telsiz ağ ortamında denenerek Ethereal[18] paket çözümleyici yazılımı ile dağıtıcı üzerinden kurbanların paketleri yakalanmıştır (Şekil 7).



Şekil 8 Yetkisiz Erişim Noktası üzerinden saldırı

İkinci açık ise yetkisiz erişim noktasına bağlanan kullanıcının B ağına da girebilmesidir. Normal şartlarda B ağına erişme hakkı olmayan saldırgan, yetkisiz erişim noktası üzerinden B ağına sızmış olacaktır ve ağın içinden saldırı yapabilecektir (Şekil 8).

Böyle bir saldırıda, yetkisiz erişim noktasından ağ yöneticisinin haberi olmaması, saldırının tespitini ve saldırıyı engellemeyi zorlaştıracaktır.

4.3 ARP Yanıltması Problemi

Telsiz ağlara özgü olmayan bu problem, önceki problemle ilişkilendirilerek deneysel çalışma yapılmıştır. Önceki deneyde, telsiz ağ'a girebilen saldırgan, yetkisiz erişim noktası üzerinden telli ağda ulaşamayacağı bir ağa da erişebiliyordu.

Yetkisiz erişim noktası probleminden faydalanıp B ağına sızan saldırganın, B ağındaki herhangi bir bilgisayara veya bilgisayarlara saldırmak için kullanabileceği etkili yöntemlerden biri ARP yanıltması problemidir. Herhangi bir kurbanın veri iletimini izlemek veya yönlendirmek isteyen bir saldırgan, bunu kurbana kendini ağ geçidi (gateway) gibi göstererek yapabilir.

Bu problem windows ve linux tabanlı sistemlerde ayrı ayrı denenerek görülmüştür. Yetkisiz erişim noktası üzerinden telsiz iletişim kurularak B ağına girilmiş ve B ağındaki açık bilgisayarlardan rastgele seçilen kurban bilgisayarların ARP tablolarında bulunan ağ geçidinin MAC adresinin saldırgan bilgisayarın MAC adresi olacak şekilde değiştirilmesi sağlanarak kurban yanıltılmıştır. Deneyde WinArpSpoof [19] adlı yardımcı bir yazılım kullanılmıştır. Bu yazılımın sahte arp paketleri yaratıp kurbana göndermek gibi basit ama etkili bir görevi vardır.

4.4 Wep Anahtarı Kırma Problemi

WEP'in etkinleştirilmemesi ciddi bir güvenlik açığı olmakla birlikte, etkinleştirilmesi de bu açığı kapatmaya yetmemektedir.

Çalışmanın bu aşamasında yeni bir telsiz erişim noktası kurulup, bu erişim noktasında WEP etkinleştirilmiş ve bir kurban kullanıcının bu erişim noktasına telsiz ağ kartı ile bağlanması sağlanmıştır. Saldırgan kullanıcı ise telsiz ağ kartı ile havadaki paketleri yakalamakta ve WEP anahtarını elde etmeye çalışmaktadır. Bu çalışma için Fluhrer-Mantin-Shamir [20] (FMS) saldırısını gerçekleyen AirCrack [21] ve AirSnort [22] gibi, Linux tabanlı sistemlerde çalışan yazılımlar kullanılmıştır. Telsiz ağda paket yakalamak için ağ donanımının, izleme (monitor) kipinde çalıştırılması gerekmektedir. Her donanım bu kipte kolaylıkla çalışamadığından sözü geçen yazılımlar donanıma bağlıdır ve dolayısıyla pratikte WEP anahtarı kırmak isteyen saldırganın donanımının uygun olmasına dikkat etmesi gerekmektedir.

5 SONUÇ

Telsiz ağlar, kullanıcılara sunduğu imkanlardan dolayı giderek yaygınlaşmaktadır. Telsiz ağlar, gönderim ortamındaki verilere herkes tarafından erişilebileceği için saldırılara açıktır. Telsiz ağlar için oluşturulan ilk güvenlik mekanizması WEP'tir. WEP'in güvenli olmadığı bir çok makale ve teknik raporda yayınlanmıştır.

Gerçeklenen uygulamalar ile de WEP'in güvenli olmadığı, bilinçsiz / dikkatsiz ağ yönetimi nedeniyle, aktif ve pasif saldırılara açık olduğu görülmüştür.

IEEE 802.11 tarafından yeni Telsiz ağ güvenlik protokolü, IEEE 802.11i'dir. Bu protokol ile WEP'te görülen zayıflıklar ve açıklar giderilmiş ve güvenli veri iletişimi sağlanmıştır.

6 KAYNAKÇA

[1] Stallings W., Data & Computer Communications, 6th Ed., Prentice Hall, 2000.

[2] Tanenbaum A., Computer Networks, 4th Ed., Prentice Hall, 2002.

[3] Çölkesen R., Örencik B., Bilgisayar Haberleşmesi ve Ağ Teknolojileri, 4. Basım, Papatya Yay., 2003.

[4] Nichols R. K., Lekkas P. C., Wireless Security: Models, Threats, and Solutions, McGraw-Hill, 2002.

[5] Arbaugh W.A., Shankar N., Wan Y.C.J., Your 802.11 Wireless Network has No Clothes, http://www.cs.umd.edu/~waa/wireless.pdf, March 2001.

[6] Wong S., The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards, http://www.sans.org/rr/papers/68/1109.pdf, May 2003.

[7] Craiger J. P., 802.11, 802.1x, and Wireless Security, http://www.sans.org/rr /papers/68/171.pdf, SANS Institute, June 2002.

[8] Walker J. R., Unsafe at Any Key Size: An Analysis of the WEP Encapsulation, http://www.dis.org/wl/pdf/unsafe.pdf, Oct. 2000.

[9] Stubblefield A., Ioannidis J, Rubin A. D., Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, AT&T Labs Technical Report TD-4ZCPZZ, Aug. 2001.

[10] Borisov N., Goldberg I., Wagner D., Intercepting Mobile Communications: The Insecurity of 802.11, MOBICOM 2001.

[11] Psion Teklogix, 802.11 WLAN Security, http://www.psionteklogix.com/assets /downloadable/80211_Security.pdf, Nov., 2003.

[12] Tyrell K., An Overview of Wireless Security Issues, http://www.sans.org /rr/papers/68/943.pdf, SANS Institute 2003.

[13] CISCO Systems, Wireless LAN Security (Overview), 2001.

[14] Eaton D., Diving into the 802.11i Spec: A Tutorial,http://www.commsdesign.com/design_library /cd/hn/OEG20021126S0003, Nov. 2002.

[15] Loeb L., Roaming Charges: Are You Ready For 802.11i?,http://www.106.ibm.com/developerworks/library/wi-roam19.html, IBM, Feb. 2004.

[16] White Paper, A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless SecuritySuite,http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf, CISCO Systems, 2002.

[17] Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices, Draft, NIST Special Publication 800-48.

[18] Ethereal, Network Protocol Analyzer, http://www.ethereal.com/.

[19] Next Security, Windows ARP Spoofer, http://www.nextsecurity.net/products/winarpspoof/WinARPSpoof.htm

[20] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the key scheduling algorithm of RC4. In Eighth Annual Workshop on Selected Areas in Cryptography, Toronto Canada, Aug. 2001.

[21] Christophe Devine, aircrack WEP key cracker, http://www.cr0.net:8040/code/network/aircrack/.

[22] The Shmoo Group, AirSnort wireless LAN tool, http://airsnort.shmoo.com/.