Wi-Fi Güvenliği ve Wi-Fi Tehditleri

Öner Ziya Baş
Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Siber Güvenlik Yüksek Lisans
onerziya@gmail.com

Mayıs 2021

Öz

Çevrimiçi ürün ve hizmetlerin yaygınlaşması ve büyük kurumların buna öncülük etmesi hayatımızı büyük oranda kolaylaştırıyor. Verilerimizin güvende olduğunu düşünüyoruz. Aksi halde başta sağlık, finans vb. olmak üzere birçok değerli verimizi eskiden olduğu gibi kullanmaya çalışırdık. Bununla birlikte son günlerde veri sızıntıları vb. veri ihlallerini çok sık duyuyoruz. Birinin (veya bir grup kişinin) büyük kurumların bile koyduğu güvenlik önlemlerini aşarak verilerimize karşı bir tehdit oluşturduğunu görüyoruz ve bu da güvenimizi sarsabiliyor. Sizlerin de bildiği gibi bir zincirin en zayıf halkası kadar güvendeyiz. Bu zincirin halkalarından biri de Kablosuz Ağlardır. Bu çalışmadaki amacımız kablosuz yerel ağlarla ilgili frekans, kanal, topoloji, kimlik doğrulama çeşitleri vb. hakkında bilgi paylaşmaktır. Ayrıca Wi-Fi (Wireless Fidelity - Kablosuz Bağlantı Alanı) güvenliğine yönelik yapılan saldırılara dair alabileceğimiz önlemler ve daha önceden yapılan saldırılara da değineceğiz.

Anahtar kelimeler: kablosuz ağlar, wlan, wireless, wifi

Wi-Fi Security and Wi-Fi Threats

Öner Ziya Baş
Marmara University, Institute of Science, Cyber Security Master's Degree
onerziya@gmail.com

May 2021

Abstract

The widespread use of online products and services and the pioneering of large institutions make our lives easier. We think our data is safe. Otherwise, health, finance, etc. We would try to use our many valuable data as we used to. However, we hear about data breaches very often lately. We see that someone (or a group of people) poses a threat to our data by circumventing security measures imposed even by large organizations, which can undermine our trust. As you know, we are as safe as the weakest link in a chain. One of the links of this chain is Wireless Networks. Our aim in this study is to share information about the frequency, channel, topology and authentication types related to wireless local networks. We will also touch on the measures we can take regarding the attacks against Wi-Fi (Wireless Fidelity) security and the attacks made before.

Keywords: wireless networks, wlan, wireless, wifi

1. GİRİŞ

Günümüzde kablosuz iletişim hemen hemen her yerdedir ve neredeyse hepimizi çepeçevre sarmış durumdadır. Hareket halindeki insanlar ve cihazlar için kablosuz iletişim kaçınılmaz bir gerçektir.

Kablosuz ağlar, **IEEE** (The Institute of Electrical and Electronics Engineers - Elektrik ve Elektronik Mühendisleri Enstitüsü) standartlarına dayanır ve genel olarak dört ana türe ayrılabilir: WPAN, WLAN, WMAN ve WWAN.

WPAN (Wireless Personal Area Network - Kablosuz Kişisel Alan Ağı)
Yakın mesafedeki cihazlarla iletişim sağlamak için kullanılır. (6 ila 9 metre). Bluetooth ve ZigBee tabanlı cihazlar, WPAN'larda yaygın olarak kullanılmaktadır. WPAN'lar, 802.15 standardına dahildir ve 2,4 GHz radyo frekansını kullanır.

WLAN (Wireless Local Area Network - Kablosuz Yerel Alan Ağı)
100 metreye kadar olan orta ölçekli bir ağı kapsamak için kullanılır. WLAN'lar evde, ofiste ve hatta bir kampüs ortamında yaygın olarak kullanılır.

WMAN (Wireless Metropolitan Area Network - Kablosuz Metropol Alan Ağı)
Bir coğrafi alanda kablosuz hizmet sağlamak için kullanılır. WMAN'ler, bir şehre veya belirli bir bölgeye kablosuz erişim sağlamak için uygundur. WMAN kullanımı lisansa tabidir.

WWAN (Wireless Wide-Area Networks - Kablosuz Geniş Alan Ağları)
Geniş bir coğrafi alanda kapsama sağlamak için kullanılır. WWAN'lar ulusal ve küresel iletişim için uygundur. WWAN kullanımı lisansa tabidir.

1.1. 802.11 Standartları

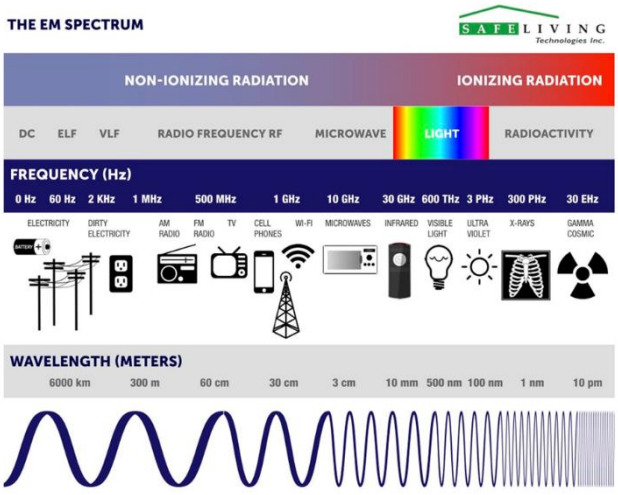
Kablosuz iletişim dünyası çok geniştir ve sadece bu konu ile ilgili birçok standart geliştirilmiştir. Bunlardan biri de IEEE tarafından oluşturulan 802.11 WLAN standartlarıdır. 802 ve 11 sayıları, IEEE standartlarında kullanılan sıra numaralarıdır, bir önem yoktur. 802 yerel alan ağı standartlarını, 11 ise kablosuz yerel alan ağı standartlarını ifade eder.

1.2. Radyo Frekansları

Tüm kablosuz cihazlar, elektromanyetik spektrumun radyo dalgaları aralığında çalışır. Aşağıdaki şekilde bazı cihazlar ve bunlar tarafından kullanılan frekans aralıkları gösterilmektedir. Şu frekans bantları 802.11 WLAN'lara ayrılmıştır:

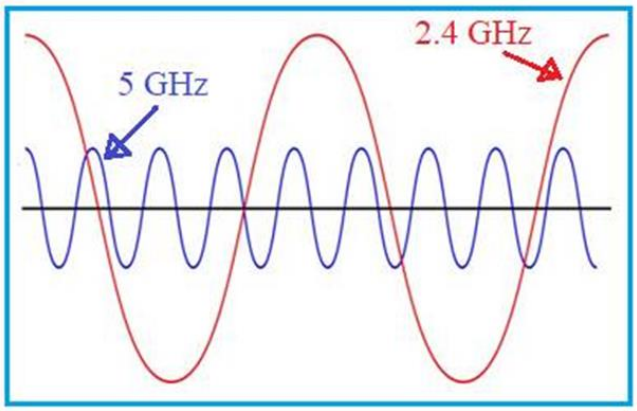
2,4 GHz (UHF) - 802.11b / g / n / ax
5 GHz (SHF) - 802.11a / n / ac / ax

Hem 2.4 hem de 5 Ghz frekans bantlarını kullanmak için bir lisans almaya gerek yoktur.



Şekil 1. Elektromanyetik Spektrum [1]

Frekans ne kadar yüksek olursa, sahip olduğumuz yayılma o kadar az olur. 2.4 GHz frekansı 0.125 metre dalga boyuna sahipken, 5 GHz frekansı 0.060 metreye sahiptir.



Şekil 2. 2.4 GHz ve 5 GHz dalga boyu [2]

2.4Ghz iç mekânda yaklaşık 36 metre, dış mekânda yaklaşık 300 metre kapsama alanı sağlar. 5Ghz ise iç mekânda yaklaşık 12 metre, dış mekânda yaklaşık 31 metre kapsama alanı sağlar

Daha büyük dalga boyu nedeniyle, 2,4 GHz sinyal duvarlardan ve katı nesnelerden daha kolay geçer. Bu nedenle daha geniş mesafeleri kapsar ve daha iyi kapsama alanı sağlar.

Kablosuz erişim noktasından sinyali kaybetmeden gidebileceğimiz maksimum mesafeyi 2.4Ghz ile sağlarız ancak bu durumda daha az bant genişliğine sahip oluruz. 5GHz ile daha fazla bant genişliğine sahip oluruz ancak gidebileceğimiz mesafe daha azdır. Buna karşılık 5GHz ile daha yüksek hıza, daha fazla kanal sayısına ve daha az sıkışıklığa sahip oluruz.

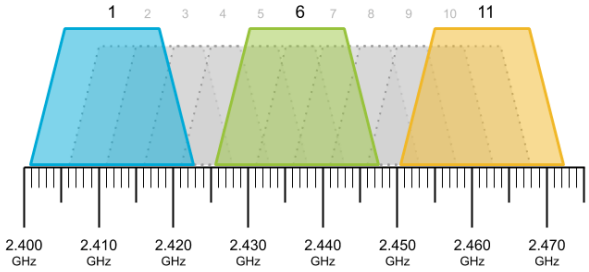
2. KANAL YÖNETİMİ

802.11b / g / n standartları 2,4 GHz ila 2,5 GHz spektrumunda çalışır.

2.1. 2.4 GHz

2,4 GHz bandında tanımlanmış on dört kanal vardır, ancak tamamının kullanımına izin verilmez, izin verilen sayı genellikle 11'dir. 2,4 GHz spektrumundaki her kanal 22 MHz genişliğindedir. Kanal merkezleri 5 MHz ile ayrılır ve tüm spektrum yalnızca 100 MHz genişliğindedir. Bu durum, kullanılan kanalların 100 MHz'e sıkıştırılması gerektiği ve sonunda üst üste geldiği anlamına gelir.

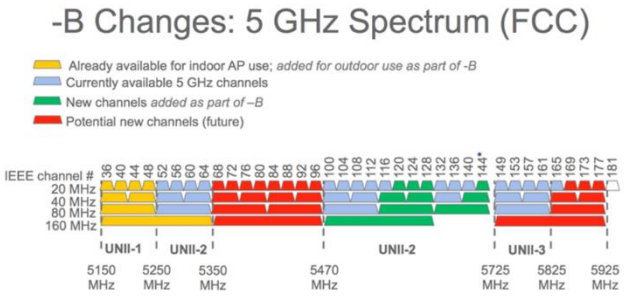
1., 6. ve 11. kanallar, kanal merkezleri arasında yeterli boşluğa sahip oldukları için çakışmayan kanallardır. Birden çok AP (Access Point – Erişim noktası) gerektiren Wi-Fi'lar için en iyi uygulama, çakışmayan kanalları kullanmaktır.



Şekil 3. 2,4 GHz bandında, 2, 3, 4, 5, 7, 8, 9 ve 10 numaralı kanalların tümü önemli ölçüde örtüşerek bitişik kanal parazitine neden olur. [3]

2.2. 5 GHz

36, 40, 44, 48'den başlayıp 149, 153, 157, 161, 165'e kadar giden önceden tanımlanmış 25 adet 5GHz kanalı vardır. Bu kanallar sadece yönlendiriciler tarafından değil, askeri istasyonlar tarafından da kullanılmakta ve bilim endüstrisi de iletişim için belirli kanalları kullanmaktadır. 36, 40, 44, 48 no.lu kanallar UNII-1 kanalları olarak adlandırılır ve ev içi amaçlar için kullanılır. UNII-1 kanalları, özellikle evde kullanıldığı için Wi-Fi 5GHz için en iyi kanal olarak kabul edilir, ancak daha fazlası da vardır.5 GHz için 24 kanal vardır. 5 GHz bandı üç bölüme ayrılmıştır. Her kanal bir sonraki kanaldan 20 MHz ile ayrılır. Her bir kanalın frekans kuyruklarında hafif bir çakışma olsa da kanallar birbirine karışmaz.



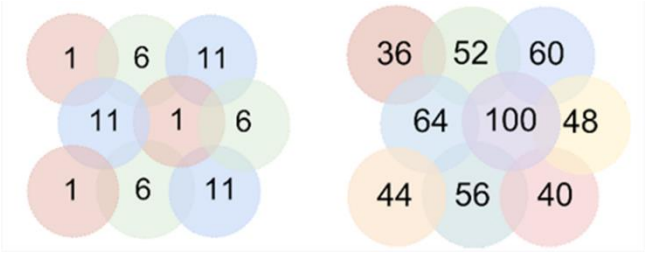
Şekil 4. 5 GHz spektrum [4]

165 no.lu kanal özellikle askeri kullanım ve hassas iletişim için ayrılmıştır. Daha yüksek bir kanala sahip olmak, daha iyi iletişim ve daha geniş bant genişliğine sahip olacağınız anlamına gelir, ancak diğer kanallarla da çakışma ihtimali vardır.

Yönlendirici Dinamik Frekans Seçimi anlamına gelen DFS özelliğine sahipse, askeri ve hava istasyonlarıyla çakışmadan en iyi kanalı otomatik olarak seçebilir.

2.3. Kanal Seçimi

2.4GHz' te olduğu gibi birbirine yakın birden çok AP yapılandırırken parazit oluşturmayan kanalları seçmek gerekir. Aşağıdaki şekilde he iki frekans için AP yerleştirme örneği verilmiştir.



Şekil 5. Çakışmayan kanallar [5]

3. KABLOSUZ TOPOLOJİ MODLARI

802.11 standardı Ad hoc modu ve Altyapı modu olmak üzere iki ana kablosuz topoloji modu tanımlar.

Şekil 6. Ad Hoc Modu ve Altyapı Modu [6]

3.1. Ad Hoc mode (Özel Mod)

Ad hoc mode - İki cihazın AP veya kablosuz yönlendirici kullanmadan kablosuz olarak eşler arası (P2P) bir şekilde bağlandığı durumdur. Örnekler, Bluetooth veya Wi-Fi Direct kullanarak birbirlerine doğrudan bağlanan kablosuz cihazlar verilebilir.

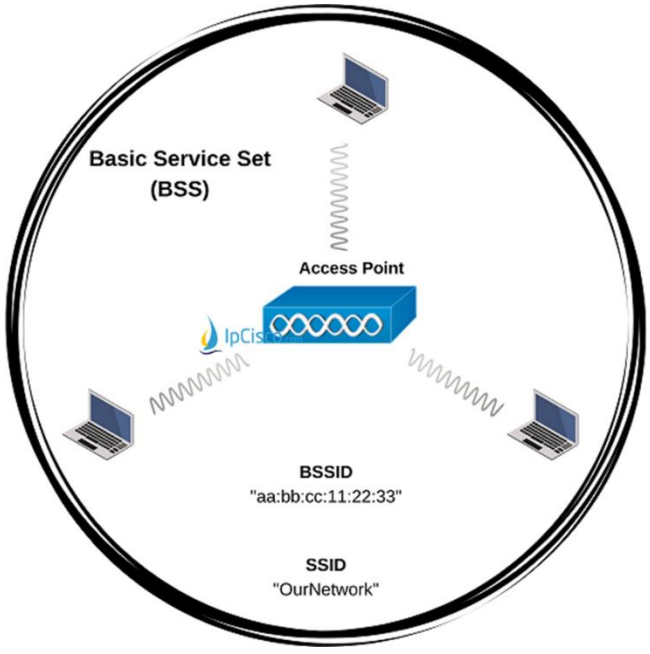
3.2. Infrastructure mode (Altyapı Modu)

Infrastructure mode - Kablosuz istemcilerin bir kablosuz yönlendirici veya AP aracılığıyla birbirine bağlandığı durumdur. AP'ler, ethernet gibi kablolu dağıtım sistemi kullanarak ağ altyapısına bağlanır.

Altyapı modu ikiye ayrılır: BSS (Basic Service Set - Temel Hizmet Kümesi) ve ESS (Extended Service Set - Genişletilmiş Hizmet Kümesi).

BSS
Bir grup kablosuz cihaz bir AP ile birbirine bağlandığında BSS kurulmuş olur. Kablosuz cihazlar birbirleriyle doğrudan iletişim kurmazlar, bunun yerine AP ile iletişim kurarlar ve AP istekleri hedef cihazlara iletir. Şekildeki daireler AP'nin kapsama alanını tanımlar, bir kablosuz cihaz BSA' nın dışına çıkarsa, artık BSA içindeki diğer kablosuz cihazlarla doğrudan iletişim kuramaz.

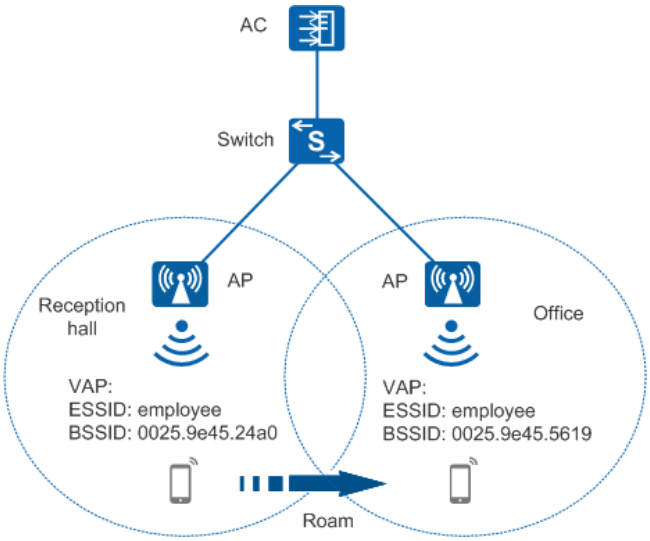
SSID/ESSID (Service Set Identifier - Hizmet Kümesi Tanımlayıcısı) ağa verilen kolay ismi tanımlar, BSSID (BSS Identifier – BSS Tanımlayıcısı) ise genellikle AP'in MAC adresidir.



Şekil 7 BSS [7]

ESS
AP'lerin kapsama alanları sınırlıdır, kapsadıkları alana hücre denmektedir. Ancak birçok şirkette ağ alanı çok geniştir ve yalnızca bir AP tüm alanı kapsayamaz. Bu nedenle, tüm alanı kaplamak için ek AP'ler kullanılır. Bu AP'ler merkezi olarak yönetilebilir ve tek bir kesintisiz bağlantı haline gelirler. Kullanıcı, kesinti olmadan bir hücreden diğerine geçebilir. Bu nedenle, AP'lerin birleştirilmesine Genişletilmiş Hizmet Kümesi (ESS) adı verilir.

Birden çok AP'e sahip bir ağda, kesintisiz ve sürekli bağlantı için tüm SSID'ler tüm AP'lerde tanımlanmalıdır. Burada, her AP'in BSSID'si farklıdır ancak SSID'ler aynıdır.



Şekil 8 ESS [8]

SSID açık olduğu durumlarda AP'ler üzerlerindeki ağın varlığını duyurmak için tekrarlanan aralıklarla yayın yaparlar. Çoğu zaman, SSID'yi gizlemek bir güvenlik mekanizması olarak düşünülür, ancak değildir. Bir dinleyici ağ trafiğinin kaynağını gösteren yönetim çerçevelerini görebilir. SSID'yi gizlemek, sadece sıradan kullanıcıların ağımıza katılmaya çalışmasını engeller.

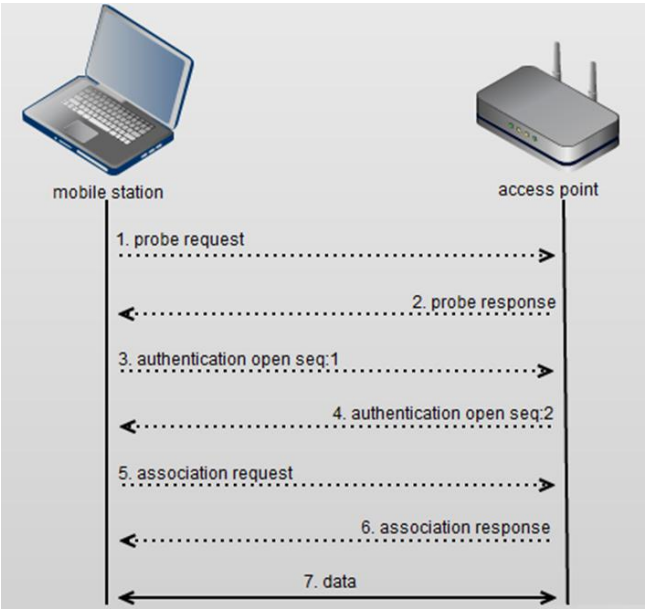
4. WLAN OTURUM KURULUMU

Erişim noktaları, mobil cihazlar ile ağdaki diğer cihazlar arasındaki trafik için köprü görevini üstlenirler.

Köprünün oluşması için mobil cihaz doğrulanmış ve ilişkili durumda olmalıdır. Bunun olması için şu adımlar gerçekleşir:

1. Kablosuz erişime sahip bir cihaz çevresindeki ağları keşfetmek için araştırma (prob) istekleri gönderir. Prob istekleri, mobil cihazın desteklediği veri hızlarını ve 802.11n gibi 802.11 yeteneklerini içerir. Araştırma talebi, hedef katman-2 adresine ve

ff: ff: ff: ff: ff: ff'nin BSSID'sine gönderildiği için, onu alan tüm AP'ler yanıt verecektir.
2. Araştırma talebini alan AP'ler, mobil cihazın en az bir ortak desteklenen veri hızına sahip olup olmadığını kontrol eder. Uyumlu veri hızlarına sahiplerse, SSID'yi, desteklenen veri hızlarını, gerekirse şifreleme türlerini ve AP'nin diğer 802.11 özelliklerini tanıtan bir yoklama yanıtı gönderilir.
3. Mobil cihaz, AP'e düşük seviyeli bir 802.11 kimlik doğrulama mesajı gönderir.
4. AP, kimlik doğrulama mesajını alır ve mobil cihaza yanıt verir.
5. Mobil cihaz hangi AP ile ilişkilendirmek istediğini belirlediğinde, bu AP'ye bir ilişkilendirme talebi gönderecektir. İlişkilendirme isteği, gerekirse seçilen şifreleme türlerini ve diğer uyumlu 802.11 özelliklerini içerir.
6. İlişki talebindeki unsurlar AP'nin yetenekleriyle eşleşirse, AP, mobil istasyon için bir İlişkilendirme ID'si yaratacak ve mobil cihaza ağ erişimi sağlayan bir ilişkilendirme mesajı ile yanıt verecektir.
7. Artık mobil cihaz AP ile başarılı bir şekilde ilişkilendirilmiştir ve veri aktarımı başlayabilir.



Şekil 9 802.11 İlişkilendirme Süreci [9]

5. WLAN GÜVENLİĞİ

Bir güvenlik uzmanı kablosuz bir ağa bağlanırken aklına gelen ilk soru "Bu Wi-Fi ağı ne kadar güvenli?" şeklinde olur. Ancak ortalama bir kullanıcı için talihsiz gerçek, Wi-Fi bağlantısının güvenlikten çok rahatlıkla ilgili olmasıdır. Bu nedenle aslında zorluk sadece kurumunuzun Wi-Fi ağların güvenliğini sağlamak değil, aynı zamanda kurum çalışanlarının hassas verilere erişmek için kullandığı mobil cihazları da korumaktır, çünkü çalışanlar kurum dışında ve başkasına ait bir ağda olabilirler.

Kablosuz sinyaller katı maddelerden geçerek evin, ofisin dışına çıkabildiği için sıkı güvenlik önlemleri almak gerekir. Güvenlik önlemi alınmadan kurulan bir WLAN, ethernet bağlantı noktasını dışarıya koymakla eşdeğer olabilir. SSID gizleme ve MAC adres filtreleme iş bilen saldırganları caydırmaz ve saldırgan bunları aşarak ağa dahil olabilir.

WLAN güvenliği, kimlik doğrulama ile başlar ve biter. Kablosuz ağınıza kimlerin erişebileceğini kontrol edemezseniz, ağınızı koruyamazsınız.

5.1. WEP (Wired Equivalent Privacy - Kabloluya Eşdeğer Gizlilik)

WEP protokolü (1997), kablosuz endüstrisinin ilk güvenlik girişimiydi. WEP'in kablolu bir ağın güvenliğine eşdeğer veri gizliliği sağlaması amaçlanmıştır. Bununla birlikte, iyi bilinen ve duyurulmuş pek çok zayıf yönü vardı ve güvenli bir kablosuz ağ kurmak için yetersizdi. WEP 64 ve WEP 128 versiyonları vardır. WEP yıllar önce kırıldı, ancak hala üzerinde çalışılıyor çünkü bu, şifrelemenin nasıl yapılmayacağına dair iyi bir ders veriyor.

5.2. WPA (Wi-Fi Protected Access - Wi-Fi Korumalı Erişim)

WEP'in zayıf yanları çıkartılıp geliştirilerek WPA (2003) oluşturulmuştur. Günümüzde güvensiz kabul edilen ve kullanmamamız gereken TKIP (Temporal Key Integrity Protocol - Geçici Anahtar Bütünlüğü Protokolü) şifreleme protokolünü kullanmaktadır. WPA AES versiyonu da vardır ancak bunu destekleyen cihazlar WPA2' yi de desteklediği için tercih edilmez. WEP gibi WPA'da güvensizdir.

5.3. WPA2

WPA2 (2004) halen kullanımda olan mevcut standarttır. WPA2 (TKIP) güvensiz TKIP şifrelemesini kullanır, genellikle tercih edilmez, AES ile bağlanamayan cihaz varsa tercih edilir. WPA2 (AES Advanced Encryption Standard – Gelişmiş Şifreleme Standardı) en güvenli seçenektir. WPA2 (TKIP / AES) iki şifreleme türü desteklenir ancak ihtiyaç yoksa önerilmez.

İki farklı türde kurgulanabilir:

WPA2 Enterprise (Enterprise Class - Kurumsal Sınıf), WPA-802.1X modu olarak da anılır. Radius sunucusu ile kimlik doğrulaması yapar.

WPA2-PSK (Pre Shared Key - Ön Paylaşımlı Anahtar), paylaşılan bir anahtar kullanır, küçük iş yeri ve ev ağları tarafından kullanılır. Tüm kablosuz ağ cihazları kimlik doğrulama yaparken aynı 256 bitlik anahtarı kullanır. Anahtar, 64 adet 16'lık karakter ile oluşturulur. Kullanıcıların 64 karakterli parolayı girmesi zor olduğundan ağ yöneticisi tarafından belirlenen parolaya kullanılan SSID

adı tuz olarak eklenir ve böylece 256 bitlik anahtar oluşturulur.

WPS Wi-Fi Korumalı Kurulum (Wi-Fi Protected Setup), şifreleme anahtarlarını almayı kolaylaştırarak tüketicileri şifrelemeyi etkinleştirmeye teşvik etmek için tasarlanmıştır (2006), ancak bazı güvenlik sorunları vardır.

5.4. WPA3

WPA2 için güvenlik risklerinin ortaya çıkması ile WPA3 standardı ortaya çıktı. WPA3, parola ve parolayla elde edilen bilgileri asla kablosuz olarak gönderilmez, kaba kuvvet saldırılarına ve bir saldırganın tüm istemci cihazlarına sürekli kimlik doğrulama paketleri göndererek herhangi birinin ağa erişmesini engellediği DoS saldırılarına karşı güvenlik sağlamaktadır. WPA 3 için mevcut donanımı değiştirmeye gerek yoktur, etkinleştirmek için gereken tek şey cihaz üreticisinin bir yazılım güncellemesi çıkarmasıdır. Ayrıca tüm WPA3 özellikli cihazlar en son güvenlik yöntemlerini kullanır, eski protokollere izin vermez.

Wi-Fi Alliance'a göre, WPA3 özellikleri, akıllı ampuller, kablosuz cihazlar, akıllı hoparlörler ve günlük işleri kolaylaştıran diğer ekransız araçlar gibi IoT cihazları için gelişmiş güvenlik içerir.

6. WLAN TEHDİTLERİ

WLAN'lar, bir AP menzilinde bulunan ve onunla ilişkilendirilecek uygun kimlik bilgilerine açık olan herkese açıktır. Bir saldırganın bir WLAN'a erişmek için kuruma fiziksel olarak girmesine ihtiyacı olmayabilir. Saldırganın, tıpkı bir radyo istasyonunu ayarlamaya benzer şekilde, kablosuz ağdan gelen sinyalleri ayarlaması mümkündür.

Saldırılar, içeriden veya dışarıdan olabileceği gibi yanlışlıkla da oluşturulabilir. Bazı tehditler:

Verilerin ele geçirilmesi

Verilerin başkaları tarafından okunmasını önlemek için şifrelenmesi gerekir.

DoS (Denial of Service - Hizmet Reddi)

WLAN hizmetlerine erişim, yanlışlıkla veya kötü niyetle kişilerce tehlikeye atılabilir.

Yapılandırma hataları WLAN'ı devre dışı bırakabilir. Örneğin, bir yönetici yanlışlıkla bir yapılandırmayı değiştirebilir ve WLAN'ı devre dışı bırakabilir.

Kablosuz iletişime kasıtlı olarak müdahale eden kötü niyetli biri kablosuz ağı tamamen veya hiçbir cihazın ortama erişemeyeceği noktaya kadar devre dışı bırakabilir.

WLAN'lar, mikrodalga fırınlar, kablosuz telefonlar, bebek monitörleri ve daha fazlası dahil olmak üzere diğer kablosuz cihazlardan kaynaklanan parazit sonucu devre dışı kalabilir. 2,4 GHz bandı, 5 GHz banda göre parazite karşı daha hassastır.

Rogue AP – (Yetkisiz AP)

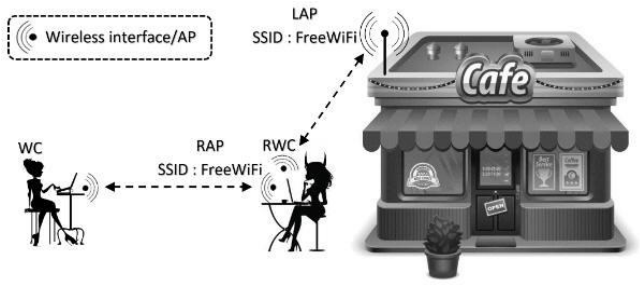
Sahte AP, yetkisi olmadığı halde ağınıza bağlanan bir AP veya kablosuz yönlendiricidir. Ağınıza erişimi olan yetkisiz bir şirket çalışanı veya kötü amaçlı birisi bunu yapabilir. Saldırgan ağa bağladığı sahte AP ile MAC adreslerini, veri paketlerini yakalayabilir, ağ kaynaklarına erişim sağlayabilir veya ortadaki adam saldırısı başlatabilir.

MITM (Man-in-the-Middle Attack – Ortadaki Adam Saldırısı)

Bir saldırgan, kurbanlarının kendisi tarafından kontrol edilen bir kablosuz ağa bağlanmasını sağlayabilir. Kablosuz MITM saldırısında saldırgan, sahte bir AP'yi ağa ekler ve ağda var olan SSID ile yayın yapar. WLAN'a bağlanmaya çalışan cihazlar, aynı SSID'ye sahip iki AP görürler. Sahte AP'nin yakınında olanlar daha güçlü sinyali tercih edeceği için büyük olasılıkla sahte AP ile ilişkilendirilir. Bundan sonra trafik sahte AP üzerinden geçer ve böylece saldırgan, kullanıcının şifrelerini, kişisel bilgilerini çalabilir.

Evil Twin - Kötü ikiz

Saldırgan gerçek bir erişim noktasını taklit eden sahte bir erişim noktası yayınlar. Örneğin, gittiğiniz bir kafe Wi-Fi hizmeti veriyorsa ve buna "Cafe Wi-Fi" diyorsa, saldırgan aynı adı taşıyan bir erişim noktası oluşturur. Ortalama bir kullanıcı, gerçek veya sahte bir erişim noktasına bağlandığını kolayca ayırt edemez. Bu nedenle bu yaklaşım, kurbanları rastgele çekmeye çalışan bir yöntemden daha fazla sayıda kullanıcıyı yakalayacaktır. Evil Twin saldırısında saldırgan genellikle kurbanını seçemez. Hedef belirli bir kurumdaki çalışanlar ise bu saldırı türü etkili bir yaklaşım değildir.



Şekil 10 Kötü İkiz Saldırısı [10]

Jasager

Evil Twin'e göre daha hedefli bir saldırı tipidir. Saldırgan, kullanıcının normalde bağlandığı erişim noktası gibi davranır. Cep telefonunuzu veya dizüstü bilgisayarınızı evinize veya ofisinize getirdiğinizde, hangi AP'yi kullanacağınızı seçmeniz gerekmez, çünkü cihazınız

önceden bağlanmış olduğu kablosuz ağların ayrıntılarını hatırlar.

Mobil cihazlar, tercih edilen bir ağın kapsama alanı içinde olup olmadığını görmek için bir işaret gönderir. Normal koşullarda, işareti alan ancak eşleşmeyen erişim noktaları onu yok sayar. İşaret, tercih edilen ağın yakınına gelmediği sürece cevapsız kalır.

Jasager saldırısı, işaret isteklerine karşı daha aktif bir yaklaşım sergilemektedir. Jasager (Almanca "evet adam" anlamına gelir) tüm işaret taleplerine yanıt verir. Böylece kurban daha önceden bağlandığı ağa tekrar bağlandığında, farkında olmadan değiştirilmiş erişim noktasına bağlanır. [11]

SSLstrip

SSLStrip HTTP ve HTTPS protokollerinin birlikte desteklendiği sistemlerde ortaya çıkan güvenlik zafiyetini kullanarak aradaki trafiği dinlemek ve değişiklik yapmak için geliştirilen bir araçtır. SSLStrip aracı kullanılarak kurbanın bilgisayarında sertifika uyarısı çıkmadan HTTPS trafiği okunabilmektedir. [12]

Emotet

Emotet, 2014 yılında ortaya çıkan ve uzun süredir spam botnet'lerinde ve fidye yazılımı saldırılarında kullanılan bir truva atıdır. Son zamanlarda türeyen bir emotet varyantının Wi-Fi yayma modülü kullandığı tespit edilmiştir. Modül, virüs bulaşmış bir cihazın yakınındaki Wi-Fi ağlarını tarayıp onlara karşı kaba kuvvet saldırısı yapmaktadır. Bir Wi-Fi ağına başarıyla bağlandıktan sonra, açık paylaşımları taramakta ve ağa bağlı diğer cihazlardaki kullanıcı adı ve şifreleri bulmak için başka bir kaba kuvvet saldırısı yapmaktadır. [13]

7. SONUÇ

Bu çalışmada kablosuz yerel alan ağları hakkında 802.11 standardı, frekans bilgileri, kanal yönetimi, topoloji modları, wlan oturum kurulumu, wlan güvenliği ve wlan tehditlerine değinilmiştir. Konunun daha iyi anlaşılması için birçok farklı kaynaktan makaleler incelenmiş ve bunlar harmanlanarak sade bir dille anlatılmaya çalışılmıştır. Araştırılan ve incelenen makalelerde de görüleceği gibi bilgi güvenliği verinin olduğu her yerde ayrı ayrı sağlanmalıdır.

Bilgi Teknolojileri bilginin gizlilik, bütünlük ve erişilebilirlik sağlanarak depolanması ve iletilmesi gibi zincirin tüm halkalarının içinde bulunduğu bir süreçte yer almaktadır. Zincirin en zayıf halkası kadar güvende olduğumuz düşünüldüğünde tüm halkaların mümkün olan en güçlü hale döndürülmesi gerekmektedir. Bu halkalardan biri de kablosuz yerel alan ağlarıdır. Verinin korunması için her ne kadar çalışılıyor ve yeni sistemler geliştiriliyor olsa da saldırganlar da her geçen gün yeni yöntemler bularak kendilerini geliştirmektedir.

Korunmak için en iyi sistemleri kullanmak tek başına yeterli değildir. Kullandığımız kaynakları çok iyi tanımalı, yeni teknoloji ve trendleri takip etmeli ve elimizdekileri mümkün olan en iyi şekilde kurgulamalı ve gözlem altında tutmalıyız.

KAYNAKÇA

[1] «What is EMF,» [Çevrimiçi]. Available: http://www.emfawaresc.org/sources-of-emf.html. [Erişildi: 04 2021].

[2] «Difference between 2.4 GHz WiFi and 5 GHz WiFi | 2.4 GHz vs 5 GHz,» [Çevrimiçi]. Available: https://www.rfwireless-world.com/Terminology/difference-between-2-4-GHz-WiFi-and-5-GHz-WiFi.html. [Erişildi: 04 2021].

[3] «Why Channels 1, 6 and 11?,» [Çevrimiçi]. Available: https://www.metageek.com/training/resources/why-channels-1-6-11.html. [Erişildi: 04 2021].

[4] «Know About the Best 5GHz Channel For Your Router,» [Çevrimiçi]. Available: https://routerguide.org/best-5ghz-channel/. [Erişildi: 04 2021].

[5] «Designing 5 GHz WiFi Networks,» [Çevrimiçi]. Available: https://www.metageek.com/training/resources/designing-5ghz-wi-fi/. [Erişildi: 04 2021].

[6] «Wireless Networking and Standards,» [Çevrimiçi]. Available: https://www.onlinecomputertips.com/support-categories/networking/627-wireless-networking-and-standards. [Erişildi: 04 2021].

[7] «Wireless Principles,» [Çevrimiçi]. Available: https://ipcisco.com/lesson/wireless-principles/. [Erişildi: 04 2021].

[8] «[From Beginner to Expert - WLAN Common Terms] Section 15 - SSID, BSSID and ESSID,» [Çevrimiçi]. Available: https://forum.huawei.com/enterprise/en/from-beginner-

to-expert-wlan-common-terms-section-15-ssid-bssid-and-essid/thread/532057-869. [Erişildi: 04 2021].

[9] «802.11 Association Process Explained,» [Çevrimiçi]. Available: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_Process_Explained. [Erişildi: 04 2021].

[10] «Evil Twin Attack in WiFi Network,» [Çevrimiçi]. Available: http://cyberforensic.net/labs/ETA/ETA.html. [Erişildi: 04 2021].

[11] «Wireless Man in the Middle,» [Çevrimiçi]. Available: https://blog.paloaltonetworks.com/2013/11/wireless-man-middle/. [Erişildi: 04 2021].

[12] «SSL Strip Aracı Ile HTTP Desteği Veren Web Uygulamasında HTTPS Protokolünde Araya Girme Saldırısını Gerçekleştirme,» [Çevrimiçi]. Available: https://www.siberportal.org/red-team/web-application-penetration-tests/ssl-man-in-the-middle-attack-using-ssl-strip-tool/. [Erişildi: 04 2021].

[13] «Emotet Evolves With New Wi-Fi Spreader,» [Çevrimiçi]. Available: https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/. [Erişildi: 04 2021].