Wİ-Fİ ŞİFRELEME SİSTEMLERİ ARASINDAKİ FARKLAR

WEP, WPA ve WPA 2 kablosuz şifreleme sistemleri arasındaki farklar

Wi-Fi ağınızın güvenliğini sağlamanız gerektiğini bilseniz de, tüm bu şifreleme ile ilgili kısaltma sözcükleri kafanızı karıştırabilir. Bu yazımızda, WEP, WPA, ve WPA2 gibi şifreleme standartları arasındaki farkları ve hangisini evinizdeki Wi-Fi ağında kullanmanız gerektiğini açıklayacağız.

Neden önemli?

Size söylenenleri yapıp, router'ınıza giriş yaptınız, şifresini ayarladınız, ilk kez bağlıyorsunuz. Şifreleme standardı ayarı olarak seçtiğiniz o küçük ayarın ne önemi var? Görünüşe bakılırsa, oldukça önemi var. Günümüzün güçlenen bilgisayarları ve keşfedilen sistem açıkları yüzünden, tüm eski şifreleme sistemlerinde olduğu gibi, Wi-Fi için de eski şifreleme sistemleri risk altında. İstenmeyen birinin Wi-Fi ağınıza girip, sizi polislik edecek seviyede yasadışı iş yapabileceği düşünüldüğünde, bu güvenliğin önemini daha iyi anlayabiliriz. Şifreleme standartları arasındaki farkları anlayıp, en gelişmiş olanını router'ınızda kullanmak, desteklemiyorsa da yenisini almak, ev ağınıza birinin rahatlıkla girebilme stresinden sizi kurtaracaktır.

WEP, WPA ve WPA2: Wi-Fi güvenliğinde dönemler

90'ların sonlarından beri, Wi-Fi güvenlik algoritmaları birçok değişikliğe uğradı. Güncellemelerle eskileri hızla değerini kaybetti ve yenileri de sürekli revize edildi. Wi-Fi tarihine yapacağımız küçük gezide, bugünün standartlarını daha iyi anlayıp, neden eski standartlardan kaçınmamız gerektiğini bileceğiz.

Wired Equivalent Privacy (WEP) – (Kabloluya Eşit Güvenlik)

Wired Equivalent Privacy (WEP), dünyada en çok kullanılan Wi-Fi güvenlik algoritması. Bunun sebebi ise, geriye uyumluluğu ve birçok router'ın kontrol panelinde ilk sırada yer alması.WEP'in bir Wi-Fi güvenlik standardı olarak kabul edilmesi Eylül 1999'da gerçekleşmişti. WEP'in ilk sürümleri, yeni çıktıklarında bile pek güçlü değildiler. Çünkü Amerika'nın bazı kriptografik teknolojilerin kullanılmasını sınırlaması, üreticilerin sadece 64-bit şifreleme kullanmasına izin veriyordu. Sınırlamalar kaldırıldığında, bu 128-bit'e çıkarıldı. Günümüzde 256-bit WEP şifrelemesi mevcut olsa da, 128-bit şifreleme halen en yaygın olarak kullanılan.

WEP'in sonu

Algoritmadaki bir çok düzeltmeye ve arttırılan anahtar boyutuna rağmen,WEP standardında zaman içinde birçok güvenlik açığı keşfedildi ve bilgisayar gücünün de artmasıyla, bu açıkları kötüye kullanmak git gide kolaylaştı. 2005 yılında FBI, WEP'in zayıflığını insanlara anlatabilmek için, ücretsiz yazılımlarla WEP şifrelerinin ne kadar kolay kırılabildiğini gösterdi.

WEP sistemini canlandırma adına yapılan geliştirmelere, geçici çözümlere, ve diğer çabalara rağmen, bu standart aşırı derecede savunmasız kalmaya devam ediyor. WEP'e güvenen bir sistem güncellenmeli, ve eğer güncellemek mümkün değilse, değiştirilmeli. Wi-Fi Alliance, 2004 yılında resmi olarak WEP'i emekli etti.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) – (Wi-Fi Korumalı Erişim)

Wi-Fi Protected Access, Wi-Fi Alliance'ın güvenlik açıkları gitgide artan WEP'e direk cevabıydı. 2003 yılında, WEP resmi olarak emekli edilmeden bir sene önce resmi olarak kabul edildi. En yaygın olan WPA konfigürasyonu, WPA-PSK (Pre-Shared Key). WPA'da kullanılan anahtarlar 256-bit, ve bu WEP sisteminde kullanılan 64-bit ve 128-bit anahtarlara göre önemli bir gelişme.

WPA'nın sahip olduğu önemli farklılıklar arasında, bir saldırgan tarafından kullanıcı ile erişim noktası arasındaki paketlerin ele geçirilip geçirilmediğini veya üzerinde oynandığını anlayabilen "message interity checks" özelliği. Bir de Temporal Key Integrity Protocol (TKIP). TKIP, paket başına anahtar sistemiyle, WEP'te kullanılan sabit anahtar sisteminden çok daha güvenli. TKIP de daha sonralarda Advanced Encryption Standard (AES)'in gölgesinde kaldı.

WPA, WEP'e oranla ne kadar daha gelişmiş olursa olsun, WEP'in hayaleti WPA'nın peşini hiç bırakmadı. WPA'nın temel bir öğesi olan TKIP, firmware güncellemeleriyle kolaylıkla WEP kullanan

cihazlara uygulanabilecek şekilde tasarlanmıştı. Öyle ki, WEP sistemindeki belli başlı bazı unsurları tekrar kullanmak zorunda kaldı, ve bunlar da zamanla tehlikeli açıklar verdi.

Atası WEP'e olduğu gibi, WPA'nın da saldırılara ne kadar açık oluğu bir çok kez gösterildi. İlginç olansa, WPA sisteminin kırılması daha çok WPA algoritmasına direk bir saldırıyla değil, aygıtları birbirine bağlamayı kolaylaştırmak amacı taşıyan Wi-Fi Protected Setup (WPS)'ın aracılığıyla yapılması

Wi-Fi Protected Access II (WPA2)

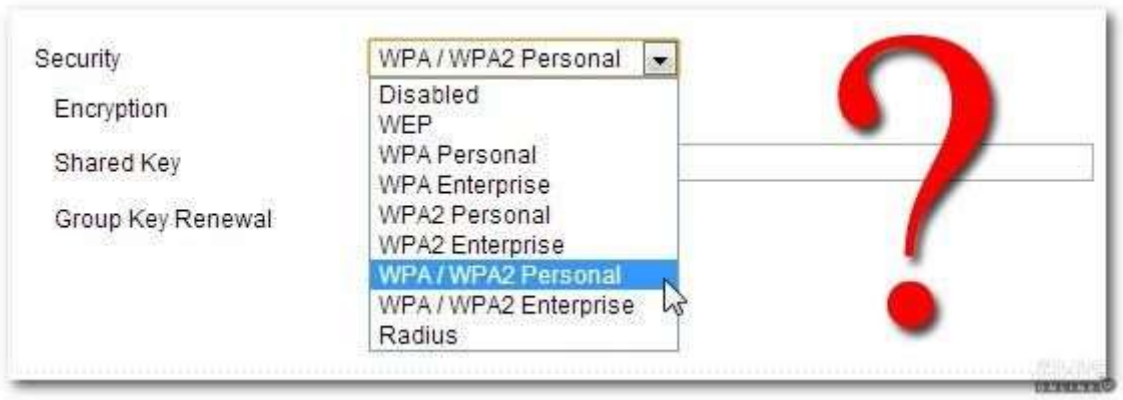
Wi-Fi Protected Access II (WPA2) – (Wi-Fi Korumalı Erişim II)

2006'ya geldiğimizde, WPA2, WPA'nın resmi olarak yerine geçti. WPA ve WPA2 arasındaki en önemli değişikliklerden biri, AES algoritmalarının zorunlu kullanımı ve CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)'nin, TKIP'ın yerini almasıydı (fakat TKIP, WPA ile birlikte çalışabilmek için hala tutuluyor).

Şu an WPA2'nin en büyük güvenlik açığı ise biraz karışık. Bu açığı kullanabilmek için, saldırıyı gerçekleştirenin Wi-Fi ağına zaten erişim sağlayabiliyor olması gerekiyor ki belli anahtarlara erişim sağlayabilsin ve ağdaki diğer cihazlara saldırı gerçekleştirebilsin. Yani, bugün için WPA2'nin açıkları, ev ağları için neredeyse hiçbir tehlike arz etmezken, kuruluş bilgisayarları için bir derece tehlike arz ediyor.

Ne yazık ki, WPA'nın zırhındaki en büyük delik, Wi-Fi Protected Setup (WPS) aracılığıyla erişilebilen "saldırı vektörü", WPA2 kullanan erişim noktalarında da varlığını sürdürüyor. Bu savunmasızlığı kullanarak bir WPA/WPA2 ağına izinsiz girmek, modern bir bilgisayarla 2-14 saatlik sürekli bir efor gerektiriyor fakat, yine de bu çok önemli bir güvenlik açığı ve WPS devre dışı bırakılmalı. Hatta mümkünse, erişim noktası WPS'yi desteklemeyen bir sürüme güncellenmeli, böylece "saldırı vektörü" tamamen ortadan kaldırılabilir.

Wi-Fi güvenlik geçmişi elinizde; şimdi ne yapmalı?



Bu noktada, ya içiniz rahat edecek (çünkü kendi Wi-Fi erişim noktanız için mümkün olan en iyi şifreleme sistemini kullanmışsınız), ya da biraz huzursuzlanacaksınız çünkü listenin en başında olduğu için WEP'i seçtiğinizi gördünüz. Eğer durum sondaki gibiyse, korkmayın, biz varız. Aşağıda verdiğimiz sıralamada, 2006'dan sonra çıkmış olan tüm router'larda bulabileceğiniz güvenlik sistemlerini, en iyiden en kötüye sıraladık.

1- WPA2 + AES

2- WPA + AES

3- WPA + TKIP/AES (TKIP burada bir geriye uyumluluk olarak var)

4- WPA + TKIP

5- WEPOpen Network (hiç güvenlik yok)

İdeal olarak, Wi-Fi Protected Setup (WPS)'i devre dışı bırakarak, router'ınızı WPA2+AES'e ayarlamalısınız. Güvenlik sisteminiz WEP olduğunda, güvenliğiniz o derece düşük ki böyle bir ağa izinsiz girmek, etrafı dikensiz tellerle çevrili bir alana kolaylıkla tırmanarak girmeye eşdeğer.