Kablosuz LAN dağıtırken, kimlik doğrulama ve şifreleme için güvenli yöntemler dağıtmak çok önemlidir.

Bu sayede ağ sadece yetkilendirilen cihazlar ve bireyler tarafından kullanılabilir. Bu makale, kablosuz LAN kimlik doğrulamasının yaygın olarak kullanılan yöntemlerine ve mevcut şifreleme yöntemlerine değinecektir.

WLAN (Kablosuz Yerel Alan AĞI) Kimlik Doğrulama Yöntemleri

Kablosuz bir ağda kimlik doğrulaması yapmak ile trafiğin şifrelenmesini sağlamak arasında bir açık şekilde bir fark söz konusudur. Zira kimlik doğrulaması yapılan bir ağda, şifrelenmemiş bir trafiğin gezmesi çok olasıdır; bu bölüm güncel olarak kullanılan kimlik doğrulama yöntemlerine değinecektir.

Bugünün kablosuz yerel ağlarında kullanılmakta olan 3 ana kimlik doğrulama yöntemi mevcuttur:

* Açık Kimlik Doğrulama
* Paylaşımlı Kimlik Doğrulama
* EAP (Extensible Authentication Protocol – Genişletilebilir Kimlik Doğrulama Protokolü)

**Açık kimlik doğrulama** metodu, kullanılan metotların en basit yapıda olanıdır ve sadece uç cihazın, ağda kullanılan SSID bilindiği sürece SSID ‘den (Hizmet Kümesi Tanımlayıcısı) haberdar olmasını gerektirir, SSID bilindiği sürece cihazın ağa girilmesine izin verilir. Bu metodun problemi ise şudur; SSID tipik olarak ağ üzerinde yayınlanır ama eğer yayınlanmazsa pasif yakalama teknikleriyle ele geçirilmesi kolay olabilir.

**Paylaşımlı kimlik doğrulama** metodu yaygın olarak bireysel ve küçük çaplı işletme kablosuz LAN uygulamaları üzerinde kullanılır; bu metot, bağlantının her iki tarafına da verilen paylaşımlı bir anahtar (Pre-Shared Key – PSK – Önceden Paylaşımlı Anahtar) kullanır. Eğer söz konusu taraflardaki anahtarlar birbirleriyle eşleşirse, cihazın ağa girmesine izin verilir.

Üçüncü metot **Genişletilebilir Kimlik Doğrulama denilen EAP** metodunu kullanır ve işletmeler tarafından kullanılan en yaygın metottur. EAP, çeşitli kimlik bilgileri seçenekleri kullanarak kimlik doğrulaması için sorgulanan bir kimlik doğrulama sunucusu kullanır.

WLAN Şifreleme Metotları

Kimlik doğrulama için kullanılan yöntemin yanı sıra, şifreleme yöntemi seçimi de kablosuz LAN dağıtımının çok önemli bir kısmını oluşturur. Önceki kablosuz LAN standartları tarafından gerçekleştirilen şifreleme yöntemlerinin birçoğunun güvensizliği kanıtlanmış ve daha modern yöntemlerin gelmesiyle kullanımdan kaldırılmışlardır. Zaman geçtikçe bunların, daha yaygın kullanıldıkları için (ki bu yüzden sömürü için bir hedef haline gelecekler) ve işlem gücü artmaya devam ettiğinden tüm şifreleme tekniklerinde olacağından emin olabilirsiniz.

Aşağıda, bugün incelenecek olan WLAN şifreleme yöntemleri mevcuttur:

* Kabloluya eş değer Mahremiyet (WEP)
* Wi-Fi Korumalı Erişim (WPA)
* Wi-Fi Korumalı Erişim 2 (WPA2)

Kablosuz LAN ‘lar için geniş çaplı olarak kullanılan ilk standart 802.11 (asal) idi; buna güvenlik için kullanılan **Kabloluya Eş Değer Gizlilik (WEP)** algoritması da dahildir. WEP, şifreleme için RC4 şifreleme algoritmasını kullanır ve güvenlik anahtarlarını bulmak için kullanılabilen zafiyetlerden ötürü kullanımdan kaldırılmıştır.

WEP’te bulunan zafiyetlerin sonucunda, **Wi-Fi Korumalı Erişim (WPA)** tanıtıldı. WPA şifreleme için, WEP ve RC4 tarafından desteklenmeyen dinamik anahtarları kullanan Geçici Anahtar Bütünlüğü Protokolünü (TKIP) kullanır. TKIP, ta ki üzerinde zafiyetler bulunana dek, WPA ile beraber kullanıldı. Söz konusu zafiyetler, TKIP nin benzer saldırılara izin veren WEP’in de kullandığı aynı mekanizmalardan bazılarını kullanması gerçeğine odaklanır.

WPA/TKIP deki zafiyetlerin sonucunda, IEEE (Elektrik-Elektronik Mühendisleri Enstütüsü) 802.11i standardı tanımlandı ve uygulandı. Ayrıca IEEE 802.11i standardı, WPA2 olarak da temsil edilir / anılır. WPA2, Sayaç Modlu olan TKIP yerine, AES (Gelişmiş Şifreleme Standardı) temelli olan CCMP (Şifre Bloğu Zincirleme Mesajı Kimlik Doğrulama Kodu Protokolü) yi getirdi; WPA2 şifreleme yönteminin AES olarak anılması yaygındır. Bu yazı itibariyle, AES’i kırmak üzere bulunan kolay bir yöntem yoktur.

ÖZETLE

Bir kablosuz LAN’ının nasıl güvenli kılındığı, büyük ölçüde düzgün bir şekilde girilmesi gereken farklı yapılandırma parametrelerinin sayısına bağlıdır. Mevcut bir sürü kablosuz LAN ile ilgili sorun: bunları uygulayan insanların kablosuz bir ağın güvenliliğini sürdürmek anlamında gerekli olan güvenlik bilgi birikimine sahip olmamasıdır.

Mevcut ve gelecekteki tüm kablosuz LAN uygulayıcıları, seçilen ekipman (ki büyük ihtimalle bu ekipman seçiminin bir parçası olacaklar) tarafından sağlanan en güvenli yöntemler ile alakalı bir şeyler öğrenmek hususunda çaba göstermelidirler. Sahip olunan modern ekipmanın avantajı, WPA2 standardını desteklemesidir ve gerçeklenmesi / uygulanması zor olmamasıdır.

İnşaalah bu makale, şuanki ve ilerideki WLAN yöneticilerine kendi ağlarını güvenli kılmak adına ihtiyaç duydukları bazı bilgileri sağlar.

Ağ Güvenliği Kapsamında Eğitim Kaynakları

* [Cisco CCNA Wireless Training](http://www.trainsignal.com/Cisco-CCNA-Wireless-Training.aspx)
* [Certified Wireless Network Administrator Training](http://www.trainsignal.com/CWNA-Training.aspx)
* [Cisco CCNA Security Training](http://www.trainsignal.com/Cisco-CCNA-Security-Training.aspx)
* [CompTIA Security+ Training](http://www.trainsignal.com/CompTIA-Security-Plus-Training.aspx)

Önerilen Okumalar

* [Wireless Security Considerations: Common Security Threats to Wireless Networks](http://www.trainsignal.com/blog/wireless-lan-security-threats)
* [How to Prevent Threats and Attacks on Your Cisco Network](http://www.trainsignal.com/blog/cisco-ccna-security-network-threat)
* [Warning: Your Wireless Communication Might Not Be Secure!](http://www.trainsignal.com/blog/wireless-lan-security)
* [Top 10 Security Threats Every IT Pro Should Know](http://www.trainsignal.com/blog/top-10-security-threats)

Kaynakça: https://www.pluralsight.com/blog/it-ops/wireless-encryption-authentication