Kablosuz Yerel Alan Ağlarda Güvenlik Uygulaması

Onur Gök[1] , Süleyman Yazıcı[2], Nevcihan Duru[3], Yaşar Becerikli[4]

[1] Kocaeli Üniversitesi , Mühendislik Fakültesi , Bilgisayar Mühendisliği Bölümü, Kocaeli, Türkiye

Özet: Bu çalışmanın amacı kablosuz yerel alan ağlarda güvenlik için gerekli uygulamaların araştırılması, geliştirilmesi ve bu çalışmaların sonucunda, KOÜ Bilgisayar Mühendisliği Bölümü ve Mühendislik fakültesi için güvenli bir kablosuz yerel alan ağ yapısını oluşturmaktır. Yapılan çalışmada kablosuz yerel alan ağ standartları, açıklar ve saldırı türleri; bu saldırı ve açıkları engellemek için gerekli uygulamalar araştırılmış ve sonucunda elimizde bulunun omni anten, köprü, erişim noktaları ve istasyonlar kullanılarak yerleşkede güvenli kablosuz yerel alan ağı kurularak, çalışma hayata geçirilmiştir.

Anahtar kelimeler: Kablosuz Yerel Alan ağları, saldırı, güvenlik,

1. GİRİŞ

Maliyet ve hareket kolaylığı gibi sebeplerle kablosuz yerel ağların kullanımı yaygın hale gelmektedir. Verinin havada iletilme düşüncesi ile beraber veri güvenliği ile ilgili kuşkulara, sorgularda hala net bir cevap alınamamıştır [1]. Bugüne kadar, önce saldırı türleri tespit edilip üzerine savunma mekanizmasının üretilmesi şeklinde güvenlik sağlanmıştır. Birkaç yıl öncesine kadar güvenli denilen yöntemler, yeni saldırı şekilleri ile kırılınca, güvenlik üzerine yapılan çalışmalar artmış ve yeni güvenlik mekanizmaları ortaya çıkmıştır. Bu mekanizmaların beraberinde yeni saldırı türleri ve uygulamaları da hızla geliştirilmiştir. Bu saldırı tiplerinin öğrenilmesi, güvenliğin sağlanması açısından önemli bir adım olacaktır.

Etkin ve genel kullanılan saldırı türlerine örnek olarak, parola saldırıları, MAC adresi kandırmaca, ARP zehirlenmesi, IP adresi kandırmaca, sahte trafik yaratma, DNS kandırmaca, HTTP trafiğinde araya girme, ve Dos saldırıları sıralanabilir[2]. Bu saldırı uygulamalarında, önceden bilgi toplama evresi, ağ tarama ve dinleme programlarının kullanılması önemli yer teşkil etmektedir.

Güvenliğin sağlanmasının yanında, ağın yönetimi de güvenlik kadar önemli bir konudur. Kablosuz yerel ağın tasarımı ve güvenlik kısıtlamalarını yerine getirirken, diğer taraftan ağ işlevini yerine getirmeli, kullanıcılar da haklarını yitirmemelidir. İletişimsiz bir güvenlik tabii ki söz konusu değildir, oluşturulan güvenli ağ, belli bir servis kalitesini de sağlamalıdır. Kablosuz ağlarda güvenlik için kullanılan yöntemlerden başlıcaları; WPA şifreleme, VPN, kapalı ağ erişim kontrolü, MAC adresi filtreleme, ateş duvarı yönetimi ve RADIUS (Remote Access Dial-In User Service - Uzak Erişim Çevirmeli Kullanıcı Hizmeti) sunucusudur [3,4].

Yapılan çalışmada, bir adet kablosuz köprü, iki adet erişim noktası ve iki adet istasyon olarak kullanılan, üzerinde kablosuz ağ kartı olan diz üstü bilgisayardan oluşan ekipmanla, genel olarak bahsedilen saldırı türlerinin uygulamaları ve kablosuz ağlarda güvenlik için kullanılan uygulamalar göz önünde bulundurularak ağın tasarımı yapılmıştır. Ağda kullanılan yöntemde, RADIUS sunucusu kablosuz ağ ile kablolu ağın arasında temel istasyon olarak yerleştirilmiştir. Kablosuz ağ üzerinden gelen her istek RADIUS sunucundan izin alarak ağa bağlanmaktadır. Oluşturulan kablosuz yerel alan ağı, Mühendislik fakültesi yerleşkesinde kullanılmaktadır.

2. UYGULAMA

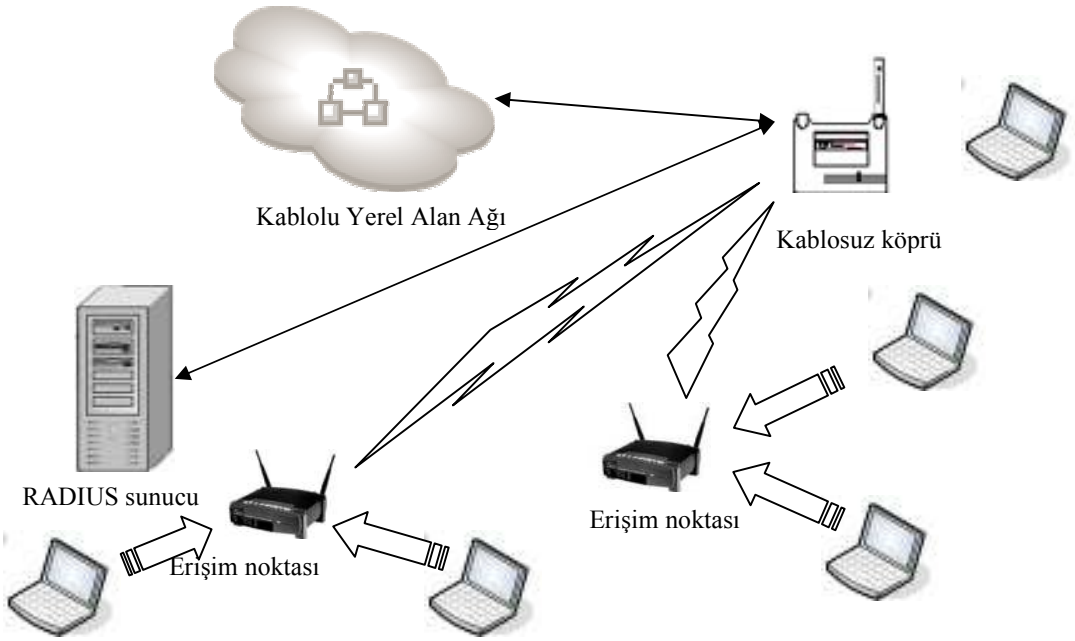
Kablosuz ağların güvenliği için ilk önce saldırı türleri ve açıkların bilinmesi gerekmektedir. Saldırı türleri ilk olarak tarama işlemi ile başlar. Tarama ile erişim noktası bulunduktan sonra dinleme işlemi başlar. Dinlemedeki amaç haberleşme yapan cihazların SSID, MAC adresi, WEP veya WPA anahtarını ele geçirmek olabilir. Bunun dışında ağ trafiğini artırarak iletim hızını

yavaşlatma ve engelleme amaçlı da olabilir. MAC adresi ve SSID bulma işlemi ağ tarama cihazları ile rahatlıkla bulunabilmektedir. Ağa giriş yaptıktan sonra , WEP anahtarının ele geçirilmesi ile artık ağ ele geçirilebilir. Bu sebeple sertifikasyon, WPA ve kimlik doğrulama metotları önem kazanır.

Yerleşke ortamında kablosuz ağ tasarımı yapılırken, ortamın ve kullanıcı sayısının, kullanıcıların kimlik doğrulama işlemlerinin nasıl yapılacağı sorularının aranması gerekmektedir. Yerel ağdaki kapsanan alan, alandaki kullanıcı sayısı kullanılacak cihazların seçiminde kullanılması gerekir. Yerleşkede kullanılacak kablosuz ağda iki en uzak nokta 500 m civarında olduğundan, bir kaç binadan oluşan yapıda olduğundan açık havada kullanılacak omni-anten ve köprü, ve bina içlerinde kullanılacak erişim noktaları gereksinimi duyulmuştur. Ağ tasarımı yapılırken tüm güvenlik kontrolünün tek bir noktadan kontrol etmeye ihtiyaç vardır. Bu sebeple kablosuz ağ ile kablolu ağ birbirinden ayrı olarak düşünülmüş, yapılandırma buna göre yapılmıştır. İki farklı ağ köprü üzerinden birbirine bağlanması gerekmiştir. Açık havada kullanılan omni-anten, bina içinde kullanılamadığından bina içleri için erişim noktaları kullanılmıştır. Her erişim noktası ayrı konfigürasyona gerek kalmadan tüm bağlantıların tek bir noktadan güvenliğinin sağlanması için kimlik doğrulama, yetkilendirme ve hesap yönetiminin yapılabileceği bir RADIUS sunucudur. Tasarlanan ağ yapısı Şekil 1 de gösterimi yapılmıştır.

- Köprü olarak Cisco Aironet 1300 serisi kullanılmıştır. Açık hava omurgada kullanılır, uçtan uca ve uçtan-çok uca bağlantı yapılabilir. IEEE 802.11 b/g standartlarını destekler. WPA, IPSec ve 802.1x kimlik denetimini destekler. Yaklaşık 2 km çapında iletim sağlar.

- Erişim noktası olarak US robotics 5461 kablosuz yönlendirici kullanılmıştır. IEEE 802.11 b/g standartlarını destekler. WPA, IPSec ve 802.1x kimlik denetimini destekler.
- Köprü için 2.4 GHz Çokyönlü Anten seçilmiştir.



Şekil.1 Tasarlanan kablosuz ağ yapısı

Uzaktan Kimlik Doğrulama Araması Kullanıcı Hizmeti (RADIUS); "Uzaktan Kimlik Doğrulama Araması Kullanıcı Hizmeti (RADIUS)" , "RADIUS Hesap Oluşturma" bölümünde açıklanmış olan endüstri standardı bir protokoldür. RADIUS; kimlik doğrulama, yetkilendirme ve hesap oluşturma hizmetleri sağlamak için kullanılır. Bir RADIUS istemcisi (genellikle bir çevirmeli sunucu, VPN sunucusu veya kablosuz erişim noktası) kullanıcı kimlik bilgilerini ve bağlantı parametresi bilgilerini bir RADIUS sunucusuna RADIUS iletisi şeklinde gönderir. RADIUS sunucusu, RADIUS istemci isteğinin kimliğini doğrular, yetkilendirir ve bir RADIUS ileti yanıtı gönderir [5].

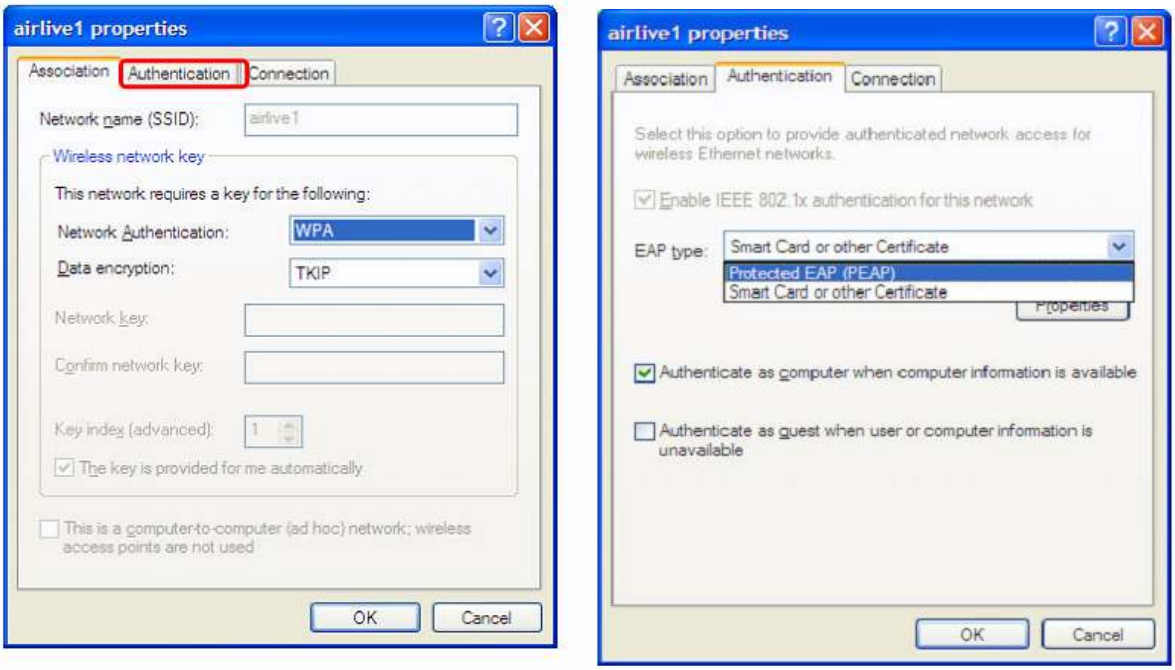
RADIUS protokolünde kimlik doğrulama şu şekilde gerçekleşir: İstemci, erişim noktasına, erişim isteği mesajını gönderir, erişim noktası kimlik bilgilerini sorar, istemci kimlik bilgilerini gönderir, erişim noktası bu bilgileri RADIUS sunucuya iletir. Yetkilenme cevabı, istemciye gönderilir ve istemcinin veri trafiğine devam etmesine izin verilir.

Uygulaması yapılan kablosuz ağda, RADIUS sunucusu Windows 2003 server Enterprise işletim sistemi üzerine, kimlik kontrolü için Active Directory, DNS, IAS servislerine ihtiyaç olduğu için kurulumu yapılmıştır. RADIUS sunucuya bu servisler sağlandıktan sonra, köprünün yapılandırılması gerekmektedir. Köprü yapılandırılması için Şekil 2'de WPA anahtarı kullanarak RADIUS metodu ve kriptolama için TKIP ve AES kullanılır. TKIP, paket düzeyinde anahtar karıştırma işlevi, Michael olarak adlandırılan bir ileti bütünlük denetimi, diziliş kuralları uygulayan genişletilmiş bir ilklendirme vektörü (IV) ve bir yeniden anahtarlama mekanizması gibi özellikler içeren önemli veri şifreleme geliştirmeleri sağlar. AES-CCMP, TKIP iletişim kuralına göre daha güçlü bir şifreleme yöntemi sağlar. RADIUS sunucu ip ve RADIUS için standart olan port no girilir. Tekrar doğrulama zamanı da belirtilir.

İstemcinin, kablosuz ağa bağlanması için, işletim sistemi kablosuz ağ ayarlarından WPA ve kimlik doğrulama protokolü için Şekil 3 teki gösterildiği gibi PEAP seçilir.

PEAP, kablosuz istemciler ve sunucular için birçok farklı kimlik doğrulaması yöntemlerinden birini seçmenize olanak verir. PEAP, kablosuz erişim noktaları arasında hızlı gezinmeye izin veren önbelleğe alınan oturum anahtarları kullanarak bir kablosuz erişim noktasına yeniden bağlanabilme ve yetkisiz kablosuz erişim noktalarının dağıtılmasına karşı kullanılabilen sunucu kimlik doğrulama gibi avantajları vardır. Kullanıcılar yeni bir kablosuz erişim noktasıyla ilişkilendirildiklerinde, istemci ve sunucu, önbelleğe alınma süresi sona erinceye kadar birbirlerine yeniden kimlik doğrulaması yapmak için önbelleğe alınan anahtarları kullanır. Anahtarlar önbelleğe alındığı için, RADIUS sunucusu hızlı bir şekilde istemci bağlantısının yeniden bağlanma olduğunu belirler. Bu, istemcinin kimlik doğrulama isteği ve RADIUS sunucusunun yanıt vermesi arasında geçen bekleme süresini azaltır. Ayrıca istemci ve sunucunun gereksinimlerini sağlar.

Şekil .2 Köprü ayarları



Şekil 3. İstemci WPA ve PEAP seçimi

3. SONUÇ

Yapılan çalışma Kocaeli Üniversitesi tarafından desteklenen araştırma projesidir. Mühendislik fakültesinin fiziksel yapısı göz ününe alındığında, 100 metre mesafe aralıklı binalar arasında toprak altından geçen kabloların olduğu düşünülürse, bağlantı kolaylığı ve yönetimi bakımından büyük yararlar sağlamıştır. Dersliklerin, labaratuvarların ve bölümlerin farklı binalarda olduğu göz önünde bulundurduğumuzda maliyet ve kurulum bakımından da yararlarının olduğu rahatlıkla söylenebilir.

Kablosuz ağlarda güvenliği sağlamak amacıyla ortaya konulan kimlik doğrulama yöntemleri güvenliği korumada yardımcı olmaktadırlar. Kablosuz ağlarda güvenlik için uygulanacak yöntemin seçimi işlemi, oluşturacak ağın fiziksel yapısına, elde bulunan cihazların modeli ve kullandığı yazılımlara göre değişebilmektedir. Güvenlik için yapılan gereğinden fazla kontrol ise ağ iletim performansını negatif olarak etkileyebilir. Ağ tasarımı yaparken sadece güvenliği göz önünde bulundurmak yeterli olmayabilir, iletim kalitesini de dikkate alarak yapılandırma yapılması gerekmektedir. Çalışmanın devamı olarak oluşturulan güvenli ağ için servis kalitesi üzerine çalışmalar yapılabilir.

KAYNAKLAR

1. Park J.S. , Dicio D. “WLAN Security: Current and Future”, IEEE İnternet Computing,2003
2. Maple C., Jacobs H., Reeve M., “Choosing the Right Wireless LAN Security Protocol for the Home and Business User”, ARES’06, 2006
3. Sankar K. , Sundaralingam S. , Balinsky A. , Miller D. , “Cisco Wireless LAN security” , Cisco Press, 2004
4. Frankie Chan K. L , Hoon A.H. , Issac B. , “Analysis if IEEE 802.11b Wireless Securirty for University Wireless LAN Design”, IEEE, 2005
5. http://technet2.microsoft.com/Windows Server/f/?tr/Library