RC4 Tabanlı WPA(Wi-Fi Protected Access)'da Kullanılan TKIP(Temporal Key Integrity Protocol) Şifrelemesinin İncelenmesi

Deniz Mertkan GEZGİN
Trakya Üniversitesi
Sarayiçi Yerleşkesi
Teknik Bilimler Meslek Yüksekokulu
Bilgisayar Tek. Ve Prog. Bölümü
EDİRNE
mertkan@trakya.edu.tr

Ercan BULUŞ
Namık Kemal Üniversitesi
Çorlu Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü
Çorlu / TEKİRDAĞ
ercanbulus@corlu.edu.tr

Anahtar Kelimeler: *RC4 Şifreleme Algoritması, Geçici Anahtar Bütünlüğü Protokolü (Temporal Key Integrity Protocol- TKIP),Wi-Fi Korumalı Erişim(Wi-Fi Protected Access - WPA)*

ÖZET

Kablosuz ağlarda güvenlik konusu kablosuz ağların kullanımı yaygınlaştıkça önem kazanmış, günümüz teknolojilerinde ise vazgeçilmez bir kıstas halini almıştır. Kablosuz ağ cihazlarında kullanılan güvenlik politikaları ile saldırganların önüne geçilmeye çalışılmaktadır.

Bu güvenlik politikalarından ilki Kabloluya Eşdeğer Gizlilik anlamına gelen WEP(Wired Equivalent Privacy)'tir. WEP, alt yapısında RC4 akış şifreleme algoritmasını kullanır.[9] Kablosuz Ağların ilk zamanlarında işe yarasa da RC4 'ün zayıflıklarını barındıran WEP, saldırılara karşı fazla dayanamamış ve kırılmıştır. WEP' in bu zayıflıklarını ortadan kaldırmak için mevcut cihazlarla uyum sağlayabilen ve WEP' in zafiyetlerini geçici olarak da olsa gideren WPA(Wi-Fi Protected Access) standardı Wi-Fi Alliance tarafından oluşturulmuştur. WPA protokolü; tüm kablosuz cihazların güncellenmesi ile yeni protokolün kullanılmasına olanak tanımış ve kablosuz teknolojileri yeni bir düzeye taşıyabilmiştir. Bu gelişmeler son olarak IEEE(Institute of Electrical and Electronics Engineers) tarafından 802.11i (WPA2) adı ile bir standart olarak tanımlanmış ve güvenli bir yapı halini almıştır. Halen her kablosuz cihazda WEP, WPA ve WPA2 protokolü güvenlik için kullanılmaktadır.

Çalışmamızda WPA protokolünün algoritmik yapısı incelenerek WPA' nın, WEP'ten üstünlüğünü sağlayan TKIP(Temporal Key Integrity Protokol)'in özellikleri ve güvenlik özellikleri üzerine incelemeler yapılmıştır.

1.WPA(Wi-Fi Protected Access)

IEEE 802.11i kablosuz ağ standardı, kablosuz yerel alan ağı (LAN) güvenliğindeki gelişmeleri belirtir. Yeni IEEE 802.11i standardı onaylanırken, kablosuz ürün satıcıları Wi-Fi Korumalı Erişim (WPA) olarak bilinen, çeşitli sistemlerin birlikte çalışmasına olanak veren geçici bir standart üzerinde anlaşmıştır.Geniş şekilde kullanılan bu iki tip WPA standardı WEP 'in zayıf yönlerini kapatmak için geçici olarak oluşturulmuştur. Mevcut cihazlar güncellenirse bu protokolü kullanabilir. Günümüzde cihazlarda desteği eklenmiş durumdadır.

WPA' nın WEP'e tercih edilmesinde üç önemli sebep vardır. Bunlar;

- 802.1X/EAP tabanlı karşılıklı asıllama sağlamaktadır.
- WEP'e göre daha güçlü bir şifreleme yöntemi olan TKIP (Temporal Key Integrity Protocol)'i desteklemektedir.

• Veri bütünlüğü için MIC (Michael-Message Integrity Code) yöntemini kullanmaktadır.

Bu üç gelişim, WEP'in üç ana amacını gerçekleştirebilmek amacıyla WPA'da yer almıştır. Bu gelişmeye rağmen WPA geçici bir protokoldür. WPA'da Anahtar uzunluğu olarak 128 bit kullanılır. WPA'da anahtar her oturum ve her paket için değişir, dolayısıyla daha yüksek bir güvenlik elde edilmiş olur. WPA'da anahtar yönetimi için 802.1x kullanılır. Kimlik doğrulama için WPA, 802.1x EAP ile güçlü bir yöntem kullanmıştır. WEP' te veri bütünlüğü ICV ile sağlanırken, WPA' da daha güçlü olan MIC(Message Integrity Code) mekanizması ile sağlanır. WPA kimlik doğrulama/yetkilendirme için iki seçenek sunmaktadır[4][5]

1.1. WPA-PSK yapısı

Ev kullanıcıları ve küçük işletmeler için tasarlanmıştır. 8-63 karakter arası bir şifre belirlenir. Bu anahtarın Erişim Noktası tarafında ve istemci tarafında girilmesi gerekmektedir. Buna pre-shared yani paylaşılmış anahtar denilir. Kablosuz ağ bağlantıları özelliklerinden authentication (kimlik doğrulama) metodu olarak WPA-PSK seçilerek uygulanır. Kurumsal kablosuz ağlarda kullanımı uygun değildir.

1.2. 802.1x yapısı

IEEE 802.1x, port tabanlı ağ erişim kontrol mekanizmasıdır ve uzaktan erişim, VPN, anahtarlama cihazı vb. uygulama/birimlerin kimlik doğrulama/yetkilendirme yöntemi olarak kablolu ağlarda kullanılmaktadır. 802.1x erişim kontrolünde yer alan bileşenler: istemci (dizüstü, PDA, cep telefonu, PC vb.) , erişim noktası ve RADIUS / TACACS erişim kontrol sunumcusudur. İstemciler bağlantı isteklerini erişim noktasına bildirirler, erişim noktası isteği RADIUS / TACAS sunumcuya yöneltir ve kimlik doğrulama / yetkilendirme işlemini RADIUS / TACACS [4][7] sunumcu gerçekleştirerek sonucu erişim noktası ve istemciye bildirir. Sonuca göre erişim noktası istemciye bağlantı için sanal bir port açar. Bu işlemler sonucunda ek olarak erişim noktası ve istemci arasındaki şifreli haberleşmelerde kullanılacak şifreleme anahtarları oluşturulur.

2.TKIP(Temporal Key Integrity Protokol)

Çokça tatbik edilen yeni şifreleme protokolü TKIP'tir. TKIP 'in geliştirilmesindeki en büyük etken, WEP tabanlı donanımın güvenliğinin arttırılması ve güncellenmesidir. Genel olarak, WEP kullanan donanımların yonga setleri RC4 şifreleme için donanım desteği sağladı. Donanıma yoğun uygulanan şifreleme ile yazılım donanım ve firmware güncellemeleri geri kalanını mümkün kılmıştır. TKIP, WEP 'in temel yapısına ve işlemlerine sahiptir. WEP tabanlı çözümlere karşılık bir yazılım güncellemesi olarak tasarlanmıştır. Esas olarak WEP kusurlu olarak gösterildiği için protokol onu WEP'ten ayırabilmek için yeniden adlandırılmıştır. TKIP yukarıda belirtildiği gibi RC4 akış şifrelemesini de kullanır. Sebebi WPA tam bir güvenlik standardı olarak gelişmemiştir. WEP'in açıklarını kapatmak için WEP 'te kullanılan donanımları değiştirmeden güncelleme ile WPA' ya geçişi sağlanmıştır. Bir saldırıya karşı WEP'in zayıf noktalarını savunabilmek için, TKIP çok çeşitli yeni protokol özellikleri ile işbirliği yapar. TKIP, WEP in temel mimarisi ve işlemlerine sahiptir. Ama ayrıca WEP 'in en zayıf noktalarına "Güvenlik Zinciri" ekler.

WEP'ten farklılıkları aşağıda sıralanmıştır.

- *Anahtar hiyerarşisi ve otomatik anahtar yönetimi(802.1x):*

Wep'te anahtar yönetimi olmadığı için, anahtarı saldırganların çözmesi ve ele geçirmesi kolaylaşmıştır. Bunun için 802.1x anahtar yönetimi mekanizması ile anahtar dinamik hale gelmiştir.

- *Frame(Çerçeve) başına anahtarlama:*

TKIP, WEP'in RC4 tabanlı frame(paket) şifrelemesi sağlamasına rağmen zayıf WEP anahtarlarına karşı saldırıları azaltmak için her frame (ana anahtardan) için tek bir RC4 anahtarı türetmektedir. Her bir anahtar için, tek bir anahtarın türediği sürece anahtar karıştırma denir.

- *Sıra Sayacı:*

Her bir frame'i sıra numarası vererek, saldırı durumunda saldırganların geçerli trafiği ele geçirmeleri ve daha sonra yeniden iletme durumunda cevap saldırılara karşı hafifleterek servis dışı frameler etkisiz hale getirilebilir.

- *Yeni mesaj Bütünlük Kontrolü (Message Integrity Check -MIC) :*

TKIP, Michael da denilen daha güvenli kriptografik bütünlük kontrol hashing algoritmasını kullanarak, WEP'in doğrusal hash'inin yerini alır. Frame hırsızlığını tespit etmek için daha güvenli hashing bunu kolaylaştırır. Ek olarak kaynak adres bütünlük kontrolü ile korunan parçalar arasındadır. Böylelikle belli bir kaynaktan geldiğini iddia eden çalınmış frameleri tespit etmek mümkündür.

- *Mesaj bütünlük kontrol hatalarındaki karşı önlemler:*

TKIP, varolan donanım üzerine uygulanmak için tasarlanmıştır ve bir sürü kısıtlamadan etkilenmektedir. Michael göreceli kolaylıkla aktif saldırı durumunda tehlikeye girebilir. Böylelikle TKIP aktif saldırından gelen zararları sınırlandırmak için karşı önemleri içermektedir.

- *Zayıf Anahtarlar kullanılmamaktadır.*

- *IV 48 bite çıkarılmıştır:*

IV(Initialization Vector) hem paketlere sıra numarası vermek, hem de her paket için tek kullanımlık anahtar üretmede de kullanılmaktadır. 48 Bitlik IV ve aynı TK(Temporal Key) ile üretilecek tek kullanımlık anahtarlar 100 yıl sonra tekrarlanır. Her paket için kullanılan IV değeri TKIP'te değişmektedir. Bu da Zayıf anahtarları önlemektedir.

- *Anahtar uzunluğu 128 bite çıkarılmıştır.*

Bu değişiklikler sayesinde kırılamayan bir mekanizma oluşturulması hedeflenmiştir.[6][8]

2.1 TKIP' de Veri İşleme Ve Çalışma Prensibi

WEP gibi, TKIP, aynı sürecin parçası olarak şifreleme ve bütünlük koruması için destek sağlar. Bu şekil-1'de gösterilir. TKIP'in tasarımı emniyetin bir takımı olarak ortaya çıkmıştır. WEP'in etrafında bir çember olarak WEP'i desteklediği tamamen açıktır.

Giriş olarak, TKIP, takip eden maddeleri içerir.

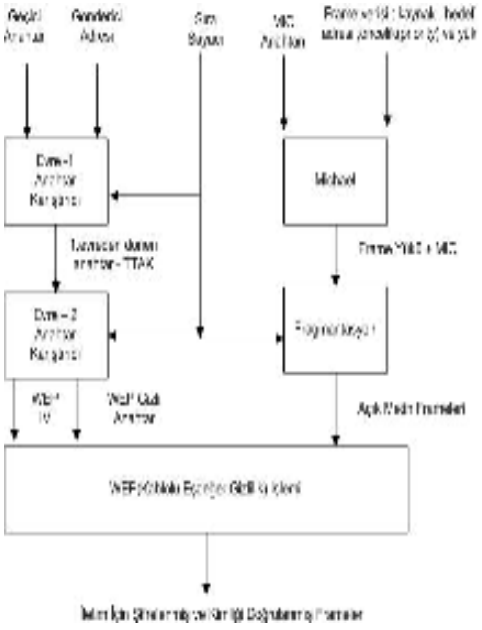
- Frame

- Temporal Key(Geçici anahtar), frame'i şifrelerdi.

- Bir MIC anahtarı Michael'le, yapı içeriğini korurdu. TKIP, anahtarların bir çiftini öyle türetir ki istemciden AP(Access Point - Erişim Noktası)'ye MIC anahtarı ile AP'den istemci arasındaki MIC anahtarından farklıdır. TKIP'in, WEP'den ayrıldığı en önemli noktalardan biri, MIC'in, bir anahtar kullandığıdır.

- Verici adresi, TKIP'e bir giriş olarak kullanılır çünkü kaynak belgelemesini yapmak için gereklidir. Verici adresi, frame ile sağlanır ve daha yüksek seviye yazılım ile sağlanmaya ihtiyaç duymaz.

- Bir sıra sayacı, sürücü veya firmware tarafından tutulur.

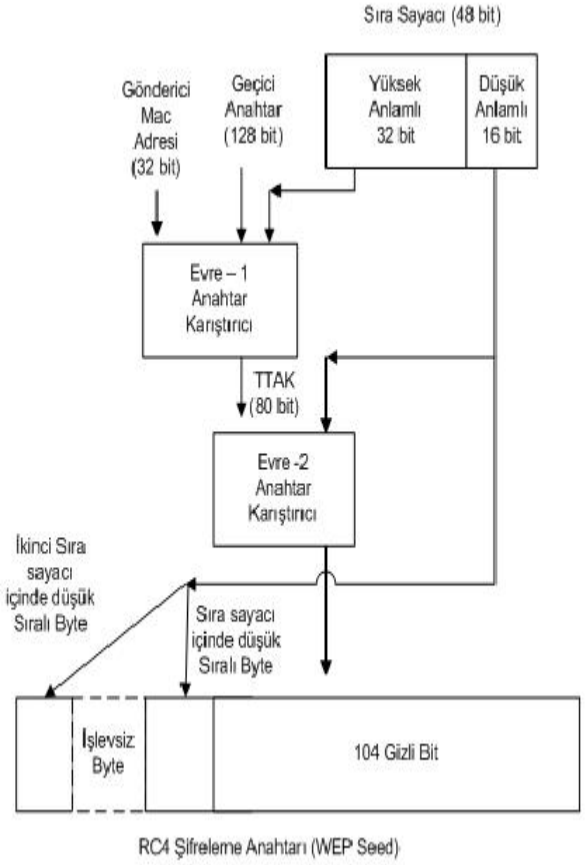


MIC– Message Integrity Check
TTAK– result of phase 1 key mixing of Temporal Key
WEP – Wired Equivalent Privacy
WEP IV – Wired Equivalent Privacy Initialization Vector

Şekil 1 – TKIP Veri Şifreleme İşlemi

2.2. TKIP' de Anahtar Karıştırma İşlemi

WEP'te aynı anahtar ile şifrelenmiş frame dayalı saldırılar yapılabilmekteydi. WPA da bu saldırıları engellemek hususunda her paket için farklı anahtarlar üretilmesi öngörülmüştür. TKIP, her yapı için benzersiz bir anahtar türetir. Anahtar, başa döndürme vektörü(IV) ,sıra sayacı, frame'in vericisinin adresi ve geçici anahtar ile üretilir. Bu ilk adımda 80 bitlik bir ara anahtar elde edilir. Buna TTAK ismi verilir. Böylece Anahtar karıştırma işlemi anahtarın, kullandığını garanti etmiş ve WEP anahtarının gizli bileşeninin, çerçevelemek için yapıdan sabit olduğunu farz eden herhangi bir saldırıyı engeller. TKIP, karışık anahtarın hesaplamasını ayırır. Evre birde giriş olarak başta belirtildiği gibi verici adresi, 48 bitlik sıra sayacının yüksek anlamlı 32 bitlik parçası(IV) ve 128-bitlik geçici anahtardır. Çıktı olarak ise 80-bitlik bir ara anahtar değerini verir. Hesaplamanın, biraz karışık olmasına rağmen, o, tamamen toplama gibi "Kolay" çalışmalarından dayanır ve özel XOR işlemleri ve S-BOX işlemlerine dayanır. Anahtar karıştırma görevin evre ikisi, her yapı için hesaplanmalıdır. Giriş olarak, ikinci evre, birinci evrenin verdiğini, geçici anahtar ve sıra sayacının(IV) düşük anlamlı 16 bitini alır. Yapıdan çerçevelemek için değiştirilen tek giriş, sıra sayacıdır. Böylece Anahtarlar her oturum, her paket için değişir.



Şekil 2 – TKIP Anahtar Karıştırma İşlemi

2.3. TKIP' de Veri İletimi

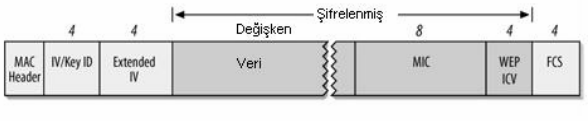
Bir frame oluşturulduğu ve aktarma için TKIP'e yollandığı zaman, olayların takip eden sırası aşağıdaki gibidir.

1. 802.11 frame'i iletim için kuyrukta beklenir. Frame, bir frame başlığı ve yükü(payload) içerir. WEP gibi TKIP'te, sadece 802.11 MAC yükünü korur ve 802.11 frame başlığını ile bağlantıyı keser.
2. Mesaj bütünlük kontrolü (MIC), hesaplanır. WEP'den farklı, TKIP'in

MIC'i, daha sağlam kriptografik bir algoritmaya sahiptir. O, onun geçerli kılma sürecinin parçasının olduğu gibi gizli bir anahtarı kullanır ve 802.11 frame yükünden çok daha fazla korur. Yapı verisine ek olarak, MIC, kaynağı birleştirir ve varış yeri, gelecek 802.11e standardı ile kullanılacak olan öncelik parçalarının toplamasına ek olarak hitap eder.

3. Sıra sayacından gelen sayılar, yukarı kısımdan gelen parçalara tayin edilir. WEP başa döndürme vektörlerinden farklı, TKIP'in sıra sayacı, her parça için sayıyı bir artırır.
4. Her frame, WEP anahtarı ile benzersiz şifrelenir. Anahtar karıştırıcılar görevleri tamamlayarak, TKIP'te, WEP anahtarını, her yapı için farklı anahtar üretir. Yapı başına anahtar, bir IV olarak WEP'e gizli bir anahtarla beraber geçilir; Her iki bileşen, her yapı için değiştirilir.
5. İkinci adımdan Michael mesaj bütünlük kontrol değeriyle beraber yapı, ve adım dörtten RC4 anahtarı ile WEP'e geçilir, Buda bize TKIP ile korunan bir yapının da, WEP bileşenlerini kapsayacak olduğunu ifade eder.[1][3]

Sonuç olarak aşağıda da TKIP'te kapsüllenmiş bir frame yapısı gösterilmektedir.



Şekil 3 – TKIP Kapsüllenmiş Frame Yapısı

3.Mesaj Bütünlük Kontrolü (MIC)

802.11 ve WEP ile, veri bütünlüğü 802.11 yüküne eklenen ve WEP ile şifrelenen bir 32 bit bütünlük denetim değeri (ICV) ile sağlanır. ICV şifrelenmiş olsa da, şifrelenmiş yüklerdeki bit değerlerini şifreleme incelemesi kullanarak değiştirebilir ve şifrelenmiş ICV'yi alıcı algılamadan güncelleştirebilirsiniz.

WPA ile, Michael olarak bilinen bir yöntem, varolan kablosuz aygıtlarda kullanılan hesaplama olanakları yardımıyla 8 baytlık bir ileti bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC, IEEE 802.11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir.[2]

Michael ayrıca yeniden gönderme koruması sağlar. Yeniden gönderme saldırılarını engellemek amacıyla, IEEE 802.11 çerçevesinde yeni bir çerçeve sayacı kullanılır.

4.SONUÇ

WEP'in açıklarını kapatmak için oluşturulan WPA standardı, ara geçiş güvenlik standardı olmasına karşın büyük ölçüde gereksinimleri yerine getirmiştir. Ev kullanıcıları ve yüksek güvenlik seviyesi gerektirmeyen sektörlerde kullanılması uygundur. WPA'da bu gelişim TKIP protokolü ile sağlanmaktadır. Fakat son zamanlarda yapılan çalışmalar, TKIP'inde RC4 yapısını kullanması ve matematiksel bazı saldırılara karşı açıkları olduğunu göstermektedir.[10][11] Sonuç olarak geçici güvenlik için TKIP bazı uygulamalar için uygun olmakla birlikte yüksek güvenlik gerektiren şirketlerde güvenli bir kablosuz ağ için AES destekli 802.11i (WPA2) standardını kullanmak en iyi seçim olarak görülmektedir.

KAYNAKLAR

1. 802.11® Wireless Networks The Definitive Guide By Matthew GastApril 2005 ISBN: 0-596-10052-3

2. Ender Yüksel , Müjdat Soytürk , Tolga Ovatman , Bülent Örencik ,"Telsiz Yerel Ağlarında Güvenlik Sorunu",2005

3. IEEE Std 802.11i-2004, \Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE, July 2004.

4. WPA and WPA2 Implementation White Paper " Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise", March 2005

5. http://en.wikipedia.org/wiki/WiFi_Protected_Access

6. Stephen Glass, Vallipuram Muthukkumarasamy," A Study of the TKIP Cryptographic DoS Attack", ICON 2007

7. Deniz Mertkan GEZGİN , Ercan BULUŞ ,Halil Nusret BULUŞ "The security suggestıons for wireless access points",Yambol,2009

8. 802.11 Security series , Part II: the Temporal Key Integrity Protocol(TKIP) , Jesse Walker Network Security Architect, Platform Networking Group Intel Corporation

9. S. Fluhrer, I. Mantin, and A. Shamir, \Weaknesses in the key scheduling algorithm of RC4," Proc. SAC2001, Lecture Notes in Computer Science, vol.2259, pp.1{24, Springer-Verlag, 2001.

10. E. Tews, R. Weinmann, and A. Pyshkin,\Breaking 104 bit WEP in less than 60seconds," Cryptology ePrint, 2007, available at http://eprint.iacr.org/2007/120.pdf

11. Toshihiro Ohigashi ,Masakatu Morii,A Practical Message Falsi_cation Attack on WPA, http://jwis2009.nsysu.edu.tw/location/paper/A Practical Message Falsification Attack on WPA.pdf