
# KABLOSUZ AĞLARA YAPILAN SALDIRILAR

# - İstanbul Şehir Üniversitesi -

# Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

**NOT:** Eğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

**Hazırlayan:** Hüseyin Uçan

**Tarih:** 29.05.2016

# Kablosuz Ağlara Yapılan Saldırılar

Kablosuz Ağların kullanımı arttıkça kablosuz güvenlik konusu da çok fazla önem kazanmıştır. Saldırganlar standart haline gelmiş kablosuz güvenliğin üzerinde açıklıklar aramakta ve çeşitli amaçlar doğrultusunda bazı yöntemler kullanarak saldırılar yapmaktadırlar. Bu saldırılar bazen hafif zararlar verse de ticari kuruluşlar ve iletişimin devamlılığının yüksek önem arz ettiği sistemler için büyük zararlara sebebiyet verebilmektedir.

Bu bölümde saldırganlar tarafından kablosuz ağlara yapılan saldırılar aşağıdaki 5 ana başlık altında anlatılmıştır: [1,2]

1. Erişim Kontrolü Saldırıları
2. Gizlilik Saldırıları
3. Bütünlük Doğrulama Saldırıları
4. Kimlik Doğrulama Saldırıları
5. Kullanılabilirlik Saldırıları

**1.Erişim Kontrolü Saldırıları**
Kablosuz ağda bulunan erişim kontrol önlemlerini atlatıp sisteme sızmak için yapılan saldırılardır.

*Kablosuz Ağları Tarama (War Driving)*: Araştırma isteklerini ya da beacon(hat kesme iletisi) denilen istemcilerin dinlemeye geçmesi için gönderilen iletileri dinleyerek kablosuz bir ağ keşfetmektir. Bu sebeple diğer saldırılar için bir başlangıç adımı sayılabilir.

*Yetkisiz Erişim Noktası (Rogue Access Point)*: Güvenli bir ağ içinde bir arka kapı yaratmak için, güvenlik duvarının iç tarafında bir güvensiz erişim noktası kurulmasıdır.

*Güvenli Olmayan Ağa Bağlanma (Adhoc Associations)*: Saldırı istasyonu ya da erişim noktası güvenliğini engellemek için doğrudan güvenli olamayan istasyona bağlanmak.

*Mac Adres Sahteciliği (Mac Spoofing)*: Güvenli bir erişim noktası veya istasyon süsü vererek saldırganın MAC adresini tekrar konfigure etmesidir.

*Ip Adresi Yanıltma (Ip Spoofing)*: Ip spoofing yaparak başkasının IP adresinden istenilen internet aktivitesi yapılabilir. Artık pratik olarak geçersizdir. Bunun

temel nedeni günümüz modern işletim sistemlerinin protokoldeki eksik noktalara kalıcı çözüm getirmeleridir.
*802.1x Radius Cracking*: Şeytan İkizi Erişim Noktası (Evil twin AP)'nın kullanması için kaba kuvvet yoluyla 802.1x erişim isteklerinden RADIUS gizlilerini elde etmektir. [1,2]

## 2.Gizlilik Saldırıları

Bu ataklar kablosuz bağlantılar üzerinden gönderilen özel bilgileri engellemek için yapılırlar.

*Gizli Dinleme (Eavesdropping)*: Yakalanmış ve şifresi çözülmüş korumasız uygulama trafiği içinde olanak dâhilinde hassas bilgiyi ele geçirir. Gizlice dinleme anlamına da gelir.

*Wep Anahtarı Kırma (Wep Key Cracking)*: WEP'in açıklık ve zafiyetlerine aktif ya da pasif saldırılar düzenlenerek WEP anahtarının ele geçirilmeye çalışılmasıdır. Frekans bandı dinlenerek sonuca varılmaya çalışılır. Pasif Saldırılar IV çakışmalarından elde edilen sonuçlara göre yapılan saldırılar olup, aktif saldırılar ise tekrar saldırıları ve mesaj içeriğini değiştirerek yapılan saldırılardır.

*Şeytan İkizi Erişim Noktası (Evil Twin Ap)*: Saldırganlar, söz konusu sistemi şaşırtmak için, kullanılmakta olan erişim noktasının bir benzerini oluşturup, kullanıcıların bu erişim noktasını kullanmasını sağlayabilirler. Böylelikle oluşturulan sahte erişim noktasına giren kullanıcıların tüm bilgileri elde edilebilir.

*Erişim Noktası Üzerinde Sahte Portal Çalıştırmak (Ap Phishing)*: Saldırganlar kullanıcıların Evil Twin AP'ye bağlanmasından sonra bir web sunucusu kurarak, bu saldırganları çeşitli web sayfalarına yönlendirip, hedef kişiler hakkında sayfadaki zararlı kodlar vasıtasıyla bilgi toplayabilirler.

*Ortadaki Adam Saldırısı (Man In The Middle)*: TCP oturumlarını veya SSL/SSH tünellerini kesmek için Şeytan İkizi Erişim Noktası(Evil Twin AP) üzerinde geleneksel ortadaki adam saldırı (Man in the Middle) araçlarını çalıştırarak yapılan araya girme saldırılarıdır. [1,2]

## 3.Bütünlük Doğrulama Saldırıları

Diğer atak tiplerini kolaylaştırmak veya alıcıyı yanıltmak için sahte kontrol, yönetim veya kablosuz iletişim üzerinden veri paketleri göndermek üzerine kuruludur.

*Servis Reddi Saldırıları (DoS Attacks)*: DoS atakları karşı sistemde çalışan servisin durdurulması veya çalışmasının aksatılmasını hedefleyen saldırı tipidir. Saldırgan

istemci diğer legal istemcilerin bilgi erişimini ya da servis erişimini engellemeye çalışır.
*802.11 Paketi Püskürtme (Frame Injection)*: Bu yöntem, sahte 802,11 paketlerini erişim noktalarına ya da saldırgana göndererek, bir süre sonra kaynağın ya servis dışı olmasını ya da gerekli bilgileri dışarı vermesini sağlar.

*802.11 Veri Tekrarlama (802,11 Data Replay)*: Bir saldırı tekrarı için hem paket toplamak, hem de aynı zamanda bu paketleri yineleyerek püskürtmek amaçlıdır.

*802.1x EAP Tekrarlama (802.1x EAP Replay)*: 802.1x genişletilebilir kimlik doğrulama protokollerinden paket yakalamak amaçlıdır. Böylece sisteme bu paketlerle tekrar saldırısı yapılabilir.

*802.1x Radius Tekrarlama (802.1x Radius Replay)*: RADIUS erişim kabul veya ret mesajlarını yakalamaktır. Erişim noktası ile kimlik doğrulama ana makinesi arasında tekrar saldırıları yapıldıktan sonra gelen adımdır. [1,2]

**4.Kimlik Doğrulama Saldırıları**
Saldırganlar bu atakları legal kullanıcıların kimlik bilgilerini çalarak özel bir ağa veya servise bağlanmak için kullanırlar.

*Shared Key Guessing*: Kırılmış WEP anahtarı ya da varsayılan sağlayıcı ile 802,11 paylaşımlı anahtar kimlik doğrulayıcısını tahmin etme girişiminde bulunmaktır.

*PSK Cracking*: Sözlük Saldırı araçları kullanarak kaydedilmiş anahtar tokalaşma (handshake) paketlerinden WPA/WPA2 PSK'yı elde etmektir.

*Application Login Theft*: Açık Metin uygulama protokollerinden kullanıcı bilgilerini yakalamadır.(e-mail, adres, şifre)

*Domain Login Cracking*: Sözlük veya kaba kuvvet saldırıları kullanan karma NETBIOS şifre kırma işlemi yoluyla kullanıcı bilgilerini (Windows Giriş ve şifre) elde etmektir.

*VPN Login Cracking*: VPN kimlik doğrulama protokolleri üzerinde kaba kuvvet saldırıları kullanarak kullanıcı kimlik bilgilerini(PPTP şifresi veya IPsec Preshared Secret Key) elde etmektir.

*802.1x Identity Theft*: Açık metin 802.1X Kimlik yanıtlama paketlerinden kimlik bilgilerini yakalamaktır.

*802.1x Password Guessing*: Elde edilen bir kullanıcı adı ile 802.1X kimlik doğrulama yönteminde kullanıcın şifresini tahmin etmek için ardı ardına girişimde bulunmaktır.

*802.1x LEAP Cracking*: NT şifre karmalarını kırmak için sözlük saldırı araçları kullanarak kayıt edilmiş EAP(LEAP) zayıf 802.1X paketlerinden kimlik bilgilerini elde etmektir.
*802.1x EAP Downgrade*: Sahte EAP-Response/Nak paketleri kullanarak 802.1X Serverı bir zayıf kimlik doğrulama tipine istekte bulunmaya zorlar. [1,2]

**5.Kullanılabilirlik Saldırıları**
Bu ataklar, yasal kullanıcılara yönelik kablosuz servislerin verimini azaltmak veya engellemek için kullanılır. Amaç, gerek bu kullanıcıların WLAN kaynaklarına erişimini engellemek gerekse de kaynaklarını azaltmaya yöneliktir.

*AP Theft*: Kullanım uzayından fiziksel olarak erişim noktasını çıkarmaktır.

*Queensland DoS*: Meşgul görünen bir kanal yapmak için CSMA/CA'dan yararlanmaktır.

*802.11 Beacon Flood*: İstasyonların yasal bir erişim noktasını bulmasını zorlaştırmak için binlerce sahte 802. 11 beacon(hat kesme iletisi) üretmektir.

*802.11 Associate / Authenticate Flood*: Bir erişim noktasının dâhil olma (association) tablosunu doldurmak için rastgele MAC adreslerinden sahte kimlik doğrulama ve dâhil olmaları göndermektir.

*802.11 TKIP MIC Exploit*: Geçersiz TKIP verileri üreterek, erişim noktasının MIC hata eşiğini aşmasını, WLAN servislerinin askıya alınmasını sağlar.

*802.11 Deauthenticate Flood*: Erişim noktasından, bağlı olmayan kullanıcıları istasyonlar aracılığıyla sahte kimlik doğrulamama ve dâhil olmama mesajlarına boğmaktır.

*802.1x EAP-Start Flood*: Hedefi çökertmek ya da kaynakları tüketmek için EAP-Start mesajları aracılığıyla erişim noktasını boğmaktır.

*802.1x EAP-Failure*: Geçerli bir 802.1x EAP değişimini gözlemledikten sonra istasyona sahte EAP-Hata mesajları göndermektir.

*802.1x EAP-ofDeath*: Hatalı oluşturulmuş 802.1x EAP kimlik yanıtı göndererek bilinen bir erişim noktasını çökertmeye çalışır.

*802.1x EAP Length Attacks*: Kötü uzun alanlar aracılığıyla EAP özel tip mesajlar göndererek bir erişim noktası veya RADIUS sunucuyu çökertmeye çalışmayı denemektir. [1,2]

## WEP Standardına Yönelik Kriptografik Saldırılar

WEP' in geliştirilme amaçlarının başında çözüm getirmesi beklenen üç başlık bulunmaktadır;

Kimlik Doğrulama (Authentication)

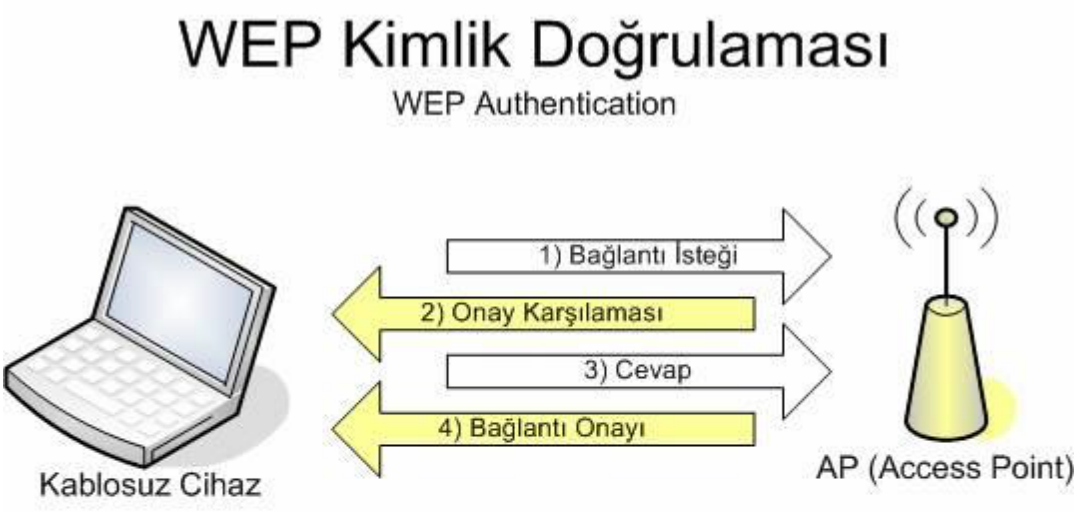
Gizlilik (Privacy)

Bilgi Değiştirme Kontrolü (Message Modification Control)

Bu başlıklar dışında aslında çözüm getirilmesi beklenen Cevap Kontrolü (*Replay Control*), Erişim Kontrolü, Anahtar Dağıtımı ve Korunması konularına WEP'in getirdiği bir çözüm yoktur. Bu problemlere WPA, RSN gibi standartlar ile çözüm getirilmeye çalışılmıştır.

## WEP Kimlik Doğrulama mekanizması

Kimlik doğrulama mekanizmasında hedef, ağa bağlanan kişinin gerçekten ağa bağlanma yetkisinin olup olmamasının kontrolü ve ağa bağlı kişinin trafiğinin diğer kişiler tarafından izlenilememesinin kontrolüdür.
WEP' in kimlik doğrulama mekanizması şu şekilde çalışmaktadır;




1) Bağlantı İsteği

2) AP rasgele bir metin oluşturur (128bit) ve Kablosu Cihaza gönderir

3) Cihaz kendisindeki WEP şifresi (secret key) ile bu gelen metni şifreler AP' ye şifrelenmiş metni gönderir

4) AP gelen geri gelen şifrelenmiş metinin doğru olduğuna onay verir

*WEP Kimlik Doğrulama Mekanizması*

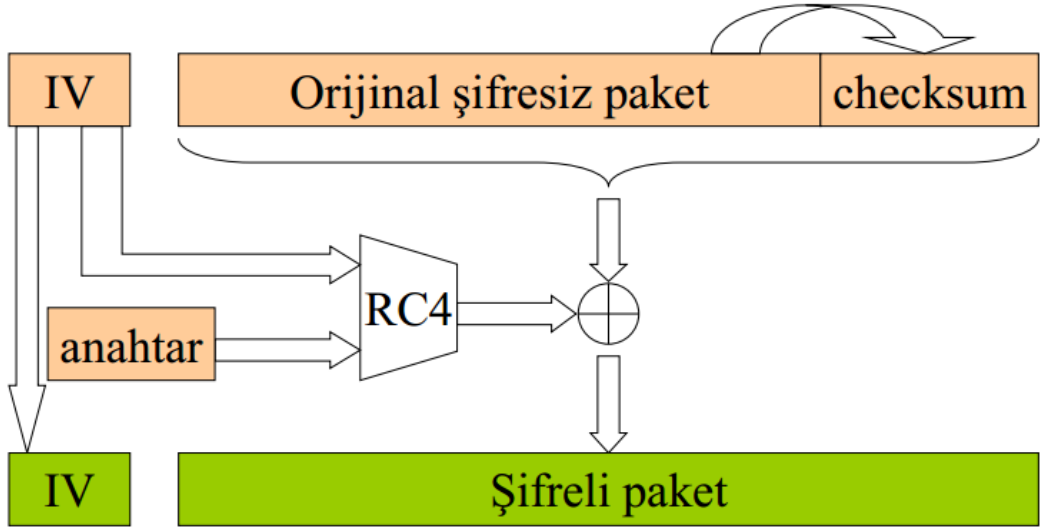
Şekilde gösterilen 3. ve 4. adımlar WEP bağlantılarında onay mekanizması için kullanılır. 4. Adım ise AP istemci cihaza Durum Kodu (***Status Code***) göndererek erişim yetkisi verir veya kısıtlar.

Burada iki ciddi sorun vardır. Birincisi; kablosuz cihaz karşıdaki AP kimliği hakkında ve AP' nin şifreyi bilip bilmemesi hakkında gerçek bir fikri olmamasıdır. Çünkü AP erişim isteyen cihaza sadece onay mesajı döner. Yani cevap dönen herhangi bir AP (fake AP) olabilir ve her isteğe doğru durum kodu ile cevap verebilir. Karşılıklı onay (*mutual*) bu durumda sağlanmamış olur.
Kimlik doğrulama mekanizması sırasında karşılaşılan implementasyon sorunlardan bir diğeri de; onay süreci ve veri trafiğinin şifrelenmesinde aynı anahtarın kullanılması durumudur.
İkinci sorun ise; bağlantı trafiğini dinleyen (*sniff*) saldırgan, iki kritik bilgiyi ele geçirebilir. Kimlik doğrulama sırasında 2. Adımdaki şifrelenmemiş metin (*plaintext*) ve 3. adımdaki şifreli metin(*chipertext*). Saldırganın elde ettiği bu bilgiler ile kriptografik saldırı gerçekleştirilebilir.
WEP şifreleme işlemi için RC4 protokolü kullanılır ve RC4' te stream şifreleme yöntemi kullanılmaktadır. RC4' şifrelemede XOR yöntemi kullanılır ve XOR işlemi gerçekleştirilirken bir data iki defa aynı anahtar ile XOR işlemine sokulur ise aynı data tekrar elde edilir. Detaylı göstermek gerekirse;

PlainText **XOR** RC4Bytes = Chipertext
ChiperText **XOR** RC4Bytes = PlainText
Bu durumda;
RC4Bytes = ChiperText **XOR** PlainText olacaktır.
Bu durumda saldırgan onay alan bir kullanıcı gibi elde ettiği anahtar ile onay sürecini başarılı bir şekilde atlatabilir(bypass).

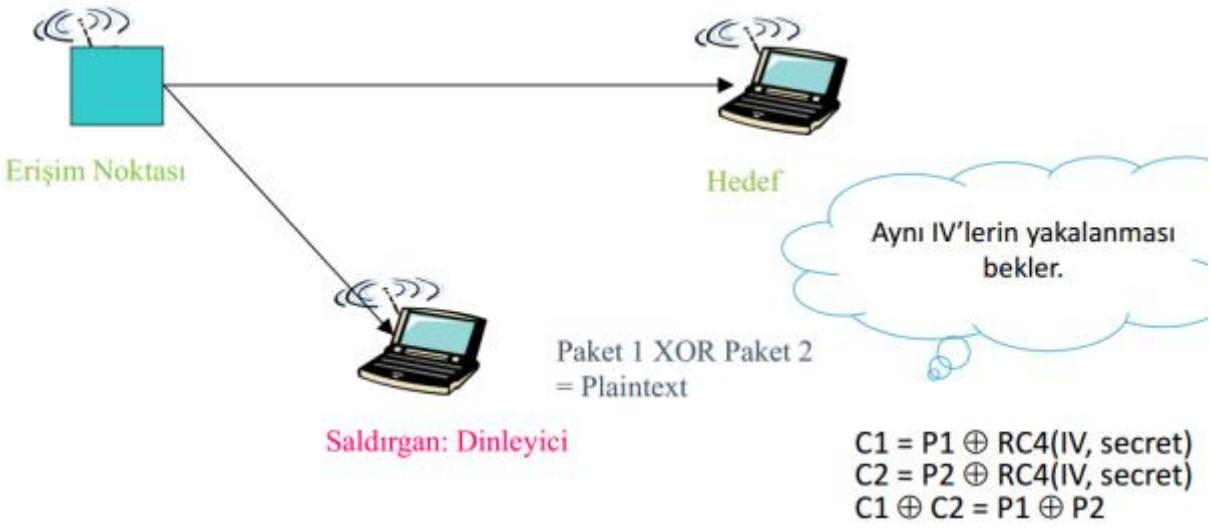
***Saldırı-1***

WEP'te şifreleme işlemi şu şekilde gerçekleştirilir;




*WEP Şifreleme Mekanizması*

Şifreleme işlemi sırasında kullanılan başlangıç vektörünün(IV) aynı olması durumunda;
C1= P1 xor RC4(IV,anahtar)
C2 = P2 xor RC4(IV,anahtar)
C1 xor C2 = P1 xor P2 şeklinde elde edilebilecektir.
Saldırgan şekilde gösterildiği gibi ağı dinler ve aynı IV değerinin kullanılması durumunda birtakım kritik bilgileri ele geçirmiş olur. IV değerinin rastgele ve tamamen farklı olarak üretilmesi gerekmektedir.




*Pasif Saldırı Vektörü* 12

***Saldırı-2***

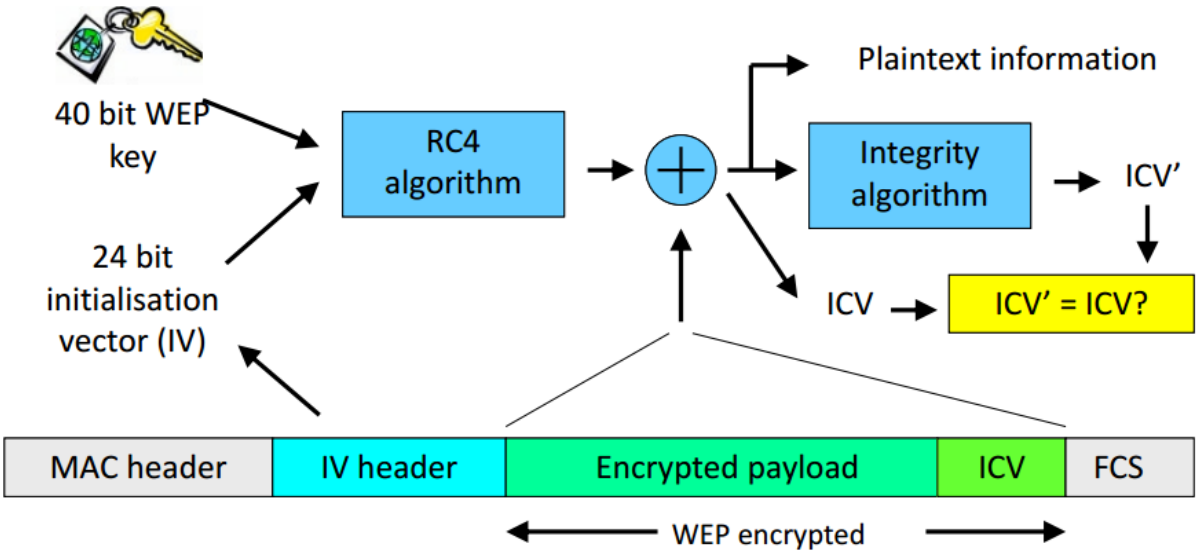
Saldırgan trafiği dinleyerek şifreli metni ele geçirir. ICV (CRC)'nin doğrusallığından faydalanarak trafiğe yeni şifreli metinler enjekte edebilir. Metin üzerinde yapılacak bir değişikliğe göre saldırgan CRC'de hangi bitlerin değişeceğini tahmin edebilir. Buna göre CRC'yi düzenleyerek Access Point'e gönderir ve yeni şifreli paketler trafiğe enjekte edilir.

CRC(x) xor X xor Y = CRC(Y) şeklinde ifade edilebilir.

X= m || CRC(m) Y = h || CRC(h) h= enjekte edilecek şifreli metin.

Bu sayede saldırgan ağa şifrelenmiş ve CRC değeri doğru hesaplanmış bir paket enjekte eder. Karşı tarafın saldırıyı tespit etmesi zordur.

***Saldırı-3***




*RC4 Şifreleme Mekanizması*

WEP paket frame'inde "Frame Header" açık olarak gitmektedir. Saldırgan trafikte araya girerek frame header'daki hedef adresleri kendi belirlediği hedefler ile değiştirir. Access Point'e giden şifreli metin çözülerek oluşturulan cevap saldırganın belirlediği hedefe gider ve böylece şifreli mesajlar çözülmüş bir şekilde saldırgan tarafından ele geçirilmiş olur.

***Saldırı-4***

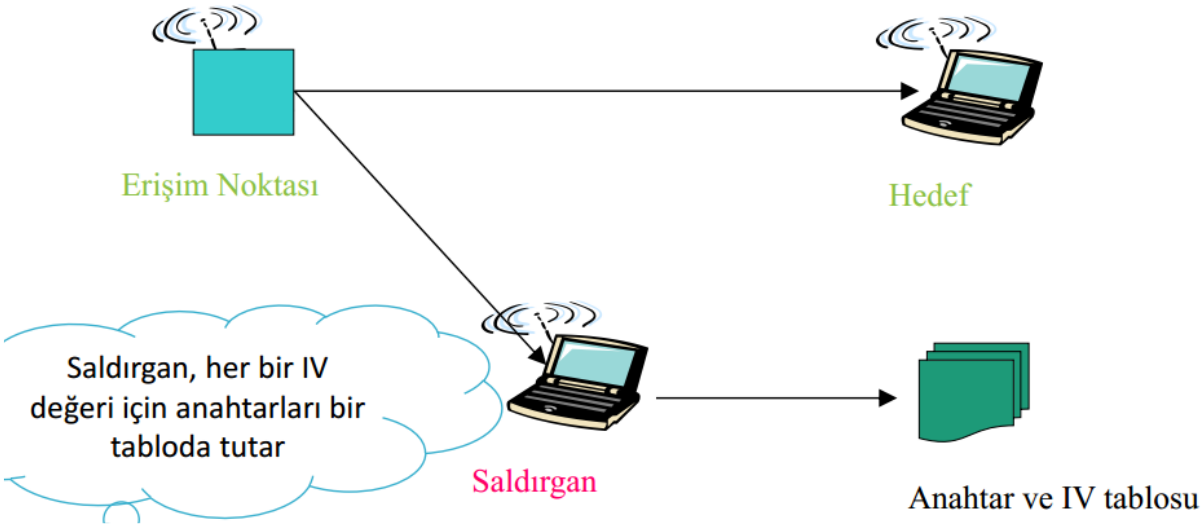
RC4 protokolü ilk açılış işlemleri sırasında 2 dizi (*array*) kullanılmaktadır. İlk dizi (*s-box / state box*) 0-255 arası tüm karakterleri içerir, ikinci 256 byte'lık dizi ise "**şifre** *(key)*" ile doldurulur, şifre kısa ise tekrar edilerek 256 byte'lık dizi tam olarak doldurulmuş olur.

RC4 çalışma mantığında her oluşturulan keystream değerinin her byte' ının bir önceki byte' tan değişik olma ihtimali %50 ancak "Weaknesses in the Key Scheduling Algorithm of RC4"[3] isimli makalesi ile RC4 ile rasgele üretim sürecinde zayıf anahtarlar (weak keys) olduğu ortaya çıkmıştır.

RC4'ün bahsedilen ilk açılış sürecinden sonra "*sbox*" ve "*kbox*" arasında belli bir algoritma ile döngü başlatılır. Bu karıştırma işlemi sırasında ilk ve belli döngülerde bazı byte'ların tahmin edilebilme oranı, normal tahmin edilebilirliğe göre çok daha yüksek olmaktadır, bu tahmin edilmesi yüksek olan byte'lar zayıf anahtar (*weak keys*) olarak kabul edilir. Buradaki tahmin edilebilirliğe asıl neden "*s-box*" içerisinde bulunan data'nın açılış süresinde biliniyor olması gösterilebilir. Ancak ilk açılış ve döngüden sonra bu problem ortadan kalkmakta ve RC4 sorunsuz ve güvenli olarak çalışmaya devam etmektedir.

Güvenlik gerekçesi ile RSA RC4' un implemantasyonunda ilk 256byte'ın kullanılmaması gerektiği ve herhangi bir data ile geçiştirilmesi, sistemin bundan

sonrakileri datayı kullanması gerektiğini bildiriliyor. Ancak WEP' te kullanılan RC4 implementasyonu bu uyarıya kulak asmamış olması sebebi ile WEB protokolünün kırılmasına zemin hazırlamıştır.




*Tablo Tutma Saldırı Vektörü*

Trafikte araya girilerek IV değerlerinin ele geçirilmesi ile WEP kırma işlemi yukarıda anlatılan zafiyet sonucu kaynaklanmaktadır. Belirtildiği gibi IV şifreleme anahtarı ile RC4 algoritmasından geçirilir, dolayısıyla her IV değeri için RC4 şifreleme işlemi gerçekleştirilir ve bu açılış sürecinde (*initialization*) elimize yeni zayıf anahtarlar(*weak keys*) geçmiş olur. Yeterli derecede tekil (*unique*) IV içeren paket toplandığı takdirde, elimizde biriken zayıf anahtarlar kullanılarak, kripto analiz yöntemi ile WEP'in kırılabilmesi sağlanır. Genelde 300.000 – 1.000.000 arasında tekil IV ile WEP şifreleri kırma başarısı yüksektir.

**KAYNAKÇA**

1. Gezgin D. M., Büyüksaraçoğlu Sakallı F., Kablosuz ağ teknolojileri ve şifreleme, Paradigma Yayınları, 1. baskı, Mayıs 2014.
2. Lisa P., 2009,"A list of wireless network attacks", http://searchsecurity.techtarget.com/
3. http://www.crypto.com/papers/others/rc4_ksaproc.pdf
4. http://www.demege.net/file/Konyamakale.pdf
5. http://www.enderunix.org/docs/kablosuz_aglar_ve_guvenlik.pdf

# BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

# BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.