# IPv4 / IPv6 Güvenlik Tehditleri ve Karşılaştırılması

Ayhan Çakın[1] Muhammed Ali Aydın[2]

[1]Enformatik Bölümü, Yıldız Teknik Üniversitesi, İstanbul
[2]Bilgisayar Mühendisliği Bölümü, İstanbul Üniversitesi, İstanbul

[1]e-posta: acakin@yildiz.edu.tr [2] e-posta: aydinali@istanbul.edu.tr

## Özetçe

Günümüzde hızla artan ağ ve ağ elemanları göz önüne alındığında, mevcut internet protokolü IPv4; gerek yetersiz adres sayısı, gerekse dahili güvenlik tasarımı açısından sorunlara yol açmaktadır. IPv6 yeni nesil internet protokolü olarak, eski protokoldeki sorunları çözmek üzere sunulmuştur. IPv6 başından beri güvenlik mekanizmaları ve bu mekanizmaları iki uçtaki konağın kontrolünde olmasını sağlamak üzere tasarlanmaktadır. Ancak henüz yeni bir protokol oluşu ve çokça kullanılmayışı, yayılmaya başladığında ne gibi sorunlara yol açabileceğini kestirmek zordur. Bu çalışmada ilk olarak IPv4'de ortaya çıkan ve IPv6 üzerinde de geçerli olan ortak tehditlerden, ikinci bölümde ise IPv6'nın yayılmaya başlaması ile ortaya çıkabilecek güvenlik sorunlarından bahsedilmektedir.

**Anahtar Kelimeler:** *IPv6, IPv4, IP Tehditleri, IP Güvenliği*

## 1. Giriş

Bilindiği üzere, mevcut internet protokolü IPv4 yetersiz adres uzayı ve güvenlik açıkları gibi sorunlarla yüzleşmektedir. Bu ve benzeri sorunları temel alarak, IETF (Internet Engineering Task Force) bunları giderebilecek yeni bir protokol için çalışmalar başlatmıştır. IPv6 olarak anılan bu yeni protokol, dahili güvenlik önlemleri, ağ yönetimi araçları ve konfigürasyon kolaylığı temel alınarak birçok RFC(RFC 1752, 2460, 2462 vb.) ile tanımlanmıştır.

IPv4'ü genel olarak değerlendirdiğimizde, iki ana sorun ile karşılaşılmaktadır. En büyük problemlerden birincisi, IPv4'ün sunabildiği adres uzayının sınırlı olması ve günümüzde neredeyse tükenmek üzere olduğudur. İlk başta yaklaşık 4 milyar adres uzayına sahip olarak tasarlanan IPv4, kablosuz ağ bileşenleri, hücresel ağların gelişimi ile yetersiz kalmıştır.

İkinci önemli sorun ise güvenliktir. IPv4 tasarlandığı dönemde "uçtan uca" modeli benimsemiş ve internet "güvenli" bir ortam olarak düşünülmüştür.[1] Bu yüzden hiçbir dahili güvenlik bileşeni olmadan tasarlanmıştır. Uçtan uca olarak tasarlanmış modeli, güvenliğin uçlardaki konaklarda sağlanması üzerine kurulmuş ve güvenlik opsiyonu da sonradan bu amaç ile protokole eklenmiştir. Bu tasarımın doğurduğu açıkları uygulama bazında kapatmak amacı ile PGP ve SSL gibi önlemler alınmaya çalışılsada, tam olarak uçtan uca güvenli bir iletişim sağlanamamaktadır. Örneğin IPv4 ün ötentikasyon mekanizmaları tarafında olan eksikliği ortadaki adam saldırılarına, zayıf tasarımı ve dar adres alanı ile konakların taşırma, servis dışı bırakma ve özellikle keşif tipi(portların kısa sürede taranabilmesinden faydalanılarak) saldırılarılara mağruz kalmasına yol açmaktadır.

## 2. IPv6'daki Değişiklikler

IPv6'nın esas tanımlamaları; RFC 2460 (Deering & Hinden,1998) IPv6 Protocol, RFC 4443 (Conta, Deering & Gupta, 2006) Internet Control Message Protocol for IPv6 (ICMPv6),

RFC 4291(Hinden & Deering, 2006) IPv6 Addressing Architecture gibi RFC dökümanları ile belirlenmiştir. IPv4 ile arasındaki bazı farklar Tablo 1'de gösterilmiştir.

| IPv4 | IPv6 |
|---|---|
| 32 bit Adres Uzunluğu | 128 bit Adres Uzunluğu |
| IPsec kullanımı seçeneğe bağlıdır. | IPsec uygulama desteği mecburidir. |
| IPv4 başlığında paket akışını tanımlamak için yönlendiricilerin kullanabileceği ortak bir standart QoS tanımlamaları yoktur. | Başlıkta bulunan "flow label" alanı yönlendiriciler tarafından kullanılır. |
| Paketin parçalanması işlemi (fragmentation) hem ağdaki ara elemanlar hem de gönderici tarafından yapılabilir. | Paketin parçalanması işlemi (fragmentation)yönlendiriciler tarafından yapılmaz. Sadece paketi gönderen istemci tarafından yapılır. |
| Checksum vardır. | Checksum içermez. |
| Seçenekler alanı bulunur. | Seçimli veriler extension header'lar ile taşınır. |
| ARP kullanılır. | ARP Request paketleri multicast Neighbor Solicitation mesajlarıyla değiştirilmiştir. |
| Varsayılan en iyi ağ geçidi tespiti için, ICMP Router Discovery kullanılabilir, fakat zorunlu değildir. | ICMP Router Discovery yerine "ICMPv6 Router Solicitation" ve "Router Advertisement" kullanılır ve kullanımı zorunludur. |
| Ağdaki tüm birimlere "broadcast" adresleri ile erişilir. | IPv6 "broadcast" adresi bulunmamaktadır. Bunun yerine "link-local scope all-nodes multicast" adresi kullanılır. |
| DHCP server yardımı ile veya elle yapılandırılır. | Otomatik olarak yapılandırılır. |

Tablo 1. IPv4 ve Ipv6 Karşılaştırılması

## 3. IPv4 ve IPv6'daki Benzer Güvenlik Tehditleri

Yeni protokol tasarımı ile gelen güvenlik önlemleri olsa da, IPv6 ağları halen farklı tipte ataklara maruz kalabilmektedir. Bu ataklar üzerinde birçok çalışma mevcuttur [2][3][4].
Bazı atak türleri IPv6 ile değişmiş ve bu protokole özel saldırı türleri bulunmaktadır, ancak IPv4 için mevcut olan tüm saldırı türleri değişmemiş ve bu saldırı mekanizmaları IPv4 ve IPv6 ağları için tehlike oluşturmaktadır.

### *3.1 Paket Koklama*

Paket koklama saldırısı basitçe ağda gezen verinin yakalanıp incelenmesi olarak tanımlanabilir. Koklama atakları hem IPv6 hem de IPv4 üzerinde etkili olan en tipik saldırı biçimidir. IPv4 de veriler ağda şifrelenmeden dolaştığı için saldırı çok çabuk sonuç vermekteydi. Ancak yeni protokolün tanımına göre, IPv4 de yalnızca bir seçenek olan IPSec[5] özelliği, IPv6 da dahili olarak desteklenmek zorundadır. Bu özellik ile veriler uçtan uca şifrelenmiş şekilde transfer edilmekte, paket aradaki bir konakta yakalanıp incelense bile şifreli olacağı için güvenlik açığı kapatılmış olmaktadır. Buradaki önemli nokta, IPv6'da IPSec desteği zorunludur ancak kullanılması tamamen isteğe bağlıdır. Anahtar paylaşımı ve konfigürasyonu gibi karışık konulardan dolayı IPSec özelliğinin IPv6'daki kullanımın eski protokolden daha fazla olup olmayacağı bir soru işaretidir.[6]

### *3.2 Ortadaki Adam Saldırıları*

Bilgisayarın meşruluğu ağ yapısında yada işletim sistemi tarafında IP kurallarına göre belirlenmektedir. Bazı durumlarda IP adresi saldırı yapan bir kişi tarafından taklit edilmekte/uydurulmaktadır (forged ID)[7]. Bu sahte IP'yi kullanarak saldırgan meşru konaktan gelmiş gibi bir paket gönderebilir. Gerekli yetkileri kazandıktan sonra, saldırgan gelen paketlerdeki veriyi birçok yöntemle yönetebilir, yeniden yönlendirebilir veya değiştirebilir.

### *3.3 Taşırma Saldırıları*

Taşırma saldırıları IPv4 ağlarını en çok istismar eden saldırı türü olarak bilinmektedir. Bu tarz saldırılar IPv6 için de geçerli olacaktır. Ağ üzerindeki hedefe kaldırabileceğinden daha fazla istek göndererek hizmet vermesini belirli bir süre boyunca engelleme yöntemi IPv6 için de geçerli olacaktır. Saldırı; bölgesel ya da dağınık hizmet dışı bırakma(DDos) yani farklı makinelerin aynı anda tek bir hedefe istek göndermesi ile uygulanmaktadır. IPv6 ağlarında, bu tarz atakları ağı analiz ederek tespit etmek daha da zorlaşmaktadır. Çünkü IPv6 ile adres uzayı büyümüş ve sahte IP'lerin tespiti zorlaşmıştır.

### *3.4 Uygulama Seviyesi Saldırıları*

Günümüzün en yaygın saldırı türlerinden olan uygulama seviyesi saldırıları, CGI saldırıları, solucan dağılımı, hafıza taşırma gibi saldırıları içermektedir. IPv6'ya geçiş ne yazık ki ağları bu tarz saldırılardan koruyamamaktadır. Çünkü bu saldırıların

hepsi uygulama seviyesindedir. IPv4 ve IPv6 protokolleri ise OSI modelinin ağ düzeyinde işlemektedir.

### *3.5 ARP, DCHP Saldırıları, Sahte Cihazlar*

IPv6 protokolü tanımlanırken, ARP ve DHCP'nin bu protokoldeki karşılıkları ile ilgili dahili bir güvenlik mekanizması eklenmemiştir.[8] Yönlendirici ve komşu istek paketleri sahte olarak üretilip bunlarla komşu tanımlama önbelleğinin üzerine yazılıp, IPv4 deki ARP sorunları tekrarlanmaktadır. Bunlara ek olarak, sahte cihazlar, ağ üzerinde yetkisi olmayan cihazların kablosuz erişim noktası, DHCP sunucusu veya basit bir bilgisayar olarak tanımlanan cihazlardır. Bu cihazların tespit edilmesi için bazı yöntemler bulunmaktadır. Ancak IPv6'da hiçbirisi değişmemiştir. Fakat IPSec özelliğinin IPv6 ağlarında etkin bir şekilde uygulanması ve cihazların yetkilendirilmesi ile bu atakların tespiti bir şekilde mümkün olabilecektir.

## 4. IPv6 ile Gelen Güvenlik Tehditleri

### *4.1 Keşif Tipi Saldırılar*

Keşif saldırıları bir saldırı türü olmaktan çok, bir saldırının başlangıç aşaması olarak görülebilir. Bir saldırı yapmadan önce ağı analiz etmek ve ağdaki cihazları tanımlamak için kullanılır. Saldırgan çeşitli tarama metotlarını kullanarak hedef ağdaki IP adreslerini belirler ve daha sonra ağdaki cihazlara özel port taraması gibi işlemlere başlar.

Yeni internet protokolünü ele aldığımızda, saldırganlar için tüm ağı taramak neredeyse imkansız hale gelmiştir. Çünkü IPv6'da alt ağ sayısı IPv4'e göre çok büyüktür(64 bit). Buna dayanarak IPv6 ağları keşif saldırılarına daha dayanıklı denilebilir. Ancak IPv6'da bulunan bazı çoklu gönderim adresleri saldırganlar tarafından kullanılarak ağdaki cihazların tespiti ve saldırı amacıyla kullanılabilir.

### *4.2 ICMPv6*

IPv4 ağlarında ağın diğer fonksiyonlarına zarar vermeden ICMP mesajlarını engellemek mümkün olduğundan, bu uygulama zamanla güvenlik sebebiyle sürekli uygulanmaya başlandı. Ancak IPv6'nın tanımlanması ile birlikte, ICMPv6'nın MTU ve komşu tanımlama gibi çok önemli mekanizmalarda kullanıldığı görüldü. Buna bağlı olarak, ağın düzgün bir şekilde işlemesi için ICMPv6 mesajlarının engellenmemesi gerekmektedir. Ancak ICMPv6 tanımlamasındaki en önemli güvenlik açığı olarak; hata mesajlarının hedef adreslerinin çoklu gönderim adresi olarak tanımlanmasına izin vermesidir. Bu özellik bir saldırgan tarafından kolayca istismar edilebilir.

### *4.3 Ek Başlıklar ile İlgili Tehditler*

IPv6 tanımlamasına göre IPv6 ağındaki bütün cihazlar yönlendirme başlıklarını işleyebilmelidir. Bu davranış; hedef adres temel alınarak yetkisiz erişim gibi bazı güvenlik açıklarına yol açabilir. Bir senaryo oluşturarak örnek vermek gerekirse: Bir saldırgan açık bir ağ üzerindeki bir cihaza, yönlendirme başlığında o cihaz üzerinde önceden yasaklı olarak belirlenmiş bir paket yolluyor. Normal koşullar altında bu paketin süzülmesi gerekirken, bu cihaz gelen paketi otomatik olarak iletmektedir. Saldırgan sahte IP adresleri üzerinden açık ağdaki bu cihazı kullanıp gönderdiği paketleri iletmesini sağlayarak hizmet dışı bırakma saldırısı yapabilir. Burada bilinmesi gereken bazı işletim sistemlerinin yönlendirme başlığı olan paketleri otomatik olarak ilettiği, diğerlerinin ise iletmediğidir.

### *4.4 Başlık Yönetimi ve Parçalama*

IPv6 protokolü tanımına göre[9], MTU keşif metodu zorunlu tutulmuş ve paketin parçalanma işleminin aradaki cihazlarda yapılması engellenmiştir. Birçok ek başlık seçeneğinin kullanılması ile birlikte, bugün ağdaki orta elemanlar tarafından yapılan paketlerin yeniden birleştirilmesi işleminde sorunlar çıkması muhtemeldir.

### *4.5 Tünelleme ve Geçiş Mekanizmaları*

IPv4 ağlarının devasa boyutunu ele aldığımızda, IPv6 ağlarına geçişin birçok uyum sorunu sonucunda yavaş olacağı görülmektedir. Bu süreci daha yumuşak hale getirmek için birden fazla geçiş mekanizmaları geliştirilmiştir. Ancak bu mekanizmalar şirketlerin yanlış konfigürasyonu, tünel metotları ve iki protokolün(IPv4 ve IPv6) beraber kullanılması gibi etkenler sonucunda şuanda tahmin edilemeyen yeni güvenlik açıkları doğuracaktır. Bu yüzden IPv6 ağlarına geçiş süreci ağ yöneticileri tarafından dikkatle değerlendirilmelidir.

## 5. Sonuçlar

Bu çalışmada IPv6 protokolü üzerinde getirdiği faydalı yönler ve eksikleri ile ilgili genel bir değerlendirme yapmaya çalıştık. IPv6; mevcut protokoldeki sorunları çözmeye yönelik tasarlanmış olsa da, güvenlik penceresinden henüz tartışılması gereken birçok nokta bulunmaktadır. IPSec özelliğinin uygulanma desteğinin zorunlu hale getirilmesi, paketlerin ağdaki orta elemanlarda parçalanmasına izin verilmemesi, adres uzayının genişletilmesi ve NAT kullanımının azaltılmaya teşvik edilmesi, IPv6 ile gelen ve bu protokolü daha güvenli bir uygulama hale getiren yönlerden sadece birkaçıdır. Ancak daha yeni bir protokol olması ve şuanda uygulamasının az olması nedeniyle, yayılması anında çıkabilecek sorunlar halen araştırılmaktadır. Şu anki tasarımın daha derin analizi ve yukarıda tartıştığımız konuların incelenmesi ile IPv6 ağlarına geçiş çok daha hızlı ve sorunsuz olacaktır.

## 6. Kaynakça


[1]. S. Sotillo, “IPv6 Security Issues”, 2006.

[2]. Q Zheng, T. Liu, G. Xiaohong, X.,Q. Yu, N. Wang N, “A new worm exploiting IPv4-IPv6 dual-stack networks,” Proceedings of the 2007 ACM workshop on Recurring malcode, Virginia, 2007

[3]. D. Zagar, K. Grgic, “IPv6 security threats and possible solutions,” World Automation Congress, 2006

[4]. Y. Xinyu, M. Ting, S.Yi, “Typical DoS/DDoS threats under IPv6,” Computing in the Global Information Technology, Guadeloupe, 2007

[5]. Kent & Seo, IETF RFC 4301 “Security Architecture for IP or IPsec”, 2005

[6]. Y.Nikolopoulos, “Security Considerations for IPv6 Networks”, March 2011

[7]. D. Yang, Xu Song, Qiao Guo, “Security on IPv6”, 2010

[8].V.Sharma,”IPv6 and IPv4 Security challenge Analysis and Best- Practice Scenario”, Jan 2010

[9]. Deering & Hinden, IETF RFC 2460 “Internet Protocol, Version 6 (IPv6) Specification”, 1998