

YENİ NESİL IP (Ipv6) VE GÜVENLİK

Murat SOYSAL
TÜBİTAK-ULAKBİM
msoysa@ulakbim.gov.tr

Onur BEKTAŞ
TÜBİTAK-ULAKBİM
onur@ulakbim.gov.tr

ÖZET

Yeni nesil Internet Protokolünün (IPv6) kullanımı beklenildiği hızla olmasa da bir çok ağ üzerinde artmakta. 128 bitlik yapısı ile adres sayısındaki artış ve Mobil IP uygulamasını temelden desteklemesi ile IPv4 'e nazaran daha avantajlı olarak sunulan yeni nesil protokolünün ön plana çıkarılan bir diğer özelliği ise güvenlik konusunda getirdiği açılımlardır.

Sadeleştirilmiş başlık yapısı, geliştirilmiş seçenekler bölümü, geniş adresleme yeteneği ve IPSec uygulamasını içermesi ile edindiği doğrulama/gizlilik özellikleri IPv6'nın daha getirdiği güvenlik konusunda su götürmez gerçeklerdir. Ancak IPv6'nın bir türlü tam anlamıyla evrenselleşemeyen kullanımı, bu teorik gelişimlerin pratik hayatta ne kadar güvenli bir iletişim sağlayacağı konusundaki soru işaretlerini henüz kaldıramamıştır.

Bu makalede, IPv4 ile IPv6'nın güvenlik açısından bir karşılaştırmasını yapıp, yeni nesil protokolün doğası gereği barındırdığı özellikleri ne kadar gerçek hayat yansıtılabileceği tartışılacaktır. Ayrıca yeni nesle geçiş aşamasında yaşanması muhtemel güvenlik sorunları hakkında genel bilgi verilecektir.

ABSTRACT

Abstract.

Anahtar Kelimeler: IPv6, yeni nesil IP, IPSec, güvenlik, tünelleme

1. GİRİŞ

1970'li yıllarda geliştirilmeye başlanılan ve 1983 yılında küçük bir araştırma ağına kullanılmaya başlanılan TCP/IP, bugün milyonlarca elemanı olan Internetin en çok kullanılan ağ protokolü haline gelmiştir. Başlangıç noktasından çok farklı yerlere gelmesi sebebiyle, Ipv4 'ün temel dizayn matığı bugünkü ihtiyaçları karşılayamaz durumdadır.

Öncelikle kısıtlı ağ adresi sayısı, NAT (Network Address Translation) gibi sonradan eklenen çözümlerle aşılmaya çalışılsa da, günümüzde ağa bağlanan cihazlar için yeterli olmamaktadır. NAT benzeri çözümler Ipv4'ün doğal yapısında yer almadığından, uçtan uca direk erişimin sağlanamaması gibi problemlere yol açmaktadır. Bununla birlikte hız artan bant genişliklerinin ses ve görüntü gibi yüksek büyüklükte dataların taşınmasına imkan sağlar hale

gelmesine rağmen, Ipv4 'ün servis kalitesi (QoS) hizmeti için yetersiz tasarımı da sorunlar yaratmaktadır.

Güvenilir ve sınırlı sayıda kullanıcıya hizmet etmek için dizayn edilen Ipv4'ün, geniş kitleler ve çok fazla uygulama tarafından kullanılır hale gelmesiyle iletişim güvenliği konusunda ciddi zaafılar ortaya çıkmıştır. Bu zaafıların üstesinden gelmek için, uygulama tarafında SSL,PGP benzeri önlemler geliştirilmişse de kullanılan protokolün (Ipv4) doğal bir güvenlik çerçevesine sahip uçtan uca güvenli iletişimi zorlaştırmaktadır.

IP sayısındaki kısıtlılığın zorlaması sonucu, 20 yılı aşkın süredir kullanımı süresince karşılaşılan problemler de göz önüne alınarak, yeni nesil bir prortokol için çalışmalar başlatılmıştır. IETF (Internet Engineering Task Force) tarafından yürütülen çalışmalar sionucunda 128 bitlik yapısı ile yeni nesil IP protokolü (Ipv6) ortaya çıktı.

IP sayısındaki artışın yanında sade başlık yapısı, geliştirilmiş seçenekler bölümü ve içerdiği güvenlik uygulması ile (IPSec) Ipv6 bir çok yenilik getirmektedir. Beklenildiği hızla yaygınlaşmasa da, özellikle Ipv4 sayısında sıkıntı çeken ülkelerde yoğun olarak kullanımına başlanılan Ipv6'yı bir çok cihaz üreticisi de desteklemeye başlamıştır. Uygulama bazında sıkıntılar yaşanılrsa da Ipv6'ya tüm Internette kademe kademe geçileceği tahmin edilmektedir.

Bu makalede, Ipv4 ile Ipv6'nın iletişim güvenliği açısından bir karşılaştırmasını yapıp, yeni nesil protokolün doğası gereği barındırdığı özellikleri ne kadar gerçek hayat yansıtılabileceği tartışılacaktır. Ayrıca yeni nesle geçiş aşamasında yaşanması muhtemel güvenlik sorunları hakkında genel bilgi verilecektir.

2. IPv4 v.s. IPv6

Bu bölümde IPv6 protokolünün getirdiği yeniliklerin detayları verilecektir.

- 32 bitlik IPv4'e nazaran 128 bitlik yapısı ile çok geniş bir IP uzayı sağlamaktadır
- IPv4'te adres yapılandırması elle veya DHCP benzeri harici bir protokol kullanılarak yapılabilmekteydi.IPv6 protokolü ile birlikte IP adresi yapılandırma işlemi IPv6 protokolünün içine entegre edilmiş ve

cihazlar IP adreslerin otomatik olarak harici bir protokol veya mekanizma kullanılmadan yapabilir hale gelmiştir. IPv6 adres yapılandırması için iki yöntem bulunmaktadır.

- **Stateless.** Bu yapılandırma biçiminde harici bir sunucu olmadan IPv6 adresi yapılandırabilmektedir. IPv6 adresinin son 64 biti ağ arabirim kartı adresinden türetilip, ilk 64 biti yönlendirici tarafından istenilen durumda sağlanmaktadır. Bu mekanizma tarafından yaratılan link local adres yerel ağda bilgisayarların birbiri ile iletişim sağlamaları için yeterlidir.
- **Stateful:** Bu yapılandırma biçiminde IPv6 adresinin yapılandırılması için harici bir sunucu kullanımına gerek vardır. Adres yapılandırılması genelde DHCPv6 kullanılarak yapılmaktadır.
- IPv6 protokolü başlığında bulunan 8 bitlik öncelik (Traffic Class) bölümü ile servis kalitesi (QoS) uygulamalarına tam uyumludur. Ses ve görüntü gibi gecikmeye tahammülsüz bilgilerin taşınmasında çok yararlıdır.
- IPv6 ilk kez hareketli (mobil) kullanıcılar için iletişimi destekleyecek altyapılar sağlamaktadır. RFC 3775 ile mimarisi tanımlanan iletişimde her bir hareketli kullanıcı, internete bağlı olduğu noktadan bağımsız olarak ev adresi (HoA) ile tanımlanmaktadır. Bir kullanıcı kendi ev ağına bağlandığında iletişimi geleneksel yöntemler ile sağlanmaktadır. Kullanıcı başka ağlara bağlandığında, kendisine atanan sıla adresi (care-of address) ile dış ağlara şu an ki konumunu duyurmaktadır. Kullanıcının ev adresine iletilen paketler, transparan bir şekilde sıla adresine yönlendirilmektedir. IPv6 ile hareketli iletişimin henüz çerçevesi çizilmiş olsa da, doğal yapısında bu tip iletişime destek vermesi IPv4'e nazaran çok büyük bir yeniliktir.
- IPv6 güvenlik konusunda çoğunlukla IPsec standartlarına dayanmaktadır. IPsec, iletişim kuran uçlar arasında doğrulama, geçerlilik ve gizlilik sağlayan bir çerçeve belirlemektedir. IPsec, iki uç, bir uç ile bir güvenlik geçidi veya iki güvenlik geçidi arasındaki iletişim için kullanılabilir. IPv4 için IPsec uygulamaları hazırlanmış olsa da, gerek IPv6'nın IPsec'i bir dış uygulama gibi değil de doğal içerik olarak görmesi gerekse IPv6 destekleyen tüm cihazların IPsec'de destekli olması büyük bir avantajdır. IPv4 ile sanal özel ağ (VPN) uygulamasından

öteye gidemeyen ve bir çok ara cihaz da desteklenmemesi sebebiyle yaygınlaşamayan IPsec'in IPv6 ile iletişim güvenliğini artırması planlanmaktadır.

3. GÜVENLİK PENCERESİNDEN IPv6

4. MEVCUT GÜVENLİK AÇIKLARININ DURUMU

Bu bölümde hali hazırda IPv4 için yaşanan saldırı türleri ve çözüm yöntemlerinin IPv6 uygulaması ile nasıl tavrı takınacağını göstermek için iki örnek üzerinden açıklamalar yapılacaktır.

4.1 Ipv4 ve IPv6 için benzerlik gösteren atak türleri:

Bu grubu oluşturan saldırı türlerine örnek olarak taşırma (flooding), ortadaki adam (man-in-the-middle) ve trafik koklama (sniffing) verilebilir.

- Taşırma saldırıları genel anlamda hedefe baş edebileceğinden daha fazla isteğin yönlendirmesiyle yapılır. Bir sunucu için çok fazla bağlantı açma isteği ya da bir istemci için bant genişliğinin tümünü dolduracak kadar trafik oluşturulmasıyla taşırma saldırıları gerçekleştirilir. IP adres yapısıyla çok bağlantılı bir saldırı türü olmadığından IPv6 için çok fazla değişikliğe maruz kalmayacaktır. Daha çok DDoS (Distributed Denial of Service) şeklinde gerçekleşen bu saldırı türünde IPv6 kullanımı, artan adres sayısı ile daha fazla değiştirilmiş (spoofed) IP kullanımına imkan sağladığından, trafik analizi ile tespiti zorlaştıracaktır.
- Ipv4 ve IPv6 adres başlıklarının hiçbir koruma altında olmaması, ortadaki adam saldırılarından korunmak için sadece IPsec güvenlik uygulamasının kullanımına imkan vermektedir (IKE).
- Trafik koklama en basit örneği ile tcpdump benzeri programlar ile ağda dolaşan paketlerin yakalanıp içeriğinin incelemesi şeklindedir. Bu saldırı türü, aslında IPv6 doğasında bulunan IPsec uygulamasıyla yapılacak uçtan uca şifreleme ile bertaraf edilebilse de, henüz IPsec için anahtar paylaşımında verimli algoritmalar önerilmediğinden yeni nesil protokolün bu saldırının şekli ve tespitine katacakları şimdilik sınırlıdır. Anılan türde bir algoritma önerildiğinde, trafik koklama saldırıları öncelikle anahtar değişimi prosedürünün üzerinde yoğunlaşacaktır.

4.2 IPv4 ve IPv6 için farklılık gösteren saldırı türleri:

Bu grubu oluşturan saldırı türlerine virüs/solucan saldırıları, smurf saldırıları verilebilir.

- Smurf tipi saldırılar bir ağda bulunan ve aynı ağ maskesini kullanan cihazlara broadcast adresi kullanılarak ping atılmasıyla yapılmaktadır. RFC 2463 de, hedef adresi IPv6 multicast, data-link seviye multicast ve broadcast adresleri olamayacağı için IPv6 için bu tip bir saldırıdan söz edilemez.
- Virüs/Solucan saldırı türlerinde IPv4'ten IPv6'ya geçiş aşamasında yaşanacak değişimi değerlendirmek için bu saldırıyı iki bölüme ayırmak gerekir. Birinci bölümde e-posta ve paylaşılan hastalanmış(Infected) dosyalar ile bulaşanlar yer alırken, ikinci bölümde bir ağ iletişimi aktivitesi (genellikle tarama) ile bulaşanlar yer alacaktır. İlk bölümü oluşturan virüs/solucanlar IP protokolü değişiminden hiçbir şekilde etkilenmeyeceklerdir. Bunun yanında ikinci bölümde yer alan virüs/solucanlar için ağ taraması yapma aşamasında IPv6 ile artan adres sayısı ciddi sorunlar yaratacaktır. Ağ adreslerinin ağ bağdaştırıcı üreticisi bilgisi ile tahmin edilebilir olması, ağ tarayan virüs/solucanlara bir kolaylık sağlasa da bulaşacak bir bilgisayar bulmaları IPv6 da IPv4'ten çok daha zordur.

Bu örneklerden yola çıkarak, IPv6 protokolünün bazı saldırı türlerini tamamıyla yok edeceğini bazılarını ise fazlaca zorlayacağı açıktır. Ancak azımsanmayacak miktarda saldırının sadece protokol değişimi ile bertaraf edilemeyeceği de ortadadır.

5. SONUÇLAR

- Kullanımın artmasıyla güvenlik uygulamaları bazında da sorunlar gözlenecek (Firewall, Network management tools)
- IP dağıtımı konusunda çok hızlı ve kolay çözümler üretilmeli. İlk uygulayan deneyimsiz ağ yöneticileri için büyük risk.
- IPSec bir yama olarak değil de doğal bir içerik olduğundan doğrulama ve şifreleme uygulamaları kullanımı IPv6'nın yaygınlaşması ile artacaktır. IPv4 IPSec kadar sınırlı ve VPN bağlı kalmayacaktır.
- Geçiş aşamasında ikili kullanım da güvenlik zaaflarına yol açabilir.
- IPv6 güvenli demek yeterli değil. Daha güvenli olmaya doğuştan yatkın ancak yönlendirme ve eğitim şart.

KAYNAKLAR