IPV6, Güvenlik Açıkları ve Hukuki Durum

Çise Mıdoğlu **Gürkan Özocak**

ÖZET

Günümüzde İnternetteki hakim protokol olan IPv4'ün artık İnternet üzerindeki ihtiyaçları karşılayamaz hale gelmesi ve birçok konuda eksiklik taşıması sebebiyle, uzunca bir süredir IPv6'lere geçiş konusunda çalışmalar yapılmaktadır. IPv6, özellikle eksikliği hissedilen ihtiyaçlara çözüm bulmakla beraber, yeni ve bilinmeyen bir protokol olarak birçok güvenlik problemi ile de karşı karşıyadır. Ülkemiz açısından düşünüldüğünde, bu problemlerin bir kısmına ilişkin ülkemizin ceza hukuku mevzuatı ve özellikle kişisel verilere ilişkin AB direktifleri ile çare bulunabilir olsa da, esas çözümün bu problemler ortaya çıkmaksızın yapılacak olan çalışmalar olduğu tartışmasızdır.

Anahtar Kelimeler

IPv4, IPv6, Güvenlik, IPsec, siber saldırılar, kişisel veriler.

SUMMARY

Since IPv4, that the dominant protocol on Internet nowadays, cannot be able to meet the needs, it has been carried out studies on IPv6 for quite some time. Although IPv6 finds solutions for problems and insufficiency of IPv4, encounters many difficulties as a new and unchartered protocol. Considering the terms of our country, even we can solve some of these problems thanks to our criminal law legislation and EU directives about especially personal data, it is clear the problems have to be solved before they occur.

Keywords

IPv4, IPv6, security, IPsec, cyber attacks, personal data.

GİRİŞ

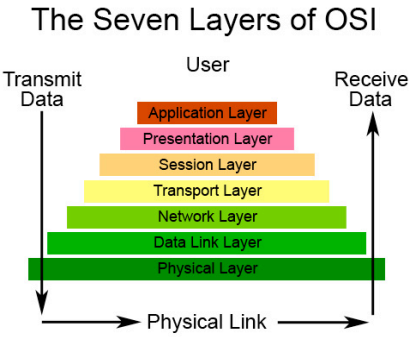
Modern Dijital İletişim Sistemlerinin Yapısı

Modern iletişim sistemleri, *Açık Sistemler Arabağlantısı* (OSI, Open Systems Interconnection) *Modeli* adı verilen ve *Uluslararası Standardizasyon Organizasyonu* (ISO, International Organization for Standardization) tarafından geliştirilmiş olan 7 katmanlı bir modele dayanır. Bu model, iletişim ağlarında yer alan cihazların birbirleriyle nasıl iletişim kuracağını, ne gibi görevler gerçekleştireceğini, ve cihazlar arasında dolaşan verilerin hangi yapıda olması gerektiğini tanımlar[1].

Bu modelde, hem ağ içerisinde hem de ağ dışında verilerin iletilmesi için, bu verinin mutlaka bütün katmanlardan geçmesi gerekir. Veri, uygulama katmanından donanım katmanına giderken, her bir katmanda ayrı bir başlık alır. Bu şekilde veri en son katman olan donanım katmanına vardığında, artık karşıdaki bilgisayara ulaşmış olur ve işlem tamamlanır.

OSI katmanları, aşağıdan yukarıya doğru şu şekilde sıralanır:

1. Fiziksel Katman (Donanım Katmanı)
2. Veri Bağlantısı Katmanı
3. Ağ Katmanı
4. Ulaşım Katmanı
5. Oturum Katmanı
6. Sunum Katmanı
7. Uygulama Katmanı



Şekil 1 – OSI Katmanları Şeması [2]

IP (İnternet Protokolü)

İnternet Protokolü (IP, Internet Protocol), *datagram* adı verilen ağ paketlerinin dağıtılmasında kullanılan temel iletişim protokolüdür. IP, Bugün bildiğimiz anlamıyla "İnternet"i oluşturan birincil protokoldür. *İnternet Protokol Takımı*'nın (IPS, Internet Protocol Suite) ağ katmanında çalışır ve paketleri yalnızca IP adreslerine göre bir makineden diğerine iletmekle görevlidir.

IP, ilk olarak Vint Cerf ve Bob Kahn tarafından 1974'te ortaya atılmıştır. İlk büyük versiyonu *İnternet Protokolü Versiyon 4* (IPv4) olarak bilinir ve şu anda internetteki hakim protokoldür.

Günümüzde kullanılmakta olan IPv4'ler, esasen 32 bit'lik sayılardan oluşurlar. Aynı ağdan İnternet bağlantısı oluşturan iki cihazın IP'lerinin ilk birkaç basamağı aynıdır. İki cihazın aynı ağda olduğunu gösteren bu basamaklara IP maskesi (IP mask) adı verilir. Örneğin, IP maskesi 255.255.255.0 ise, ilk üç basamağı (yani 32 bit'lik IP'nin, ilk 24 bit'i) aynı olan iki cihaz, aynı ağdan bağlantı kuruyor demektir. O halde, 192.168.0.1 ile 192.168.0.2 aynı ağda, 192.168.1.1 ise başka bir ağdadır [3].

IPv4 versiyonun halefi IPv6 ise gün geçtikçe daha yaygın olarak kullanılmaya başlanmakta olup, bu versiyon IPv4'e göre birçok avantaj barındırdığı gibi, bazı güvenlik sorunlarıyla da karşı karşıyadır.

IPv4'ün Eksiklikleri

Şüphesiz ki, IPv4, uzun bir dönem kolay uygulanabilirliği ve başka protokollerle çalışabilir olması nedeniyle popüler olmuştur. Ancak günümüzde İnternet kullanımının bu denli artmış olması nedeniyle, bazı ihtiyaçları karşılayamamış olup, bu nedenle IPv6'ya geçişi zorunlu hale getirmiştir. Bu nedenle, IPv6'nın özelliklerine geçmeden önce, bu geçişi zorunlu kılan IPv4'ün eksikliklerinden bahsetmek gerekmektedir:

- İnternete bağlı cihaz sayısının günden güne müthiş bir artışla büyümesi sonucu, IPv4 adres uzayı bu ihtiyacı karşılamakta yetersiz kalmıştır,
- IPv4 adres yapılanması statik olarak veya Dinamik İstemci Kontrol Protokolü (DHCP) kullanılarak yapılabilmektedir. Ancak, IP adresleri ihtiyacının artması sebebiyle, yeni bir otomatik yapılandırma yönteminin geliştirilmesine gereksinim duyulmuştur,
- IPv4'te kullanılan NAT (Network Address Translation) IP maskeleme yoluyla gerçek IP ihtiyacını azaltmak ve yerel ağ ile İnternet arasında adeta bir firewall kurarak güvenlik sağlama gibi avantajları olmakla beraber, dosya aktarım (FTP) gibi birçok uygulama kullanılırken sorun çıkarmak veya IPsec güvenliğini bozmak gibi dezavantajları vardır. Bu nedenle, NAT kullanımına gerek duymayarak güvenliği arttırıcı etkisi olduğu söylenen IPv6'ya ihtiyaç duyulmuştur[4].

Bunun dışında, IPv4'ün İnternet kullanımı üzerinde artan ihtiyaçları karşısında daha birçok eksikliği sayılabilir. Bütün bu sebeplerle, ortak kanaat, IPv6'ya geçişin zorunlu olduğu yönünde oluşmuştur.

IPv6

İnternet Mühendisliği Özel Çalışma Grubu (IETF, İnternet Engineering Task Force) IPv6'yı geliştirmeye 1992 yılında, artan internet kullanımının sınırlı sayıdaki IPv4 adreslerini tüketeceği öngörüldüğünde başlamıştır. Ekip IPv6'yı 1996 yılında yayınlamıştır.

IPv4 32 bitlik bir adres alanı kullanmakta, bu da toplamda 2^{32} (yani yaklaşık 4,3 milyar) özgün adrese denk düşmektedir. IPv6 ise 128 bitlik bir adres alanı kullanmaktadır, ki bu da toplamda 2^{128} (yani $3{,}4x10^{38}$) özgün adres anlamına gelmekte olup, IP adresi ihtiyacını günümüz koşullarında fazlasıyla karşılar durumdadır.

En son IPv4 adresleri 2011 yılında, internete bağlı adreslerin dağıtımı ve takibinden sorumlu olan *İnternet Tahsis Edilen Sayılar Otoritesi* (IANA, Internet Assigned Numbers Authority) tarafından dağıtılmıştır. Bununla birlikte protokolün yeni versiyonu olan IPv6'ya olan ilgi ve ihtiyaç daha da artmıştır.

IPv6 6 Haziran 2012'de katılımcı İnternet sitelerinin protokolü kalıcı olarak etkinleştirdiği büyük bir kampanya ile piyasaya sürülmüştür. *İnternet hizmet sağlayıcıları* (ISP, Internet Service Provider) da aynı zamanda IPv6 bağlanabilirliği sunmaya başlamış ve *yönlendirici* (*router*) üreticileri varsayılan ayar olarak bu teknolojiyi destekleyen cihazlarını piyasaya sürmüştür.

Sürdürülen bu seferberliğe rağmen birçok uzman IPv6'nın ciddi güvenlik açıklarına sebep olduğunu da belirtmektedir[5]. Endişelerden en büyüğü, IPv6 çalıştıran *router*, güvenlik duvarı, ve *spam* filtreleri için geliştirilebilecek olan en iyi uygulamaların henüz tasarlanıp kullanılmaya başlanmamış olmasıdır. Bunun sebebi, yeni işletim sistemleri ve ağ cihazları IPv6'yı desteklemesine rağmen, hala eski ağ cihazlarının çoğunluğunun IPv4 çalıştırmasıdır.

Google tarafından toplanan istatistikler, IPv6'nın toplam küresel kullanımının bütün internet trafiğinin % 0.2'sinden (2010) % 2'sine (Eylül 2013) yükseldiğini göstermektedir [6]; fakat bu rakam hala oldukça düşüktür.

IPv6'nın destekleyicileri, İnternete bağlı cihazlara selefi IPv4'e göre çok daha fazla IP adresi sağlayan IPv6'nın daha yüksek bir oranda kullanılmaya başlanmasıyla daha güvenli hale geleceği fikrindedir[7].

IPv6 GÜVENLİK KONULARI

IP adreslerinin sınırlı sayıda olması sorununu çözmek üzere yenilenen internet protokolü IPv6 gittikçe daha yaygın şekilde benimsenmesine ve taraftar sayısı artmasına rağmen, protokolün hala çözülmemiş olan birçok güvenlik problemi bulunmaktadır. Örneğin var

olan yönlendirici, güvenlik duvarı ve diğer ağ cihazlarının herhangi bir koruması olmadığı için şimdiye kadar birçok *Hizmet Aksatma* (DoS, Denial of Service) ve spam saldırısı yaşanmıştır.

Rocky Mountain IPv6 Çalışma Grubu üyesi Scott Hogg, birçok *hacker*ın IPv6 hakkında yeterince bilgi sahibi olmadığını, hatta bazılarının IPv6'dan haberleri bile olmadığını; fakat bazen yapılan genel saldırıların tesadüfen IPv6 ağlarına dair bazı zayıflıkları ortaya koyduğunu belirtmiştir [8].

IPv6 Güvenlik Açıkları

Kuruluşlar açısından bakıldığında, yeni protokolün temel sorunlardan bir tanesi IT çalışanlarının, kendi ağları bu teknolojiyi kullanmasına rağmen, IPv6'yı incelemek için yeterince zaman harcamamış olmalarıdır. Oysa IPv6'nin IPv4'e göre daha farklı güvenlik açıkları vardır ve IPv6 kod gelişkinliği şu anda olgunlaşmamış bir durumda olduğundan ötürü güvenlik uzmanları bu farkları incelemeye ve IPv6'yı daha güvenli yapmak için planlar geliştirmeye zaman ayırmalıdır.

Aynı şekilde cihaz üreticileri tarafından geliştirilmiş olan güvenlik uygulamaları da henüz sağlamlığı kanıtlanmış olamayacak kadar yenidir.

IPv6 konusundaki güvenlik problemlerinden bir tanesi de, güncel güvenlik duvarı yazılımlarının protokole uygun olmamasıdır.

Güvenlik Duvarı / Ateş Duvarı (*Firewall*)

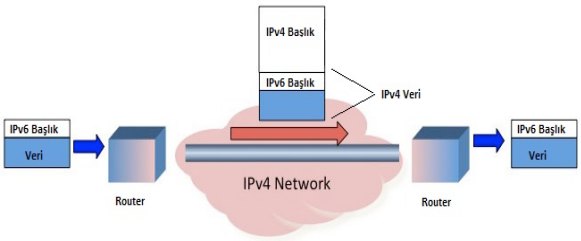
Güvenlik duvarı (firewall), İnternet trafiğini kontrol altında tutmak amacıyla gelen ve giden paketler üzerinde farklı filtreler uygulayan bir yazılımdır. Bu filtreler IP, port, ya da içeriğe göre tanımlanabilir [9].

IPv4 adreslerine göre tanımlanmış güvenlik duvarı filtreleri IPv6 paketleri üzerinde çalışmaz. Bu, IPv6'ların saldırılara karşı korunma mekanizması ile ilgili ilk endişedir.

Bir diğer endişe ise, Windows makinelerin varsayılan ayar olarak IPv6 tünellemelerini olanaklı kılıyor olmalarıdır. Tünelleme yöntemi, IPv4 ağını kullanmakta olan; fakat herhangi bir IPv6 güvenlik önlemi yerleştirmemiş olan kuruluşlar için büyük sorunlar anlamına gelebilir.

IP Tünelleme

Tünelleme (*IP Tunneling*), IPv6 trafiğinin şu anda yaygın olarak kullanılan IPv4 ağları ile taşınmasına olanak veren bir yöntemdir. Bu yöntem ile IPv6 paketleri IPv4 paketlerinin içine yerleştirilerek, IPv4 ağları üzerinde bir sanal tünel ile gönderilmesi anlamına gelir.



Şekil 2 – IP Tünelleme şeması

Bu yöntemde IPv6 paketleri başlık ve verileriyle birlikte bir bütün olarak IPv4 paketinin içine (*başlıktan sonra, IPv4 paketinin verisi olarak*) yerleştirilir.

Bu konudaki sorun, güvenlik duvarları da dahil eski IPv4 cihazların, yeni protokol kullanılarak oluşturulan trafiği kolay çözümleyemiyor olmalarıdır. Bu anlamda saldırganlar bahsedilen tüneller üzerinden kolaylıkla IPv4 cihazlarının algılayamayacağı kötü amaçlı yazılım ve *spam* gönderebilirler.

Saldırı Yazılımları

Bir başka sorun da, İnternet üzerinden dağıtıma açılan ve amatör *hacker*ların kullanımına sunulan IPv6 saldırı araçlarıdır. Buna bir örnek *Hacker'ların Seçimi* (THC, The Hackers Choice) isimli grubun Yerel Ağ temelli IPv6 cihazlarına yönelik olarak güncellediği saldırı yazılımıdır. THC bunu IPv6 üzerinde bulduğu güvenlik açıklarına dikkat çekmek ve yetkililerin bu güvenlik açıklarını tamir etmelerini sağlamak içi yaptığını belirtmekte; fakat bu araçlar hackerların internet trafiğini yavaşlatmalarına da sebebiyet vermektedir [10].

IPv6 kimlik doğrulama vb. konularda büyük imkanlar veren ilave başlıklara (*header*) olanak tanımaktadır; fakat henüz cihaz üreticilerinin kendileri de bu ilaveleri güvenli şekilde nasıl destekleyeceklerini yeni öğrenmektedirler. Bunun bir örneği, bir araştırmacının fazla uzun bir ilave başlık kullanarak bir yönlendiriciyi işlevsizleştirmesi ve bu yöntemle saldırgan olması muhtemel olan bazı paketlerin kimlik doğrulamasına takılmaksızın yönlendiriciden geçmelerine imkan tanındığını göstermesi olmuştur.

Bir başka tehlike de, eski IPv6 cihazlarının varsayılan ayar olarak belli bir tip (*Type 0*) yönlendirme başlıklarını desteklemesidir. Bu başlıklar paketlerin hedeflerine ulaşana kadar uğrayacakları bütün ara yönlendiricilerin bir listesini içermektedir. Bu uygulama normalde ağ performansını iyileştirmesine rağmen saldırganlar bu başlıkları içeren sahte paketler oluşturup paketlerin iki yönlendirici arasında birçok

kere gidip gelmesine, dolayısıyla da internet trafiğinin aksamasına, ve hizmetlerin yavaşlamasına, bazen de tamamen kesilmesine sebep olabilmektedir. Bu, sistemin içerisine sızmaksızın, yalnızca çalışmasını engelleme amacı güden saldırılara DoS (Denial of Service) Saldırıları denilmektedir[11].

Mevcut IPv6 Güvenliği

IPv6'nin şu anki güvenlik mekanizmalarından bir tanesi iletişim sırasında kullanılan bütün IP paketlerinin doğrulanmasına ve kriptolanmasına (şifrelenmesine) yarayan *IPsec* protokolüdür. Fakat eski cihazların varsayılan ayar olarak *IPsec*'i çalıştırmama ihtimali her zaman mevcuttur.

IEEE 802.1X standartlar ailesi, ağa erişmeye çalışan yönlendiricilerin kimlik doğrulamasını yaparak erişim kontrolü sağlamaktadır.

IETF'nin IPv6 Yönlendirici Duyuru Koruması (RA-Guard) yönlendirici duyurularını incelemekte ve yetkili olmayan yönlendiricilerden gönderilen sahte duyuruları filtrelemektedir. *Router spoofing* adı verilen ve saldırganın başka bir routermış gibi davranması anlamına gelen saldırılar bu şekilde önlenebilmektedir.

Bununla birlikte Windows varsayılan olarak bu imkanları desteklememekte, dolayısıyla kuruluşların kendilerini koruma altına almak için bütün bilgisayarlara RA-Guard sürücülerini yüklemeleri gerekmektedir.

POTANSİYEL (TEKNİK) ÇÖZÜMLER

Birçok durumda kuruluşların bütün ağ cihazlarını IPv6'nın imkanlarını destekleyecek şekilde güncellemeleri gerekmektedir. Bazı durumlarda bu basit bir yazılım güncelleme anlamına gelirken, *tek amaçlı* (dedicated purpose) çipler kullanan cihazlar için bütün bir platformun değişmesi anlamına gelmektedir.

Bu güncellemelerin yanı sıra IT personelinin de IPv6 konusunda yeterince eğitimli olması gerekmektedir.

Bazı kuruluşlar IPv6 protokolünün saldırıya açık, hassas yönlerinin bulunması için ödül vermektedir. Örneğin ağ cihazları üreticisi D-Link şirketinin ürün geliştirme müdürü Will Brown, doğrudan güvenlikle ilgilenen topluluklarla çalıştıklarını ve güvenlik açıklarını doğrulanabilir şekilde ortaya çıkarılmasını desteklemek üzere bir ödül programı geliştirdiklerini belirtmiştir [12].

IPv6, IT kuruluşları ve cihaz üreticileri için önümüzdeki yıllarda da büyük bir endişe kaynağı olmaya devam edecektir. Fakat uzun vadede güvenlik duvarları, spam filtreleri ve paket inceleme araçları geliştikçe IPv6 güvenliğinin de bir rutinden ibaret olması beklenebilir.

HUKUKİ DURUM

Yukarıda ayrıntısıyla açıklandığı üzere, IPv6, henüz birçok yönüyle bilinmeyen bir protokol olduğundan, IPv4'ten farklı birçok saldırıya da açık hale gelmekte, dolayısıyla farklı güvenlik problemlerini bünyesinde barındırmaktadır.

IPv4'ten farklı olarak, IPv6'lerde keşif saldırılarının görülmesi mümkündür. Bu saldırılar, esasen bir saldırı türün olmaktan öte, bir saldırının başlangıç aşaması olarak görülebilir. Zira bunlar, bir saldırı yapmadan önce o ağı analiz etmek ve ağdaki cihazları tanımlamak için kullanılır. Saldırgan çeşitli tarama yöntemlerini kullanarak hedef ağdaki IP adreslerini belirler ve daha sonra daha detaya inerek, ağdaki cihazlara özel bir port taraması yapar. IPv6'teki ağ sayısı, IPv4'e göre çok daha geniş olduğundan, bütün ağı taramak imkansız hale gelmiştir. Bu nedenle, IPv6'lerin IPv4'lara nazaran keşif saldırılarına daha dayanıklı olduğu söylenebilirse de, bu protokoldeki bazı çoklu gönderim adresleri kullanılarak ağdaki cihazların tespiti ve saldırı amacıyla kullanılabilir[13].

Yine yukarıda, birçok spam vb. saldırıya sebep olan yönlendirici başlık konusunda, IPv6 ağındaki tüm cihazların yönlendirme başlıklarını işleyebildikleri söylenmiş olup, bu da yetkisiz erişim gibi bazı güvenlik sorunlarına yol açabilir. Örneğin; bir saldırgan, açık bir ağ üzerindeki bir cihaza, yönlendirme başlığında o cihaz üzerinde önceden yasaklı olarak belirlenmiş bir paket yollamış olsun. Normal şartlarda bu paketin farkedilmesi gerekirken, bu cihaz gelen paketi otomatik olarak iletmektedir. Saldırgan, sahte IP adresleri üzerinden açık ağdaki bu cihazı kullanıp, gönderdiği paketleri iletmesini sağlayarak da DoS saldırısı yapabilir. Burada önemli olan ve bilinmesi gereken, bazı işletim sistemlerinin yönlendirici başlığı olan paketleri otomatik olarak ilettiği, bazılarının ise iletmediğidir [14].

Protokolün güvenlik açığı nedeniyle maruz kalacağı bu saldırılarda, saldırganların fiilleri 5237 sy. Türk Ceza Kanunu'nun 243 ve 244. Maddeleri uyarınca cezalandırılacaktır. TCK m. 243'te "bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir." Denilerek, yetkisiz erişim suçu düzenlenmiştir. Ancak, özellikle çalışmamızda bahsettiğimiz ve IPv6'lardaki güncel tehlike olarak görülen saldırılar, daha çok sistemin içine sızmaksızın trafiği veya hizmeti engelleme şeklinde ortaya çıkan (Bunlar DoS veya DDoS olabileceği gibi, başka saldırılar da olabilir)

saldırılardır. Eğer saldırgan, sistemin içine girmeksizin, yalnızca işleyişi engelleme şeklinde bir eylemde bulunduysa, bu durumda sorumlu olacağı hüküm TCK m. 244'tür. Bu hükme göre; "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır." O halde, DoS ve DDoS saldırıları "*bir bilişim sisteminin işleyişinin engellenmesi*" fiiline karşılık geldiğinden, TCK m. 244'te öngörülen suça vücut vermektedir.

Aynı hükmün 3. fıkrasında ise, "*Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır*" şeklinde düzenleme yer almakta olup, bu saldırıların hükümde sayılan kurumların bilişim sistemleri hedef alınarak gerçekleştirilmesi halinde, bu durum kanun koyucu tarafından ağırlaştırıcı neden olarak kabul edilmiştir. Örneğin, Türkiye'de IPv6 üzerinden sistemine saldırılan ilk kurum TÜBİTAK Ulakbim olup[15], bu kuruma yapılan saldırı TCK m. 244/3 kapsamına girecektir.

Açıkladığımız üzere, IPv4 adreslerine göre tanılanmış firewall filtreleri IPv6 paketleri üzerinden çalışmayacağından, bazı işletim sistemlerinin IPv6 uygulamalarından doğan problemleri ortaya çıkacağından, mevcut yazılımların IPv6 uyumluluğu sırasında yazılımın güvenlik açıklarını ayıklaması için zaman gerekeceğinden, geçiş aşamasında IPv4 ile IPv6 ikili kullanımı sorun çıkarabileceğinden, otomatik IP yapılandırması problemler çıkaracağından ve yeni bir protokol uygulaması söz konusu olacağından daha birçok güvenlik sorunu ortaya çıkacağından, bir süre daha IPv6 üzerinden saldırılar görülecektir. Bu bağlamda, saldırganlar bakımından TCK m. 243-244 uyarınca cezai yaptırımlar uygulanabilecekse de, özellikle DDoS gibi dağıtık yapılan ve zombi IP'ler kullanılarak gerçekleştirilen saldırılarda saldırganlara ulaşmak son derece zor olduğundan, yaptırımdan ziyade kullanımın artmasıyla *Firewall, Network management tools* gibi güvenlik araçlarında sorun olacağı ihtimali nedeniyle, bu sorunların ivedi bir şekilde çözülmesi gerekmektedir.

Son olarak, IPv6 protokolünün, içerisinde çok sayıda bilinmeyeni barındırması dolayısıyla, kişisel verilerin korunmasında zafiyete sebebiyet vereceği de öngörülmektedir[16]. Aynı şekilde, bu denli mutlak bir biçimde belirlenebilir ve uzayda eşsiz bir kimlik tanıtma sistemi olan IPv6 ile, kişilerin kimliğine ilişkin, kültürel, mental, fiziksel her türlü bilgisine ulaşılabileceği ve bunun da kişisel veriler üzerinde ihlal oluşturabileceği söylenmektedir[17]. Bu bağlamda, IP adresleri gibi trafik verilerinin silinmesi veya birkaç kural dışı durum haricinde iletimin tamamlanması üzerine bu verilerin isimsizleştirilmesi ve İnternet Servis Sağlayıcılarına haberleşme verilerinin acilen silinmesi veya isimsizleştirilmesi zorunluluğunu kabul ettiren prensiplerin yayımlanması önerilmektedir[18].

Gerçekten de, özellikle Avrupa Birliği 95/46/EC sayılı Veri Koruma Direktifi uyarınca, AB üyesi ülkeler, kullanıcıların açık rızası olmadıkça yasadışı durdurma ve gözetimi yasaklayarak haberleşme ve bu haberleşmeyle ilgili tüm veri trafiğinin gizliliğini sağlamak zorundadır (E-Privacy D. 2002/58/EC Art. 5(3))[19]. Bu nedenle, söz konusu trafik bilgilerinin saklanmasına ilişkin önlemler alınması gerekmekte olup, buna uyulmaması halinde TCK'nun 135-136. Maddelerindeki kişisel verilerin korunmasına ilişkin ceza hükümleri uygulama alanı bulacaktır. Bunun yanında, yıllardır tasarı halinde bekleyen ve henüz yürürlüğe girmemiş olan '*Kişisel Verilerin Korunması Hakkındaki Kanun*'da da IPv6'lere ilişkin bu hukuki soruna ilişkin yasal düzenleme yapılması düşünülmelidir.

SONUÇ

Günümüzde IPv4 protokolünün müthiş bir hızla artan ihtiyaçlara cevap veremeyecek duruma gelmesi nedeniyle, kimi potansiyel sorunlarına rağmen IPv6'e geçişin kaçınılmaz olduğu ortadadır. Özellikle bu geçiş sürecinde IPv6'in, belli bir süre IPv4 ile birlikte kullanılacak olması ve her şeyiyle yeni bir olgu olarak hayatımıza girmesi nedeniyle, IPv4'dan çok daha farklı sorunlar ortaya çıkarabileceği, kendine özgü kimi güvenlik problemleri yaratabileceği ve saldırganların yeni saldırı aracı haline geleceği açıktır. Bununla ilgili olarak, özellikle bilişim sistemlerine yapılan saldırılara ilişkin olarak Türk Ceza Kanunu ve diğer mevzuatın uygulama alanı bulması ve öte yandan, kişisel verilerin korunmasıyla ilgili AB direktifleri ve ülkemizde yapılma aşamasında olan kanun çalışmaları ile çözüm bulunabilir olsa da; esas çözüm, IPv6 kullanımının artmasıyla beraber yeni yöntemler oluşturularak, sorunu yine kendi alanında bertaraf etmek, bu yolda da teknik personeli IPv6 konusunda eğitmek, güvenlik yazılımlarının ve programlarının IPv6 uyumluluğu konusunda fizibilite çalışması yapmak ve son kullanıcı bazında IPv6 desteği için çalışmaları hızlandırmak [20] olacaktır.

KAYNAKÇA

[1] Herbert, T. (1999). Introduction to TCP/IP, part I. *Embedded Systems Programming*, *12*(13), s. 58. Kasım,2012, ftp://216.97.234.108/uconline/iad/esptcp1.pdf (11.10.2013).

[2]http://www.washington.edu/lst/help/computing_fundamentals/networking/img/osi_model.jpg

[3] http://www.sustworks.com/site/prod_ipr_subnets.

Html (12.10.2013).

[4] TÜBİTAK – Ulakbim, *Ipv6 EL Kitabı*, https://www.ulakbim.gov.tr/ulaknet/ulak6net/IPv6_El_Kitabi.pdf (11.10.2013).

[5] LAWTON, George; "*Is IPv6 Secure Enough*?", http://www.computer.org/portal/web/computingnow/news/is-ipv6-secure-enough?utm_source=dlvr.it&utm_medium=twitter, (08.10.2013).

[6] http://www.google.com/ipv6/statistics.html

[7] KARA, Mehmet; *IPv6'ya Geçiş*, TÜBİTAK UEKAE, Nisan 2009, www.bilgiguvenligi.gov.tr/dokuman.../3...**ipv6**ya-**gecis**/download.html (10.10.2013).

[8] http://www.ipv6tf.org/ (09.10.2013).

[9] http://tr.wikipedia.org/wiki/Ate%C5%9F_duvar%C4%B1 (10.10.2013).

[10] van Hauser; "*Attacking the IPv6 Protocol Suite*", 2008, https://www.thc.org/papers/vh_thc-ipv6_attack.pdf (12.10.2013).

[11] ÖZOCAK, Gürkan; "*DDoS Saldırısı ve Failin Cezai Sorumluluğu*", Bilişim 2012 – 28. Ulusal Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2012, s. 23.

[12] http://newsroom.cisco.com/press-release-content?articleId=633565 (11.10.2013).

[13] ÇAKIN, Ayhan / AYDIN, Muhammet Ali; "*IPv4 / IPv6 Güvenlik tehditleri ve Karşılaştırması*", http://www.emo.org.tr/ekler/e964cf77e41a4da_ek.pdf. (12.10.2013).

[14] ÇAKIN/AYDIN, a.g.e.

[15] BEKTAŞ, Onur / SOYSAL, Murat; "*Yeni Nesil IP Protokolü (IPv6) ve Güvenlik*", s. 11, 2006 http://www.ipv6.net.tr/index.php?option=com_content&view=article&id=58&Itemid=53 (12.10.2013).

[16] II. Ulusal IPv6 Konferansı Raporu, "*IPv6 Geçiş ve Sonrası*", Şubat 2012, http://www.ipv6turkey.org (09.10.2013).

[17] RADHAKISSOON, Ashok; "*Legal Aspect of IPv6 and of the IPv4 to IPv6 Transition*" http://meeting.afrinic.net/afrinic-10/legal_aspects_of_IPv6_and_IPv4.pdf (11.10.2013).

[18] BOLAT, Ayşegül / TÖZER, Ayhan; IPv6 ve Türkiye, http://www.ipv6.net.tr/docs/11.pdf (10.10.2013).

[19] Directive on privacy and electronic communications, 2002/58/EC, *Article 5(3),* 12.07.2002.

[20] BEKTAŞ/SOYSAL, a.g.e.

Çise MIDOĞLU, MSc

Gürkan Özocak, LL.M.