

Yeni Nesil IP Protokolü (IPv6) ve Güvenlik



Onur BEKTAŞ (onur at ulakbim.gov.tr)

Murat SOYSAL (msoysal at ulakbim.gov.tr)



İçerik

- IPv6 Tanıtım, Giriş.
- IPv6'nın güvenlik yönünden artıları.
- IPv6'nın güvenlik yönünden eksileri.
- Mevcut güvenlik açıklarının ve saldırı çeşitlerinin IPv4 ve IPv6'da durumları.
- Sonuçlar, tahminler, öneriler.



IPv6 Nedir ?

- IPv6 "Internet Protocol Version 6" kelimesinin başharflerinin kısaltılmış halidir.70'li yıllarda geliştirilen ve hala kullanılan IP versiyon 4 (IPv4) protokolünün yerini alması için 90 lı yılların başından itibaren IETF (Internet Engineering Task Force) tarafından ilk çalışmalarına başlatılmış ve IPv4'ün yerini alması öngörülmektedir.



IPv4 & IPv6

- 32 Bit Adresleme.
- Karışık başlık yapısı.
- Değişken başlık (header) uzunluğu.
- Fragmentasyon Var.
- IPsec opsiyonel.
- NAT var.
- 128 Bit Adresleme.
- Sade başlık yapısı.
- Sabit başlık (header) uzunluğu.
- Fragmentasyon yok (*).
- Ipsec protokol içine entegre .
- NAT yok.



IPv6'ya geçmelimiyiz ?

■ EVET !!!!!



IPv6 & UlakNET

- UlakNET ađının 2003 Yılından itibaren IPv6 desteđi var.
- 8 Üniversite IPv6 adresi almıř durumda.
- ULAKBİM 3 senedir sunucu servislerini ve İ alan ađını IPv4 & IPv6 olarak iřletiyor.
- IPv6 konusunda Telekomünikasyon Kurumu ile ortak alıřmalarımız var.
- www.ipv6.net.tr www.ipv6.gov.tr alan adlarının sahibiyiz.
- www.ipv6.org.tr kullanım hakkı alan adı sahibi tarafından ULAKBİM'e verilmiřtir.



IPv6'nın güvenlik yönünden artıları

- IP seviyesinde protokol içine entegre edilmiş güvenlik (AH ve ESP).
- Adres yapısı.
- Sadeleştirilmiş başlık yapısı.
- Fregmentasyonun engellenmesi.
- Protokol sadeleştirmeleri (Arp protokolünün olmaması vb).
- IP paketlerinin yolunun izlenmesinin kolaylaşması.
- NAT'a izin verilmemesi.

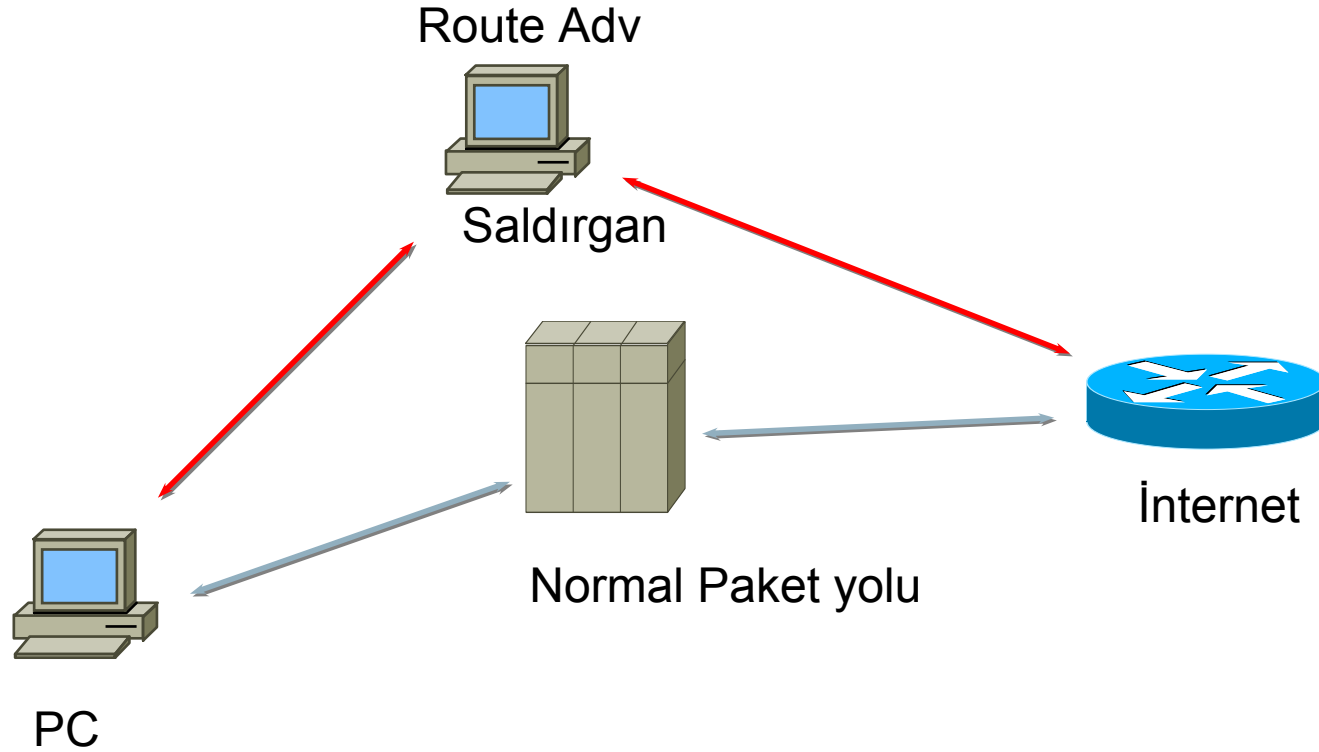


IPv6'nin güvenlik yönünden eksileri

- Ağ ve sistem yöneticilerinin IPv6 eğitim eksiklikleri ve bilgi seviyelerinin az olmasından doğacak sorunlar.
- İşletim sistemlerinin IPv6 uygulamalarından doğan problemler (Windows).
- Mevcut yazılımların IPv6 uyumluluğu sırasında yazılımın güvenlik açıklarının ayıklanması için zaman gerekliliği.
- İkili Yığın (Dual-Stack) yapının getirdiği problemler.
- Otomatik IP yapılandırması problemleri.
- Mobilite uygulamalarından kaynaklanacak problemler.



Windows XP Adres saldırısı.



IPv6

23/12/2006 InetTR

Tübitak-Ulakbim

9



Mevcut güvenlik açıklarının ve saldırı çeşitlerinin IPv4 ve IPv6'da durumları.

■ Farklı olanlar

- Keşif (Reconnaissance)
- Broadcast yüksetgenme saldırıları (Smurf)
- Virüs/Solucan
- ARP ve DHCP
- Fregmentasyon
- ICMP

■ Benzer olanlar

- taşıma (flooding),
- ortadaki adam (man-in-the-middle)*
- trafik koklama (sniffing) *
- Uygulama katmanı saldırıları.



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 kimlik doğrulama ve şifreleme uygulamaları kullanımı IPv6'nın yaygınlaşması ile artacaktır. IPv4 IPSec kadar sınırlı ve VPN bağlı kalmayacaktır.
- Geçiş aşamasında ikili kullanım güvenlik zaaflarına yol açabilir.
- IPv6 güvenli demek yeterli değil. Daha güvenli olmaya doğuştan yatkın ancak yönlendirme ve eğitim şart.
- Türkiye'de IPv6 üzerinden kırılan muhtemelen ilk kurumumuz 😊



Beklentiler

- IPv6 uygulamaların güvenlik açıklarının zamanla azalması.
- DNS güvenliğinin önemi artacak.
- IPv6'ya geçişte itici güç bilgisayarlar ihtiyaçları değil PDA, cep telefonu, sensör ağları ve benzeri cihazların bağlantı gereksinimleri olacak.



Öneriler

- IPv6'ya geis alıřmalarını ilk olarak mevcut ađ ekipmanlarının, gvenlik yazılımlarının ve programların IPv6 uyumluluđu konusunda fizibilite alıřması yapılmalı
- Teknik personel IPv6 konusunda eđitilmeli.
- IPv6 destek durumuna gre geiře ađ cihazlarından bařlayıp daha sonra sunucu sistemlerde IPv4 ile verilen hizmetlerin IPv6 destekler hale getirilmesi ile devam edilmeli en son olarak kullanıcı seviyesinde IPv6 desteđi iin alıřmaları.
- Geiř ařamasında yařanacak problemler iin dkmantasyon yapılmalı.(www.ipv6.net.tr)
- IPv6 treninin hala kaırmıř deđiliz!!!.



SORULAR ?
