IPv6 Üzerindeki Güvenlik Tehditleri

Ayhan Çakın
acakin@yildiz.edu.tr

M. Ali Aydın
aydinali@istanbul.edu.tr

İçerik

- IPv6'ya Giriş ve Özellikleri
- IPv6 Üzerindeki Güvenlik Tehditleri
  - Mevcut ve Yeni Saldırılar
  - Saldırı Türlerinin Eski ve Yeni Protokol Üzerinde Etkileri
    - Yetkisiz Erişim
    - Keşif Tipi Saldırlar
    - …
- Sonuçlar
- Gelecek Çalışmaları

IPv6 Özellikleri

- Genişletilmiş Adres Uzayı
- Zorunlu IPSec Uygulama Desteği
- Qos Standartları
- Mobilite
- Başlık Yapısı – Ek Başlıklar
- Otomatik Yapılandırma

IPv6 Güvenlik Tehditleri

- Mevcut ve Yeni Tehditler
  - Yetkisiz Erişim
  - Keşif Tipi Saldırılar
  - Uygulama Seviyesi Saldırıları
  - Yayınla Saldırıya Maruz Bırakma
  - Taşırma Saldırıları
  - Başlık Yönetimi ve Parçalama
  - ARP, DCHP Saldırıları, Sahte Cihazlar
  - Koklama Saldırıları ve IPSec Etkisi
  - Ortadaki Adam Saldırıları
  - Ek başlıklar ile İlgili Tehditler
  - ICMPv6
  - Tünelleme ve Geçiş Mekanizmaları ile İlgili Saldırılar

Saldırıların IPv4/IPv6 Üzerinde Etkileri: 1.Yetkisiz Erişim

- IPv4
  - Açık veri aktarımı zayıflığı
  - Uç konaklarda – Erişim Kontrol Listeleri
- IPv6
  - IPSec Etkisi
  - Adresleme ve Yönlendırme Mekanizmalarında Yapılan Değişiklikler

2. Koklama ve Ortadaki Adam Saldırıları

- IPv4
  - Veriler temel oalrak düz metin olarak aktarılmakta
- IPv6
  - IPSec Uygulama Desteği Zorunlu.
- **Önemli Nokta:** IPv6 da IPSec uygulama destegi zorunlu olsada, IPSec özelliğinin kullanımı zorunlu değildir ve bundan dolayı eskisinden daha çok kullanılacağı söylenemez.(Anahtar değişimindeki zorluklar göz önüne alındığında)

3.Taşırma Saldırıları

- IPv4 Üzerindeki en yaygın saldırı türlerinden
- IPv6
  - Bu saldırı türü uygulama mantığı yeni protokol ile değişmeyeceği için aynı kalacaktır.
  - Saldırı üzerindeki tek değişiklik IPv6 ile genişleyen adres uzayından dolayı saldırıda görev alan sahte IP'lerin network analizi ile bulunması zorlaşması olacaktır.

4. Uygulama Seviyesi Saldırıları

- IPv4 ten IPv6'ya geçiş uygulama sevıyesi saldırıları açısından bir değişiklik yaratmayacaktır.
- Bilindiği Üzere bu tarz saldırılar uygulama seviyesinde gerçekleşirkeni IPv4/v6 ISO/OSI modelinin ağ katmanı protokolleridir.

5.ARP, DHCP and Sahte Cihazlar

- ARP ve DHCP nin IPv6 karşılıklarına hiçbir dahili güvenlik önlemi eklenmemiştir.
- ‘Router Solicitation’ ve ‘Neighbour Solicitation’ mesajları sahte olarak üretılebilmekte ve üzerine yazılabilmektedirç
- Sahte Cihazların tespiti icin bilinen yöntemler IPv6 için değişmemiştir.
- IPSec özelliğinin ve ağdaki cihazların doğrulama prosedürünün etkin olarak uygulanması, bu tarz sahte cihazların tespitine yardımcı olacaktırç

6.Keşif Tipi Saldırılar

- IPv6 nın geniş adres uzayı nedeniyle tüm ağı taramak imkansız hale gelmektedir
- Yeni protokol bu tarz saldırılara daha dayanıklı gözükmekte
- Ancak, IPv6 da çoklu gönderim adreslerinin kullanılması bu paketlerin saldırgan tarafından ele geçirildiği takdirde bir zayıflık yaratmaktadır

7.ICMPv6

- IPv4 ağlarında güvenliği sürdürmek açısından ICMP mesajlarını bloklamak yaygın bir davranış
- Ancak yeni protokolde, ICMPv6 mesajları ‘Neighbour Dıscovery’ ve ‘MTU Discovery’ gibi birçok önemli protokolde kullanılmaktadır.
- ICMPv6 tanımlanmasında göze çarpan bir risk, hata mesajlarının hedef adreslerinin çoklu gönderim adresi olarak tanımlanabilmesdir. Bu tanımlama saldırganlar tarafından kullanılmaya müsaittir.

8.Ek Başlıklar ile İlgili Tehditler

- Bilindiği üzere bazı işletim sistemleri yönlendirme başlığı taşıyan paketleri otomatik olarak iletmektedir
- Yeni protokolün tanımına göre tüm konaklar yönlendirme başlığını işleyebilmelidir.
- Kaynak adreslerin sahte olarak hazırlanması ile herkese açık bir hostun paketleri yönlendirmesi sağlanarak servis dışı bırakma atağı uygulanabilir

9.Fragmentation

- IPv6 tanımlamasına göre IPv6 ağlarındaki konaklar ‘Path MTU Discovery’ özelliğini uygulamalı ve IPv6 en küçük bağlantı ölçütünden büyük olan yollarda avantaj sağlamalılardır
- IPv6 ağlarında orta konaklarda parçalanma yapılmasına ızın verilmemektedir
- Birden çok ek başlığın kullanılması halinde paketin parçalarının uç konaklarda birleştirilmesinde sorun yaratabilir

10.Tünelleme Mekanizmaları Bağlantılı Saldırılar

- IPv4 ağlarının şu anki devasa boyutunu göz önüne aldığımızda, IPv6ye geçişin yavaş olacağı öngörülebilir
- Tünelleme mekanizmaları kurmak ve iki protokolü aynı anda işletmek şuanda tahmin edilemeyen zayıflıklar oluşturabilir
- Ayrıca IPv6ye geçiş sürecince kaçınılmaz olarak yapılacak olan yanlış/eksik yapılandırma hataları da bu ağlarda birçok zayıflık yaratacaktır

Gelecek Çalışmaları

- IPv6 protokolü tanımlamasında “Hop-by-hop” isimli bir ek başlık yer almaktadır.
- Bu başlıkla ilgili en göze çarpan noktaö başlığın paketin yolu üzerindeki her konakta işlenmesidir

‘Hop-by-Hop’

- Bu başlığın tanımında yer alan bazı karakteristik özellikleri servis dışı bırakma saldırıları için zayıflıklar oluşturmaktadır

  (http://tools.ietf.org/html/draft-krishnan-ipv6-hopbyhop-05)
- Bunlardan bazıları:
  - Paketin yolu üzerindeki tüm konaklar bu başlığı işlemelidir
  - Başlıktaki TLV’ler aynı sıra ile işlenmelidir
  - Bir konak bu başlıktaki bazı seçenek tiplerini tanımasa dahii bu bir hataya yol açmayacak
  - Bir seçenek tipinin bu başlıkta kaç kez yer alabileceğine dair bir kısıtlama bulunmamaktadır

Sonuçlar

- IPv6 eski protokoldeki birçok soruna yeni çözüm yaklaşımları getirmektedir.
- IPSec uygulama desteği zorunluluğuö paketlerinin ara konaklarda parçalanmasının kaldırılmasıö adres uzayının genişletilmesi ve NAT kullanımının azaltılmasına yönelik çalışmaları IPV6 yı çok daha güvenli bir protokol yapmıştır
- Unutlmaması gereken en önemli nokta: IPv6 henüz yaygın olarak kullanılmamaktadır ve bundan dolayı kullanılmaya başlandığında ortaya çıkabilecek birçok zayıflığın şimdiden öngörülemediğir

Sorular

?