
# IPv6 Ağlar İçin Güvenli DHCP Sistem Tasarımı ve Gerçeklemesi


| Gürsoy DURMUŞ | İbrahim SOĞUKPINAR |
|---|---|
| Havelsan A.Ş. | GYTE Bilgisayar Mühendisliği Bölümü |
| gdurmus@havelsan.com.tr | ispinar@bilmuh.gyte.edu.tr |



HAVELSAN

# İçerik

- Giriş
  - DHCP protokolü ve gerekliliği...
  - DHCP protokolünde güvenlik...
- Güvenli DHCPv6 Sistemi
  - Sistem bileşenleri ve özellikleri...
  - Geliştirme süreci ve ortamı...
  - Sistem testlerinin değerlendirmesi...
- Sonuç

# DHCP Protokolü ve Gerekliliği...

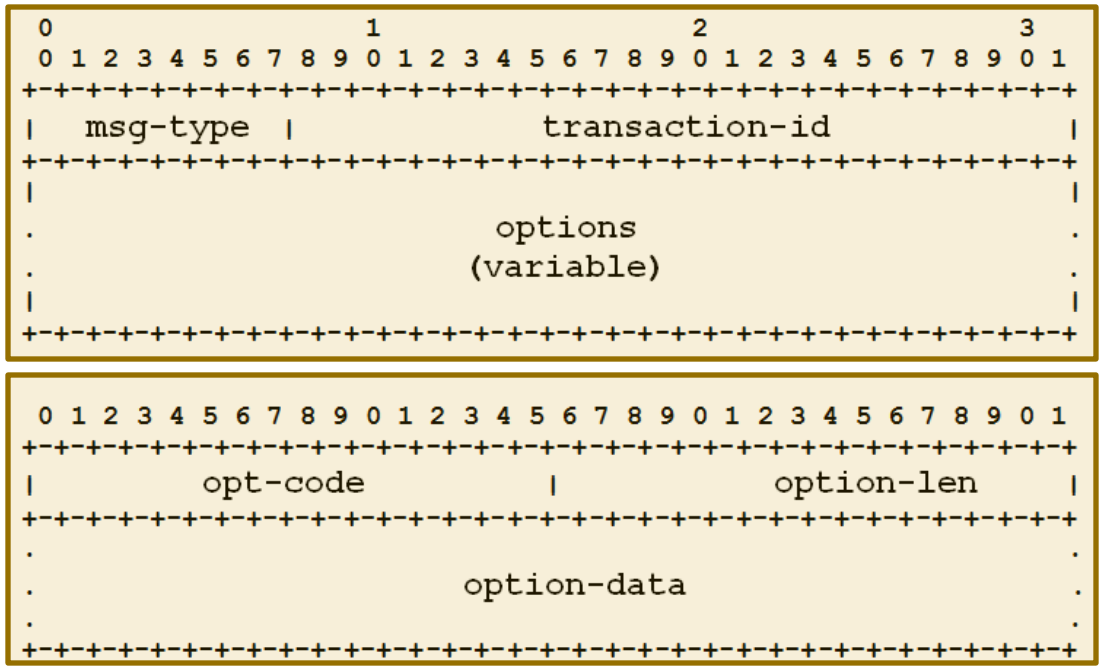
- Bilgisayar ağlarında konakların birbirleri ile iletişim kurabilmeleri için
  - Tekil IP adreslerine sahip olmaları
  - Bazı ayarlarının (DNS, ağ maskesi vb.) yapılmış olması gerekmektedir.
- IP adres tahsisi ve diğer ayarlar elle yapılabileceği gibi otomatik te sağlanabilir.
- Bu gereksinimlerin otomatik karşılanması için DHCP (Dynamic Host Configuration Protocol) protokolü tasarlanmıştır.

# DHCP Protokolü ve Gerekliliği...

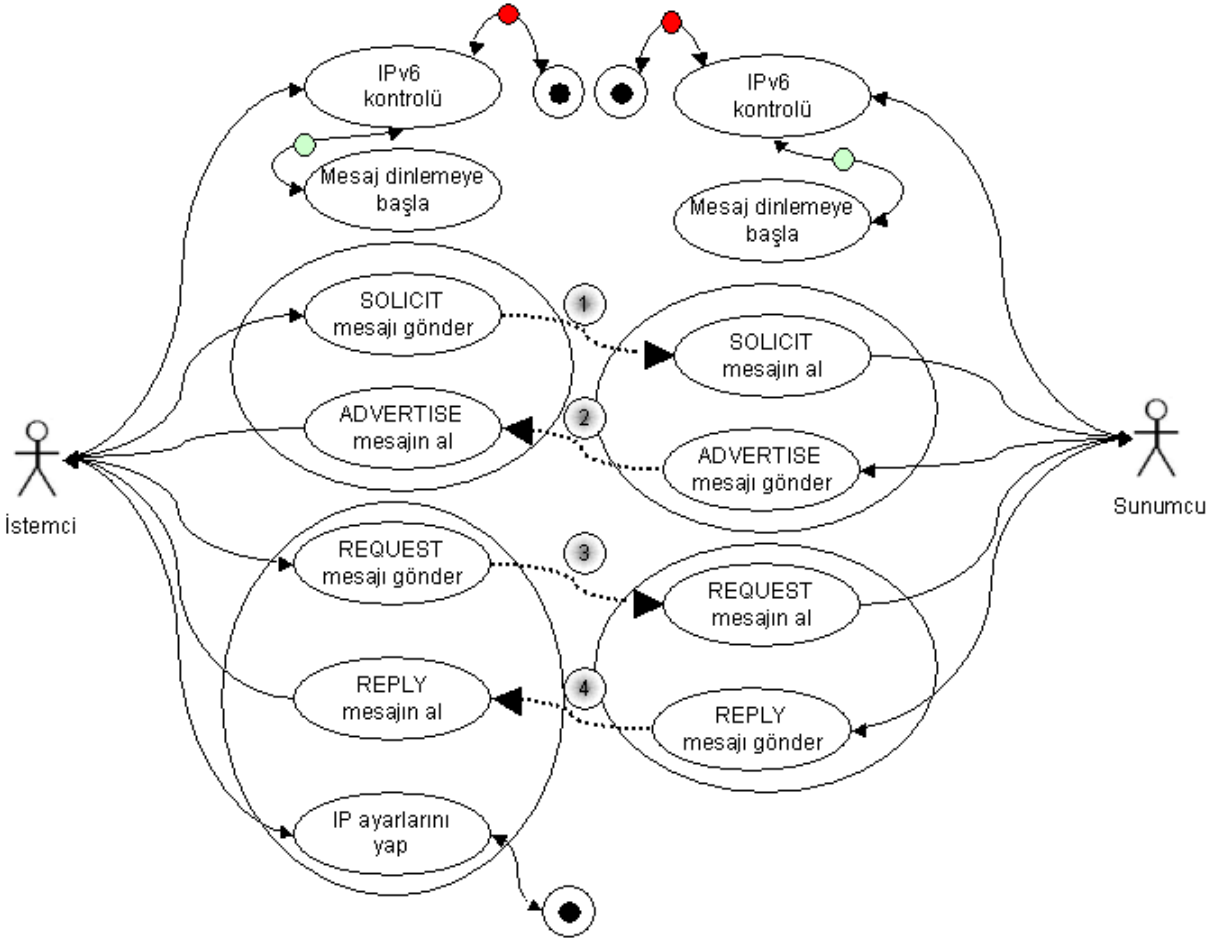
- DHCP İşlevleri
  - IP adres tahsisi ve yapılandırılması
  - Diğer ağ ayarlarının yapılandırılması
  - IP adresleri kaynak yönetimi
- IPv6 ile IP adres tahsisi için otomatik yöntemler gelmiş olmasına karşın diğer ağ ayarlarının yapılandırılmasında DHCP`ye olan ihtiyaç devam etmektedir.

# DHCPv6 Mesaj Yapıları

- DHCPv6 protokolünde istemci ve sunumcu mesajlarının hepsi esnek bir veri yapısına sahiptir.
- Mesaj içeriğine özgün veriler *"opsiyonel bilgiler"* alanı üzerinden iletilir.



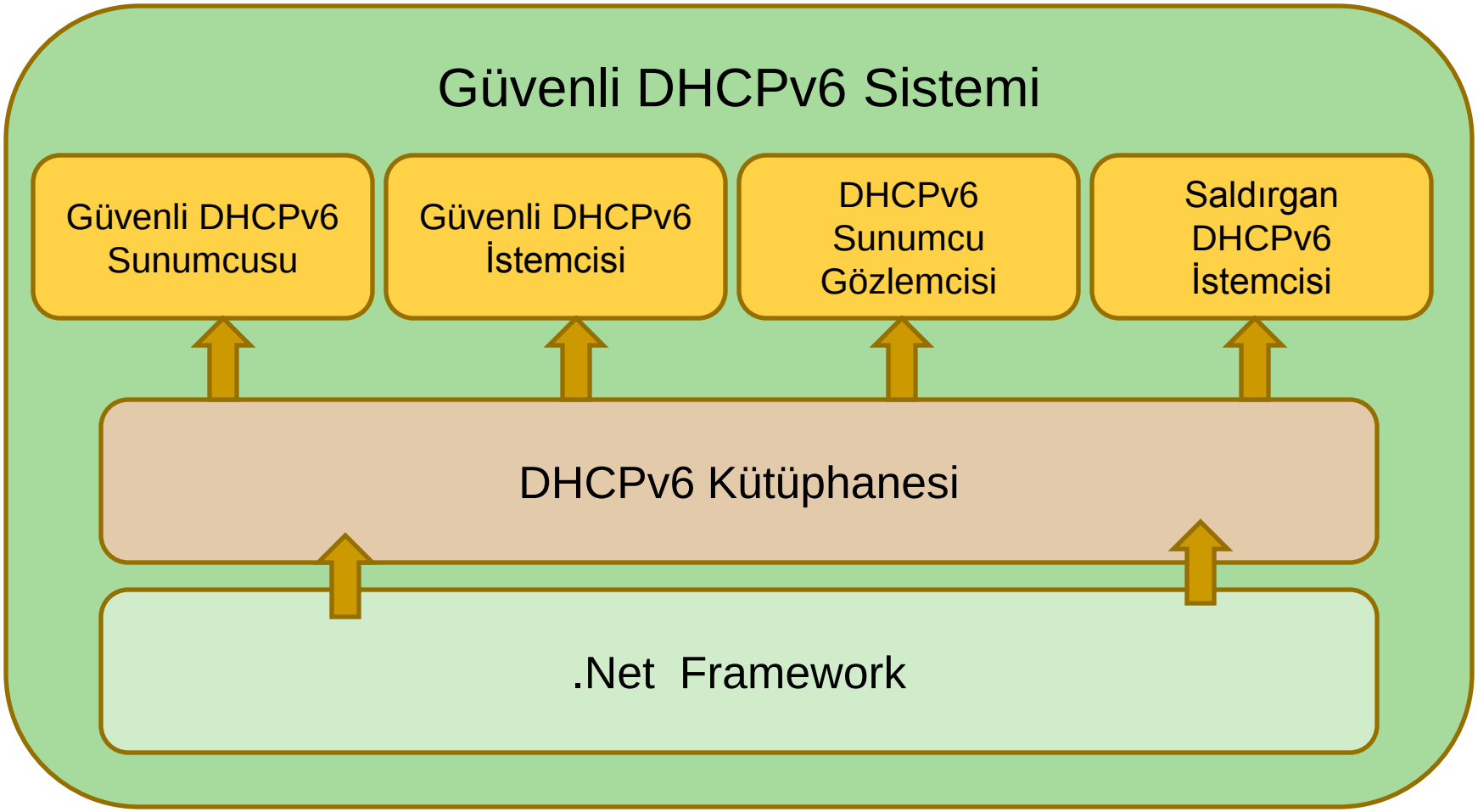
# Bir DHCPv6 Mesajlaşma Senaryosu



# DHCP Protokolünde Güvenlik

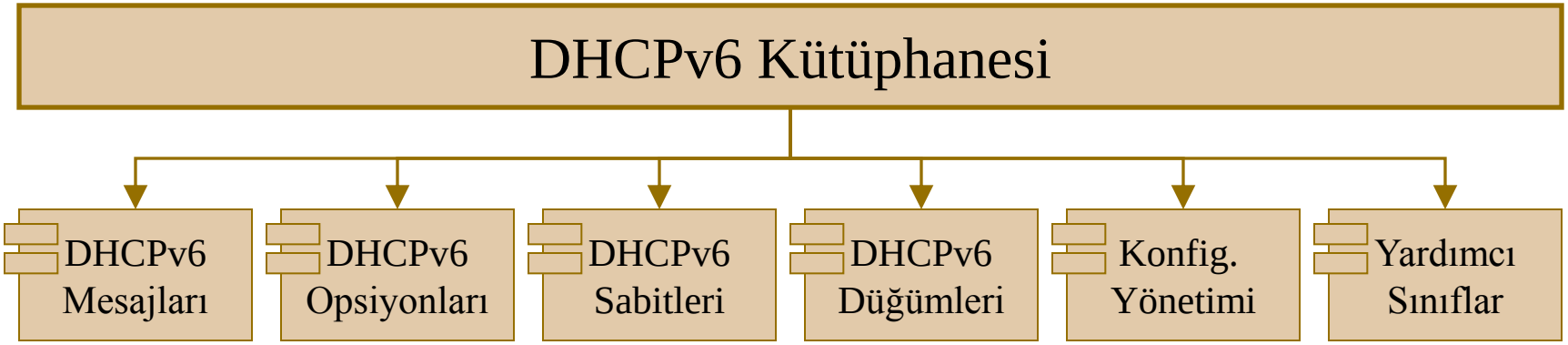
- DHCP mesaj içeriklerinin gizli/önemli veri içermediği varsayıldığından herhangi bir doğrulama mekanizması mesajlara dâhil edilmemiştir. Bu durumun yaratmış olduğu riskler:
  - DHCP mesajlarına müdahale edilebilmesi
  - Art niyetli veya hatalı yapılandırılmış sunumcuların ağda hizmet verebilmesi
  - Art niyetli istemcilerin ağda dolaşabilmesi
- Sonuç olarak:
  - ☹ DHCPv4 güvenli değildi…
  - ☹ DHCPv6 da güvenli değil…
  - ☺ Ama esnek yapısı sayesinde DHCPv6 güvenli hale getirilebilir…

# Güvenli DHCPv6 Sistemi



# DHCPv6 Kütüphanesi

- DHCP sistem öğelerinde ortak kullanılan, istemci ve sunumcu mantıksal gerçeklemeleri, IPv6 çoklu gönderim yardımcı bileşenleri, günlük tutma ve doğrulama altyapı bileşenlerini içerir.
- Güvenli DHCPv6 Sunumcusu, Güvenli DHCPv6 İstemcisi, DHCPv6 Sunumcu Gözlemcisi ve Saldırgan DHCPv6 İstemcisi uygulamalarının farklı biçimlerde gerçeklenmesinde büyük kolaylıklar sağlamıştır.



# Güvenli DHCPv6 Sunumcusu

- RFC-3315, RFC-3646 ve RFC-3118 ile kısmen uyumludur.
- SOLICIT, REQUEST, DECLINE, RELEASE, RENEW, CONFIRM ve INFORMATION-REQUEST mesajlarına karşılık verebilir.
- RECONFIGURE mesajı gönderip istemcilerin yeniden istekte bulunmalarını tetikleyebilir.
- İstemcilere IPv6 adres tahsis yapabilir.
- DNS bilgilerini istemciye iletebilir.
- Sahip olduğu güvenlik kipi, çalışma anında devreye alınıp devre dışı bırakılabilir.
- Sadece IPv6 adres tahsisi veya ağ ayarlarının gönderilmesi için ayarlamalar yapılabilir.
- Güvenlik kipi devrede iken anahtarı bulunmayan istemciler için MAC adreslerini anahtar olarak kullanıp kullanmayacağı çalışma anında belirlenebilir.
- Sunumcu ayarlamaları için kullanıcı arayüzüne sahiptir.

# Güvenli DHCPv6 İstemcisi

- RFC-3315, RFC-3646 ve RFC-3118 standartları ile kısmen uyumludur.
- ADVERTISE, REPLY ve RECONFIGURE mesajlarını işleyebilir.
- IP adresinin iadesi için RELEASE-REPLY mesajlaşması yapabilir.
- IP adreslerinin yenilenmesi için RENEW-REPLY mesajlaşması yapabilir.
- Tespit edilen DHCP Sunumculardan önceliğine göre hizmet alır.
- Konağın IPv6 adres ayarını yapabilir.
- Konağın DNS sunumcusu ayarlarını yapabilir.
- Sahip olduğu güvenlik kipi, çalışma anında devreye alınıp devre dışı bırakılabilir.
- Sadece ağ ayarlarının temini ve yapılandırılması için kullanılabilir.
- Konak için tahsis edilmiş bir anahtar yoksa MAC adresini anahtar olarak kullanabilir.
- İstemci ayarlamaları için kullanıcı arayüzüne sahiptir.

# DHCPv6 Sunumcu Gözlemcisi

- IPv6 ağlarda hizmet veren DHCPv6 sunumcuların gözlemlenmesini, sistem yöneticisi tarafından oluşturulan kurallara uymayan sunumcuların tespiti ve rapor edilmesi için tasarlanmış ve gerçeklenmiş bir ağ yönetim uygulamasıdır.
- Sistem yöneticisi, sunumcunun doğrulanması için sunumcunun DUID sini (DHCP Unique ID) ve/veya sunumcu önceliğini kural olarak tanımlayabilir. Tanımlı kurallara uymayan sunumcu tespitinde e-posta yoluyla veya özel hazırlanmış betiklerin çalıştırılması ile sistem yöneticisi uyarılır.
- DHCPv6 Gözlemcisi ile sistem yöneticisi, ağında hizmet veren sunumcuları takip edebilir, istem dışı veya art niyetli hizmet vermeye başlayan sunumculardan konaklarını koruyabilir.

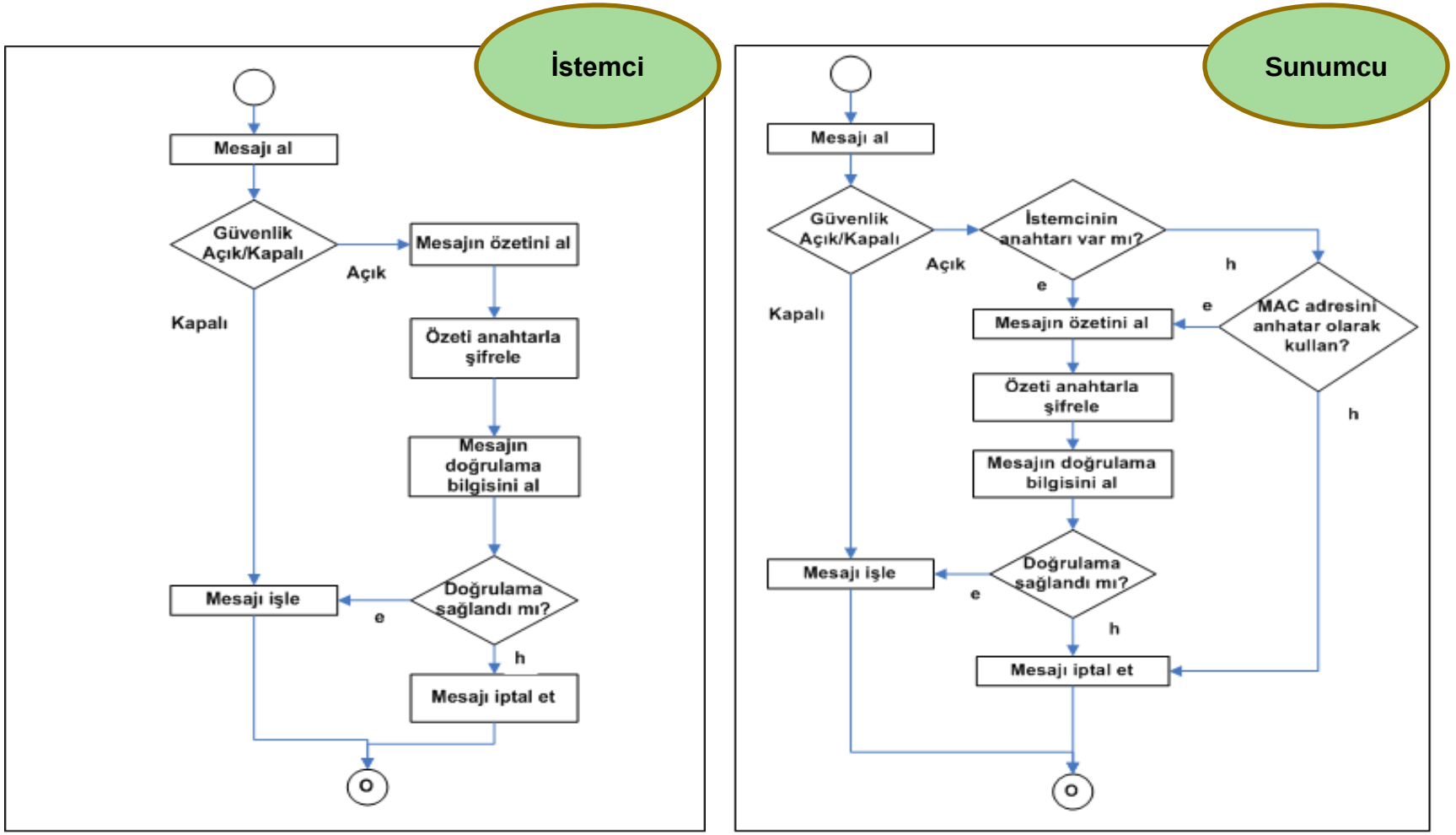
# Saldırgan DHCPv6 İstemcisi

- DHCPv6 sisteminin güvenlik testlerinde kullanılmak üzere tasarlanan ve gerçeklenen bir uygulamadır.
- Ağda hizmet veren DHCPv6 sunumcularını tespit ederek seçilen sunumcu üzerinde IP adreslerinin tüketimi ve sunumcunun diğer istemcilere geç yanıt vermesi için meşguliyet saldırıları yapar.

# Güvenlik Mekanizmasının Tasarımı

- DHCP Sistemleri için önerilmiş güvenlik yöntemleri:
  - Anahtar doğrulama
  - Sonradan doğrulama
  - Kerberos-V  ile doğrulama
  - Sertifika bazlı doğrulama
  - Kullanıcı doğrulama
- Neden "sonradan doğrulama" tercih edildi?
  - İstemci ve sunumcuların birbirlerini doğrulamalarını sağlaması
  - DHCP mesaj içeriğinin doğrulanmasını sağlaması
  - Harici bir sisteme ihtiyaç duyulmaması
  - Yerel alan ağlarında kullanımının kolay olması
- Uygulanabilirliğini artırmak için "varsayılan anahtar" yaklaşımı tasarlandı ve gerçeklendi.
- Mesaj tekrarlama saldırılarına karşın önlemler alındı.

# Güvenlik Mekanizmasının İşleyişi



# Geliştirme Ortamı ve Süreci

- Tasarlanan DHCPv6 sistemi;
  - Nesneye yönelik programlama yöntem bilimine göre,
  - C# programlama dilinde,
  - .NET Framework 1.1 altyapısı kullanılarak,
  - Visual Studio 2003 geliştirme ortamında gerçeklenmiştir.

# Uyum Testleri

- Gerçeklenen DHCPv6 sisteminin uyum testleri, New Hampshire Üniversitesi bünyesinde oluşturulan IPv6 Konsorsiyumunun hazırlamış olduğu test adımlarına göre yapılmıştır.
- Uyumluluk testleri esnasında, istemci ve sunumcu tarafından yayımlanan DHCPv6 mesajları açık kaynak kodlu Ethereal programı kullanılarak çözümlenmiştir.
- Yayınlanan bütün mesajlar Ethereal programı tarafından düzenli bir şekilde ayrıştırılabilmiş ve RFC uyumlulukları kontrol edilmiştir.

DHCPV6 UYUM TEST SONUÇLARI

| İster | Sonuç |
|---|---|
| İstemci, mesajlarını tanımlı sabit IPv6 adreslerine gönderir. | Başarılı |
| İstemci, 546 numaralı portu dinler ve gelen mesajları okur. | Başarılı |
| Sunumcu, 547 numaralı portu dinler ve gelen mesajları okur. | Başarılı |
| İstemci, istemci kaynaklı mesajları ( Solicit, Request, Confirm, Renew, Rebind, Decline, Release, Information-Request, Relay-forward ve Relay-reply) işleme almaz. | Başarılı |
| Sunumcu, sunumcu kaynaklı mesajları (Advertise, Reply ve Reconfigure)işleme almaz. | Başarılı |
| İstemci, geçersiz Advertise mesjlarını işleme almaz. | Başarılı |
| İstemci, geçersiz Reply mesajlarını işleme almaz. | Başarılı |
| İstemci, geçersiz Reconfigure mesajlarını işleme almaz. | Başarılı |
| İstemci, Solicit mesajlaşmasını düzenli olarak yapar. | Başarılı |
| İstemci, Request mesajını düzenli olarak gönderir. | Başarılı |
| İstemci, Confirm mesajını düzenli olarak gönderir. | Başarılı |
| İstemci, Renew mesajını düzenli olarak gönderir. | Başarılı |
| İstemci, Information-Request mesajını düzenli olarak gönderir. | Başarılı |
| İstemci, Release mesajını düzenli olarak gönderir ve IP adresini konaktan siler. | Başarılı |
| İstemci, kullanımda olan IPv6 adresi tahsisinde Decline mesajını düzenli olarak gönderir. | Başarılı |
| İstemci, Advertise mesajını kabul eder ve işler. | Başarılı |
| İstemci, Reply mesajını kabul eder ve işler. | Başarılı |
| İstemci, Reconfigure mesajını kabul eder ve işler. | Başarılı |

# Güvenlik Testleri

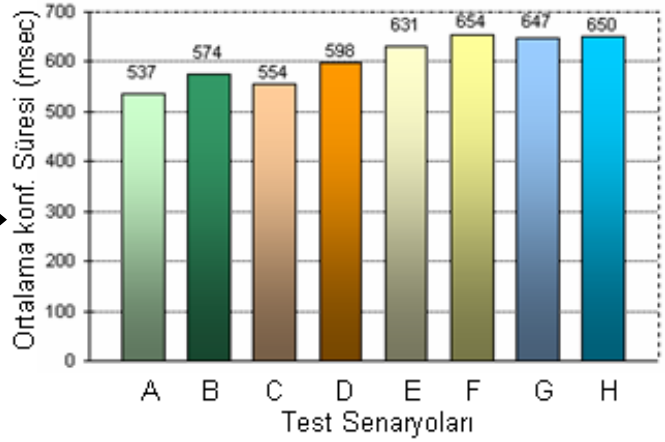
| Saldırı Yöntemi | Güvenlik Kipi Kapalı | | Güvenlik Kipi Açık | |
|---|---|---|---|---|
| | İstemci | Sunumcu | İstemci | Sunumcu |
| Değiştirilmiş mesaj içeriği |  |  |  |  |
| Yetkisiz taraf |  |  |  |  |
| Mesaj tekrarlama |  |  |  |  |

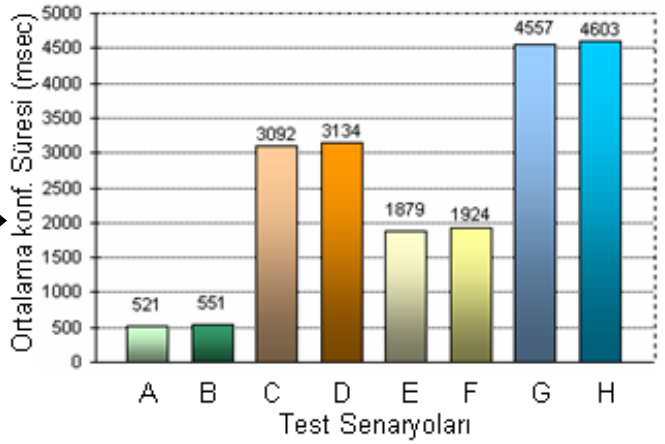
# Performans Testleri

| TESTLER | Fonksiyonel seçenekler | | |
|---|---|---|---|
| | IPv6 adresi al | DNS bilgisini al | Güvenli mesajlaş |
| A | ✗ | ✗ | ✗ |
| B | ✗ | ✗ | ✓ |
| C | ✗ | ✓ | ✗ |
| D | ✗ | ✓ | ✓ |
| E | ✓ | ✗ | ✗ |
| F | ✓ | ✗ | ✓ |
| G | ✓ | ✓ | ✗ |
| H | ✓ | ✓ | ✓ |

**Sadece mesajlaşma**

**Mesajlaşma ve yapılandırma**




Gerçeklenen
"güvenlik mekanizması"nın
sisteme getirdiği yük
göz ardı edilebilir.

# Diğer DHCPv6 Sistemlerle Mukayese

| Sistem özelliği | WIDE-DHCPv6 Sistemi | Dibbler-DHCPv6 Sistemi | Güvenli DHCPv6 Sistemi |
|---|---|---|---|
| RFC Uyumluluk | RFC3315<br>RFC3319<br>RFC3633<br>RFC3646 | RFC3315<br>RFC3898<br>RFC3646 | RFC3315<br>RFC3118<br>RFC3646 |
| DHCP Uçları | İstemci<br>Sunumcu<br>Ajan | İstemci<br>Sunumcu<br>Ajan | İstemci<br>Sunumcu |
| İşletim Sistemi | Linux<br>BSD | Linux<br>Windows XP<br>Windows 2003 | Windows XP<br>Windows2003<br>Windows 7 |
| Güvenlik |  |  |  |
| Arayüz |  |  |  |

# Sonuç

- Bu çalışmada, DHCP protokolünün IPv6 ağlarda daha güvenli bir şekilde nasıl kullanılabileceği uygulamalı olarak gösterilmiştir.
- DHCP protokolü ve gerçeklemeleri barındırdığı güvenlik açıklıklarına rağmen, IPv4 ağlarda kullanıldığı kadar IPv6 ağlarda da kendine olan ihtiyacı hissettirecek ve kullanılmazsa olmaz hizmetlerden biri olmaya devam edecektir. Kablosuz ağların yaygınlaşması, IPv6'nın getirileri göz önüne alındığında bu hizmetin güvenli bir şekilde sunulması önem arz etmektedir.
- Gerçeklenen bu sistemde, protokol seviyesinde sistem güvenliğinin sağlanabilirliliği gösterilmiştir. IPv6 ya özgün ek güvenlik önlemlerinin uygulama seviyesinde de artırılması, sunumcu performansının iyileştirilmesi ve IPv6 adres kaynaklarının yönetimine ilişkin çalışmaların yapılması planlanmaktadır.

# Teşekkürler…

# Kaynaklar


1. R. Droms, "Dynamic Host Configuration Protocol", RFC 1541, IETF, October 1993, http://www.ietf.org/rfc/rfc1541.txt
2. R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, IETF, March 1997, http://www.ietf.org/rfc/rfc2131.txt
3. S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification" RFC 1883, December 1995, http://www.ietf.org/rfc/rfc1883.txt
4. S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration" RFC 2462, December 1998, http://www.ietf.org/rfc/rfc2462.txt
5. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6" RFC 3315, July 2003, http://www.ietf.org/rfc/rfc3315.txt
6. C. E. Perkins, J. Bound, "DHCP for IPv6", Computers and Communications, 1998. ISCC '98. Proceedings. Third IEEE Symposium, Page(s): 493-497, July 1998
7. KAME Project, http://wide-dhcpv6.sourceforce.net
8. T. Mrugalski, "Dibbler – a portable Dynamic Host Configuration Protocol for IPv6 implementation", The 8th International Conference on Telecommunications, Contel'2005, June 2005
9. R. Droms, W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, IETF, June 2001, http://www.ietf.org/rfc/rfc3118.txt
10. R. Droms, Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, IETF, December 2003, http://www.ietf.org/rfc/rfc3646.txt
11. R. Hibbs, C. Smith, B. Volz, M. Zohar, "Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Threat Analysis", Internet-Draft, IETF, June 2003
12. O. Annala, "The Hot Topics in DHCP Protocol Development", May 2004, https://www.cs.helsinki.fi/u/kraatika/courses/IPsem04s/DHCP_HotTopics.pdf
13. K. Hornstein, T. Lemon, B. Aboba, J. Trostle "DHCP Authentication via Kerberos V.", Internet Draft (c) The Internet Society, November 2000.
14. G. Glazer, C. Hussey, R. Shea "Certificate-Based Authentication for DHCP", March 2003, http://www.cs.ucla.edu/chussey/proj/dhcpcert/cbda.pdf
15. T. Komori, T. Saito, "The Secure DHCP System with User Authentication", Local Computer Networks, 2002. Proceedings. LCN 2002. 27th Annual IEEE Conference. Page(s): 123 -131, ISBN 0-7695-1591-6, November 2002
16. IPv6 Consortium, Interoperability Laboratory, Research Computing Center, University of New Hampshire, http://www.iol.unh.edu/testsuites/IPv6
17. Ethereal : A Network Protocol Analyzer, http://www.ethereal.com
18. Ş. Sağıroğlu, O. Bektaş, M. Soysal, "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması", 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Aralık 2008, Ankara, Sayfa 132-138
19. M. Khadilkar, N. Feamster, R. Clark, M. Sanders , "Usage-Based DHCP Lease Time Optimization", Proc. ACM/USENIX Internet Measurement Conference, San Diego, CA, October 2007
20. T.V. Do, "An efficient solution to a retrial queue for the performability evaluation of DHCP", Computers and Operations Research archive Volume 37 , Issue 7 (July 2010), Pages: 1191-1198