IPv6 Balküpü Tasarımı

Yavuz Gökırmak[1] Emre Yüce[2] Onur Bektaş[3] Murat Soysal[4] Serkan Orcan[5]

[1,2,3,4,5] TÜBİTAK ULAKBİM, Ankara

[1]e-posta: yavuzg@ulakbim.gov.tr [2] e-posta: emre@ulakbim.gov.tr [3] e-posta: onur@ulakbim.gov.tr
[4] e-posta: msoysal@ulakbim.gov.tr [5] e-posta: serkan@ulakbim.gov.tr

Özetçe

Gelecekte IPv6[1] protokolünün, kişisel eğlence uygulamalarından e-ticaret uygulamalarına kadar farklı uygulamalarda alt yapıyı oluşturması beklenmektedir. Geniş bir kullanım alanına ve dolayısıyla kullanıcıya ulaşacak protokolün, bilgi güvenliği penceresinden incelenmesi önem taşımaktadır. IPv6, dolaşılabilirlik, çoklu gönderim, servis kalitesi, IP seviyesinde şifreleme ve kimlik doğrulama benzeri özellikleri tasarımında barındırmaktadır. IPv6 protokolü, geniş adres aralığı sayesinde adres taramalarına ve otomatik yayılan solucanlara karşı direnç gibi çeşitli özellikler içermektedir. IPSec [2] desteğinin zorunlu hale getirilmesi de IPv6'nın, IPv4'e [3] oranla daha güvenli olarak görülmesine sebep olmuştur. Ancak yeni protokolün uygulaması aşamasında doğacak güvenlik sorunları ve saldırganların yaklaşımları, protokol henüz yaygın olarak kullanılmadığı için, tam olarak bilinememektedir.

Saldırgan davranışları hakkında bilgi sahibi olma ve saldırılar hakkında inceleme yapma imkânı sağlayan Balküpleri, IPv6 protokolündeki güvenlik sorunlarını saptamada kullanılabilirler. Bu makalede, IPv6 protokolü üzerine inşa edilmiş ağlardaki tehditleri saptamada kullanılabilecek bir IPv6 balküpü tasarımı önerilmektedir.

1. Giriş

Balküpleri, gücünü saldırılabilirliğinden alan güvenlik sistemleri olarak tanımlanabilirler[4]. İnternetten erişilebilecek bir ağda konumlandırılan balküpleri, saldırganları kendilerine çekerek saldırgan ve saldırı davranışları hakkında inceleme yapılması olanağını sağlamaktadırlar.

Saldırı tespit sistemleri ya da Ateş Duvarı gibi güvenlik mekanizmalarından farklı olarak Balküpleri, özel bir problemin çözümünde kullanılmazlar. Balküpleri, güvenlik sisteminin sadece bir parçasıdırlar ve hangi problemlerin çözümüne yardımcı oldukları tasarımları/kullanım şekilleriyle doğrudan bağlantılıdır [5]. Bu yüzden her sorunun çözümüne katkı sağlayacak genel geçer bir balküpü tasarımı düşünülemez.

IPv6 balküpü tasarım sürecinde öncelikle genel balküpü tasarımı tercihleri incelecektir. Sonrasında IPv4 ve IPv6 protokollerinin balküpü tasarımında etkili olacak yanları üzerinde durularak IPv6 balküpü tasarımında dikkat edilmesi gereken noktalara değinilecektir.

2. İlgili Çalışmalar

Literatürde, balküpü tasarımıyla ilgili yapılan çalışmalar [6,7] incelendiğinde göz önüne alınması gereken temel noktalar ortaya çıkmaktadır. Çalışmalardan elde edilen temel noktalar aşağıdaki beş başlık altında toplanabilmektedir:

- Balküpünün saldırgana sunacağı bilginin içeriği, değeri ve seviyesi
- Balküpünün ele geçirilmesi durumunda, saldırganın erişebileceği kaynaklar
- Balküpünün ağda hizmet vereceği konum
- Balküpü verisinin balküplerinden toparlanması
- Balküpünün saldırganlar tarafından tespit edilmesi

Balküpünün saldırgana sunacağı bilgiler ve imkânlar, onun etkileşim seviyesiyle bağlantılıdır. Düşük ve orta etkileşimli balküpleri [8,9] saldırgandan veri alabilmek için bazı servislere öykünürken, yüksek etkileşimli sistemlerde [10] saldırganın hareketlerini izleyebilmek için Sebek [11] benzeri izleme yazılımları kullanılmaktadır. Veriyi yakalayabilmek için saldırganın balküplerine çekilebilmesi gerekmektedir. Düşük seviyeli bir balküpü kullanılması durumunda yalancı servislerle iletişim sağlanan saldırganın, gerçek işletim sistemine erişimi olmadığı için balküpünün ele geçirilme riskinin çok azaldığını belirtmektedirler [12]. Etkileşim seviyesinin artmasıyla balküpünün ele geçirilmesi riski artmaktadır öte yandan saldırganların gerçek sistemle etkileşime girmeleri sonucu saldırgan ve saldırı hakkında daha fazla bilgi elde edilmektedir.

Saldırgan tarafından ele geçirilme olasılığına karşın, ele geçirilen balküpünden başka sistemlere saldırı yapılmasını engelleyici önlemler almak gerekmektedir. Honeynet projesinde [13], saldırganın, balküpü dışına olan aktivitelerini kısıtlayabilmek için ateş duvarları kullanılmıştır [14]. Ateş duvarlarının trafiği kesme özelliklerinden faydalanarak, balküpünden dışarıya yönelen belirli bir seviyenin üstündeki trafik engellenmektedir.

Balküplerinin konumlandırılmalarıyla ilgili üç tercih belirtilmektedir[12]. Balküpünü ateş duvarının önüne koymak, arkasına koymak ya da DMZ'ye (Demilitarized Zone - Korunmasız Bölge) koymak önerilen 3 yöntemdir.

Balküpü tasarımında dikkate edilmesi gereken bir nokta da balküpünün saldırganlar tarafından algılanmamasını sağlamaktır. Saldırgan, etkileşimde olduğu sistemi bir balküpü olarak değil gerçek bir servis olarak algılamalıdır.

Sanallaştırma platformları üstünde çalışan bir balküpünü ele geçiren saldırgan işlemci/bellek kullanımı değerlerinden yola çıkarak ele geçirdiği bilgisayarın bir sanal bilgisayar olduğunu anlayabilmektedir [15]. Sanal bilgisayarların balküpü mimarisinde kullanılmasıyla ilgili Kasım 2008'de Honeypots haber grubunda yapılan bir tartışmada [16] sanal bilgisayarların gün geçtikçe yaygınlaşmasına paralel olarak ele geçirilen bir sanal bilgisayarın balküpü olması yönünde verilecek bir kararın zorlaşması yönünde bir yorumda bulunulmuştur. Sanallaştırma çözümlerinin kullanımı hakkında tartışmalar olmasına karşın genel geçer bir çözüme henüz ulaşılamamıştır.

Balküplerinin saptanması konusunda yapılan başka bir çalışmada [17] sanallaştırma çözümlerinin saptanmasına ek olarak iki yöntemden bahsedilmektedir. İlk yöntemde, yüksek etkileşimli balküplerinde kullanılan ve saldırganın hareketlerini izlemeye yarayan Sebek yazılımının nasıl saptanacağı üzerinde durulmuştur. İkinci yöntemde ise düşük etkileşimli balküpü Honeyd'nin öykündüğü servisler üzerinden bir saptama yapılmıştır. Honeyd, servisleri kısıtlı olarak öykündüğü için, saldırganın bu servisleri saptama imkânı bulunmaktadır. Çalışmada Honeyd'nin hatalı öykündüğü bir servisten hareketle balküpü saptamasında bulunmuştur. Bu çalışma, benzeri saptamaların yapılabileceğine bir örnek teşkil etmektedir.

Ele geçirilen bir bilgisayarın balküpü olup olmadığını anlamak için kullanılan bir yöntemde ise [18], ele geçirilen bilgisayardan, bilinen bir kurbana yeni bir saldırı düzenlemesi tasarlanmıştır. Bu yöntemde, balküplerinin ele geçirilmeleri durumunda yeni saldırılara izin vermemeleri özelliklerinden faydalanılmaktadır. Eğer bilinen kurbana yapılan saldırı bir şekilde ele geçirilen bilgisayar tarafından engellenirse, bu bilgisayarın balküpü olduğu kararı verilmektedir.

3. IPv6 Balküpü Tasarımı

IPv4 ağlarından kullanılmakta olan balküplerinden; solucan dağılımı analizi, ilk-gün saldırılarının tespiti ve servis açıklarının saptanması konularından faydalanılmaktadır. IPv4 balküplerinden elde edilen faydalı verilere rağmen, IPv6 ağlarından çalışabilecek bir balküpü henüz üretilmemiştir. Tasarlanacak IPv6 balküpünün, yeni protokolün güvenlik sorunlarını saptamada faydalı olacağını öngörmekteyiz.

IPv6 Balküpü: Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi kapsamında yapılacak olan çalışmalar doğrulusunda, IPv6 üzerinden yapılabilecek saldırıların incelenebilmesi için geliştirilecektir.

IPv6 Balküpü ağı bileşenlerinin belirlenebilmesi için öncelikle IPv4 balküpleri incelenmiştir. ULAKNET ağında Mart 2007 tarihinden itibaren düşük iletişimli balküpü servisi verilmektedir. ULAKNET ağında kullanılan balküpünün, üzerine çektiği saldırgan profillerinden hareketle, IPv6 balküpünün öykünmesi gereken servislere karar verilmiştir. Balküpü verilerinin analiz edilmesi amacıyla geliştirilen sistem incelenerek, IPv6 verisinin analizi aşamasında hayata geçirilecek olan sistemin gereksinimleri belirlenmiştir.

Literatürde yapılan mevcut çalışmalar ve ULAKNET bünyesindeki balküpü deneyimleri ışığında, balküpünün; Saldırı Çekme, Veri toplama ve Veri analizi bileşenlerinden oluşturulması kararı verilmiştir.

3.1. Saldırı Çekme

Balküpünü saldırganlar için çekici hale getirecek bu bileşen, IPv6'da kullanılması öngörülen saldırı yöntemlerini balküpüne çekecek mekanizmaları içermektedir.

Saldırganlar, saldıracakları bilgisayarları belirlemek için saldırı öncesi keşif yaparlar. Keşif sonucu saldırılabilecek potansiyel bilgisayarlar, bunların kullandıkları işletim sistemleri, portlarında çalışan servisler ve sürümleri gibi birçok bilgi elde edilebilmektedir. IPv4 ağlarında bu bilgileri elde edebilmek nmap [19] gibi tarama araçları kullanılmaktadır. IPv4'te bir adres aralığını sıralı olarak tarama mantığı üzerine inşa edilen tarama araçları IPv6 ağlarının geniş adres aralığından dolayı kullanışlı olmayacaktır. Saldırı çekme bileşeni, IPv6 ağlarının bu özelliğini göz önüne alarak, kullanılacak yeni tarama yöntemlerinin balküpünü kolaylıkla bulabileceği mekanizmaları içerecektir. Saldırganları balküplerine kolayca çekebilmek için aşağıdaki yöntemler kullanılabilir:

- Bilgisayarların IPv6 adreslerinin [önek]::1'den başlayarak sıralı olarak atanması,
- Yaygın kullanılan ethernet kartı üreticilerinin kartlarına öykünme, (yaygın sağlayıcı öneklerini deneyen saldırganlara kolaylık sağlanacaktır)
- Balküpü ağının ikili yığında çalıştırılıp, IPv6 adreslerinin IPv4 adreslerinden üretilmesi,
- Balküpü ağındaki bir DNS'in dışarıdan yapılacak AXFR sorgularına açık olması,
- Balküpü ağında iki DNS'in şifresiz Zone transferi yapması

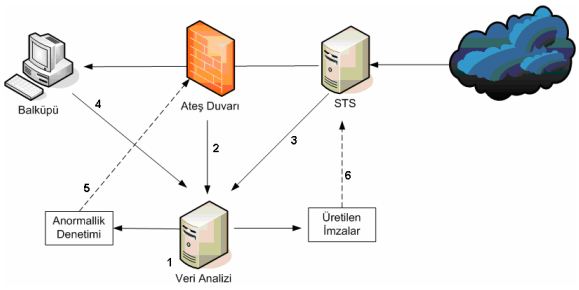
3.2. Veri Toplama

Saldırgan balküpüne çekildikten sonra saldırı ve saldırganla ilgili farklı kanallardan veri toplamayı sağlayacak olan bileşendir. Bu bileşende öykünülen servisler, sistem günlükleri, ateş duvarı günlükleri, Saldırı Tespit Sistemleri (STS) uyarıları ve izleme araçlarıyla bilgi toplanacaktır. Balküpü yazılımı SMTP, HTTP, DNS ve FTP servislerine öykünerek saldırganın gerçek bir sisteme saldırdığını düşünmesini sağlayacaktır. Bu servislerin öykünülmesiyle, saldırı yakalama olanağı arttırılmaktadır. Bu servislerin gerçekten çalıştırılması yerine öykünmelerin kullanılması sayesinde gerçek servis için geliştirilen saldırıların öykünmede başarılı olmaması sağlanabilmektedir. Ayrıca, öykünme servisler sayesinde, saldırı sırasında istenen seviyeden bilgi alınarak imza üretilmesi ya da uyarı sistemlerinin çalıştırılması sağlanabilmektedir.

3.3. Veri Analizi

Toplanan verinin verimli bir şekilde analizini gerçekleştirecek olan bileşendir. Büyük veriler üzerinden analiz yapacak olan bileşenin sistem kaynaklarını tüketmeden ve yapılacak analizin değerinin kaybolmayacağı bir sürede çıktılar üretmesi gerekmektedir.

Veri analizi aşamasında karşılaşılacak zorlukları önceden belirleyebilmek ve olası çözümleri üretebilmek için ULAKBİM bünyesinde kullanılan IPv4 balküpünün veri analizi sistemi yeniden tasarlanmıştır. IPv4 balküpü veri analizi sürecinde edinilen tecrübeler ışığında IPv6 balküpünde tasarlanacak bileşende benzer bir yöntem izlenecektir.



Şekil 1: Balküpü veri analizi

Şekil 1'de yapısı özetlenen veri analizi, balküpünden başka merkezi bir bilgisayarda yapılacaktır (1). Merkezi bir analiz bilgisayarı kullanılmasının iki nedeni bulunmaktadır. Birinci neden, balküplerinin birden fazla noktaya yerleştirilme ihtimalidir. Birden fazla balküpü algılayıcısı kullanıldığı takdirde bunlardan gelen verilerin ortak bir analize tabi tutulmaları önem taşımaktadır. İkinci neden ise, balküpü bilgisayarına işlem yoğunluğu yüklememektir. Veri analizinde kullanılan yöntemler sistem kaynaklarını yoğun olarak ihtiyaç duyduklarından balküpünün çalışmasına olumsuz şekilde etkileyebilirler. Analizin merkezi bir sistemde yapılması, balküpünün çalışmasını aksatmayacaktır.

Balküpü, Ateş duvarı (2) ve STS'den (3) gelen veriler analiz bilgisayarında bir veri tabanında saklanmalıdır. IPv4 balküpü veri analiz sistemi yenilenmeden önce kullanılan sistem, günlüklerin dosyalara yazılıp okunması temelinde çalışmaktaydı. Yapılan çalışmalar sonunda veri tabanına -ön inceleme yapılarak- atılan bilgiler üzerinden karmaşık sorguların kısa sürelerde yapıldığı görülmüştür. Dosya yazma/okuma işlemlerinin uzun süre alması, kaynakları yoğun olarak kullanılmaları ve karmaşık sorguların yapılmasının zorluğu/verimsizliği bu yöntemin tercih edilmemesinde rol oynayan en önemli faktörlerdir. Veritabanı olarak MySQL [ref] kullanılacaktır.

Verinin balküpü, ateş duvarı ve STS'den analiz bilgisayarına gönderiminde dikkat edilmesi gereken iki nokta bulunmaktadır. Birincisi, analiz bilgisayarına giden trafiğin koklanması olasılığına karşın trafiğin güvenli bir tünel üzerinden gönderilmesidir. İkincisi ise, balküpüne giren bir saldırganın trafiği görerek şüphelenmemesi için, balküpünden çıkan trafiğin (4) saklanmasıdır.

Veri analizi iki başlık altında toplanılabilir: trafik akışı analizi ve paket yapısı analizi. Trafik akışı analizi, trafikteki paketlerin içeriğiyle ilgilenmeden sadece paket başlıklarından çekilen veri üzerinden yapılır. Trafik akışı analizi sayesinde elde edilebilen, en çok saldırı yapan/yapılan adresler/portlar gibi bilgiler bize saldırgan davranışları hakkında bilgi verebilir. Trafik analizi, servis engelleme saldırılarının saptanması aşamasında da kullanılmaktadırlar. IPv6 balküpünün servis engelleme saldırısına maruz kalmaması için, trafikte bir anormallik saptandığında ateş duvarına gereken kurallar eklenerek savunma yapılacaktır(5). Paket yapısından hareketle yapılan analizde, balküpüne giren/çıkan trafik yapısal olarak incelenecektir ve saldırı imzaları çıkartılacaktır. Üretilen imzalar STS'ye gönderilerek (6) ilk-gün saldırılarına önlem alınması hedeflenmektedir.

4. Sonuçlar

IPv6 ağları henüz yaygın olarak kullanılmamaktadır. Protokol, son kullanıcı tarafından kullanılmadığı için ortaya çıkabilecek güvenlik açıkları ve saldırganların bu açıkları nasıl kullanacakları henüz kesin olarak tahmin edilememektedir. IPv6 ağlarının güvenliğini analiz etmek ve yeni saldırı türlerini inceleyebilmek amacıyla, "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında ve makalede önerilen tasarımın ışığında bir IPv6 balküpü yazılımı geliştirilecektir.

Geliştirilen yazılım sayesinde, yeni nesil saldırılar hakkında bilgi sahibi olunarak, saldırıların yıkıcı etkisinin ortadan kaldırılması hedeflenmektedir.

5. Teşekkür

Bu çalışma Türkiye çapında IPv6 altyapısı oluşturmak ve Türkiye'nin IPv6 protokolüne geçişini planlamak amacıyla TÜBİTAK – ULAKBİM'in yönetici, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi'nin yürütücü, Bilgi Teknolojileri ve İletişim Kurumu'nun müşteri kurum olarak katıldığı "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi" kapsamında gerçekleştirilmiştir. [20] Bu proje TÜBİTAK tarafından desteklenmektedir.

6. Kaynakça

[1] S. Deering, R. Hinden , "Internet Protocol, Version 6 (IPv6) Specifications", RFC 2460, Aralık 1998
[2] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Kasım 1998
[3] "Internet Protocol", RFC 791, Eylül 1981
[4] R. McGrew, "Experiences With Honeypot Sytems: Development, Deployment, and Analysis"
[5] Lance Spitzner, Honeypots: Tracking Hackers.
[6] Iyatiti Mokube, Michele Adams, "Honeypots: Concepts, Approaches, and Challenges"
[7] Honeynet Definitions, Requirements, and Standards, http://old.honeynet.org/alliance/requirements.html
[8] Nepenthes orta etkileşimli balküpü uygulaması, http://nepenthes.carnivore.it/
[9] Honeyd düşük etkileşimli balküpü uygulaması, http://www.honeyd.org/
[10] Argos yüksek etkileşimli balküpü uygulaması, http://www.few.vu.nl/argos/
[11] Sebek işletim sistemi çekirdeği düzeyinde veri yakalama aracı, https://projects.honeynet.org/sebek/

[12] Reto Baumann, Christian Plattner, “Honeypots”
[13] Balküpü ağı, http://www.honeynet.org/
[14] “Know your enemy: User Mode Linux”
[15] http://www.seifried.org/security/ids/20020107-honeypot-vmware-basics.html
[16] Honeypots haberleşme grubu, http://seclists.org/honeypots/2008/q4/0012.html
[17] Joseph Corey, Phrack Magazine, “Advanced Honeypot Identification and Exploitation”
[18] Honeypot-Aware Advanced Botnet Construction and Maintenance
[19] Nmap ağ tarama aracı, http://nmap.org/
[20] TÜBİTAK - ULAKBİM, Gazi Üniversitesi ve Çanakkale 18 Mart Üniversitesi, Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi, http://www.IPv6.net.tr/