MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(7. Hafta)

İçerik

- 2.Bilgisayar Güvenliği Teknolojisi ve İlkeleri
  - 2.1 Şifreleme Araçları
  - 2.2.Kullanıcı doğrulama
  - 2.3 Giriş/Erişim Kontrolu
  - 2.4 Veritabanı ve Veri Merkezi Güvenliği
  - 2.5 Kötü amaçlı yazılımlar
  - 2.6 Hizmet Reddi Saldırıları
  - 2.7 İzinsiz giriş tespiti
  - 2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.6 Hizmet Reddi Saldırıları

2.6.İçerik

- Hizmet Reddi Saldırıları
- Taşma (Sel) Saldırıları
- Dağıtılmış Hizmet Reddi Saldırıları
- Uygulama Tabanlı Bant Genişliği Saldırıları
- Yansıtıcı ve Amplifikatör Saldırıları
- Hizmet Reddi Saldırılarına Karşı Savunmalar
- Hizmet Reddi Saldırısına Yanıt Verme

Hizmet Reddi (DoS) Saldırı

NIST SP 800-61 Bilgisayar Güvenliği Olayını Yönetme Kılavuzu, DoS saldırısını:

"Merkezi işlem birimleri (CPU), bellek, bant genişliği ve disk alanı gibi kaynakları tüketerek ağların, sistemlerin veya uygulamaların yetkili kullanımını engelleyen veya bozan bir eylemdir"

olarak tanımlar

Hizmet Reddi (DoS)

- Bazı hizmetlerin kullanılabilirliğine yönelik bir saldırı biçimidir
- Saldırıya uğrayabilecek kaynak kategorileri şunlardır:

Ağ band genişliği

Bir sunucuyu İnternete bağlayan ağ bağlantılarının kapasitesiyle ilgilidir.

Çoğu kuruluş için bu, İnternet Servis Sağlayıcılarına (ISP) olan bağlantılarıdır.

Sistem kaynakları

Ağ işleme yazılımını aşırı yüklemeyi veya çökertmeyi amaçlar

Sistemde bulunan sınırlı kaynakları tüketen belirli paket türleri gönderilir

Uygulama kaynakları

Tipik olarak, her biri önemli kaynakları tüketen ve dolayısıyla sunucunun diğer kullanıcılardan gelen isteklere yanıt verme yeteneğini sınırlayan bir dizi geçerli istek içerir

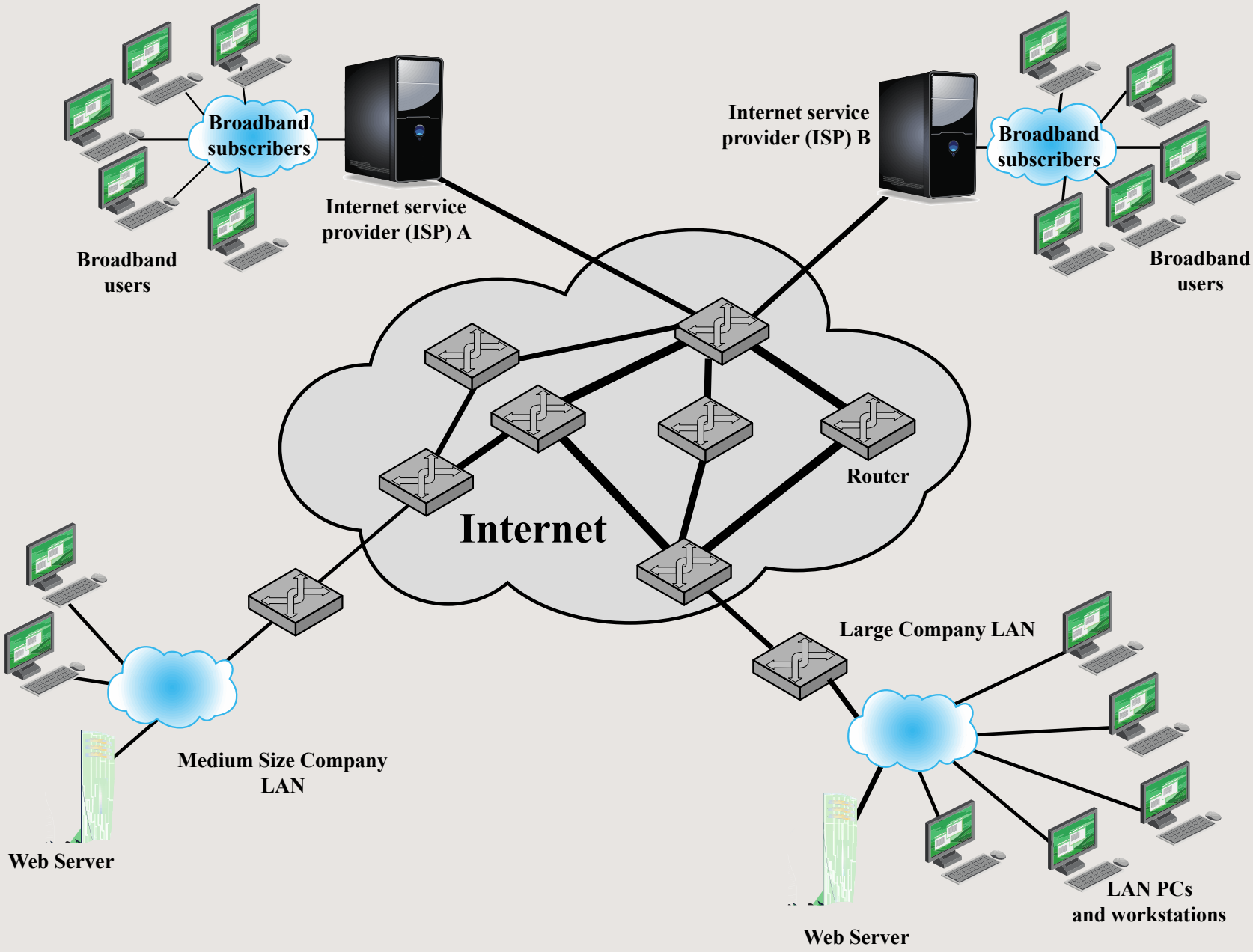


Figure 7.1 Example Network to Illustrate DoS Attacks

Klasik DoS saldırıları

- Taşan ping komutu
  - Bu saldırının amacı, hedef kuruluşun ağ bağlantısının kapasitesini aşmaktır.
  - Trafik, yol üzerindeki daha yüksek kapasiteli bağlantılar tarafından işlenebilir, ancak kapasite düştükçe paketler atılır.
  - Sahte bir adres kullanılmadığı sürece saldırının kaynağı açıkça tanımlanır
  - Ağ performansı belirgin şekilde etkilenir

Kaynak Adresi Sahtekarlığı

- Sahte kaynak adresleri kullanılır
  - Genellikle işletim sistemlerinde ham soket arabirimi aracılığıyla yapılır
  - Saldıran sistemlerin tespit edilmesini zorlaştırır
- Saldırgan, hedef sistemi hedef adres olarak alan büyük hacimli paketler üretir.
- Tıkanıklık, daha düşük kapasiteli bağlantıya sahip son yönlendiricide oluşur.
- Ağ mühendislerinin yönlendiricilerinden akış bilgilerini özel olarak sorgulamasını gerektirir
- *Geri saçılım trafiği*
  - Saldırı trafiğini izlemek için kullanılmayan IP adreslerine giden yolları tanıtır

SYN Sahtekarlığı

- Yaygın DoS saldırısıdır
- Bir sunucunun, onları yönetmek için kullanılan tabloları aşarak gelecekteki bağlantı isteklerine yanıt verme yeteneğine saldırır.
- Böylece meşru kullanıcıların sunucuya erişimi reddedilir.
- Bu nedenle, sistem kaynaklarına, özellikle işletim sistemindeki ağ işleme koduna yönelik bir saldırıdır.

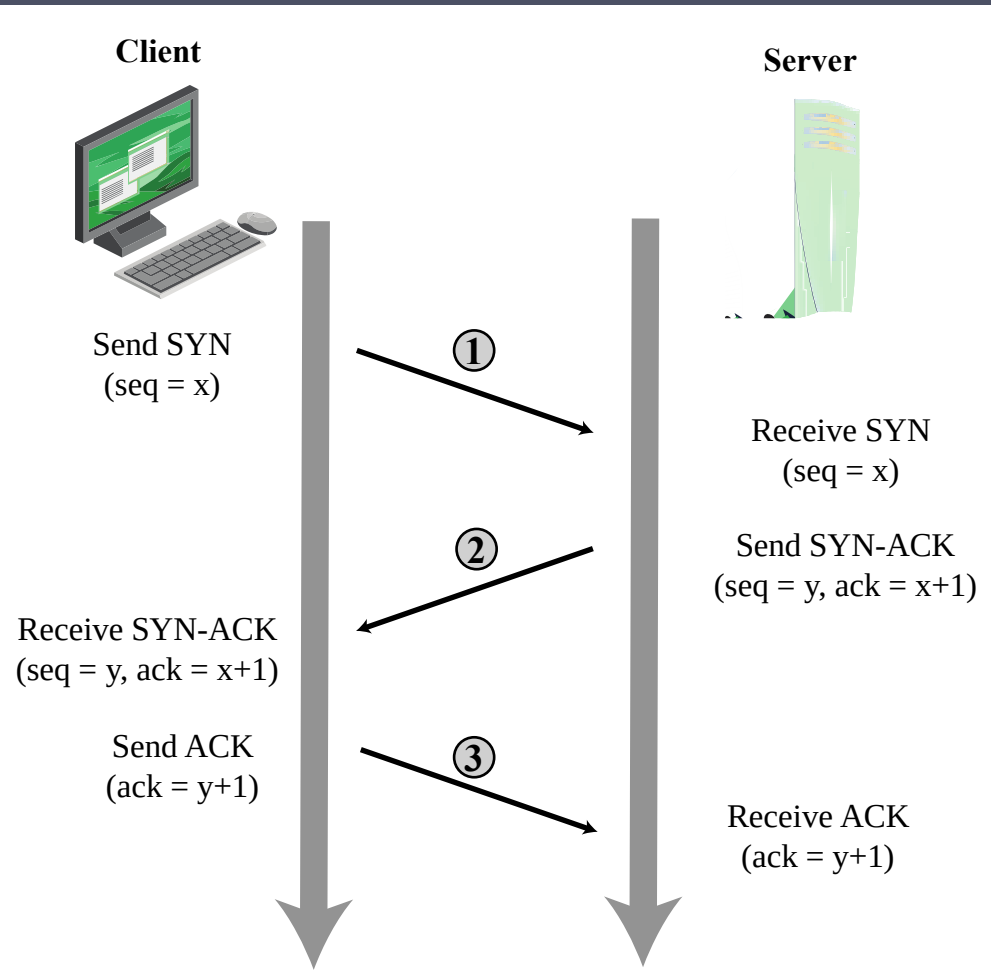


Figure 7.2 TCP Three-Way Connection Handshake

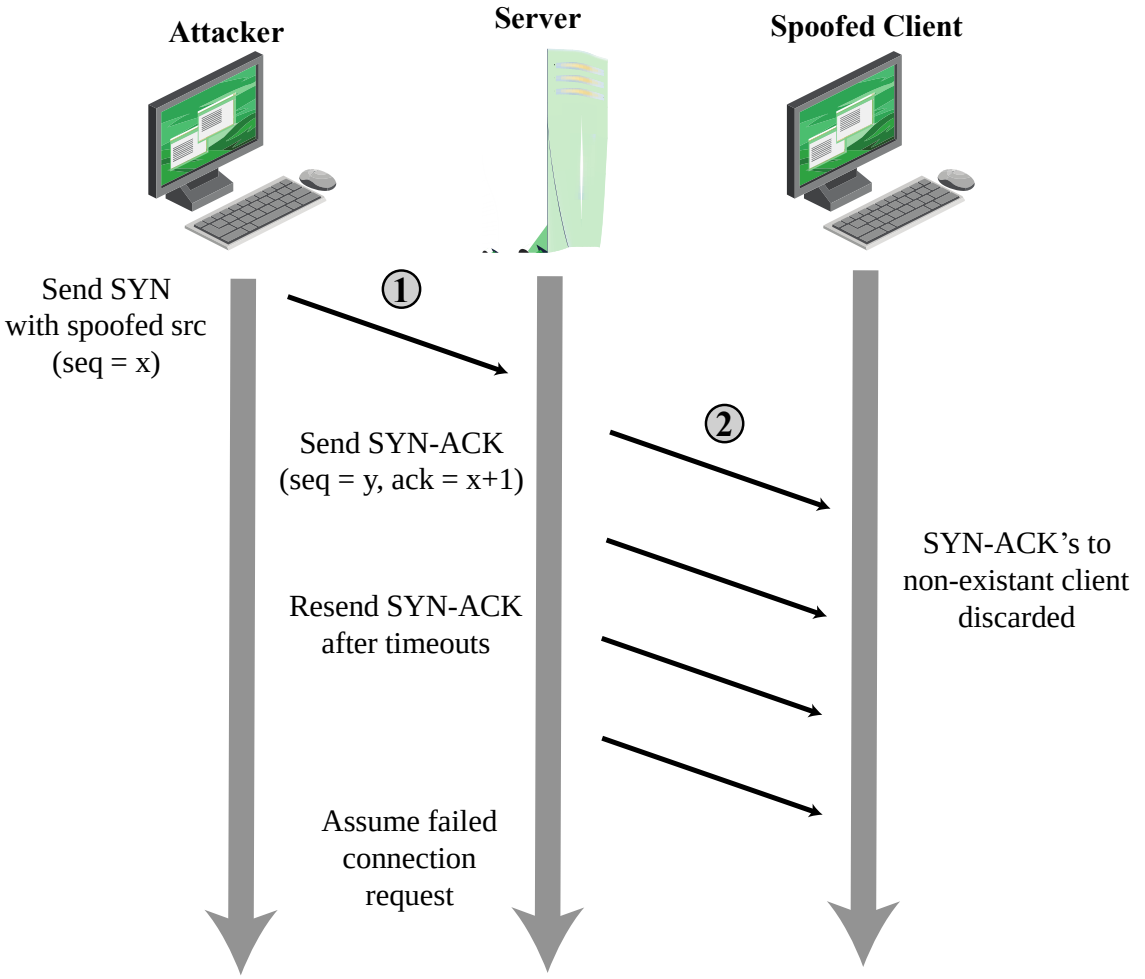


Figure7.3 TCP SYN Spoofing Attack

Taşma (Sel) Saldırıları

- Kullanılan ağ protokolüne göre sınıflandırılmıştır
- Amaç, bir sunucuya giden bağlantılarda ağ kapasitesini aşırı yüklemektir.
- Sunucunun bu trafiği işleme ve yanıt verme becerisini aşırı yüklemeyi hedefleyin.
- Hemen hemen her tür ağ paketi kullanılabilir

ICMP Seli	• ICMP yankı istek paketlerini kullanarak ping seli oluşturur • Geleneksel olarak ağ yöneticileri bu tür paketlerin ağlarına girmesine izin verir çünkü ping kullanışlı bir ağ teşhis aracıdır
UDP Seli	• Hedef sistemdeki bazı port numaralarına yönlendirilmiş UDP paketlerini kullanır
TCP SYN Seli	• Hedef sisteme TCP paketleri gönderir • Saldırının amacı, sistem kodundan ziyade toplam paket hacmidir

Dağıtılmış Hizmet Reddi (DDoS) Saldırıları

Saldırı oluşturmak için birden çok sistem kullanılır

Saldırgan, erişim elde etmek için işletim sistemindeki veya ortak bir uygulamadaki bir kusuru kullanır ve programını buna yükler (zombi)

Bir saldırganın kontrolü altındaki bu tür sistemlerin büyük koleksiyonları oluşturularak bir botnet oluşturulabilir

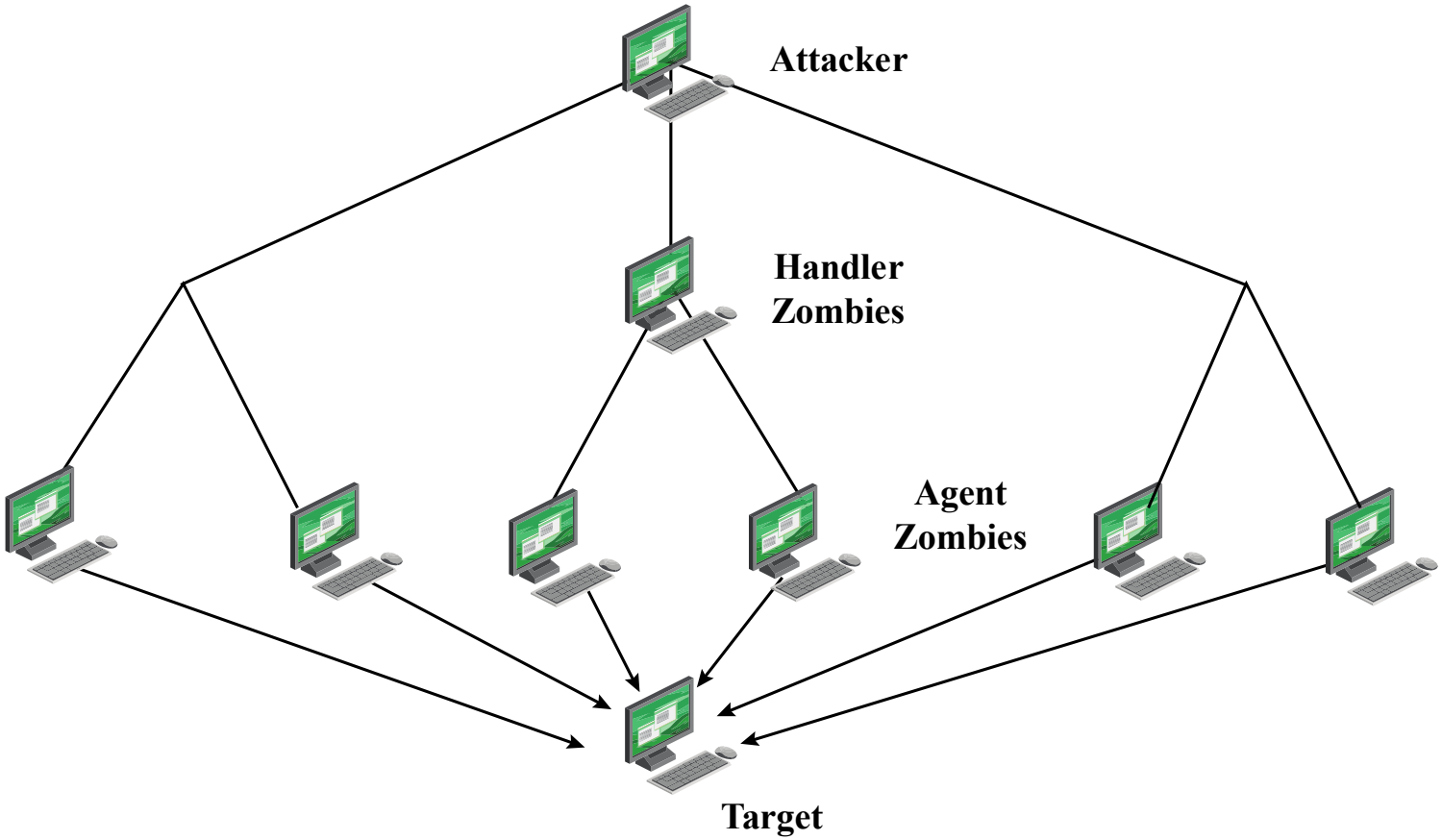


Figure 7.4 DDoS Attack Architecture

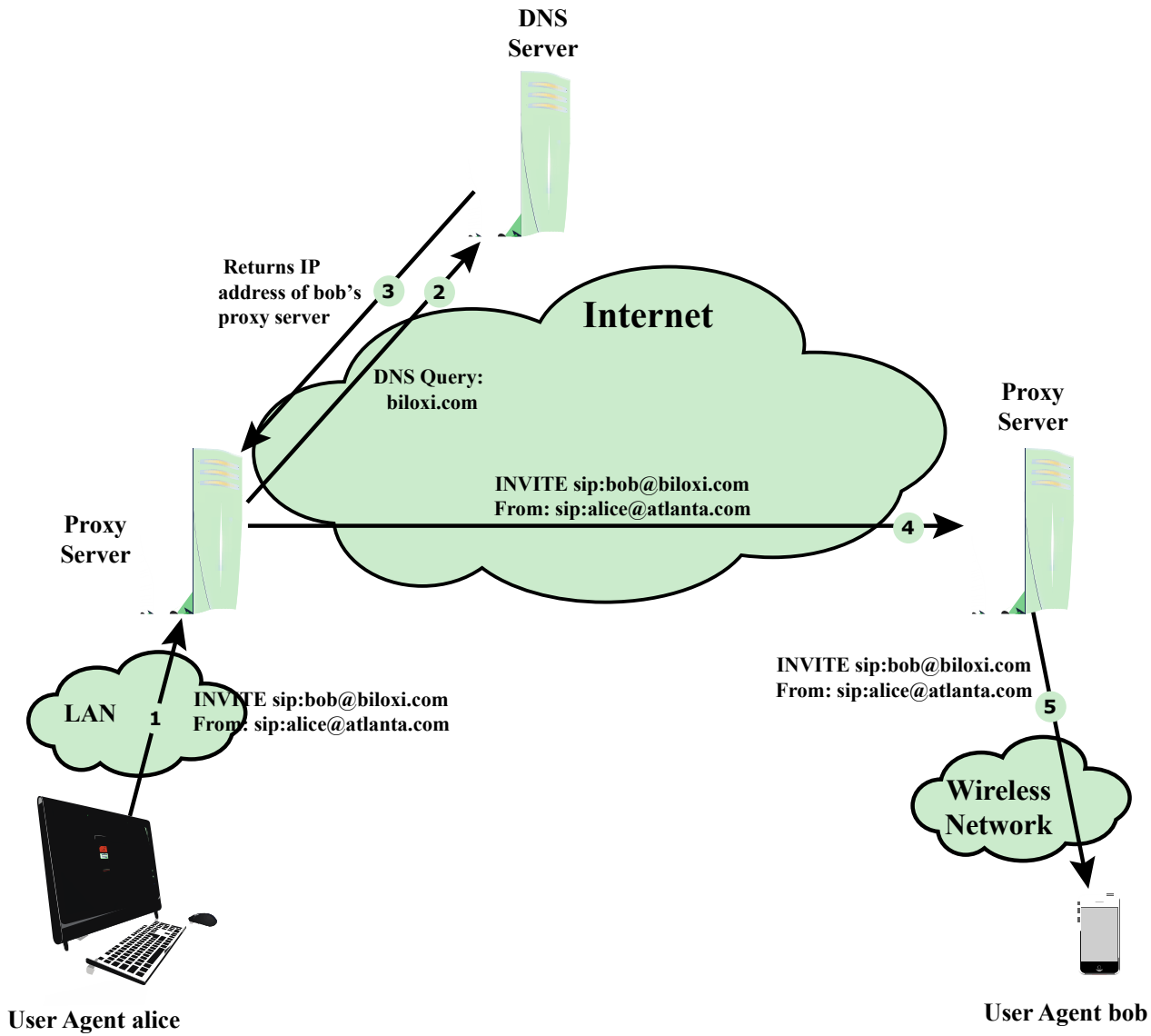


Figure 7.5 SIP INVITE Scenario

Köprü Metni Aktarım Protokolü (HTTP) Tabanlı Saldırılar

HTTP seli

- Web sunucularını HTTP istekleriyle bombalayan saldırıdır
- Önemli miktarda kaynak tüketir
- Örümcek
  - Belirli bir HTTP bağlantısından başlayan ve sağlanan Web sitesindeki tüm bağlantıları yinelemeli bir şekilde izleyen botlar

Slowloris

- Asla tamamlanmayan HTTP istekleri göndererek tekelleştirme girişimleri
- Sonunda Web sunucusunun bağlantı kapasitesini tüketir
- Meşru HTTP trafiğini kullanır
- Saldırıları tespit etmek için imzalara dayanan mevcut saldırı tespit ve önleme çözümleri genellikle Slowloris'i tanımlayamaz.

Yansıma Saldırıları

- Saldırgan, paketleri gerçek hedef sistemin sahte bir kaynak adresiyle aracıdaki bilinen bir hizmete gönderir.
- Aracı cevap verdiğinde, cevap hedefe gönderilir
- Aracının saldırısını "yansıtır" (yansıtıcı)
- Amaç, aracıyı uyarmadan hedef sisteme bağlantıyı akıtmak için yeterli hacimde paket oluşturmaktır.
- Bu saldırılara karşı temel savunma, sahte kaynaklı paketleri engellemektir.

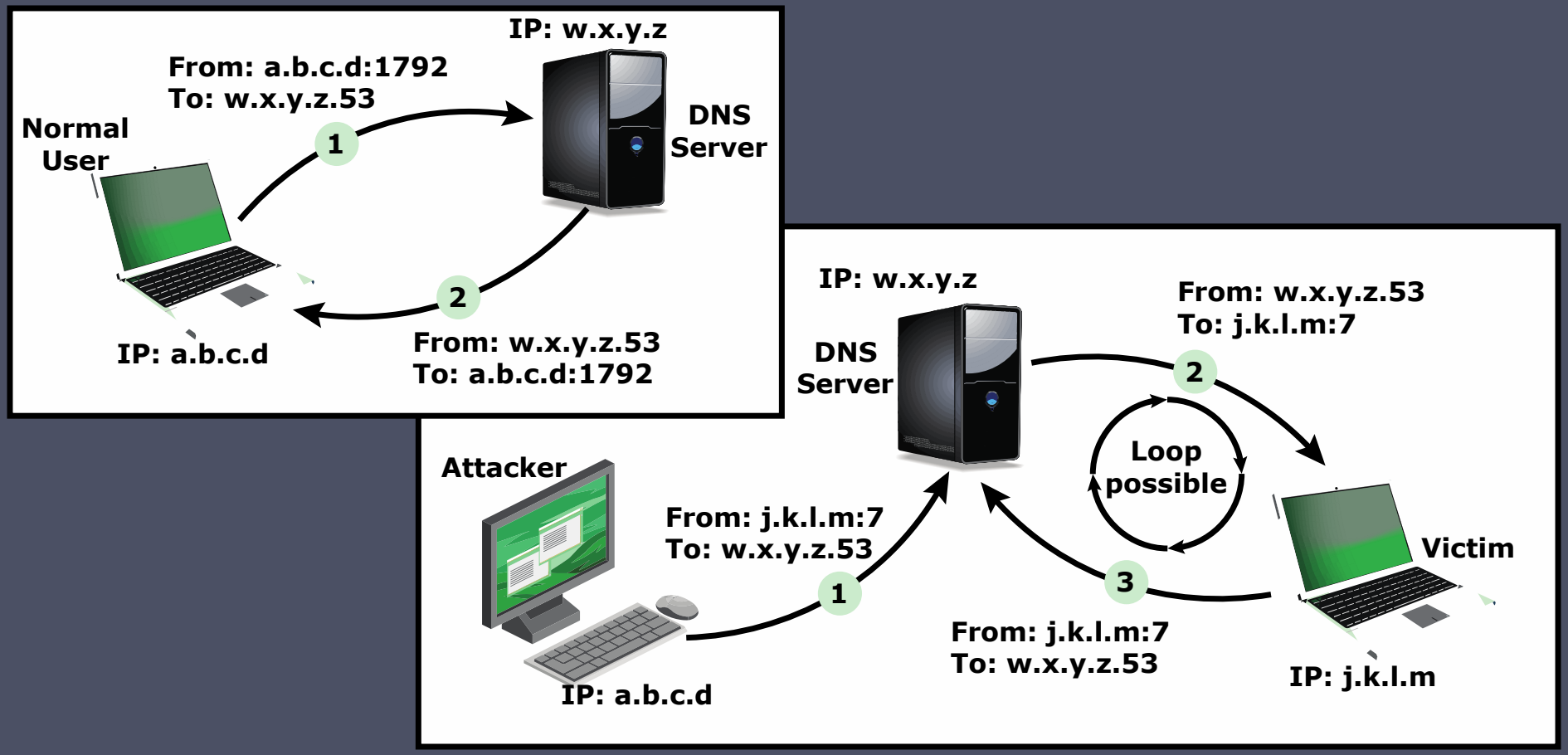


Figure 7.6 DNS Reflection Attack

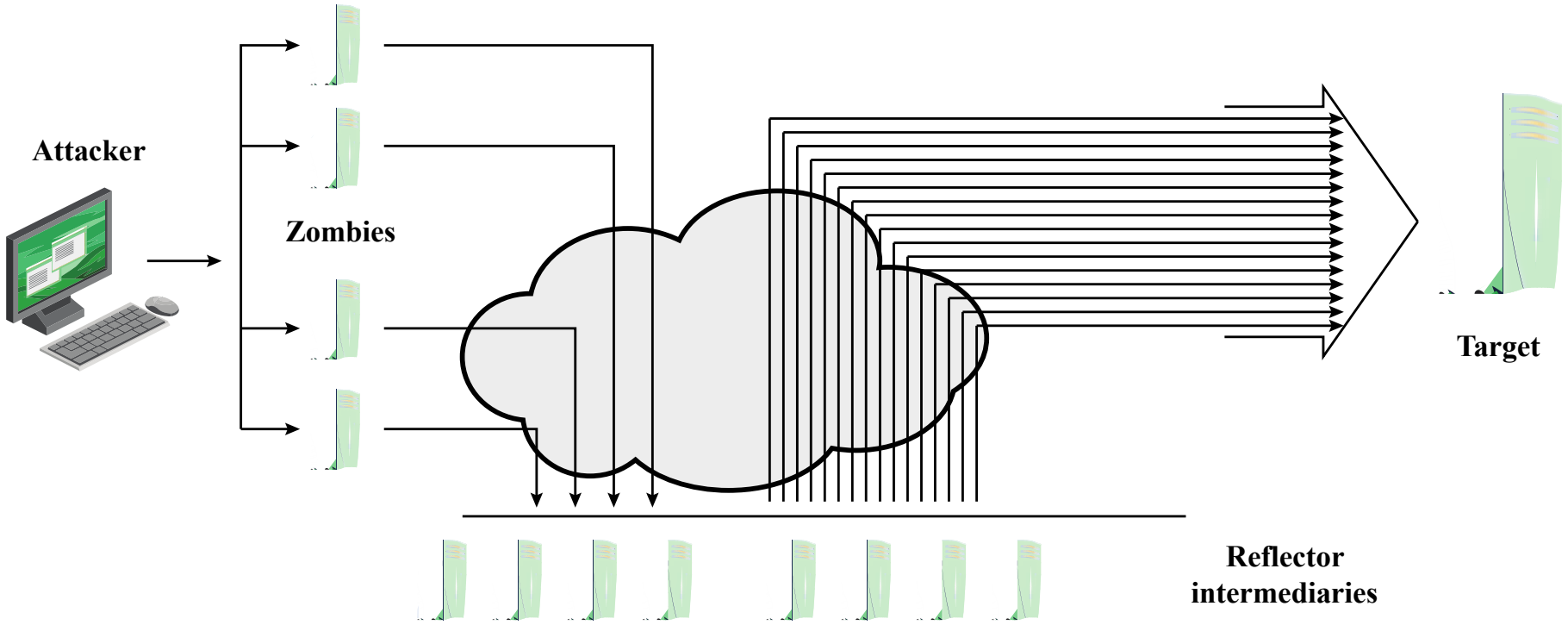


Figure 7.7 Amplification Attack

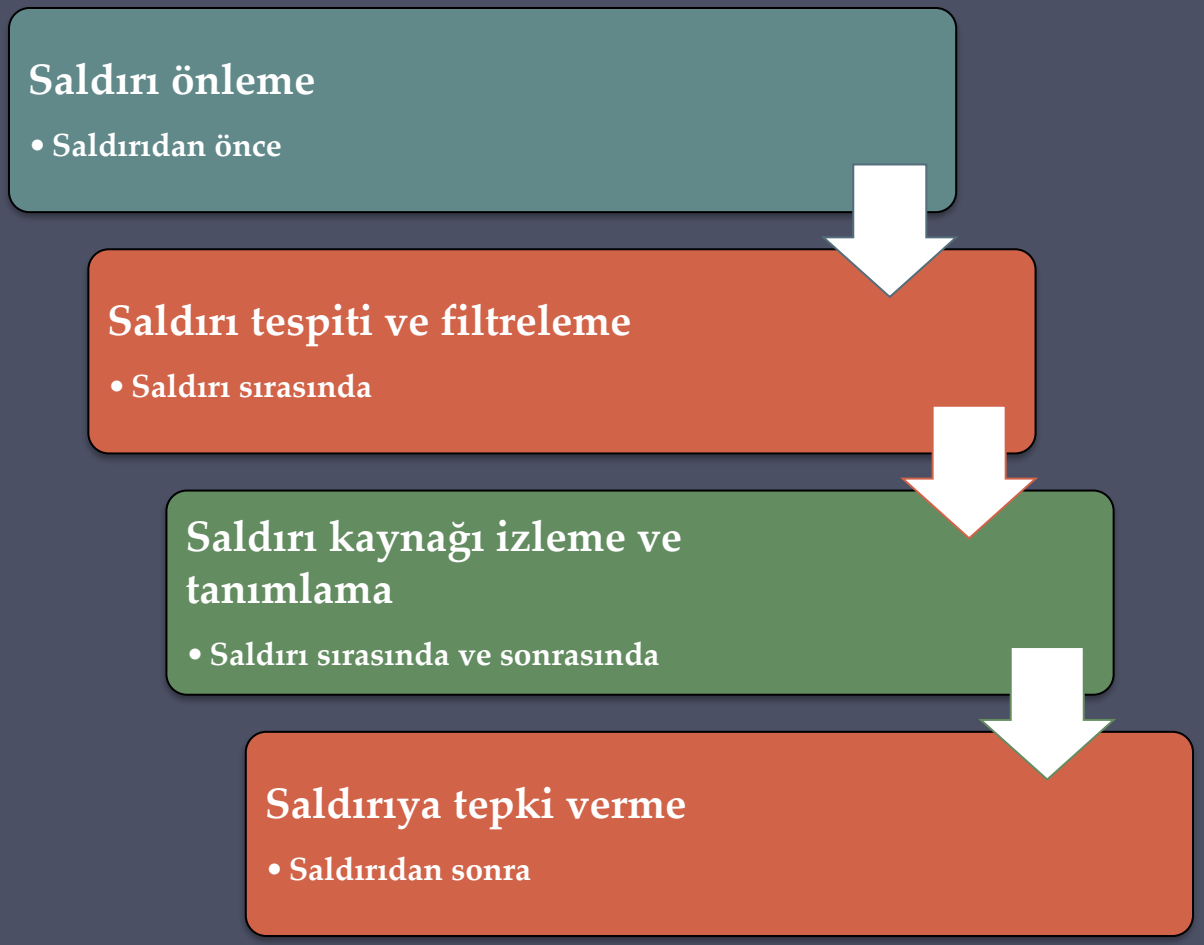
DNS Amplifikasyon Saldırıları

- Aracı sistem olarak meşru bir DNS sunucusuna yönlendirilen paketleri kullanır
- Saldırgan, hedef sistemin sahte kaynak adresini içeren bir dizi DNS isteği oluşturur.
- Küçük bir isteği çok daha büyük bir yanıta dönüştürmek için DNS davranışını kullanır (güçlendirme)
- Hedef yanıtlarla dolup taşar
- Bu saldırıya karşı temel savunma, sahte kaynak adreslerinin kullanımını önlemektir.

DoS Saldırı Savunmaları

- Bu saldırılar tamamen önlenemez.
- Yüksek trafik hacimleri yasal olabilir
  - Belirli bir site hakkında yüksek tanıtım
  - Çok popüler bir sitede etkinlik
  - Flaş kalabalık veya flaş olay olarak tanımlanır

DDoS saldırılarına karşı dört savunma hattı:



DoS Saldırı Önleme

- Sahte kaynak adreslerini engelle
  - Kaynağa mümkün olduğunca yakın yönlendiricilerde
- Talep edilen kaynak adresine giden yolun mevcut paket tarafından kullanılan adres olduğundan emin olmak için filtreler kullanılabilir.
  - Filtreler, trafiğe ISP'nin ağından ayrılmadan önce veya kendi ağına giriş noktasında uygulanmalıdır.
- Değiştirilmiş TCP bağlantı işleme kodunu kullan
  - Kritik bilgileri, sunucunun ilk sıra numarası olarak gönderilen bir tanımlama bilgisinde kriptografik olarak kodlayın
    - Meşru müşteri, artırılmış sıra numarası tanımlama bilgisini içeren bir ACK paketiyle yanıt verir
  - Taştığında, tamamlanmamış bir bağlantı için TCP bağlantıları tablosundan bir giriş bırakın

DoS Saldırı Önleme

- IP yönlendirmeli yayınları engelleyin
- Şüpheli hizmetleri ve kombinasyonları engelleyin
- meşru insan isteklerini ayırt etmek için uygulama saldırılarını bir tür grafik bulmacayla yönetin (captcha)
- İyi genel sistem güvenlik uygulamalarını kullanın
- Yüksek performans ve güvenilirlik gerektiğinde ikizlenmiş ve çoğaltılmış sunucuları kullanın

DoS Saldırılarına Yanıt Verme

İyi Olay Müdahale Planı

- ISP için teknik personelle nasıl iletişime geçileceğine ilişkin ayrıntılar
- Yukarı akışta trafik filtreleme uygulamak için gerekli
- Saldırıya nasıl yanıt verileceğinin ayrıntıları

- Kimlik sahtekarlığına karşı koruma, yönlendirilmiş yayın ve oran sınırlayıcı filtreler uygulanmış olmalıdır.
- Anormal trafik modellerini tespit etmek ve bildirmek için ideal olarak ağ monitörlerine ve IDS'ye sahip olunmalıdır.

DoS Saldırılarına Yanıt Verme

- Saldırı türünü tanımlayın
  - Paketleri yakalayın ve analiz edin
  - Giriş yönündeki saldırı trafiğini engellemek için filtreler tasarlayın
  - Veya sistem/uygulama hatasını tanımlayın ve düzeltin
- ISP'nin paket akışını kaynağa geri izlemesini sağlayın
  - Zor ve zaman alıcı olabilir
  - Yasal işlem planlanıyorsa gerekli
- Acil durum planını uygulayın
  - Alternatif yedekleme sunucularına geç
  - Yeni adreslerle yeni bir sitede yeni sunucular devreye alın
- Olay müdahale planını güncelleyin
  - Gelecekteki işlemler için saldırıyı ve yanıtı analiz edin