



OSI Katman Modeli ve Güvenliđi

Ađ Güvenliđi Perspektifiyle Katmanlar
Arası Koruma

Dr. Fatih KALEMKUŞ

Kafkas Üniversitesi



OSI Modeline Giriş

- OSI (Open Systems Interconnection) modeli, iletişimi 7 katmanda tanımlar.
- Her katman farklı işlev ve güvenlik gereksinimlerine sahiptir.

Dr. Fatih KALEMKUŞ



Fiziksel Katman Güvenliği

- ❖ Ağdaki cihazlar arasındaki veri iletiminin gerçekleştiği katmandır.
- Donanım güvenliği (kablo, cihaz, erişim noktası)
- Kablosuz ağlar için sinyal engelleme ve fiziksel koruma
- Kesintisiz güç kaynakları ve fiziksel erişim kontrolü

1. Fiziksel Katman Saldırıları:

Donanım Saldırıları: Saldırganlar, fiziksel ağ bileşenlerine (örneğin, kablolar, anahtarlar) fiziksel erişim elde etmek için fiziksel bir saldırı gerçekleştirebilirler.

Kablo Kesme (Wiretapping): Saldırganlar, ağ trafiğini izlemek veya çalmak için ağ kablosunu keserek fiziksel erişim sağlayabilirler.

DoS (Denial of Service): Ağ hedefi olarak, kaynakları aşırı kullanarak veya hizmet reddi yaratmak için ağ istismar ederek gerçekleştirilir.

DDoS (Distributed Denial of Service): Birçok farklı kaynaktan aynı anda yürütülen DoS saldırısıdır. Büyük miktarda trafikle ağ hedeflenir, bu da ağ işlemez hale getirir.

Dr. Fatih KALEMKUŞ



Veri Bağlantı Katmanı Güvenliği

- ❖ Bir programdaki verilerin bir ağdaki fiziksel bir bağlantıya nasıl girip çıktığını yöneten protokol katmanıdır
- MAC adres filtreleme
- Anahtarlama tabanlı saldırıların önlenmesi (CAM flooding, MAC spoofing)
- 802.1X kimlik doğrulama

2. Veri Bağlantısı Katmanı Saldırıları:

MAC Flooding: Ağ cihazlarının MAC tablolarını doldurarak, iletişimi engelleyen bir tür saldırıdır.

ARP Spoofing: Yanıltıcı ARP (Address Resolution Protocol) mesajları göndererek, ağdaki cihazların trafiklerini yönlendirmeye çalışır.

Dr. Fatih KALEMKUŞ



Ağ Katmanı Güvenliği

- ❖ Veri paketinin farklı bir ağa gönderilmesi gerektiğinde, veri paketine yönlendiricilerin kullanacağı bilginin eklendiği katmandır. (IP iletişim kuralı vb.)
- IP Spoofing'e karşı IPSEC kullanımı
- ACL (Access Control List) ile trafik kontrolü
- Yönlendirme protokolü güvenliği

3. Ağ Katmanı Saldırıları:

IP Spoofing: IP adreslerini yanıltıcı şekilde değiştirerek, kimlik gizleme veya güvenilirlik sağlama amaçlanır.

ICMP Flood: Aşırı miktarda ICMP (Internet Control Message Protocol) trafik göndererek, hedefin aşırı yüklenmesine neden olabilir.

Dr. Fatih KALEMKUŞ



Taşıma Katmanı Güvenliği

❖ Uygulama (Application) ve Ağ (Network) katmanları arasında mantıksal bir bağlantı kurulmasını sağlayan bir katmandır.

- TCP/UDP saldırılarına karşı güvenlik önlemleri (SYN flood vb.)

SYN Flood, açık bağlantıları boğmak için bir sunucuya büyük miktarda SYN isteği gönderen yaygın bir Dağıtılmış Hizmet Reddi (DDoS) saldırısı biçimidir.

- TLS/SSL gibi güvenli taşıma protokolleri
- Port güvenliği ve segmentasyon

Bir bilgisayar ağında, port güvenliği, **hangi cihazların belirli bir anahtar portuna bağlanabileceğini kısıtlayan bir özelliktir.**

Ağ segmentasyonu, bir ağı her biri daha küçük, bireysel bir ağ olarak işlev gören birden fazla segmente (alt ağlar) bölen bir ağ mimarisi tasarımıdır.

4. Taşıma Katmanı Saldırıları:

SYN/ACK Flooding (TCP SYN Flood): TCP üçlü el sıkışma mekanizmasını aşırı yükleyerek, hedef sunucunun kaynaklarını tüketir.

UDP Flood: Hedef sunucuya büyük miktarda UDP (User Datagram Protocol) trafik göndererek, kaynakların aşırı kullanılmasına neden olur.

Dr. Fatik KALEMKUŞ



Oturum Katmanı Güvenliđi

- ❖ Bir oturumda iki ayrı uygulama arasındaki ađ koordinasyonundan sorumludur.
- Oturum yönetimi ve zaman aşımı politikaları
- Şifreli oturumlar (SSL/TLS)
- Kimlik doğrulama mekanizmaları

5. Oturum Katmanı Saldırıları:

Session Hijacking: Geçerli bir oturumun kontrolünü ele geçirme girişimidir. Bu, oturum bilgilerini çalarak gerçekleştirilebilir.

Dr. Fatih KALEMKUŞ



Sunum Katmanı Güvenliđi

- ❖ En önemli görevi gönderilen verinin karşı bilgisayar tarafından anlaşılabilir halde olmasını sağlamaktır.
- Veri şifreleme (AES, RSA vb.)
- Veri bütünlüğü ve imzalama algoritmaları
- Kodlama biçimlerinin güvenliđi (ör. Base64)

6. Sunum Katmanı Saldırıları:

XSS (Cross-Site Scripting): Kötü niyetli kodların web uygulamalarına enjekte edilmesi ve son kullanıcılarda çalıştırılmasıdır.

SQL Injection: Kötü niyetli SQL kodları ekleyerek, veritabanı sorgularının yanıtılması ve yetkisiz erişim sağlanmasıdır.

Dr. Fatih KALEMKUŞ



Uygulama Katmanı Güvenliđi

- ❖ Ağdaki kullanıcı uygulamalarının iletişim kurmasını sağlayan en üst seviyedeki ağ protokolü katmanıdır.
- Uygulama güvenlik açıkları (XSS, SQL injection)
- Kimlik doğrulama ve erişim kontrolü
- Güvenli yazılım geliştirme ve güncellemeler

7. Uygulama Katmanı Saldırıları:

DDoS: Uygulamalara yönelik büyük miktarda trafik gönderilerek, hedef uygulamanın kaynaklarını tüketme veya hizmet reddi yaratma amaçlanır.

Brute Force Attack: Kullanıcı adı ve şifre kombinasyonlarını deneyerek, hesaplara yetkisiz erişim sağlama girişimidir.

Dr. Fatih KALEMKUŞ



OSI Katmanlarında Güvenlik Stratejileri

- Savunma derinliđi ilkesi
- Her katmanda özelleştirilmiş güvenlik
- Saldırı yüzeyini azaltma ve izleme sistemleri

Dr. Fatik KALEMKUŞ



Sonuç

- Her OSI katmanında farklı güvenlik önlemleri gereklidir.
- Katmanlı savunma ile daha etkili güvenlik sağlanabilir.

Dr. Fatik KALEMKUŞ

Sorular



Dr. Fatik KALEMKUŞ



TEŞEKKÜRLER

Dr. Fatih KALEMKUŞ