



Güvenlik Protokolleri: Tasarım, Uygulama ve Analiz

Bilgi Güvenliği ve Kriptografi Perspektifi

Dr. Fatih KALEMKUŞ

Kafkas Üniversitesi



Güvenlik Protokolü Nedir?

- Bilgi ve veri güvenliğini sağlamak için geliştirilen kurallar bütünüdür.
- İletişim sırasında veri bütünlüğü, gizlilik ve doğrulama sağlar.

Dr. Fatih KALEMKUŞ



Temel Amaçlar

- Kimlik Doğrulama
- Yetkilendirme
- Gizlilik
- Veri Bütünlüğü
- İnkâr Edilemezlik

Dr. Fatik KALEMKUŞ



Tasarım Aşaması

- Amaçların belirlenmesi
- Saldırı senaryolarına karşı önlemler
- Kriptografik algoritmaların seçimi (AES, RSA, ECC)

Dr. Fatih KALEMKUŞ



Uygulama

- Yazılım & Donanım düzeyinde uygulama
- Güvenli yazılım geliştirme süreçleri
- Açık kaynak protokol örnekleri (TLS, IPsec)

Dr. Fatih KALEMKUŞ



Analiz ve Test Süreci

- Formal analiz (matematiksel modelleme)
- Zafiyet tarama (penetrasyon testleri)
- Otomatik analiz araçları (ProVerif, AVISPA)

Dr. Fatih KALEMKUŞ



Yaygın Güvenlik Protokolleri

- TLS/SSL
- HTTPS
- SSH
- IPsec
- Kerberos

Dr. Fatih KALEMKUŞ



Yaygın Güvenlik Protokolleri

SSL

SSL (Secure Sockets Layer), internet üzerinden veri iletimini şifreleyerek güvenli hale getirmek için geliştirilmiş bir güvenlik protokolüdür.

Ancak:

🔔 SSL artık kullanılmıyor. Yerini daha güvenli olan TLS (Transport Layer Security) aldı.

📌 SSL Ne İşe Yarar?

- Web tarayıcıları ve sunucular arasındaki iletişimi şifreler
- Gönderilen bilgilerin üçüncü kişiler tarafından görülmesini veya değiştirilmesini engeller
- Kimlik doğrulama ve veri bütünlüğü sağlar

🔒 SSL Nasıl Çalışır? (Kısaca)

1. Tarayıcı ve sunucu bağlantı kurar
2. Sunucu, SSL sertifikasını gönderir
3. Tarayıcı sertifikayı doğrular
4. Güvenli bir anahtar oluşturulur
5. Veri, bu anahtarla şifrelenerek gönderilir

Dr. Fatih KALEMKUŞ

🔔 **Neden Artık SSL Kullanılmıyor?**

- SSL 2.0 ve 3.0 sürümleri güvensiz bulundu
- Yerine TLS protokolü geliştirildi (TLS 1.0 → 1.3'e kadar)

🌐 SSL Nerelerde Kullanılırdı?

- Web siteleri: HTTPS bağlantılarında
- E-posta servisleri
- VPN bağlantıları
- Dosya aktarım protokollerinde (FTPS)



Yaygın Güvenlik Protokolleri

TLS

📌 Temel Tanım:

TLS, iki taraf arasında (örneğin bir tarayıcı ile bir web sunucusu) veri alışverişini şifreleyerek üçüncü kişilerin bu verileri okuyamamasını veya değiştirememesini sağlar.

🔒 Ne İşe Yarar?

- **Gizlilik:** Veri şifrelenir, dışarıdan okunamaz.
- **Bütünlük:** Veri iletim sırasında değiştirilmemiştir.
- **Kimlik Doğrulama:** Sunucunun (ve bazen istemcinin) gerçekten kim olduğunu doğrular (örneğin: SSL sertifikaları).

📌 Kullanım Alanları:

- **HTTPS:** Web sitelerinin güvenli bağlantılarında (httpS)
- **E-posta güvenliği:** SMTPS, IMAPS, POP3S
- **VPN bağlantıları**
- **VoIP ve mesajlaşma uygulamaları**

Dr. Fatih KALEMKUŞ



Yaygın Güvenlik Protokolleri

HTTPS

HTTPS (HyperText Transfer Protocol Secure), web tarayıcıları ile web sunucuları arasındaki iletişimi şifreleyerek güvenli hale getiren bir iletişim protokolüdür.

🔒 "HTTP" protokolünün TLS/SSL ile şifrelenmiş versiyonudur.

🚩 HTTPS Ne İşe Yarar?

- **Veri Gizliliği:** Gönderilen bilgiler şifrelenir, dışarıdan okunamaz.
- **Veri Bütünlüğü:** Veriler iletim sırasında değiştirilmemiştir.
- **Kimlik Doğrulama:** Web sitesinin gerçekten iddia ettiği site olduğunu doğrular.

🌐 HTTPS Nerede Kullanılır?

- Tüm modern **web siteleri** (Google, e-Devlet, bankalar, sosyal medya)
- E-ticaret işlemleri
- Kişisel bilgi formları
- Giriş sayfaları ve parola alanları

🔒 HTTPS Nasıl Çalışır?

1. Tarayıcı, siteye **HTTPS ile bağlanır**
2. Sunucu, **TLS sertifikasını** gönderir
3. Tarayıcı bu sertifikayı doğrular
4. Şifreli iletişim başlatılır
5. Veriler şifreli şekilde aktarılır

Dr. Fatih KALEMKUŞ



Yaygın Güvenlik Protokolleri

SSH

SSH (Secure Shell), bir bilgisayara uzaktan, güvenli bir şekilde erişmeni ve o bilgisayarda komut çalıştırmanı sağlayan bir ağ protokolüdür.

Basitçe söylemek gerekirse:

👉 Bilgisayar A'dan, Bilgisayar B'ye güvenli bir şekilde bağlanmak istiyorsan **SSH** kullanırsın.

💡 Ne işe yarar?

- Uzak bir sunucuya bağlanıp komut çalıştırmanı sağlar.
- Dosya transferi (SCP, SFTP) yapabilirsin.
- Şifrelenmiş bağlantı sağlar, böylece veriler ağda dinlenmeye karşı korunur.

🔒 Neden güvenli?

- Kullanıcı adı/şifre veya **anahtar tabanlı kimlik doğrulama** kullanır.
- Verileri şifreler, böylece ağ üzerinde veri çalınmasını zorlaştırır.

Dr. Fatih KALEMKUŞ



Yaygın Güvenlik Protokolleri

IPSec

IPSec (Internet Protocol Security), internet üzerinden gönderilen verileri **şifreleyen ve güvenli hale getiren** bir protokoller bütünüdür. Genelde **VPN'lerin temelini** oluşturur.

💡 IPSec Ne İşe Yarar?

- İki cihaz (örneğin iki şirket ağı, iki router ya da bir bilgisayar ile bir sunucu) arasında **IP paketlerini** şifreler.
- **Veri gizliliği, bütünlüğü ve kimlik doğrulaması** sağlar.
- Özellikle **VPN tünellerinde** çok kullanılır (örneğin: site-to-site VPN).

💡 Nasıl Çalışır?

IPSec iki ana modda çalışır:

1. 🗝️ Transport Mode (Taşıma Modu)

- Sadece IP paketi içeriği (veri kısmı) şifrelenir.
- Genelde uç cihazlar arasında (ör: iki bilgisayar) kullanılır.

2. 🌐 Tunnel Mode (Tünel Modu)

- Tüm IP paketi şifrelenir, yeni bir IP başlığı eklenir.
- Genelde ağ geçitleri (ör: iki ofis ağı) arasında kullanılır.

🔧 IPSec'in Sağladıkları:

- **Şifreleme:** Veriler okunamaz hale gelir.
- **Kimlik doğrulama:** Verinin kaynağı doğrulanır.
- **Veri bütünlüğü:** Veri aktarılırken değişmediğinden emin olunur.
- **Replay koruması:** Eski paketler tekrar gönderilip ağın kandırılması önlenir.

💡 Nerelerde Kullanılır?

- VPN (Virtual Private Network) bağlantıları
- Güvenli site-to-site ağlar
- Kablosuz ağ güvenliği (bazı durumlarda)
- Uçtan uca şifreli bağlantılar

Dr. Fatih KALEMKUŞ



Yaygın Güvenlik Protokolleri

Kerberos

🐱 Kerberos Nedir?

Kerberos, ağ üzerinde güvenli kimlik doğrulama (authentication) sağlayan bir protokoldür.

En basit haliyle:

👉 Kullanıcı şifreyi sürekli sunucuya göndermeden, kimliğini kanıtlayıp güvenli bir şekilde ağdaki kaynaklara erişmesini sağlar.

💡 Neden Kerberos Kullanılır?

- Kimlik doğrulamasını şifreyi ortalıkta dolaştırmadan yapar.
- Ağ içindeki tüm sistemlerde tek oturum açma (Single Sign-On, SSO) imkanı sağlar.
- Güvenli, çünkü şifreler değil, şifreli biletler (ticket) kullanılır.

🔒 Nasıl Çalışır?

Kerberos'un 3 temel oyuncusu vardır:

1. Client (istemci) — Kullanıcı / cihaz.
2. KDC (Key Distribution Center) — Kimlik doğrulama merkezidir.
 - AS (Authentication Server): İlk doğrulamayı yapar.
 - TGS (Ticket Granting Server): Erişim için bilet verir.
3. Service (Hizmet Sunucusu) — Kullanıcıların erişmek istediği uygulama ya da sunucu.

🔥 Avantajları:

- Güvenli: Şifreler ağda açıkça dolaşmaz.
- Merkezi kimlik doğrulama sağlar.
- Tek oturum açma desteği (SSO).

💡 Dezavantajları:

- Saat senkronizasyonu çok kritik. Sistem saatleri uyumsuzsa doğrulama çalışmaz.
- KDC çalışmazsa sistem çöker, çünkü doğrulama yapılamaz.

💡 Nerelerde Kullanılır?

- Windows Active Directory
- Linux sistemlerde (özellikle NFS, SSH kimlik doğrulamada)
- Hadoop gibi büyük veri sistemlerinde
- Modern kurumsal ağlarda SSO için.

Dr. Fatih KALEMKUŞ



Saldırı Türleri

- Man-in-the-Middle (MitM)
- Replay Attack
- Spoofing

Dr. Fatih KALEMKUŞ



Saldırı Türleri

Man-in-the-Middle (MitM)

"Man-in-the-Middle (MitM)", yani "Ortadaki Adam Saldırısı", bir iletişimdeki iki taraf arasına gizlice girerek verileri dinlemeyi veya değiştirmeyi amaçlayan bir siber saldırı türüdür.

📌 Nasıl Çalışır?

1. Kurban A ve Kurban B iletişim kuruyor.
2. Saldırgan, bu iletişimi gizlice kendi üzerinden yönlendiriyor.
3. Her iki taraf, birbirleriyle güvenli şekilde iletişim kurduklarını sanırken, saldırgan tüm verileri görebiliyor, hatta değiştirebiliyor.

Dr. Fatih KALEMKUŞ



Saldırı Türleri

Replay Attack

Replay Attack (Yineleme Saldırısı), daha önce yakalanmış geçerli veri paketlerinin izin alınmadan tekrar gönderilmesi ile yapılan bir siber saldırı türüdür.

📌 Ne Olur?

Saldırgan, bir kullanıcının kimlik doğrulama veya işlem yaparken gönderdiği veri paketini (örneğin: "giriş yap" komutu) yakalar ve daha sonra aynısını tekrar gönderir.

Bu, sanki kullanıcı yeniden işlem yapmış gibi görünmesine neden olur.

💡 Örnek Senaryo:

1. Kullanıcı bankaya giriş yapar.
2. Saldırgan, bu **giriş paketini yakalar** (şifrelenmiş olsa bile).
3. Daha sonra saldırgan bu paketi tekrar göndererek izin almadan kullanıcı gibi giriş yapar.

🔑 Replay Attack'e Karşı Önlemler:

- Zaman damgaları (timestamp) kullanmak
- Tek kullanımlık kodlar (nonce)
- İmza veya token geçerlilik süresi
- Şifreli bağlantı (TLS) ile veri iletimi

Dr. Fatih KALEMKUŞ



Saldırı Türleri

Spoofing

Spoofing (Sahtecilik/Spoof Saldırısı), saldırganın bir sistem, cihaz ya da kullanıcı gibi kimliğini taklit ederek kandırma yoluyla veri erişimi sağlamaya çalıştığı bir saldırı türüdür.

📌 Spoofing Ne Yapar?

Saldırgan, güvenilir bir kaynaktan geliyormuş gibi görünerek:

- Kimlik doğrulama süreçlerini atlayabilir,
- Hassas verileri ele geçirebilir,
- Kullanıcıları sahte yönlendirmelere çekebilir.

🔵 Spoofing'e Karşı Alınabilecek Önlemler:

- Kimlik doğrulama sistemleri (2FA, dijital imzalar)
- Şifreli iletişim protokolleri (TLS/SSL)
- E-posta doğrulama sistemleri (SPF, DKIM, DMARC)
- Ağ seviyesinde IP/MAC doğrulama mekanizmaları

💡 Spoofing Türleri:

- **IP Spoofing:** Başka bir IP adresini taklit ederek ağda dolaşmak
- **Email Spoofing:** Güvenilir bir e-posta adresinden gelmiş gibi sahte e-posta göndermek
- **DNS Spoofing:** Kullanıcıyı sahte bir web sitesine yönlendirmek
- **MAC Spoofing:** Donanım adresi değiştirerek ağda farklı bir cihaz gibi davranmak

Dr. Fatih KALEMKUŞ



Geleceğin Protokolleri

- Kuantum güvenliği
- Post-kuantum kriptografi
- Zero-trust mimariler

Dr. Fatih KALEMKUŞ



Sonuç ve Öneriler

- Güvenlik protokolleri yaşam döngüsü boyunca değerlendirilmelidir
- Tasarım kadar analiz de kritik öneme sahiptir

Dr. Fatih KALEMKUŞ

Sorular



Dr. Fatik KALEMKUŞ



TEŞEKKÜRLER

Dr. Fatih KALEMKUŞ