**grafik, siyah beyaz, tasarım içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.**

**Bursa Teknik Üniversitesi**

**Bilgisayar Ağları**

**Low-Level IP İşleme ve Ağ Performans Analizi ile Gelişmiş Güvenli Dosya Transfer Sistemi**

*Proje Final Raporu*

**Ad:** Eren

**Soyad:** KÖSE

**Öğrenci Numarası:** 22360859075

**Introduction - Tanıtım**

Bu proje, güvenli dosya transferi için geliştirilmiş kapsamlı bir ağ uygulamasıdır. Sistem hem TCP hem de UDP protokollerini destekleyen, dosya transferlerinde uçtan uca şifreleme kullanan ve çeşitli ağ analiz araçları sunan bir yapıya sahiptir.

Projenin ana bileşenleri şunlardır:

* **Güvenli Dosya Transferi**: AES-256 şifreleme ve RSA asimetrik şifreleme kullanılarak uçtan uca güvenli dosya transferi sağlanmaktadır. Dosyalar önce AES ile şifrelenir, AES anahtarı ise RSA ile korunur.
* **Çoklu Protokol Desteği**: Hem TCP hem de UDP protokolleri üzerinden dosya transferi yapılabilmektedir. UDP transferlerinde özel parçalama ve yeniden birleştirme mekanizmaları kullanılmaktadır.
* **Ağ Analizi ve Güvenlik**: Uygulama, ağ performansını ölçen (gecikme, bant genişliği, paket kaybı), güvenlik testleri yapan (MITM tespiti, paket enjeksiyonu analizi) ve protokol karşılaştırmaları sunan kapsamlı analiz araçları içermektedir.
* **Gelişmiş IP Başlık İşlemleri**: IP paketlerinin düşük seviyeli manipülasyonu, özelleştirilmiş MTU boyutları, TTL değerleri ve IP bayrakları gibi detaylı kontroller sağlanmaktadır.
* **Kullanıcı Arayüzü**: Tüm bu işlevler, kullanıcı dostu bir grafik arayüz üzerinden erişilebilir şekilde tasarlanmıştır. GUI, sunucu yönetimi, dosya transferi ve ağ analizi için ayrı sekmeler içermektedir.

Proje, modern ağ programlama tekniklerini kullanarak güvenli ve güvenilir dosya transferi sağlamayı amaçlamaktadır. Aynı zamanda, ağ performansı ve güvenliği konusunda detaylı analizler yaparak sistem yöneticilerine ve geliştiricilere değerli bilgiler sunmaktadır.

Bu sistem, özellikle güvenli dosya transferi gerektiren kurumsal ortamlar, uzaktan çalışma senaryoları ve hassas veri paylaşımı gerektiren uygulamalar için uygundur. Projenin modüler yapısı, yeni özelliklerin kolayca eklenebilmesine ve mevcut özelliklerin geliştirilebilmesine olanak sağlamaktadır.

**Technical Details – Teknik Detaylar**

**Yazılım Dili**

* Python

**Şifreleme Kütüphaneleri**

* **cryptography**
  + Simetrik şifreleme (AES-256-CBC)
  + Asimetrik şifreleme (RSA-2048)
  + Hash fonksiyonları (SHA-256)
  + PKCS7 padding
  + Key serialization

**Ağ Kütüphaneleri**

* **socket**
  + TCP/UDP soket programlama
  + Özel buffer boyutları
  + Timeout yönetimi
* **scapy**
  + IP başlık manipülasyonu
  + Paket yakalama ve analiz
  + Checksum hesaplama ve doğrulama

**Güvenlik Kütüphaneleri**

* **secrets**
  + Kriptografik güvenli rastgele sayı üretimi
  + Token oluşturma

**Sistem Kütüphaneleri**

* **subprocess**
  + Harici komut çalıştırma
  + Ağ analiz araçları entegrasyonu
* **os**
  + Dosya işlemleri
  + Path yönetimi

**Ağ Analiz Araçları**

* **ping**
  + Gecikme ölçümü
  + Paket kaybı tespiti
* **iperf3**
  + Bant genişliği ölçümü
  + Performans analizi
* **Wireshark**
  + Paket yakalama ve analiz
  + Protokol analizi

**GUI Araçları**

* **tkinter**
  + Grafiksel kullanıcı arayüzü
  + Widget yönetimi
  + Event handling

**Ek Özellikler**

* Paket parçalama ve birleştirme
* Güvenlik analizi
* MITM tespit simülasyonu
* Paket kaybı simülasyonu
* Checksum doğrulama
* Protokol karşılaştırması

metin, ekran görüntüsü, yazı tipi, sayı, numara içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

* Dosya Sistemi 🡪

**gui.py**

* Bu dosyada,

**ip\_header.py**

* Bu dosyada,

**network\_analysis.py**

* Bu dosyada,

**server.py**

* Bu dosyada,

**client.py**

* Bu dosyada,

**security\_analysis.py**

* Bu dosyada,

**Limitations and Improvements – Kısıtlamalar ve Geliştirmeler**

**Geliştirmeler**

* Projemde kullanıcıların daha iyi bir deneyim elde etmesi ve her işleme daha kolay ulaşıp kullanabilmesi amacıyla bir Graphical User Interface (GUI) tasarımı yaptım. Bu GUI tasarımında uygulamayı kullanırken yardımcı olabilecek Wireshark uygulaması için de belirli yolda bulunması dahilinde uygulamaya erişim sağlanacak bir buton ekledim. Ayrıca gerekli parametrelerin girilebileceği girdi kısımları ve kolaylıkla anlaşılabilecek işlem butonları da GUI içerisinde bulunmakta.

**Kısıtlamalar**

* Parçalı veri gönderip birleştirme sistemini doğru şekilde kurdum ancak dosyanın kaydedilmesi işlemini gerçekleştirmedim. Proje teslimi sonrası bireysel proje olarak devam ettirdiğim dönemde bu özelliği eklemeyi planlıyorum.
* Bazı durumlarda özellikle Windows Defender’ın Firewall sistemi yapılmaya çalışılan işlemleri engellediğinden dolayı bazı sistemlerde uygulama istendiği gibi çalışmayabiliyor.

metin, ekran görüntüsü, yazılım, ekran, görüntüleme içeren bir resim

Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

**References - Kaynakça**

* [1] Comer, D. E. (2018). *Internetworking with TCP/IP: Principles, Protocols, and Architecture* (6th ed.). Pearson.
* [2] Milanov, E. (2009). The RSA algorithm. *RSA laboratories*, *1*(11).
* [3] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer Science & Business Media.
* [4] Taso, K., & Tirumala, A. (2005). *iPerf: Bandwidth Measurement Tool*. <https://iperf.fr>
* [5] Jagt. (2016). *Clumsy* [Computer software]. GitHub. <https://github.com/jagt/clumsy>
* [6] The Wireshark Team. (n.d.). *Wireshark user documentation*. Wireshark. <https://www.wireshark.org/docs/>