# FİZİKSEL KATMAN (PORT) SİNYAL ENJEKSİYONU ANOMALİSİ

1. ANOMALİ TAMIMI: Şarj kablosu/portuna takılan kötü amaçlı bir cihaz, aracın veya istasyonun algıladığı fiziksel sinyalleri taklit ederek veya değiştirmek suretiyle şarj oturumunu bozan ya da yetkisiz kontrol sağlayan bir saldırıdır.

## 2. OLASI NEDENLER:

1-Açıklama: Bir kişi/cihaz port veya tabancaya fiziksel olarak takılır (PORTulator tipi).
2-İşaretler: Port çevresinde yabancı cihaz, bant, leke veya gevşek parçalar; ani ve tekrarlayan oturum hataları.
3- Donanım arızası / bakım eksikliği
4- **EMI/elektromanyetik girişim ve çevresel etkenler:**
-Açıklama: Yakınlarda güçlü elektromanyetik kaynaklar veya yüksek gürültü hataları sinyal okumalarını bozuyor.
5- İşaretler: Hava koşullarına/cihaz çalışmasına bağlı anlık bozulmalar; manyetik alan ölçümlerinde sapma.
6- Tedarik zinciri / sahte parça kullanımı
7- İçeriden kötü niyetli eylem (insider threat)

## 3-OLASI RİSKLER VE ETKİLER:

1- **Şarj kesintisi (DoS)** — Kullanıcı şarj yapamaz; gelir ve itibar kaybı.
2- **Kimlik doğrulama atlatma** — Yetkisiz şarj ve enerji hırsızlığı; mali kayıp.
3- **Yanlış faturalama / veri bozulması** — Telemetri hatalı kayıt yapar; yanlış ücretlendirme ve itirazlar.
4- **Donanım hasarı (batarya/istasyon)** — Aşırı akım/gerilim kaynaklı fiziksel arıza; onarım maliyeti.
5- **Yangın / kullanıcı güvenliği riski** — Elektriksel arıza veya kaçak; yaralanma veya yangın.

## 4-İLGİLİ STANDART REFERANSI:

### 1. ISO/IEC 15118 — Araç ve Şarj İstasyonu Arası İletişim Standardı

- **Ne işe yarar:** Elektrikli araç ile şarj istasyonu arasındaki dijital haberleşmenin kurallarını belirler.
- **İçeriği:** Veri şifreleme, kimlik doğrulama (authentication), dijital sertifikalar ve güvenli bağlantı yöntemleri.

- **Neden önemli:** Saldırganların sahte kimlik veya veri enjeksiyonu (anomalisi) yapmasını önler.

### 2. IEC 61851 — Elektrikli Araç Şarj Sistemi Güvenliği

- **Ne işe yarar:** Şarj sisteminin elektriksel güvenliğini tanımlar.
- **İçeriği:** Gerilim ve akım limitleri, topraklama, izolasyon, koruma devreleri.
- **Neden önemli:** Aşırı akım, kısa devre veya hatalı bağlantı gibi fiziksel anomalileri önler.

### 3. ISO/SAE 21434 — Kara Taşıtlarında Siber Güvenlik Mühendisliği

- **Ne işe yarar:** Araç sistemleri ve şarj altyapısında siber güvenlik risklerinin nasıl yönetileceğini belirler.
- **İçeriği:** Tehdit analizi, risk değerlendirmesi, güvenlik izleme ve anomali tespit yöntemleri.
- **Neden önemli:** Yazılım ve ağ temelli saldırılara (ör. veri manipülasyonu) karşı koruma sağlar.

5-TESPİT YÖNTEMLERİ VE ANALİZ:

1- **Makine Öğrenmesi (Machine Learning) Tabanlı Yöntemler:**

Bu yöntemler, geçmiş verilerden “normal” davranışı öğrenir, sonra sapmaları tespit eder.

2- İstatistiksel ve Kural Tabanlı (Rule-Based / Statistical): Veri dağılımındaki sıra dışı değerleri bulur.

3- Hibrit (Hybrid) Sistemler: Kural sistemi ilk tespiti yapar, ML modeli hatalı alarmı eleyip doğruluk artırır.

6- ÇÖZÜM ÖNERİLERİ: (donanım/yazılım)

# 1. Fiziksel Katman (Physical Layer) Çözümleri:

1. **Gerilim ve akım sensörleriyle sürekli izleme:**
    a. Şarj kablosundaki voltaj/akım dalgalanmaları anında algılanmalı.
    b. *Anomali örneği:* Saldırgan sinyal enjekte ettiğinde sistem fark eder ve şarjı keser.
2. **EMI (Elektromanyetik Parazit) filtreleme devreleri:**

    Saldırganın sisteme yüksek frekanslı sinyal sokmasını önler.

3. **Donanım tabanlı güvenli bileşenler (secure hardware module):**

    Şarj kontrol ünitesine fiziksel erişimle yapılan sabotajlara karşı koruma sağlar.

4. **Topraklama ve kısa devre koruma röleleri:**

    Fiziksel anomaliler sonucu oluşabilecek yangın/hasar riskini engeller

## 2. İletişim ve Protokol Güvenliği (Network & Protocol Layer):

1. **TLS (Transport Layer Security) zorunluluğu (OCPP Security Profile 2):**

    Şarj istasyonu ile sunucu arasındaki tüm veri trafiği şifrelenmeli.

2. **Kimlik doğrulama (Mutual Authentication):**

    Araç, istasyon ve bulut sistemleri karşılıklı dijital sertifikalarla doğrulanmalı (ISO/IEC 15118).

3. **Mesaj bütünlüğü kontrolü (Message Integrity Check):**

    Gönderilen komut veya verinin sonradan değiştirilmediği doğrulanmalı.

4. **Zaman damgası senkronizasyonu:**

    Eski veya tekrar gönderilen (replay) paketlerin reddedilmesi için.

# 7-SİMİLASYON SONUÇLARI:

### Siber/Fiziksel Köprü Zafiyetinin Doğrulanması:

Bu simülasyon çalışması, Elektrikli Araç Şarj İstasyonu (CP) ile Merkezi Yönetim Sistemi (CSMS) arasındaki OCPP (Şarj İstasyonu Protokolü) kanalındaki zafiyetlerin, CP'nin lokal CAN-bus üzerindeki fiziksel cihaz kontrolüyle nasıl sonuçlanacağını göstermek amacıyla gerçekleştirilmiştir.

#### *1. Protokol Katmanı (OCPP) Bulguları:*

CSMS tarafından başlatılan normal bir `RemoteStartTransaction` akışı sırasında , MitM proxy kullanılarak trafik başarılı bir şekilde yakalanmış ve değiştirilmiştir. Orijinal komut, CP'ye ulaşmadan önce kötü amaçlı bir `RemoteStopTransaction` komutuna dönüştürülmüştür. Bu bulgu, OCPP kanalının güçlü bir TLS/WSS koruması olmadan **Mesaj Değiştirme** tehdidine açık olduğunu doğrulamıştır.

#### *2. Kontrol ve Fiziksel Etki Katmanı (CAN-bus) Bulguları:*

Değiştirilmiş `RemoteStopTransaction` komutunu alan CP simülatörü, bu komutu başarılı bir şekilde CAN-bus seviyesinde yerel bir kontrol mesajına çevirmiştir.

- **Gözlemlenen Anomali:** `vcan0` üzerinde, normal akışta beklenmeyen, **CAN ID `0x201`** (payload: `[tx_id, stop_cmd]`) çerçevesi yayınlanmıştır.
- **Nihai Sonuç:** CAN-bus'taki bu kontrol mesajı, simüle edilen şarj modülünde **anlık şarj kesintisi (DoS)** ile sonuçlanmıştır. Bu, uzaktan gerçekleştirilen bir siber saldırının, Sinyal Enjeksiyonu Anomalisi belgesinde belirtilen

**Şarj Kesintisi (DoS)** riskini doğurabileceği sonucunu desteklemiştir.

**3-Savunma Simülasyonu Sonuçları (İyileştirme):**

- **Mutual TLS Uygulaması:** Simülasyon ortamı, OCPP iletişimi için Mutual TLS (WSS) kullanacak şekilde değiştirildiğinde. MitM saldırısı **engellenmiştir**. Şifrelenmiş trafiğin MitM proxy tarafından çözülememesi nedeniyle komut değiştirilememiş ve CAN ID `0x201` üretilememiştir.
- **Gateway Filtreleme Uygulaması:** CP yazılımına bir Gateway filtreleme/izin listesi (whitelisting) uygulandığında , zararlı firmware simülasyonunda üretilen beklenmedik **CAN ID `0x9FF`** bus'a iletilmeden **reddedilmiştir**. Bu, CP'nin ele geçirilmesi durumunda dahi hatalı davranışın (rölenin sürekli açık kalması gibi) önüne geçilebileceğini göstermiştir.

## 8-SONUÇ VE DEĞERLENDİRME:

Bu çalışmada elektrikli araç şarj istasyonlarında oluşabilecek güvenlik açıkları incelendi.
Araştırmalar sonucunda bu istasyonların sadece elektrik veren cihazlar değil, aynı zamanda veri iletişimi yapan akıllı sistemler olduğu anlaşıldı.

## 9- KAYNAKÇA:


1- **Li, Y., Kumar, R. ve Chen, H. (2025).**
*Elektrikli Araç Şarj Portlarında Fiziksel Katman Sinyal Enjeksiyonu Saldırıları*.
arXiv ön baskı, arXiv:2506.16400.

2- **Zhou, T. ve Park, S. (2025).**
*Grid Sentinel: Elektrikli Araç Şarj Ağlarında Yapay Zekâ Tabanlı Anomali Tespiti*.
*Nature Scientific Reports*.

*3-* **Alshahrani, M. ve diğerleri. (2024).**
*Elektrikli Araç Şarj İstasyonlarının Güvenliği: Tehdit Modelleri ve Önlemler*.
*IEEE Access / ResearchGate*.

*4-* **Nguyen, L. ve Patel, A. (2025).**
*Elektrikli Araç Şarj Altyapısında Siber Güvenlik Üzerine Sistematik Bir İnceleme*.
*MDPI Electronics*.