**ANOMALİ SENARYO RAPORU: Stealthy Federated Energy Drift (SFED) -Gizli (Federatif) Enerji Kayması Anomalisi**

1. AMAÇ

   Bu raporun temel amacı, OCPP tabanlı elektrikli araç şarj altyapılarında meydana gelebilecek yeni nesil, düşük görünürlüklü bir enerji anomalisini (“Stealthy Federated Energy Drift - SFED”) analiz etmektir.

   Senaryo, bir saldırganın veya kötü yapılandırılmış bir sistemin, şarj istasyonlarının (Charge Point – CP) enerji ölçüm verilerini çok küçük oranlarda (ör. %0,5–2) manipüle ederek ve bu manipülasyonları zaman içinde koordineli biçimde yürütmesi üzerine kuruludur. Bu saldırı, merkezi yönetim sistemi (CSMS) tarafından tekil bazda normal olarak algılanırken, toplu ölçekte mikroşebeke dengesinde önemli sapmalara ve faturalama hatalarına yol açar.

Bu çalışma, SFED tipi anomalinin teknik düzeyde nasıl gerçekleştiğini, hangi sistem zafiyetlerinden faydalandığını, bu anomalinin tespit edilmesi için uygulanabilecek yöntemleri ve olası önleme stratejilerini ortaya koymayı hedefler.

2. KAPSAM VE ÖZET

**2.1. Kapsam**

Bu senaryo, OCPP protokolü ile haberleşen üç ana bileşene odaklanır:

- **CSMS (Merkezi Sistem)** – tüm istasyonları yöneten, ölçüm ve faturalama verilerini toplayan “beyin”.
- **Şarj Noktası (CP)** – sahadaki fiziksel istasyon, ölçüm ve enerji dağıtımını yapan “kol”.
- **Enerji Ölçüm Sistemi / Smart Meter** – istasyonun enerji verisini üreten “duyusal katman”.

SFED saldırısı bu üç bileşen arasındaki güven zincirine sızarak, özellikle “ölçüm doğruluğu” ve “zaman senkronizasyonu” katmanlarını hedef alır. Bu saldırı türü, Man-in-the-Middle gibi açık müdahalelerden farklı olarak sistem içinde görünüşte “meşru” davranış sergiler; dolayısıyla tespiti zordur.

**2.2. Genel Özet**

Senaryoda saldırgan, bir grup şarj istasyonunda (ör. 5–10 adet) meter verilerini çok küçük oranlarda yukarı yönlü sapmalarla değiştirir. Aynı anda bazı istasyonlarda zaman senkronizasyonu (NTP) birkaç saniye kaydırılarak, kayıtların korelasyonu bozulur.

Bu küçük farklar tekil bazda olağan dalgalanma gibi görünür; ancak sistem genelinde kümülatif olarak ciddi enerji farklarına yol açar.

Sonuç: CSMS tarafından algılanamayan fakat mikroşebeke (MG) kontrolünde veya faturalamada hissedilen, sinsi ve uzun süreli bir enerji anomalisi.

## 3. TEHDİT SINIFLANDIRMASI (STRIDE)

**S (Spoofing - Kimlik Sahteciliği):**
Kötü niyetli bir CP veya yerel yönetici düğüm, kimliğini doğrulamadan ölçüm sonuçlarını "meşru" görünümlü biçimde CSMS'ye rapor eder.

**T (Tampering - Kurcalama):**
Meter Values mesajlarının içeriği, küçük enerji offset'leriyle değiştirilir. Bu kurcalama genellikle imzasız veya kontrolsüz OCPP değişkenleri üzerinden yapılır.

**R (Repudiation - İnkâr Edememe):**
Zaman sapması nedeniyle CSMS ile CP logları arasında tutarsızlık oluşur. Taraflar hatanın kimden kaynaklandığını inkâr edebilir.

**I (Information Disclosure - Bilgi İfşası):**
Saldırgan, enerji verilerinin akışına erişerek tüketim alışkanlıkları, istasyon yük profilleri ve kullanıcı davranışları hakkında bilgi toplayabilir.

**D (Denial of Service - Hizmet Reddi):**
Uzun vadede MG kontrol algoritmaları yanlış enerji değerlerine göre çalışarak bazı istasyonları devre dışı bırakabilir.

**E (Elevation of Privilege - Yetki Yükseltme):**
Yerel öğrenme süreçlerine (örneğin federated AI modeline) sızarak, merkezi sistemin tespit eşiğini yükseltir ve gizli kalma süresini artırır.

## 4. GEREKLİ KOŞULLAR (SALDIRI ÖN KOŞULLARI)

SFED anomalisi aşağıdaki koşullar altında gerçek hayatta meydana gelebilir:

- **İmzalanmamış veya doğrulanmamış meter değerleri:** OCPP mesajlarının dijital imza içermemesi.
- **Zaman senkronizasyonunun zayıf olması:** CS ve CSMS farklı saatlerde çalıştığında, küçük sapmalar fark edilemez.
- **Federated öğrenme altyapısında zafiyet:** Yerel modellerin doğrulama mekanizmalarının eksikliği.

- **Veri toplama sıklığının düşük olması:** Düşük çözünürlüklü kayıtlar, küçük enerji drift'lerini gizler.

- **Yetersiz korelasyon analizi:** CSMS'in çoklu istasyon verilerini topluca analiz etmemesi.

5. SALDIRI YÖNTEMLERİ VE AKIŞ (ADIM ADIM)

6. **Hazırlık:** Saldırgan, CSMS ile CP arasında meşru OCPP bağlantısına sahip olan bir istasyonda yerel erişim veya yazılım konfigürasyonu sağlar.

7. **Mikro Manipülasyon:** Her bir Meter Values mesajında enerji değeri +%0,5–2 oranında artırılır.

8. **Zaman Kaydırma:** Bazı istasyonlarda OCPP `DateTime` değişkenleri veya NTP konfigürasyonları birkaç saniye ileri/geri ayarlanır.

9. **Koordinasyon:** Bu sapmalar, aynı zaman dilimlerinde (ör. her 10 dakikada bir) birden fazla istasyonda uygulanır.

10. **Toplu Etki:** CSMS, tekil istasyonlardaki farkı normal dalgalanma olarak yorumlar; ancak toplamda mikroşebeke enerji dengesi bozulur.

11. **Model Zehirleme (opsiyonel):** Eğer sistem federated öğrenme tabanlı anomaly detector kullanıyorsa, saldırgan model güncellemelerini küçük bias'larla değiştirir ve tespit eşiğini yükseltir.

6. TESPİT YÖNTEMLERİ VE ANOMALİ GÖSTERGELERİ

**Kural K1 – Toplu Enerji Korelasyon Sapması:**
Tekil istasyonlar normal görünürken, bir bölgedeki toplam enerji üretimi/tüketimi beklenenden sistematik biçimde farklıysa (ör. >%3), SFED riski vardır.

**Kural K2 – Zaman Uyumsuzluğu:**
CS log zaman damgaları ile CSMS logları arasında 5–30 saniyelik sapmalar artmaya başlarsa, zaman temelli drift göstergesidir.

**Kural K3 – İstatistiksel Sinyal:**
Bir istasyonun enerji artış oranı düşük varyanslı uzun periyotlu dalgalanma gösteriyorsa (ör. istatistiksel olarak $p<0,01$ anlamlı), bilinçli sapma olasılığı yüksektir.

**Kural K4 – Federated Model Bozulması:**
Yerel anomaly modellerinin hassasiyeti (precision/recall) beklenenden düşükse veya global model güncellemeleri sıra dışı ağırlık değişimi içeriyorsa, model zehirlenmesi gerçekleşmiş olabilir.

## 7. OLASI ETKİLER

**İşlevsel Etkiler:**
Mikroşebeke yük dengesinin bozulması, planlanan güç limitlerinin aşılması veya yanlış kısıtlamaların uygulanması.

**Ekonomik Etkiler:**
Kümülatif olarak birkaç yüz kWh'lik fark yaratılabilir; bu faturalama sistemlerinde gelir kaybına neden olur.

**Operasyonel Etkiler:**
Yanlış enerji raporlaması, bakım planlarının ve enerji tahsis algoritmalarının bozulmasına yol açar.

**Güvenlik (Safety) Etkileri:**
Gerçek zamanlı enerji tahsisi yapan sistemlerde (ör. acil durum istasyonları), aşırı yüklenme veya gerilim dengesizliği riskleri oluşabilir.

## 8. ÖNLEMLER VE AZALTMA STRATEJİLERİ

- **Dijital İmza / Payload Signing:** Her Meter Values mesajının HMAC veya dijital imza ile doğrulanması.
- **Zaman Senkronizasyon Güvencesi:** Tüm CS'lerin NTP ile merkezi olarak senkronize edilmesi; sapma tespitinde uyarı üretimi.
- **Korelasyon Tabanlı İzleme:** CSMS üzerinde çoklu istasyon verilerinin kümelenmiş analizini yapan anomaly detector kullanımı.
- **Federated Model Güvenliği:** Model güncellemelerinde "Krum" veya "Median Aggregation" gibi savunma mekanizmaları uygulanmalı.
- **Anomali Eşiği Uyarlaması:** Lokal modellerden gelen küçük sapmalar global analizde ağırlıklandırılmalı.
- **Audit Trail ve SIEM Entegrasyonu:** Zaman, enerji ve kimlik loglarının tekleştirilmesiyle SIEM sisteminde çapraz doğrulama yapılmalı.

KAYNAKÇA

[1] Alcaraz, C., et al. *“OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0.”* (2023).

[2] *Federated AI-OCPP Framework for Secure and Scalable EV Charging Systems*, 2024.

[3] *Temporal Convolutional Network Approach to Anomaly Detection in EV Charging Systems*, 2023.

[4] *MitM Cyber Risk Analysis in OCPP Enabled EV Charging*, 2022.

[5] *Survey on Meter Tampering and Charging Fraud in Electric Mobility Infrastructure*, 2023.