Stealthy Federated Energy Drift (SFED) -Gizli (Federatif) Enerji Kayması Anomalisi – SWOT Analizi

1. Güçlü Yönler (Strengths)

- **Düşük Görünürlük (Stealthiness):** Enerji ölçüm verileri çok küçük oranlarda (örneğin, %0,5–2) manipüle edildiği için, merkezi yönetim sistemi (CSMS) tarafından tekil bazda normal dalgalanma olarak algılanır. Bu, anomaliyi tespit etmeyi zorlaştırır.
- **Kümülatif Etki:** Tekil istasyonlarda tespit edilemeyen küçük manipülasyonlar, toplu ölçekte mikroşebeke dengesinde önemli sapmalara ve ciddi faturalama hatalarına yol açar.
- **Çift Yönlü Saldırı:** Hem enerji ölçüm verisini (Tampering - Kurcalama) hem de zaman senkronizasyonunu (Repudiation - İnkar Edememe) hedef alarak, kayıtların korelasyonunu bozma yeteneği vardır.
- **Güven Zinciri Zafiyeti Kullanımı:** Özellikle "ölçüm doğruluğu" ve "zaman senkronizasyonu" katmanlarını hedefleyerek, OCPP'nin üç ana bileşeni arasındaki güven zincirine sızar.

2. Zayıf Yönler (Weaknesses)

- **Yerel Erişim Gereksinimi:** Saldırının başarılı bir şekilde başlaması için saldırganın, CSMS ile meşru OCPP bağlantısı olan bir istasyonda **yerel erişim veya yazılım konfigürasyonu** sağlaması gerekir.
- **Koordinasyon Zorunluluğu:** Etkili bir toplu etki yaratmak için manipülasyonların aynı zaman dilimlerinde birden fazla istasyonda **koordineli** biçimde yürütülmesi gerekir.
- **Statik Sapma Riski:** Manipülasyon, düşük varyanslı uzun periyotlu bir dalgalanma (sistematik sapma) gösterdiğinde, gelişmiş istatistiksel analiz yöntemleriyle tespit edilme olasılığı artar.
- **Tekil İzlemenin Etkisizliği:** CSMS, çoklu istasyon verilerini topluca analiz eden korelasyon tabanlı izleme kullanmaya başladığında, saldırının gizliliği önemli ölçüde azalır.

3. Fırsatlar (Opportunities)

- **Zayıf Zaman Senkronizasyonu:** CS ve CSMS'in farklı saatlerde çalışması durumunda, küçük sapmaların fark edilmemesi saldırının gizlenmesi için bir fırsattır.
- **İmzalanmamış Ölçüm Değerleri:** OCPP mesajlarının dijital imza içermemesi, saldırganın Meter Values içeriğini değiştirmesini kolaylaştıran temel bir ön koşuldur.
- **Federated Öğrenme Altyapısındaki Zafiyet:** Eğer sistem, federated öğrenme tabanlı anomali detektörü kullanıyorsa, saldırgan "Model Zehirleme" ile sistemin tespit eşiğini yükselterek gizli kalma süresini artırma fırsatı bulur.

4. Tehditler (Threats)

- **Toplu Enerji Korelasyonu Tespiti:** CSMS'in bir bölgedeki toplam enerji üretimini/tüketimini sistematik biçimde beklenenden farklı bulması (örneğin >%3 sapma) SFED riskini ortaya çıkarır.

- **Güçlü Önlemler:** Dijital imza (Payload Signing) ve merkezi NTP senkronizasyonu gibi önlemlerin uygulanması, saldırının en önemli iki zafiyetini (kurcalama ve zaman kayması) doğrudan engeller.
- **SIEM Entegrasyonu:** Zaman, enerji ve kimlik loglarının tekleştirilerek SIEM (Security Information and Event Management) sisteminde çapraz doğrulanması, anomaliyi tespit etme şansını önemli ölçüde artırır.
- **Hizmet Reddi (DDoS) Riski:** Yanlış enerji değerlerine göre çalışan MG kontrol algoritmalarının, bazı istasyonları devre dışı bırakma potansiyeli, saldırganın kendi amacına zarar verme (Denial of Service) riskini de taşır.