# **Sayaç Değerlerinin (MeterValues) Manipülasyonu ve Hatalı Faturalandırma**

## **1. AMAÇ**

Bu raporun temel amacı, bir Şarj Noktasının (CP - Charge Point) periyodik olarak gönderdiği MeterValues (Sayaç Değerleri) OCPP mesajlarını hedef alan bir veri manipülasyonu (Data Tampering) saldırı senaryosunu analiz etmektir. Rapor, saldırganın faturalandırmayı etkilemek amacıyla CSMS'e (Merkezi Sistem) iletilen enerji tüketim verilerini nasıl değiştirebileceğini teknik düzeyde tanımlamayı hedefler.

Bu çalışma, özellikle zaman serisi (time-series) verilerine dayalı anomali tespit sistemlerinin (IEEE makalesinde bahsedilen konuyla uyumlu olarak) bu tür bir anomaliyi nasıl tespit edebileceğine odaklanır ve potansiyel etkiler ile azaltma stratejilerini belgeler.

## **2. KAPSAM VE ÖZET**

### **2.1. Kapsam**

Bu rapor, OCPP v1.6 ve üzeri standartları kullanan bir CP ile CSMS arasındaki iletişimi kapsar. Analiz, özellikle MeterValues.req mesajlarının içindeki sampledValue (örneklenmiş değer) ve value (değer) alanlarının (genellikle Wh veya kWh cinsinden enerji) manipülasyonuna odaklanır.

### **2.2. Genel Özet**

Saldırı senaryosu, CSMS ile CP arasındaki iletişim kanalına sızan (MitM) veya doğrudan CP'nin yerel ağına ya da kendisine erişim sağlayan bir saldırganın, şarj oturumu sırasında gönderilen kritik MeterValues mesajlarını yakalamasına ve değiştirmesine dayanır.

Saldırgan, meşru bir şarj işlemi devam ederken, tüketilen enerji miktarını kasıtlı olarak düşük gösteren (örn. 5 kWh tüketim yerine 0.5 kWh bildiren) sahte MeterValues mesajları oluşturur ve bunları CSMS'e iletir. Bu durum, CSMS tarafında hem anlık izlemede hem de oturum sonu faturalandırmada ciddi tutarsızlıklara yol açar. Tespit edilmezse, bu saldırı doğrudan gelir kaybına neden olur. Bu tür bir anomali, enerji tüketiminin zaman serisi analizinde (örn. beklenen şarj eğrisinden ani ve mantıksız sapmalar) tespit edilebilir.

## **3. TEHDİT SINIFLANDIRMASI (STRIDE)**

Söz konusu saldırı senaryosu, STRIDE tehdit modellemesi çerçevesinde aşağıdaki kategoriler altında sınıflandırılabilir:

* **T (Tampering - Kurcalama):** Saldırının temelini oluşturur. Saldırgan, faturalandırmayı etkilemek için transit haldeki veya CP'de üretilen MeterValues mesajının içeriğini (tüketim verisi) aktif olarak değiştirir.
* **S (Spoofing - Kimlik Sahteciliği):** Saldırgan, CSMS'e sahte veriyi gönderirken kendisini meşru Şarj Noktası (CP) olarak tanıtır. Bu, genellikle MitM sırasında oturumun devam ettirilmesiyle veya CP'nin kimlik bilgilerinin (örn. TLS sertifikası) çalınmasıyla yapılır.
* **R (Repudiation - İnkâr Edememe):** Eğer saldırı CP'nin kendisinden (ihlal edilmiş bir cihaz) kaynaklanıyorsa, CSMS kayıtları meşru bir CP'den düşük veri geldiğini gösterir. CP'nin "Ben bu veriyi göndermedim" demesi (inkâr) zorlaşır. Saldırgan, eylemin kaynağını gizleyerek inkâr edilebilirliği artırır.
* **I (Information Disclosure - Bilgi İfşası):** Saldırganın bu veriyi manipüle edebilmesi için önce (genellikle şifresiz iletişim kanalını dinleyerek) meşru MeterValues mesajlarının yapısını, transactionId'yi ve normal tüketim paternlerini öğrenmesi gerekir.
* **D (Denial of Service - Hizmet Reddi):** Doğrudan bir hizmet reddi olmasa da, sürekli hatalı faturalandırma ve gelir kaybı, operatörün o istasyonu güvenilmez bularak hizmet dışı bırakmasına (dolaylı DoS) yol açabilir.

## **4. GEREKLİ KOŞULLAR (SALDIRI ÖN KOŞULLARI)**

* **Güvensiz İletişim Kanalı:** Zayıf TLS profilleri veya şifresiz (Unsecured Transport) bir WebSocket bağlantısı, MitM saldırganının mesajları okumasını ve değiştirmesini kolaylaştırır.
* **Zayıf Cihaz Güvenliği (CP):** Şarj Noktasının (CP) kendisinde zayıf fiziksel güvenlik, varsayılan (default) yönetici parolaları veya güncellenmemiş firmware bulunması, saldırganın doğrudan cihaza sızarak veriyi kaynağından manipüle etmesine olanak tanır.
* **Yetersiz Uygulama Katmanı Doğrulaması:** CSMS'in, gelen MeterValues verilerini sadece kabul etmesi ve bu verilerin (enerji tüketiminin) beklenen fiziksel şarj eğrisine (örn. zamanla doğrusal veya logaritmik artış) uygunluğunu kontrol eden bir zaman serisi anomali motoruna sahip olmaması.

## **5. SALDIRI YÖNTEMLERİ VE AKIŞ (ADIM ADIM)**

Senaryo, bir MitM (Ortadaki Adam) saldırısı üzerinden ele alınmıştır:

1. **Erişim ve Dinleme:** Saldırgan, CP ve CSMS arasına girer (örn. ARP spoofing) ve OCPP trafiğini dinlemeye başlar.
2. **Oturum Tespiti:** Saldırgan, bir StartTransaction.req ve ardından gelen MeterValues.req mesajlarını izleyerek aktif bir şarj oturumunu (ve ilgili transactionId'yi) tespit eder.
3. **Manipülasyon (Tampering):** Saldırgan, periyodik olarak (örn. her 60 saniyede bir) gönderilen MeterValues.req mesajını yakalar.
   * Orijinal Mesaj (JSON Payload):  
     [2, "msg123", "MeterValues", {"transactionId": 1001, "meterValue": [{"timestamp": "...", "sampledValue": [{"value": "5120", "context": "Sample.Periodic", "measurand": "Energy.Active.Import.Register"}]}]}]
   * Manipüle Edilmiş Mesaj: Saldırgan value değerini (örn. 5120 Wh) çok daha düşük bir değerle (örn. 512 Wh) değiştirir.  
     [2, "msg123", "MeterValues", {"transactionId": 1001, "meterValue": [{"timestamp": "...", "sampledValue": [{"value": "512", "context": "Sample.Periodic", "measurand": "Energy.Active.Import.Register"}]}]}]
4. **İletim:** Manipüle edilmiş mesaj, sanki orijinal CP'den geliyormuş gibi CSMS'e iletilir.
5. **Kayıt ve Sonuç:** CSMS, bu sahte ve düşük değeri kendi veritabanına kaydeder. Oturum StopTransaction ile sonlandığında, CSMS toplam tüketimi bu manipüle edilmiş verilere dayanarak hesaplar ve kullanıcıya eksik fatura keser.

## **6. TESPİT YÖNTEMLERİ VE ANOMALİ GÖSTERGELERİ**

Bu tür bir saldırı, IEEE makalesinde belirtildiği gibi, zaman serisi (timeseries) ve günlük (log) anomali tespiti ile yakalanabilir.

### **6.1. Zaman Serisi ve İstatistiksel Tespit**

Sistemin normal operasyonunun bir temeli (baseline) oluşturulur.

* **Kural T1 (Negatif veya Durgun Tüketim):** Bir şarj oturumu (Transaction) aktifken, Energy.Active.Import.Register (Toplam Tüketilen Enerji) değerini içeren MeterValues zaman serisinde, değerin bir önceki ölçümden daha düşük gelmesi veya anormal derecede yavaş artması (fiziksel olarak imkansız veya beklenmedik bir durum). Bu, en net anomali göstergesidir.
* **Kural T2 (Şarj Eğrisi Sapması):** Enerji tüketim eğrisi, bilinen araç modelleri veya genel şarj profilleri (örn. ilk başta hızlı, sona doğru yavaşlayan) ile karşılaştırılır. Saldırganın gönderdiği veri (örn. her dakika 0.1 kWh artış gibi sabit ve düşük bir değer) bu beklenen eğriden istatistiksel olarak (örn. Z-skoru veya İzolasyon Ormanı modeli ile) saptığında anomali olarak işaretlenir.

### **6.2. Günlük (Log) Temelli Tespit**

* **Kural L1 (İmza Uyuşmazlığı):** (Bkz. Önlem 8.2) Eğer mesaj imzalama kullanılıyorsa, CSMS'in aldığı mesajın imzasının geçersiz olması, loglarda "Geçersiz Mesaj İmzası" hatası olarak görünür ve bu doğrudan bir manipülasyon (Tampering) alarmıdır.
* **Kural L2 (Oturum Anormallikleri):** Saldırganın MitM proxy'sinin neden olduğu ağ gecikmeleri (latency) veya TCP/TLS el sıkışma (handshake) anormallikleri, normal dışı oturum logları üretebilir.

## **7. OLASI ETKİLER**

* **Ekonomik Etkiler (Gelir Kaybı):** Saldırının birincil hedefidir. Şarj operatörü (CPO) için doğrudan ve ciddi gelir kaybı yaratır. Sistematik hale gelirse, operatörün iflasına yol açabilir.
* **Veri Bütünlüğünün Bozulması:** CSMS veritabanındaki kayıtların güvenilirliği kalmaz. Bu durum, hem geçmişe dönük analizleri hem de enerji şebekesi yönetimi için kullanılan (örn. talep-tahmin) verileri bozar.
* **Güven Kaybı ve Yasal Sorunlar:** Hatalı faturalandırmanın (hem eksik hem de potansiyel olarak fazla) fark edilmesi, müşterilerin sisteme olan güvenini sarsar ve yasal denetimlerde sorunlara yol açar.

## **8. ÖNLEMLER VE AZALTMA STRATEJİLERİ**

* **Güvenli İletişim (mTLS):** Sağladığınız örnekte olduğu gibi, Güvenlik Profili 3 (Security Profile 3) yani karşılıklı TLS (mTLS) kullanımı zorunlu kılınmalıdır. Bu, MitM saldırılarını büyük ölçüde engeller.
* **Uygulama Katmanı İmzalama (OCPP Security Whitepaper):** Sadece TLS'e güvenmek yerine, OCPP mesajlarının (JSON payload) kendisinin bir imza (örn. HMAC veya JWS/JWT) içermesi. CSMS, mesajı işlemeden önce bu imzayı doğrulamalıdır. Bu, TLS kırılsa bile mesajın değiştirilmediğini (Tampering) garanti eder.
* **Sunucu Tarafı Anomali Tespiti (CSMS):** (IEEE makalesinin ana konusu) CSMS tarafında, gelen MeterValues verilerini sürekli analiz eden makine öğrenimi tabanlı bir anomali tespit sistemi kurulmalıdır. Bu sistem, Kural T1 ve T2'de belirtilen fiziksel olarak imkansız veya istatistiksel olarak beklenmedik tüketim desenlerini (örn. "negatif tüketim", "anormal yavaş şarj") gerçek zamanlı olarak yakalamalı ve alarm üretmelidir.
* **Güvenli Cihaz Yönetimi (CP):** Şarj noktalarının firmware'leri güncel tutulmalı, varsayılan parolalar değiştirilmeli ve cihazlara fiziksel/ağ erişimi kısıtlanmalıdır. Bu, saldırganın veriyi kaynağından (CP üzerinden) değiştirmesini zorlaştırır.