Anomali Senaryosu

1. Normal Akış

1. **Bağlantı ve Kimlik Doğrulama:** Kullanıcı aracını istasyona (CS) bağlar. OCPP protokolü üzerinden merkeze (CSMS) `BootNotification`, `Authorize` ve `StartTransaction` komutları gider.
2. **Şarj Başlangıcı:** Merkez (CSMS), şarjı onaylar. İstasyon (CS), aracın iç iletişim protokolü üzerinden araçla konuşarak güvenli şarj parametrelerini belirler.
3. **Raporlama:** Şarj devam ederken, istasyonun içindeki "Smart Meter", CAN-bus üzerinden kontrolcüye "X kWh enerji harcandı" bilgisini gönderir. Kontrolcü, bu bilgiyi kullanarak periyodik olarak merkeze (CSMS) bir OCPP `MeterValues` mesajı gönderir.
4. **Bitiş:** Kullanıcı şarjı bitirdiğinde CSMS, CAN-bus'tan gelen son `MeterValues` verisine göre kullanıcıyı doğru bir şekilde faturalandırır.

2. Anormal Akış

1. **Aşama 1: Sızma (Firmware Zafiyeti):**
    - Saldırgan, istasyonun **imzasız firmware güncellemelerini kabul etme** zafiyetini keşfeder.
    - Merkez (CSMS) gibi davranarak (Spoofing) veya istasyonun yönetim paneline sızarak istasyona kötücül bir `UpdateFirmware` komutu gönderir.
2. **Aşama 2: Kontrolü Ele Geçirme (Yetki Yükseltme):**
    - İstasyon, bu sahte ve kötücül firmware'i yükler. Bu firmware, saldırgana cihaz üzerinde **Uzaktan Kod Çalıştırma (RCE)** veya tam "root" erişimi sağlar.
3. **Aşama 3: Saldırı (CAN Enjeksiyonu ve Veri Manipülasyonu):**
    - Saldırgan artık istasyonun beynindedir. İstasyonun iç ağı olan **CAN-bus**'a doğrudan müdahale etmeye başlar.
    - **Hedef (Hırsızlık):** Saldırgan, akıllı sayaçtan (Smart Meter) gelen gerçek `MeterValues` verisini (örn. 50 kWh) okur, ancak merkeze (CSMS) giden OCPP

`MeterValues` paketini yolda yakalayıp **değiştirir** (Tampering) ve "5 kWh" olarak gönderir. Kullanıcıya %90 daha az fatura çıkar.