EV Şarj İstasyonu Anomali Senaryosu - SWOT Analizi

Bu analiz, dokümanda belirtilen **Sızma (Firmware)**, **Yetki Yükseltme (Root)** ve **Veri Manipülasyonu (CAN Enjeksiyonu)** aşamalarını temel alır.

---

1. Strengths (Saldırının Güçlü Yönleri ve Etkinliği)

Saldırının başarı şansını artıran ve saldırganı avantajlı kılan teknik faktörler.

- **İmzasız Firmware Zafiyeti:** İstasyonun imzasız yazılım güncellemelerini kabul etmesi, saldırının en güçlü giriş kapısıdır . Bu, saldırganın karmaşık exploitler yazmasına gerek kalmadan, meşru bir işlem gibi görünerek (CSMS spoofing ile) sisteme girmesini sağlar.
- **Tam Yetki (Root Access):** Kötücül firmware sayesinde saldırganın cihaz üzerinde "root" yetkisi kazanması, sistemin tüm savunma mekanizmalarını devre dışı bırakabilmesine olanak tanır.
- **İç Ağın (CAN-bus) Güvenine Dayalı Yapı:** Saldırganın kontrolcü ile Smart Meter arasındaki iletişimi dinleyip manipüle edebilmesi, CAN-bus mimarisinin genellikle şifresiz ve "güvenilir ağ" varsayımına dayanmasından güç alır.
- **Finansal Motivasyonun Yüksekliği:** Saldırı doğrudan faturalandırma verisini (Meter Values) hedef aldığı için saldırgan için anında %90 oranında somut bir finansal kazanç sağlar .

2. Weaknesses (Saldırının Zayıf Yönleri ve Tespit Noktaları)

Saldırının iz bırakabileceği, başarısız olabileceği veya tespit edilebileceği noktalar.

- **Enerji Uyumsuzluğu (Grid vs. Meter):** Saldırgan CSMS'e giden veriyi "5 kWh" olarak değiştirse de , şebekeden (Grid) çekilen gerçek enerji 50 kWh olacaktır. Operatör, şebeke sayaçları ile istasyon verilerini karşılaştırdığında bu büyük farkı kolayca tespit edebilir.
- **Firmware Güncelleme Logları:** Planlanmamış bir zamanda, yetkisiz veya bilinmeyen bir kaynaktan gelen "Update Firmware" komutu , merkezi izleme

sistemlerinde (SIEM) büyük bir anomali alarmı oluşturacaktır.

- **Araç Tarafı Verisi:** Araç batarya yönetim sistemi (BMS), aldığı enerjiyi bilir. Kullanıcı faturada 5 kWh görse de, araç ekranında "50 kWh şarj edildi" bilgisi yer alacaktır. Bu tutarsızlık, dürüst kullanıcıların şikayetiyle saldırıyı açığa çıkarabilir.
- **Bağlantı Kesintisi:** Firmware yükleme (reboot) süreci sırasında istasyonun kısa süreliğine offline olması veya servis dışı kalması, operasyon merkezinin dikkatini çekebilir.

3. Opportunities (Savunma ve Önleme Fırsatları)

Sistemi güçlendirmek için bu senaryodan çıkarılabilecek dersler ve iyileştirmeler.

- **Secure Boot ve Code Signing:** İstasyonun yalnızca üretici tarafından dijital olarak imzalanmış firmware paketlerini kabul etmesini sağlayan "Secure Boot" mekanizmasının devreye alınması, saldırıyı daha 1. Aşamada durdurur .
- **Ağ Segmentasyonu ve CAN Şifreleme:** İstasyon içindeki kontrol ünitesi ve sayaç arasındaki CAN-bus trafiğinin şifrelenmesi veya MAC (Message Authentication Code) kullanılması, "Enjeksiyon" ve "Tampering" riskini ortadan kaldırır .
- **Anomali Tespit Algoritmaları:** CSMS tarafında, beklenen şarj eğrisi ile gelen veriyi karşılaştıran yapay zeka tabanlı algoritmalar kullanılabilir. Örneğin, bir aracın 1 saat bağlı kalıp sadece 5 kWh çekmesi (bataryası dolu değilse) şüpheli bir durumdur.
- **Karşılıklı Kimlik Doğrulama (mTLS):** CSMS ile İstasyon (CS) arasındaki OCPP bağlantısında, sunucunun istasyonu doğruladığı gibi istasyonun da sunucuyu doğruladığı sertifika tabanlı çift yönlü doğrulama (mTLS), Spoofing saldırılarını engeller .

4. Threats (Riskler ve Tehditler)

Saldırı başarılı olursa sistem, operatör ve kullanıcılar için doğacak sonuçlar.

- **Gelir Kaybı:** Senaryodaki %90'lık fatura manipülasyonu, operatörler için doğrudan ve büyük ölçekli gelir kaybı anlamına gelir .

- **Operasyonel Güven Kaybı:** Kullanıcıların veya enerji sağlayıcıların sisteme olan güveni sarsılır. CSMS'in doğru faturalandırma yapamadığı algısı markaya zarar verir.
- **Fiziksel Hasar Riski (Güvenlik Kapsamı Dışı ama Kritik):** Saldırgan "root" erişimi ve CAN-bus kontrolüne sahip olduğunda , sadece faturayı değil, voltaj ve akım sınırlarını da değiştirerek bataryaya veya istasyona fiziksel zarar verebilecek komutlar gönderebilir.
- **Botnet Olasılığı:** RCE (Uzaktan Kod Çalıştırma) yetkisi , saldırganın bu istasyonları birer "zombi" cihaza dönüştürüp başka ağlara (DDoS saldırıları vb.) saldırmak için kullanmasına yol açabilir.