Anomali Senaryosu Raporu

Senaryo Adı: "Hareket Halinde Şarj" Tutarsızlık Anomalisi (In-Motion Charging Inconsistency)

Referans Makale: Aliwa, E., Perera, C., Rana, O., & Burnap, P. (2020). *CYBERATTACKS AND COUNTERMEASURES FOR IN-VEHICLE NETWORKS*.

Hazırlayan: Mehmet Erdem Abacı

Tarih: 02.11.2025

1. Senaryonun Amacı

Saldırının amacı, bir elektrikli aracın (EV) temel güvenlik mekanizmalarından birini (araç hareket halindeyken şarjı kesme) atlatmaktır. Bu senaryo, aracın araç içi ağına (CAN-Bus) sahte veri enjekte ederek, araç fiziksel olarak hareket halindeyken bile şarj istasyonundan (CS) enerji çekmeye devam etmesini hedefler.

2. Senaryo Özeti

Saldırgan, aracın CAN-Bus ağına (uzaktan Telematik veya fiziksel OBD-II portu üzerinden) erişim sağlar. Araç, bir DC hızlı şarj istasyonuna bağlıyken, saldırgan CAN-Bus'a sürekli olarak sahte "Vites: Park (P)" ve "Hız: 0 km/s" mesajları enjekte etmeye başlar. Bu sahte mesajlar, aracın Batarya Yönetim Sistemi'ni (BMS) kandırır. Saldırgan (veya işbirlikçisi) aracı "Drive (D)" vitesine takıp sürmeye başladığında, BMS sahte "Park" sinyalini gördüğü için şarjı kesmez. Sonuç olarak, araç hareket halindeyken (gerçek GPS ve tekerlek verisi hızı raporlarken) aynı anda şarj istasyonundan aktif olarak enerji çekmeye (OCPP meterValues akışı devam ederken) devam eder.

3. Hedef Varlıklar

- **Araç İçi CAN-Bus:** Özellikle Vites Kutusu Kontrol Ünitesi (TCU) ve Motor Kontrol Ünitesi (ECU) mesajlarının yayınlandığı kritik veri yolu.
- **Batarya Yönetim Sistemi (BMS):** Şarjı fiziksel olarak kesme veya devam ettirme kararını veren ECU.
- **Telematik Kontrol Ünitesi (TCU) / Ağ Geçidi (Gateway):** Saldırganın CAN-Bus'a sızdığı giriş noktası.
- **Merkezi Yönetim Sistemi (CSMS):** Anomaliyi tespit etmesi beklenen, hem OCPP hem de Telematik verisini toplayan ana sunucu.

4. İlişkili Tehditler (STRIDE)

- **Spoofing (Kimlik Sahteciliği):** Saldırgan, meşru Vites Kutusu ECU'sunun kimliğine bürünerek (kaynak makalede "ECU Impersonation" olarak geçer) onun CAN ID'si ile sahte mesajlar gönderir.
- **Tampering (Veri Manipülasyonu):** Aracın gerçek "Hız" ve "Vites" durumu verisi, saldırganın enjekte ettiği sahte veri ile "maskelenir" veya bastırılır. Bu, kaynak makalede "CAN Falsifying Attack" (Sahte Veri Üretme Saldırısı) olarak tanımlanır .
- **Elevation of Privilege (Yetki Yükseltme):** Saldırgan, normalde "imkansız" olan bir eylemi (hareket ederken şarj etme) gerçekleştirerek sistemin güvenlik kurallarını (Safety) atlatmış olur.

5. Saldırıda Faydalanılan Zafiyetler

- **CAN-Bus'ta Kimlik Doğrulama Eksikliği:** *Kaynak makalede* belirtildiği gibi, CAN protokolü "tasarım gereği güvenlik mekanizmalarından yoksundur". Bir mesajın gerçekten doğru ECU'dan gelip gelmediğini doğrulayamaz.
- **Güven Alanlarının Ayrılığı (Siloed Trust):** Araç içi güvenlik (BMS'in CAN verisine güvenmesi) ile altyapı güvenliğinin (CSMS'in OCPP verisine güvenmesi) birbirinden ayrı çalışması ve verilerin çapraz doğrulanmaması.
- **Yetersiz Tutarlılık Kontrolü:** Kaynak makaledeki "Consistency sensor" (Tutarlılık Sensörü) bölümünde belirtilen mantığın (örn. "tekerlek dönerken GPS duruyorsa bu bir hatadır") eksikliği.

6. Saldırı Adımları (Adım Adım Simülasyon)

1. **Aşama 1: Erişim:** Saldırgan, aracın Telematik ünitesindeki (örn. 4G/Wi-Fi) bir zafiyeti kullanarak veya OBD-II portuna fiziksel olarak (örn. sahte bir dongle ile) bağlanarak CAN-Bus ağına yazma erişimi elde eder.
2. **Aşama 2: Şarj Başlatma:** Saldırgan, aracı normal bir şekilde DC hızlı şarj istasyonuna bağlar. RFID kartını okutur ve CSMS'ten StartTransaction onayı alınır. Şarj işlemi (OCPP) ve enerji akışı (fiziksel) başlar.
3. **Aşama 3: Sahte Veri Enjeksiyonu (CAN Falsifying Attack):**
    - Saldırgan, CAN-Bus'a yüksek öncelikli sahte mesajlar enjekte etmeye başlar .
    - ID: 0x1F0, Data: [0x01] (Anlamı: Vites Konumu = PARK)
    - ID: 0x153, Data: [0x00, 0x00] (Anlamı: Araç Hızı = 0 km/s)
4. **Aşama 4: Anormal Eylem:**
    - Saldırgan (veya işbirlikçisi) aracı çalıştırır ve vitesi "D" (Drive) konumuna alır.

    - Araç fiziksel olarak hızlanmaya başlar (örn. 30 km/s).
5. **Aşama 5: Güvenlik Atlatma:**
    - Aracın Batarya Yönetim Sistemi (BMS), gerçek vites ("D") ve hız (30 km/s) mesajlarını *görmez*, çünkü saldırganın daha yüksek öncelikli veya daha sık gönderdiği sahte "Park" ve "0 km/s" mesajlarını okur.
    - BMS, aracın park halinde olduğunu düşündüğü için güvenlik protokolünü tetiklemez ve şarjı kesmez.
    - Araç, fiziksel olarak hareket halindeyken şarj olmaya devam eder.

7. Olası Sonuçlar ve Etkiler

- **Kritik Güvenlik İhlali (Safety):** En önemli etki budur. Hareket halinde şarj, kablonun kopmasına, yüksek voltajlı ark oluşumuna, yangına veya istasyonun fiziksel olarak parçalanmasına yol açabilir.
- **Protokol İhlali:** Hem ISO 15118 hem de OCPP'nin temel güvenlik varsayımları (aracın sabit olduğu) ihlal edilir.

8. Tespit Yöntemleri (Detection) - Projenin YZ Çözümü

Bu senaryo, projenin YZ tabanlı "Anomali Tespit Sistemi" için mükemmel bir hedeftir. YZ modeli, CSMS seviyesinde iki farklı veri kaynağını (OCPP ve Telematik) çapraz kontrol etmelidir:

- **Veri Kaynağı 1 (OCPP):** İstasyondan gelen TransactionEvent veya meterValues mesajları. (Durum: "Şarj Ediyor", Enerji Akışı: "Var").
- **Veri Kaynağı 2 (Telematik/GPS):** *Aynı* aracın Telematik ünitesinden gelen GPS ve hücresel konum verisi . (Durum: "Hareket Halinde", Hız: "30 km/s").

Anomali Tespiti: YZ modeli, (Şarj Ediyor = DOĞRU) VE (Hareket Halinde = DOĞRU) mantıksal tutarsızlığını yakalar. Bu, tam olarak kaynak makalede tarif edilen "Consistency sensor" (Tutarlılık Sensörü) mantığıdır . YZ, bu imkansız durumu %100 kesinlikle bir anomali olarak etiketler.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Araç İçi (CAN):** Blokzincir teknolojisi veya *kaynak makalede* detaylandırılan Kriptografik MAC yöntemleri ile CAN-Bus mesajlarının bütünlüğünü ve kaynağını doğrulamak.
- **Ağ Geçidi (Gateway):** Telematik/Infotainment gibi "güvensiz" alanlardan gelen CAN mesajlarını filtreleyen (firewall) bir ağ geçidi (Gateway) kullanmak.
- **Altyapı (CSMS):** Bu senaryoda anlatılan YZ tabanlı "Tutarlılık Kontrolü"nü CSMS tarafında zorunlu kılmak. CSMS, bir işlem sırasında Telematik'ten hareket verisi alırsa, araca güvenmeyip OCPP üzerinden RemoteStopTransaction komutu göndermelidir.