Güvenlik Senaryosu: Maksimum Güçte Anormal Şarj (BMS Manipülasyonu)

Tarih: 03 Kasım 2025
Hazırlayan: İbrahim Halil Yilmaz
İlgili Sistemler: DC Hızlı Şarj (CCS/ISO 15118), Araç BMS, CSMS İş Mantığı

1. Senaryonun Amacı ve Kapsamı

1.1. Amaç

Bu raporun amacı, bir DC hızlı şarj (DCFC) istasyonunda başlatılan bir şarj işleminin, normal fiziksel ve operasyonel beklentilerin (örn: batarya şarj eğrisi - "tapering") dışında, anormal derecede uzun süreler boyunca istasyonun nominal maksimum gücünde (veya bu güce çok yakın bir seviyede) devam etmesi senaryosunu analiz etmektir. Bu durumun, araç Batarya Yönetim Sistemi (BMS) sinyallerinin kasıtlı olarak manipüle edilmesi (BMS Spoofing) veya protokolün istismar edilmesi yoluyla bir sabotaj girişimi olabileceğini vurgulamayı amaçlar.

1.2. Kapsam

Bu senaryo, DC şarj istasyonunun güç elektroniği (güç modülleri), şarj kabloları, konnektörler ve istasyonun güvenlik denetleyicileri (EVSE) ile araç arasındaki dijital iletişim protokolünü (örn: ISO 15118, DIN SPEC 70121, CHAdeMO) kapsar. Temel odak noktası, aracın şarj cihazına ilettiği "talep edilen güç" ve "batarya durumu" sinyalleridir.

2. Özet

Normal bir DC hızlı şarj işleminde, aracın BMS'i batarya doluluk oranı arttıkça (genellikle %80'i geçince) bataryayı korumak için talep ettiği gücü kademeli olarak düşürür (buna "tapering" veya "güç azaltma eğrisi" denir). Bu senaryoda ise, kötü niyetli bir aktör, aracın BMS sinyallerini taklit eden bir cihaz (BMS Spoofing) veya hack'lenmiş bir araç kullanarak, şarj istasyonundan sürekli olarak maksimum güç talep eder. İstasyon, 2-3 saat boyunca (normalde 180kW'lık bir aracın 30-40 dakikada %80'e ulaşması gerekirken) aralıksız %100 kapasitede çalışmaya zorlanır. Bu durum, istasyon bileşenlerinin (güç modülleri, kablolar, konnektörler) aşırı ısınması, erimesi ve potansiyel olarak alev almasıyla sonuçlanabilecek kritik bir sabotaj eylemidir.

3. Tehdit Modeli ve Vektörleri

3.1. Tehdit Aktörleri

- **Vandallar / Sabotajcılar:** Birincil amacı şarj ağı altyapısına fiziksel olarak zarar vermek

(yangın çıkarmak, ekipmanı eritmek) olan aktörler.
- **Kötü Niyetli Güvenlik Araştırmacıları:** Sistemin sınırlarını tehlikeli bir şekilde test edenler.

3.2. Giriş Noktası

- DC Şarj Konnektörü (CCS veya CHAdeMO).

3.3. Saldırı Vektörleri

- **Vektör 1 (BMS Spoofing Cihazı):** Saldırganın, şarj konnektörüne takılan, "Man-in-the-Middle" (MitM) görevi gören veya doğrudan bir aracı taklit eden özel bir donanım (örn: Raspberry Pi, CAN bus emülatörü) kullanması. Bu cihaz, şarj istasyonuna sürekli olarak "Bataryam %20 dolu, 180kW istiyorum" mesajını gönderir.
- **Vektör 2 (Araç İçi Manipülasyon):** Aracın kendi BMS veya telematik kontrol ünitesinin (TCU) yazılımının değiştirilerek (root'lanarak) normal güvenlik protokollerinin devre dışı bırakılması.

4. Etkilenen Varlıklar (Assets)

4.1. Birincil Fiziksel Varlıklar

- DC Güç Modülleri, güç dağıtım baraları, yüksek voltajlı şarj kabloları, şarj konnektörleri (özellikle pinler).

4.2. İkincil Varlıklar

- Şarj istasyonunun kasası, bağlı olan araç (ve bataryası), çevredeki diğer mülkler (yangın durumunda).

4.3. Soyut Varlıklar

- Marka itibarı, operasyonel devamlılık.

5. Zafiyetler (Vulnerabilities)

5.1. Z-1 (Körü Körüne Güven)

- Şarj istasyonunun (EVSE), aracın BMS'inden gelen güç talebi komutlarına, bu taleplerin süresi mantıksız olsa bile "körü körüne güvenmesi" ve sadece bu taleplere göre hareket etmesi.

5.2. Z-2 (Yetersiz Sunucu Tarafı Denetimi)

- CSMS (Merkezi Yönetim Sistemi) tarafında, bir şarj işleminin süresi ve ortalama gücü hakkında mantıksal kontrollerin (sanity checks) bulunmaması veya zayıf olması.

5.3. Z-3 (Protokol Zayıflığı)

- Özellikle eski DC protokollerinin, aracın kimliğini (ve BMS'inin meşruluğunu) güçlü bir şekilde doğrulamadan (örn: kriptografik imza olmadan) iletişime izin vermesi.

6. Potansiyel Saldırı Akışı

1. **Bağlantı:** Saldırgan, özel olarak hazırladığı "BMS Spoofing" cihazını veya hack'lenmiş aracını istasyonun DC konnektörüne bağlar.
2. **Kimlik Doğrulama:** Saldırgan, işlemi (muhtemelen çalıntı bir RFID kart veya mobil uygulama ile) başlatır.
3. **İletişim Başlatma:** Şarj istasyonu ve (sahte) araç arasındaki dijital iletişim (handshake) başlar.
4. **Manipülatif Talep:** İstasyon, "Güç talebin nedir?" diye sorduğunda, sahte BMS sürekli olarak (TalepEdilenGüç = 180kW, BataryaDurumu = %20) mesajını gönderir.
5. **Güç Aktarımı:** İstasyon, talep edilen 180kW'ı sağlamaya başlar.
6. **Kilitleme (Döngü):** Normalde 30 dakika sonra batarya %80'e ulaştığında talebin 80kW'a, sonra 50kW'a düşmesi gerekirken, sahte BMS 2 saat boyunca aynı (180kW, %20) mesajını göndermeye devam eder.
7. **Fiziksel Arıza (Aşırı Isınma):** İstasyonun güç modülleri ve kabloları, "tapering" olmadan %100 yükte sürekli çalışmak üzere tasarlanmamıştır. Sıcaklık tehlikeli seviyelere yükselir, kablo izolasyonu erir, konnektör pinleri hasar görür ve potansiyel olarak yangın başlar.
8. **Sonuç:** İstasyon ve muhtemelen bağlı olan (sahte) cihaz fiziksel olarak yok olur.

7. Risk ve Etki Analizi

7.1. Güvenlik Riski (Kritik - Yüksek)

- **Yangın Tehlikesi:** Bu senaryonun birincil riski, ekipmanın erimesi ve alev almasıdır. Bu, sadece istasyona değil, araca, yakındaki diğer araçlara ve tüm tesise (örn: otopark, AVM) sıçrayabilir.
- **Can Güvenliği:** Halka açık bir alanda yangın çıkması, doğrudan can güvenliğini tehdit eder.

7.2. Operasyonel Etki (Yüksek)

- İstasyonun tamamen (kalıcı olarak) hizmet dışı kalması.
- Tüm şarj lokasyonunun güvenlik soruşturması nedeniyle kapatılması.

7.3. Finansal Etki (Yüksek)

- On binlerce dolarlık ekipman değişimi ve onarım maliyeti.
- Potansiyel yasal davalar ve sigorta maliyetleri.

7.4. İtibar Etkisi (Kritik)

- "X firmasının şarj istasyonu alev aldı" haberi, marka itibarını geri dönülemez bir şekilde

zedeler ve müşteri güvenini tamamen yok eder.

8. Önlemler ve Azaltma Stratejileri

8.1. CSMS ve EVSE Katmanında Katı İş Mantığı (Business Logic Rules)

- **Zaman ve Güç Limiti:** CSMS veya istasyonun kendisi, katı kurallara sahip olmalıdır. (ÖRN: EĞER (SessionSüresi > 60 Dakika) VE (OrtalamaGüç > MaksGücün %90'ı) İSE İşlemiDerhalDurdur(HardStop) VE AlarmGönder).
- **Enerji Limiti:** Bir seansta sağlanabilecek toplam kWh miktarı (örn: 150 kWh) için mantıksal bir üst sınır belirlenmeli ve bu aşıldığında işlem durdurulmalıdır.

8.2. Bağımsız Donanımsal Termal Koruma

- İstasyonun BMS iletişiminden *bağımsız* çalışan fiziksel sıcaklık sensörleri (kablolarda, konnektörde, güç modüllerinde) kritik eşiklere ulaşıldığında (örn: 85°C) gücü otomatik olarak kesmeli (derating yapmalı) veya işlemi sonlandırmalıdır.

8.3. Protokol Güvenliğini Artırma (ISO 15118-20 & PnC)

- "Plug & Charge" (PnC) gibi gelişmiş protokollerin kullanılması. PnC, aracın kimliğini (ve dolayısıyla BMS'inin meşruluğunu) kriptografik sertifikalarla doğrulayarak, sahte cihazların veya manipüle edilmiş araçların ağa bağlanmasını engeller.

8.4. Anomali Tespiti (Akıllı Analiz)

- (Bir önceki DDoS raporundaki gibi) Trafik ve işlem logları, normal olmayan şarj eğrilerini (örn: 2 saat boyunca %100 güçte giden seanslar) tespit etmek için makine öğrenimi ile analiz edilmeli ve otomatik olarak alarm üretilmelidir.