Anomali Senaryosu: Kapasite Sahtekarlığı (Phantom SoC Report)

Hazırlayan: Şevval Öcal
Tarih: 02.11.2025

1. Senaryonun Hedefi ve Tanımı

Bu anomali, şarj işlemi sırasında EVSE'nin (Şarj İstasyonu) Elektrikli Araca (EV) ve kullanıcıya gösterdiği Batarya Durumu (State of Charge - SoC) veya şarj edilen enerji miktarı (kWh) verilerinin gerçeği yansıtmaması durumudur. Temel amaç, şarj süresini erken sonlandırarak veya enerji miktarını gizleyerek, kullanıcıya sanki tam hizmet almış gibi bir illüzyon yaratmaktır.
Saldırgan, EVSE'yi manipüle ederek, aracın bataryası %60 doluyken, kullanıcının arayüzünde (araç içi ekran veya istasyon ekranı) şarjın %90'a ulaştığı bilgisini gösterir. Kullanıcı, hedefine ulaştığını düşünerek seansı bitirir, ancak fiilen eksik enerji şarj etmiştir.

2. Saldırının Gerçekleşme Yolları (Vektörler)

Bu tür bir donanım/firmware manipülasyonu, EVSE'nin yerel kontrol sistemlerine yetkisiz erişim gerektirir. Erişim, genellikle aşağıdaki gibi sistem açıklarından faydalanarak sağlanır:
• **Firmware Geri Kapıları (Debug Backdoors) Yoluyla Erişimi İstismar Etmek:** Geliştiricilerin sistemde test ve bakım amaçlı bıraktıkları, ancak üretim ortamında kapatılmayı unutulan gizli erişim noktaları (backdoor'lar) kullanılabilir. Bu tür bir erişim, saldırganın EVSE'nin işletim sistemine sızmasına ve sensör verilerini işleyen düşük seviyeli yazılımları (firmware) değiştirmesine olanak tanır.
• **Yazılım Zafiyetleri Üzerinden Sızma:** OCPP (Open Charge Point Protocol) gibi iletişim protokolleri üzerinden gönderilen kötü amaçlı komutlar veya istasyonun yönetim paneline yönelik bilinen siber güvenlik açıkları (örneğin kalıcı komut çalıştırma zafiyetleri), saldırganın EVSE'nin kontrol katmanına erişmesine ve manipülatif firmware'i sisteme yüklemesine imkan tanır.
• **Fiziksel Sensör Zehirlenmesi:** Entegre devreler veya fiziksel sayaçlar üzerinden okunan akım, gerilim ve enerji (kWh) değerlerini toplayan donanım bileşenleri doğrudan hedef alınarak, bunların raporladığı sayısal değerler değiştirilir.

3. Anomalinin Operasyonel ve Finansal Etkileri

Bu anomali, sadece kullanıcıyı kandırmakla kalmaz, aynı zamanda EVSE sisteminin bütünlüğünü de tehlikeye atar:

A. Hizmet Kalitesinin Sabotajı (Kullanıcı Güveni Kaybı)
Saldırı sonucunda, kullanıcı parasını ödemiş olsa bile beklediği menzil ve enerji miktarını alamaz. Bu durum, elektrikli araç sahipleri için operasyonel bir felç durumu yaratır, zira araç beklenmedik bir şekilde yetersiz şarj nedeniyle yolda kalma riskiyle karşı karşıya kalır. Hizmet kalitesinin düşürülmesi, şarj ağına olan genel güveni sarsar.

B. Çift Yönlü Veri Manipülasyonu ve Kör Kayıt
Saldırgan, Kapasite Sahtekarlığını gizlemek için iki seviyede veri manipülasyonu yapar:
1. Araç/Kullanıcı Seviyesi (Yanılsama): Araca yüksek (sahte) SoC değeri bildirilir.
2. Merkezi Sistem Seviyesi (Gizleme): Merkezi Şarj İstasyonu Yönetim Sistemine (CSMS) gönderilen gerçek enerji tüketim kayıtları (Sayaç Değerleri/MeterValues) de kurcalanabilir.
Eğer saldırgan, kullanıcıya %90 raporu verip seansı sonlandırır, ancak CSMS'e yalnızca gerçek tüketilen enerjinin (örneğin 6 kWh) faturasını gönderirse, bu durum Fatura Yönlendirme Hilesi olarak adlandırılan bir senaryoya yol açar. Saldırganın amacı ya kullanıcıdan fazla ücret almak ya da istasyonu işleten şirketten enerji çalmaktır (bu, "Hayalet Şarj" olarak bilinen, enerjinin tüketildiği ancak faturalandırılmadığı durumlara benzer).
Bu manipülasyon, sistemde kasıtlı olarak tutarsız veya eksik kayıtların oluşmasına neden olur. Kayıtlar, şarj işlemini yapan kullanıcıyı ve alınan enerjiyi doğru şekilde eşleştiremiyorsa veya sahte veriler içeriyorsa, bu duruma Kör Kayıt (Blind Logging) denir. Denetim sırasında, hem EVSE'nin yerel kayıtları hem de CSMS'teki kayıtlar, sahtekarlığı ortaya çıkarmakta yetersiz kalabilir.

4. Alınabilecek Önlemler

"Kapasite Sahtekarlığı" senaryosu, EVSE'nin dahili verilerinin (SoC ve Sayaç Değerleri) bütünlüğünü hedeflediği için, önlemler donanım, yazılım ve iletişim katmanlarını kapsamalıdır:

A. Donanım ve Firmware Bütünlüğü İçin Önlemler
1. Güvenli Önyükleme (Secure Boot) Mekanizmaları: EVSE'nin açılışında yüklenen firmware'in (yazılımın) üretici tarafından kriptografik olarak imzalanmış olup

olmadığının kontrol edilmesi zorunludur. Bu, **Debug Backdoor Anomalisi** gibi yetkisiz erişim yollarıyla cihaza yüklenmiş kötü amaçlı yazılımların çalıştırılmasını engeller.
2. Kritik Sensör Verilerinin İzolasyonu: Şarjı başlatan/bitiren ve Sayaç Değerlerini (MeterValues) tutan fiziksel sensörler, ana işlemci ve iletişim modülünden izole edilmeli ve bu verilere erişim, donanımsal güvenlik modülleri (TPM/HSM) aracılığıyla korunmalıdır.
3. Fiziksel Güvenlik ve Kurcalama Tespiti (Tamper Detection): EVSE kasalarının fiziksel olarak açılmasını veya sensörlere doğrudan müdahale edilmesini engelleyecek kurcalama algılama mekanizmaları (mikro anahtarlar veya optik sensörler) kullanılmalıdır.

B. İletişim ve Protokol Güvenliği İçin Önlemler
1. Uçtan Uca Şifreleme (TLS/DTLS): EVSE ile Merkezi Şarj İstasyonu Yönetim Sistemi (CSMS) arasındaki tüm iletişimin (OCPP) şifreli kanallar (TLS/DTLS) üzerinden yapılması zorunludur.
2. Veri Tutarlılığı Kontrolü (Çift Kontrol): Sayaç verileri (MeterValues) CSMS'e gönderilirken, sadece tek bir kaynaktan değil, aynı zamanda aracın kendisinden (eğer mümkünse) veya şarjın başladığı/bittiği anlara ait zaman damgaları ve seans kimlikleri gibi ek verilerle karşılaştırılarak tutarsızlıklar tespit edilmelidir.
3. Anomali Tespiti ve Zaman Senkronizasyonu Kontrolü: CSMS, belirli bir süre zarfında aşırı hızlı SoC artışı gibi fiziksel olarak imkansız olan veri raporlamalarını anomali olarak etiketlemelidir. Ayrıca, **Zaman Senkronizasyonu Manipülasyonu** senaryosunu engellemek için, tüm cihazların NTP (Network Time Protocol) gibi güvenilir ve şifreli kaynaklar üzerinden zamanlarını senkronize etmesi sağlanmalıdır.

C. Yazılım ve Yönetim Önlemleri
1. Yetkilendirme ve Erişim Yönetimi: EVSE'nin sadece yetkili kullanıcıların ve sistem yöneticilerinin erişimine açık olması sağlanmalıdır. Uzaktan erişim için güçlü kimlik doğrulama (MFA) kullanılmalı ve varsayılan parolalar kesinlikle değiştirilmelidir.
2. Kayıt ve Denetim (Logging): Tüm kritik olaylar (şarj başlangıcı/bitişi, firmware güncellemeleri, hata kodları) zaman damgasıyla birlikte yerel olarak ve merkezi sistemde (CSMS) yedeklenmelidir. **Kör Kayıt** senaryolarını önlemek için, bu logların değiştirilemez bir formatta saklanması (Write Once, Read Many – WORM) veya dağıtık defter teknolojileriyle bütünlüğünün sağlanması önerilir.

Kapsamlı Özet

Kapasite Sahtekarlığı, bir EVSE'nin içten zehirlenmesiyle, hizmetin kendisinin bir illüzyon haline getirilmesine dayanır. Enerji hırsızlığının sadece bir finansal kayıp değil, aynı zamanda hizmet kalitesinin kasıtlı olarak düşürülmesi ve kullanıcı deneyiminin sabote edilmesi anlamına geldiği nadir bir anomali türüdür.