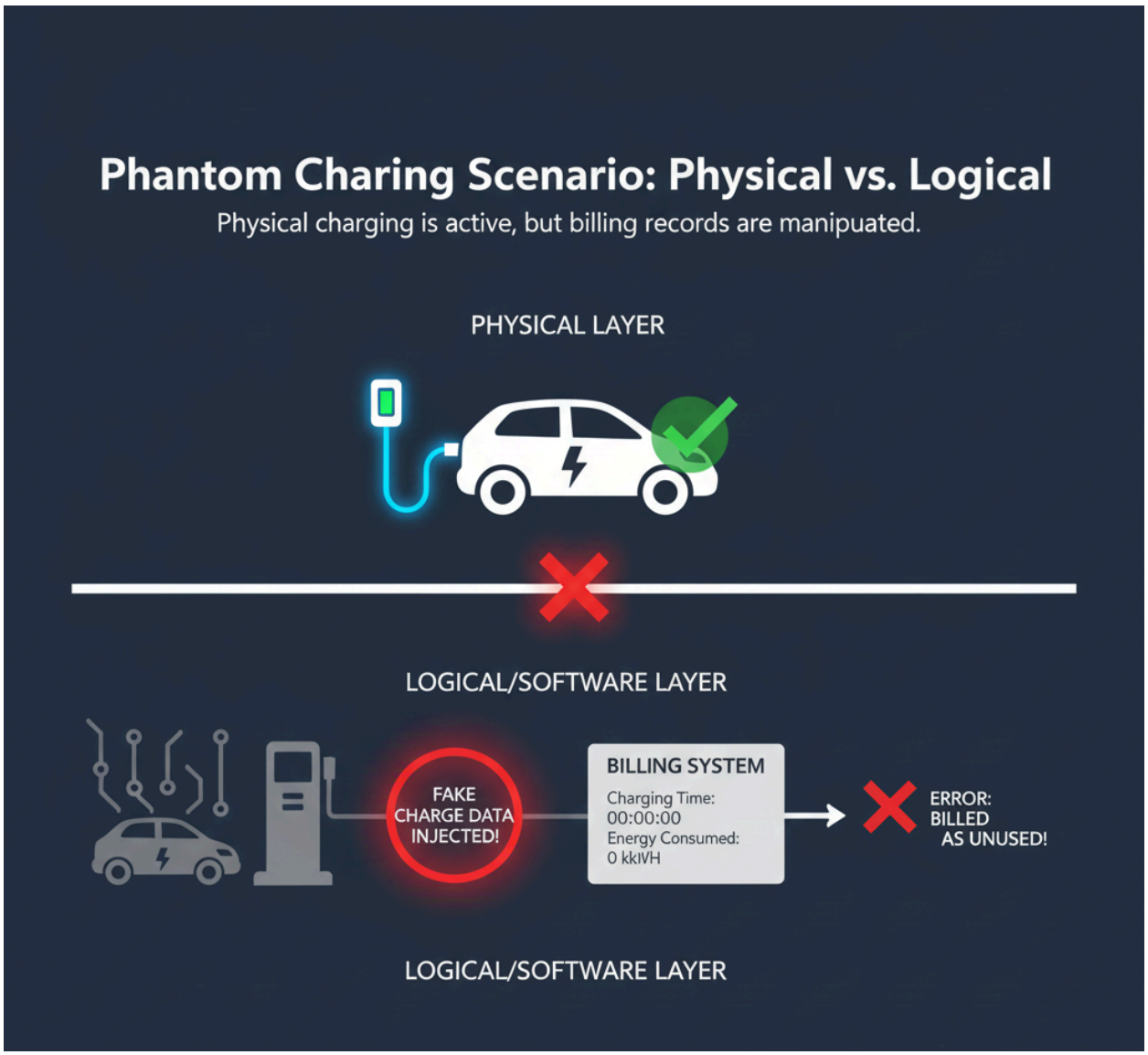
Anomali Senaryosu 1

"Hayalet Şarj" ile Enerji Hırsızlığı

Tarih: 20.10.2025
Versiyon: 1.0
Hazırlayan: Hüseyin Enes Ertürk



1. Senaryonun Amacı ve Kapsamı

Amaç: Bu senaryonun temel amacı, bir Şarj Noktası Operatörünün (CPO) faturalandırma ve yönetim altyapısını atlatarak, yetkisiz bir şekilde elektrikli bir aracı şarj etme ve bu yolla finansal kazanç sağlama (enerji hırsızlığı) yöntemini detaylandırmaktır.

Kapsam: Senaryo, Şarj İstasyonu (CP) ile Merkezi Yönetim Sistemi (CSMS) arasındaki OCPP iletişimini ve CP'nin dahili yazılım (bellenim) katmanını hedef alan birleşik bir siber saldırıyı kapsamaktadır. Saldırı, hem kimlik taklidi (Spoofing) hem de veri manipülasyonu (Tampering) tekniklerini içermektedir.

2. Özet

"Hayalet Şarj", saldırganın iki aşamalı bir yöntemle şarj hizmetini istismar ettiği gelişmiş bir siber-fiziksel saldırı senaryosudur. İlk aşamada saldırgan, ağdaki zafiyetlerden faydalanarak kendini Merkezi Yönetim Sistemi (CSMS) gibi tanıtır ve hedef şarj istasyonunda yetkisiz bir şarj oturumu başlatır. İkinci ve kritik aşamada ise, şarj istasyonunun bellenimindeki bir güvenlik açığını kullanarak, tüketilen gerçek enerji miktarını gizleyen veya yanlış raporlayan bir yazılım değişikliği yapar.

Sonuç olarak, araç fiziksel olarak şarj olurken, CPO'nun kayıtlarına ya hiç enerji tüketilmemiş ya da önemsiz derecede az bir tüketim yapılmış gibi yansır. Bu durum, tespit edilmesi zor, doğrudan finansal kayba yol açan ve CPO'nun gelir modelini tehdit eden ciddi bir güvenlik ihlalidir.

3. STRIDE Tehdit Sınıflandırması

- **Spoofing (Taklit Etme):** Saldırgan, meşru bir CSMS'in kimliğine bürünerek şarj istasyonuna RemoteStartTransaction gibi yetkili komutlar gönderir.
- **Tampering (Kurcalama/Manipülasyon):** Saldırgan, şarj istasyonunun bellenimine müdahale ederek, CSMS'e gönderilen MeterValues (Ölçüm Değerleri) mesajlarının içeriğini yetkisiz bir şekilde değiştirir.
- **Repudiation (İnkar):** Saldırı başarılı olursa, CPO sisteminde geçerli bir faturalandırma kaydı oluşmadığı için, saldırgan işlemi gerçekleştirdiğini inkar edebilir.

4. Gerekli Koşullar ve İstismar Edilen Zafiyetler

Saldırının başarılı olması için aşağıdaki koşullardan bir veya daha fazlasının mevcut olması gerekir:

- **Zayıf Ağ Güvenliği:** OCPP iletişiminde karşılıklı kimlik doğrulaması (mutual authentication) sağlayan Güvenlik Profili 3'ün (TLS ile İstemci Tarafı Sertifikaları) kullanılmaması. Bu durum, Ortadaki Adam (MitM) saldırılarını ve CSMS taklidini mümkün

kılar.
- **Güvensiz Bellenim Güncelleme Süreci:** Şarj istasyonunun, kriptografik olarak imzalanmamış veya imza doğrulaması yapmadan bellenim güncellemelerini kabul etmesi.
- **Bellenimdeki Bilinen Zafiyetler:** Cihaz yazılımında uzaktan kod çalıştırmaya veya yetkisiz erişime izin veren bilinen bir güvenlik açığının (CVE) bulunması.
- **Veri Bütünlüğü Kontrolü Eksikliği:** Faturalandırma için kritik olan MeterValues gibi OCPP mesajlarının dijital olarak imzalanmaması.

5. Saldırı Yöntemleri ve Adım Adım Akış

Saldırgan Profili: Orta düzeyde teknik bilgiye sahip, ağ dinleme araçlarını kullanabilen ve bellenim analizi yapabilen bir siber suçlu veya grup.

Adım 1: Keşif ve Hazırlık
Saldırgan, halka açık şarj ağlarını tarayarak zayıf güvenlik profiline sahip veya bilinen bellenim zafiyetleri olan şarj istasyonlarını tespit eder. Hedef istasyonun bulunduğu ağa (örneğin, halka açık Wi-Fi) erişim sağlar.
Adım 2: Yetkisiz Oturum Başlatma (Spoofing Aşaması)

1. Saldırgan, hedef şarj istasyonu ile CSMS arasına girerek bir MitM saldırısı gerçekleştirir.
2. Kendisini CSMS olarak tanıtarak, sahte bir RemoteStartTransaction OCPP komutu oluşturur. Bu komut, kendi aracına ait bir idTag (kimlik etiketi) veya rastgele bir etiket içerebilir.
3. Komutu şarj istasyonuna gönderir. Zayıf kimlik doğrulama nedeniyle, şarj istasyonu bu komutu meşru kabul eder ve aracı şarj etmeye başlar.

Adım 3: Faturalandırma Verisini Manipüle Etme (Tampering Aşaması)

1. Şarj oturumu devam ederken, saldırgan önceden tespit ettiği bellenim zafiyetini istismar eder.
2. İstasyona, giden MeterValues mesajlarını yakalayan ve değiştiren küçük bir kod parçacığı (payload) enjekte eder.
3. **Siber-Fiziksel Ayrışma Noktası:**
    - **Fiziksel Katman (CAN-bus):** İstasyonun içindeki fiziksel sayaç, aracın çektiği enerjiyi (örneğin, 15 kWh) doğru bir şekilde ölçer ve bu bilgiyi periyodik olarak CAN-bus üzerinden ana kontrolcüye iletir.
    - **Yazılım Katmanı (OCPP):** Ana kontrolcüdeki kötü amaçlı kod, bu 15 kWh verisini alır, ancak CSMS'e göndereceği MeterValues mesajını oluşturmadan hemen önce bu değeri 0.01 kWh gibi sahte bir değerle değiştirir.
4. CSMS, manipüle edilmiş bu sahte veriyi alır ve faturalandırma sistemine işler.

6. Tespit Yöntemleri ve Anomali Göstergeleri

Bu saldırıyı tespit etmek için çok katmanlı bir yaklaşım gereklidir:

- **Protokoller Arası Korelasyon Analizi (En Etkili Yöntem):**
    - **Anomali:** CAN-bus üzerinden okunan fiziksel sayaç verileri ile OCPP MeterValues ile

raporlanan enerji verileri arasında büyük ve mantıksız bir fark olması.
    - **Uygulama:** Şarj istasyonlarından periyodik olarak ham sayaç verilerini (log olarak) toplayan ve bunları CSMS'teki faturalandırma verileriyle karşılaştıran bir denetim mekanizması oluşturmak.
- **Davranışsal Analiz ve Kural Tabanlı Uyarılar:**
    - **Anomali:** Bir şarj oturumunun belirli bir süredir (örneğin, 30 dakika) aktif olmasına rağmen raporlanan enerji tüketiminin sıfır veya ihmal edilebilir düzeyde kalması.
    - **Uygulama:** CSMS'te "Eğer durum == Şarj Oluyor VE süre > 30dk VE tüketim < 0.1 kWh ise alarm üret" gibi kurallar tanımlamak.
- **Bellenim Bütünlüğü İzleme:**
    - **Anomali:** Şarj istasyonunun çalışan belleniminin kriptografik özet (hash) değerinin, bilinen ve onaylanmış sürümün özet değeriyle eşleşmemesi.
    - **Uygulama:** Periyodik olarak uzaktan bellenim bütünlük kontrolleri yapmak.

7. Olası Etkiler

- **Finansal Etki:** CPO için doğrudan gelir kaybı ve enerji maliyetinin haksız yere üstlenilmesi. Saldırının ölçeği büyürse, bu durum şirketin kârlılığını ciddi şekilde etkileyebilir.
- **Operasyonel Etki:** Faturalandırma verilerinin güvenilirliğinin kaybolması, yanlış kapasite ve kullanım planlamasına yol açması.
- **İtibar Kaybı:** Saldırının kamuoyuna yansıması durumunda, müşterilerin ve yatırımcıların CPO'ya olan güveninin sarsılması.

8. Önlemler ve Azaltma Stratejileri

Bu tehdide karşı "Derinlemesine Savunma (Defense-in-Depth)" prensibi benimsenmelidir:

- **Ağ Güvenliğini Sağlama:**
    - **Zorunluluk:** Tüm şarj istasyonlarında, karşılıklı kimlik doğrulaması sağlayan OCPP Güvenlik Profili 3'ün (TLS 1.2/1.3 ve İstemci Sertifikaları) kullanımını zorunlu kılmak.
- **Cihaz Bütünlüğünü Koruma:**
    - **Güvenli Önyükleme (Secure Boot):** Cihazların yalnızca üretici tarafından imzalanmış, orijinal bellenim ile başlamasını sağlamak.
    - **İmzalı Bellenim Güncellemeleri:** Tüm bellenim güncellemelerinin kriptografik olarak imzalanmasını ve istasyonun bu imzayı doğrulamadan güncellemeyi reddetmesini sağlamak.
- **Veri Bütünlüğünü Garanti Altına Alma:**
    - **OCPP Mesaj İmzalama:** OCPP 2.0.1'in desteklediği "SignedMeterValues" özelliğini kullanarak, ölçüm verilerinin istasyon tarafından dijital olarak imzalanmasını ve CSMS'in bu imzayı doğrulamasını sağlamak.
- **"Sıfır Güven" Yaklaşımı:**
    - **Sunucu Tarafı Doğrulama:** CSMS'in, şarj istasyonundan gelen verilere körü körüne güvenmemesi. Gelen veriler üzerinde mantık kontrolleri (sanity checks) yaparak bariz anormallikleri (örneğin, 2 saatlik şarjda sıfır tüketim) otomatik olarak reddetmesi ve inceleme için işaretlemesi.