ANOMALİ SENARYOSU: "Dijital İkiz" Yaratımı ile İstasyon Taklidi ve Hizmet Engelleme

Hazırlayan: Alperen Yasemin

Hazırlanma Tarihi: 02.11.2025

Konu: Elektrikli Araç Şarj İstasyonu (EVSE) siber güvenliği, OCPP diagnostik (tanılama) ve provizyon (yapılandırma) protokol zafiyetleri kullanılarak ağ düzeyinde kimlik taklidi ve mantıksal hizmet engelleme (DoS) saldırıları.

1) Mantıksal İlişki ve Sistem Modeli

Bu senaryo, şarj işleminin kendisinden ziyade, şarj ağının "yönetim" ve "bakım" katmanlarındaki zafiyetlere odaklanmaktadır.

1. **OCPP (Open Charge Point Protocol):** EVSE (Şarj Noktası - CP) ile Merkezi Yönetim Sistemi (CSMS) arasındaki "arka uç" (back-end) iletişim protokolüdür.
2. **CSMS (Central System Management System):** Tüm şarj istasyonlarının (EVSE) bağlandığı, onları yöneten, izleyen, faturalandıran ve yapılandıran merkezi sunucudur.
3. **EVSE (Electric Vehicle Supply Equipment):** Şarj istasyonunun kendisidir. CSMS'e OCPP protokolü ile bağlanır.
4. **CSO (Charge Station Operator):** İstasyonların bakımından ve yapılandırılmasından sorumlu olan (genellikle CSMS'e web arayüzü üzerinden bağlanan) teknik operatör veya yönetici rolüdür.
5. **Kritik Protokol İşlevleri (Zafiyet Alanı):**
    - **Provisioning (B) / Diagnostics (N):** OCPP içindeki bu işlev blokları, istasyonun bakımı için kullanılır.
    - `GetConfiguration.req` (B06): Bir istasyonun tüm dahili konfigürasyon parametrelerini CSMS'e (veya yetkili operatöre) göndermesini sağlar.
    - `GetDiagnostics.req` (N01): İstasyonun detaylı log ve tanılama verilerini bir sunucuya yüklemesini tetikler.

2) Tehdit Modeli (STRIDE Analizi)

Bu senaryo, tek bir bilgi sızıntısı ile başlayan ve tüm sistemin bütünlüğünü bozan zincirleme bir saldırıyı modeler.

- **Saldırı Vektörü:** Zayıf yetkilendirilmiş OCPP bakım komutları (`GetConfiguration`). Saldırgan, düşük seviyeli bir Şarj İstasyonu Operatörü (CSO) hesabını ele geçirerek veya CSMS'i taklit ederek, bir istasyonun kritik kimlik bilgilerini sızdırır.
- **STRIDE Sınıflandırması:**
    - **Information Disclosure (Bilgi İfşası):** Saldırının ilk adımıdır. `GetConfiguration.req` komutu kötüye kullanılarak, istasyonun CSMS'e

bağlanmak için kullandığı `Identity` (Kimlik) ve `BasicAuthPassword` (Temel Kimlik Doğrulama Şifresi) gibi en kritik bilgileri ifşa edilir. Bu durum `TC-4 (Conflict of interest of sensitive information)` tehdidini oluşturur.
    - **Spoofing (Taklit):** Saldırgan, elde ettiği bu kimlik bilgileriyle, *gerçek istasyonu* birebir taklit eden sanal bir EVSE ("Dijital İkiz") oluşturur ve bunu CSMS'e bağlar. Bu, `CS spoofing` (İstasyon taklidi) tehdididir.
    - **Denial of Service (Hizmet Engelleme):** Saldırganın "dijital ikizi", CSMS'e sürekli olarak sahte `StatusNotification(Faulted)` (Arızalı) mesajları gönderir. CSMS, gerçek istasyonun çalışır durumda olmasına rağmen, mobil uygulamalarda ve haritalarda onu "Arızalı" veya "Hizmet Dışı" olarak gösterir. Bu, `TC-3 (DoS to the CSs)` tehdidini tetikler.
    - **Tampering (Manipülasyon):** Saldırgan, CSMS'in "dijital ikiz" (sahte istasyon) ile mi yoksa "gerçek" istasyon ile mi konuştuğu konusundaki kafa karışıklığını istismar eder. Gerçek istasyona gitmesi gereken meşru `RemoteStartTransaction` komutlarını (bir "race condition" yaratarak) kendi sanal istasyonuna yönlendirebilir ve komut akışını manipüle edebilir.

3) Köprü Bileşenler (Bridge Components)

1. **Meşru Köprü (CSMS):** Normalde OCPP üzerinden tüm istasyonlarla iletişim kuran ve onları yöneten merkezi varlıktır.
2. **Gayrimeşru Köprü (Saldırganın Sanal EVSE Sunucusu):** Saldırganın kontrolündeki bir sunucu üzerinde çalışan ve çalınan kimlik bilgileriyle CSMS'e bağlanan sahte bir OCPP istemci yazılımıdır. Bu yazılım, gerçek istasyonun "dijital ikizi" olarak hareket eder.

4) Saldırı Senaryosu Uygulama Adımları

Aşama 0 (Keşif ve Hazırlık):

1. Saldırgan, bir sosyal mühendislik saldırısı (phishing) veya zayıf parola denemesi ile düşük yetkili bir Şarj İstasyonu Operatörü (CSO) hesabının web paneli giriş bilgilerini ele geçirir.
2. Saldırgan, bu paneli kullanarak veya doğrudan CSMS API'sine bağlanarak, hedef olarak seçtiği bir istasyona (ID: `IST-001`) bakar.

Aşama 1 (Veri Sızıntısı - Information Disclosure):

1. Saldırgan, ele geçirdiği CSO hesabı ile `IST-001` istasyonuna (zayıf yetkilendirilmiş) bir `GetConfiguration.req` (B06) komutu gönderir.
2. `IST-001` istasyonu, bu komutu meşru bir bakım talebi olarak algılar ve tüm konfigürasyonunu `GetConfiguration.conf` mesajıyla saldırgana (operatör paneli üzerinden) yanıtlar.

3. Saldırgan, bu yanıtın içinde OCPP Güvenlik Profili 1 kullanıldığını ve kritik bilgileri (`{"key": "Identity", "value": "IST-001"}` ve `{"key": "BasicAuthPassword", "value": "SuperS3cret!"}`) elde eder.

Aşama 2 (Klonlama - "Dijital İkiz" Yaratımı):

1. Saldırgan, kendi kontrolündeki bir sunucuya (IP: `185.x.x.x`) basit bir OCPP istemci betiği (script) kurar.
2. Bu betiği, Aşama 1'de çalınan `Identity: "IST-001"` ve `BasicAuthPassword: "SuperS3cret!"` bilgileriyle yapılandırır.
3. Sanal istasyon (`IST-001`), CSMS sunucusuna bağlanma talebi gönderir (`BootNotification.req`).

Aşama 3 (Anomali Başlangıcı - CSMS İkilemi):

1. CSMS, `IST-001` kimliğinden gelen `BootNotification` talebini (IP: `185.x.x.x`) alır. Kimlik bilgileri doğru olduğu için bağlantıyı kabul eder.
2. **ANOMALİ (Ağ Seviyesi):** CSMS'in oturum yönetim tablosunda artık `IST-001` kimliğine ait, *aktif* (ESTABLISHED) durumda iki farklı TCP bağlantısı görünür:
    - **Bağlantı 1 (Gerçek):** Kaynak IP `85.x.x.x` (Fiziksel istasyonun internet çıkış IP'si)
    - **Bağlantı 2 (Sahte):** Kaynak IP `185.x.x.x` (Saldırganın sunucusunun IP'si)

Aşama 4 (Hizmet Engelleme - DoS):

1. Her iki istasyon da (gerçek ve sanal) CSMS'e düzenli olarak `Heartbeat.req` (G02) göndermeye başlar.
2. Saldırgan, bu "Heartbeat çarpışmasını" (race condition) kendi lehine kullanır ve sanal istasyonundan (IP: `185.x.x.x`) CSMS'e `StatusNotification.req(connectorId: 1, status: Faulted, errorCode: InternalError)` mesajını gönderir.
3. CSMS'in durum makinesi (state machine), en son gelen `Heartbeat` ve `StatusNotification` mesajına göre istasyonun durumunu `Faulted` (Arızalı) olarak günceller.
4. **Sonuç:** Gerçek istasyon (IP: `85.x.x.x`) fiziksel olarak `Available` (Müsait) durumda olmasına ve `Heartbeat` göndermesine rağmen, CSMS'teki kaydı "Arızalı" olarak görünür. Kullanıcılar mobil uygulama veya harita üzerinden bu istasyonu kullanamaz. Gerçek istasyon, saldırgan tarafından dijital dünyada (CSMS üzerinde) izole edilmiştir.

5) Tespit Edilebilir Anomaliler ve Göstergeler

Bu saldırı, fiziksel gerçeklikle ağ kayıtları arasında belirgin ve mantıksal olarak imkansız çelişkiler yaratır:

1. **Anomali: "Aynı Kimlik, Çoklu Aktif IP" (Identity vs. IP Conflict):**

    - **Normal Veri:** Bir EVSE kimliği (`IST-001`), `CSMS`'e *sadece bir* TCP/IP oturumu (kaynak IP adresi) ile bağlı olmalıdır. Bağlantı koparsa, yeni bir IP'den *tekrar* bağlanabilir, ancak *aynı anda* (eş zamanlı) iki IP'den `ESTABLISHED` (Kurulmuş) durumda olamaz.
    - **Anormal Veri:** `CSMS`'in oturum (session) yönetim tablosunda, `IST-001` kimliğine ait, *aktif* durumda olan iki farklı TCP bağlantısı ve iki farklı kaynak IP adresi (`85.x.x.x` ve `185.x.x.x`) görülür. Bu, fiziksel olarak imkansızdır ve bir "dijital ikiz" (`Spoofing`) saldırısının kesin bir göstergesidir.
2. **Anomali: "Heartbeat Çarpışması" (Heartbeat Race Condition):**
    - **Normal Veri:** `CSMS`, `IST-001`'den tanımlanmış periyotlarda (örn. her 60 saniyede bir) *tek bir* `Heartbeat.req` alır.
    - **Anormal Veri:** `CSMS` logları, `IST-001` kimliğinden, beklenen periyodun çok dışında (örn. 60 saniyelik periyotta 30. saniyede de) veya mükerrer (`Heartbeat`) mesajlar aldığını gösterir. Bu durum, CSMS'in durum makinesinin sürekli olarak "en son konuşan" IP'yi meşru kabul etmesine ve kararsızlığa yol açar.
3. **Anomali: "Durum Çelişkisi" (Status Flapping / Conflicting Reports):**
    - **Normal Veri:** Bir istasyonun durumu (`Available`, `Charging`, `Faulted`) mantıksal bir sıra izler.
    - **Anormal Veri:** `CSMS` logları, aynı istasyon (`IST-001`) için *farklı IP adreslerinden* gelen ve birbiriyle çelişen durum bildirimlerini kaydeder:
        - `19:30:01` (IP: `85.x.x.x` - Gerçek): `StatusNotification(Available)`
        - `19:30:05` (IP: `185.x.x.x` - Sahte): `StatusNotification(Faulted)`
        - `19:31:01` (IP: `85.x.x.x` - Gerçek): `StatusNotification(Available)`
        - `19:31:05` (IP: `185.x.x.x` - Sahte): `StatusNotification(Faulted)`
    - Bu "durum çırpınması" (flapping), bir DoS saldırısının veya ciddi bir ağ yapılandırma hatasının değil, aktif bir `Spoofing` saldırısının göstergesidir.

6) Savunma ve İyileştirme Stratejileri

1. **OCPP Kimlik Doğrulama (Temel Çözüm):** `OCPP 1.6`'da kullanılan `BasicAuth` (Güvenlik Profili 1) derhal terk edilmelidir. `OCPP 2.0.1`'in sunduğu **Güvenlik Profili 3 (Security Profile 3)** zorunlu kılınmalıdır. Bu profil, `BasicAuth` yerine, her istasyon için benzersiz olan ve donanımsal olarak (örn. TPM/Secure Element içinde) saklanan istemci tarafı TLS sertifikaları ile karşılıklı kimlik doğrulama (mTLS) kullanır. Saldırgan `BasicAuth` şifresini çalsa bile, istasyona ait özel anahtarı (private key) çalamayacağı için klonlama yapamaz.
2. **CSMS Mantıksal Güvenliği (Anomali Tespiti):** `CSMS` yazılımı, **"Aynı Kimlik, Çoklu Aktif IP" (Anomali 1)** durumunu tespit etmek için acilen programlanmalıdır. Bir istasyon kimliği, zaten `ESTABLISHED` bir bağlantısı varken ikinci bir IP'den

bağlanmaya çalışırsa, CSMS *her iki* bağlantıyı da derhal sonlandırmalı ve operatöre (CSO) kritik bir "Potansiyel İstasyon Klonlama Saldırısı" alarmı göndermelidir.

3. **Rol Tabanlı Erişim Kontrolü (RBAC) (Zafiyeti Azaltma):** `GetConfiguration` gibi tehlikeli "diagnostik" ve "provizyon" komutları, normal CSO hesaplarının yetkisi dışına çıkarılmalıdır. Bu komutlar, yalnızca yüksek ayrıcalıklı "Bakım" (Maintenance) hesaplarına (veya sadece belirli, güvenli IP aralıklarından gelen bağlantılara) kısıtlanmalıdır.