**Temel Makale-Senaryo**

**Ana Sorun (Problem Statement)**

OCPP protokolünün en güncel sürümü olan OCPP-v2.0.1, yeni güvenlik önlemleri içermesine rağmen, bu yeni işlevlerin (özellikle mikro şebekelere bağlı şarj istasyonlarında) siber ve fiziksel tehditlere karşı hâlâ savunmasız olup olmadığının belirsizliğidir. Yazarlar, protokolün gelişmesine rağmen potansiyel güvenlik risklerinin devam edip etmediğini sorgulamaktadır.

**Ana Teknik Terimler (Terminoloji)**

* **Industry 4.0 (Endüstri 4.0):** Enerji sektöründe otomasyon ve dağıtım.
* **Electric Vehicle (EV) (Elektrikli Araç)**
* **Charging Infrastructures (Şarj Altyapıları)**
* **Charging Stations (CSs) (Şarj İstasyonları)**
* **OCPP (Open Charge Point Protocol):** Şarj istasyonları için standart iletişim protokolü (özellikle **v.2.0.1**).
* **Microgrids (Mikro şebekeler):** Küçük ölçekli, bağımsız çalışabilen enerji şebekeleri.
* **Cyber and physical threats (Siber ve fiziksel tehditler)**
* **STRIDE:** Bir tehdit analizi ve modelleme metodolojisi.
* **DREAD:** Bir risk değerlendirme metodolojisi.
* **Cybersecurity (Siber güvenlik)**
* **Risk management (Risk yönetimi)**
* **V2G (Vehicle-to-Grid):** Çift yönlü şarj (araçtan şebekeye enerji aktarımı).
* **Wireless Charging (Kablosuz Şarj)**

**Çalışmanın Sınırlılıkları (Limitations)**

Yazarlar, bu makalenin kapsamını şu şekilde sınırlamıştır:

1. Çalışma, mevcut OCPP-v2.0.1 protokolü kapsamındaki (tek yönlü) şarj altyapılarına odaklanmıştır.
2. Çalışma, gelişmekte olan **çift yönlü şarj ağlarını (V2G)** kapsamamaktadır.
3. Çalışma, **kablosuz şarj** senaryolarını kapsamamaktadır.

**Gelecek Çalışmalar ve Belirlenen Boşluklar (Gaps)**

1. **Önerilen Gelecek Çalışmalar:**
   * Analizin, **çift yönlü şarj (V2G)** ağlarını içerecek şekilde genişletilmesi.
   * Analizin, **kablosuz şarj (wireless charging)** senaryolarını içerecek şekilde genişletilmesi.
2. **Literatürdeki Boşluk (Gap):**
   * Yazarlar, bu iki yeni senaryonun (V2G ve kablosuz şarj) getirdiği **yeni tehditlerin**, **elektroniklerin**, **kontrol mekanizmalarının** ve **güç akışlarının (power flows)** literatürde **henüz analiz edilmemiş** olduğunu vurgulamaktadır.

**Örneklerle Durumu Kavrayalım ;**

**1. V2G (Vehicle-to-Grid / Araçtan Şebekeye)**

**Standart Şarj (G2V - Grid-to-Vehicle):** Bu, şu anki sistemdir. Bir otoyoldaki "tek yönlü" bir yol gibidir. Elektrik, şebekeden (Grid) araca (Vehicle) akar. Arabanız bir "tüketici"dir.

**V2G (Vehicle-to-Grid) Senaryosu:** Bu senaryoda, otoyol "çift yönlü" hale gelir. Arabanızın bataryası sadece enerji tüketen değil, aynı zamanda **enerji depolayan ve satan** bir birime dönüşür.

**Örnek (Ahmet'in Akıllı Evi):**

1. **Gündüz (Pahalı Tarife):** Ahmet işteyken, evindeki güneş panelleri elektrik üretir. Bu elektriği şebekeye satmak yerine, evinin garajındaki **çift yönlü (bidirectional) şarj cihazına** bağlı olan elektrikli arabasının bataryasında depolar.
2. **Akşam (Pik Saatler - En Pahalı Tarife):** Saat 19:00'da Ahmet evdedir. Herkes evinde ışıkları, fırını, televizyonu açar. Şebeke üzerindeki yük (talep) tavan yapar ve elektriğin fiyatı en yüksek seviyededir.
3. **V2G Devreye Girer:** Ahmet'in akıllı ev sistemi, şebekeden pahalı elektrik çekmek yerine, OCPP protokolü üzerinden şarj cihazına bir komut gönderir: "Şebekeye enerji sat" (Discharge).
4. **Sonuç:** Ahmet'in arabası, gündüz depoladığı ucuz (hatta bedava) güneş enerjisini, akşam pahalı fiyattan şebekeye geri satar. Arabası, evi için bir "jeneratör" veya "powerbank" görevi görür ve Ahmet para kazanır.

**Neden Yeni Güvenlik Boşluğu Yaratıyor?**

* **Yeni Kontrol Akışı:** Artık komut sadece "Şarj Et" değil. "Deşarj Et", "Şu kadar ($X) fiyata ulaşınca sat", "Batarya %30'un altına düşerse satmayı durdur" gibi onlarca yeni ve karmaşık komut var.
* **Makalenin İşaret Ettiği Tehdit:** Bir hacker, OCPP üzerinden bu "Deşarj Et" komutunu ele geçirirse ne olur?
  + **Grid'e Saldırı (Enerji Tehdidi):** Hacker, bir mahalledeki 1.000 araca aynı anda "Şebekeye tüm gücünüzü boşaltın!" komutu gönderebilir. Bu ani ve beklenmedik güç dalgalanması, yerel trafoları yakabilir ve şebekeyi çökertebilir (Bu, makalenin bahsettiği **"enerji"** odaklı bir tehdittir).
  + **Kullanıcıya Saldırı (Kontrol Tehdidi):** Hacker, sizin sabah 07:00'de uzun yola çıkacağınızı bilir ve gece gizlice arabanızın tüm şarjını şebekeye boşaltır. Sabah arabanızı boş bulursunuz (Bu da **"kontrol"** odaklı bir tehdittir).

**2. Kablosuz Şarj (Wireless Charging)**

**Standart Şarj (Kablolu):** Fiziksel bir bağlantı vardır. Arabanızı bir kabloyla istasyona bağlarsınız. Güvenlik, büyük ölçüde bu fiziksel kablo ve içindeki pinler üzerinden sağlanır.

**Kablosuz Şarj Senaryosu:** Fiziksel kablo yoktur. Arabanızı, yere gömülü bir şarj pedinin (plakasının) üzerine park edersiniz. Enerji, manyetik indüksiyon yoluyla "havadan" araca aktarılır.

**Örnek (Ayşe'nin Otoparkı):**

1. **Park Etme:** Ayşe, bir AVM otoparkında kablosuz şarj destekli bir yere park eder. Arabasının altındaki alıcı plaka, yerdeki verici plaka ile hizalanır.
2. **Kimlik Doğrulama (İletişim):** Ayşe'nin arabası, şarj işlemini başlatmak için yerdeki ped ile kablosuz olarak (örneğin Wi-Fi, NFC veya Bluetooth üzerinden) "konuşur". Arabası, "Ben Ayşe'nin arabasıyım, üyelik numaram bu, şarja hazırım" der.
3. **Şarj Başlangıcı:** Ped, bu bilgiyi merkezi sisteme (CSMS) iletir, onay alır ve yüksek güçte enerji aktarımını başlatır.

**Neden Yeni Güvenlik Boşluğu Yaratıyor?**

* **Yeni Elektronikler:** Artık devrede sadece kablolar değil, indüksiyon bobinleri, hizalama sensörleri ve kablosuz iletişim modülleri var.
* **Makalenin İşaret Ettiği Tehdit:** Fiziksel kablo yerine havadan giden sinyallere güvendiğimiz için:
  + **Sinyal Bozma (Jamming):** Bir saldırgan, basit bir sinyal bozucu (jammer) ile araba ve ped arasındaki o ilk "el sıkışma" (handshake) sinyalini engelleyebilir. Ayşe arabasını doğru park etse bile şarj işlemi asla başlamaz (Bu bir **Denial of Service - Hizmet Reddi** saldırısıdır).
  + **Ortadaki Adam (MITM):** Daha tehlikelisi; saldırgan, AVM otoparkında sahte bir Wi-Fi sinyali yayabilir.
    1. Ayşe'nin arabası şarj pedine bağlanmaya çalışırken, aslında saldırganın dizüstü bilgisayarına bağlanır.
    2. Saldırgan, Ayşe'nin kimlik (ödeme) bilgilerini kopyalar.
    3. Sonra bu bilgileri gerçek şarj pedine iletir.
    4. **Sonuç:** Ayşe şarj olduğunu zannederken, saldırgan onun oturum (session) bilgilerini çalmıştır ve belki de o gittikten sonra kendi arabasını Ayşe'nin hesabından şarj edecektir.
  + **Güvenlik Tehdidi (Safety):** Bu pedler çok yüksek güç aktarır. Pedin üzerinde "yabancı bir metal cisim" (kedi, konserve kutusu, anahtar) olup olmadığını algılayan sensörler vardır. Bir hacker bu sensör verisini manipüle edip "Üzeri temiz" derse ve sistem metal varken çalışırsa, o metal aşırı ısınıp yangın çıkarabilir.