OCPP Protokolü ve Elektrikli Araç Şarj Ekosisteminde Güvenlik Mimarisi: Kapsamlı SWOT Analizi ve Stratejik Öngörüler

Yönetici Özeti

Küresel enerji altyapısının hızla dönüşümü ve ulaşım sektörünün elektrifikasyonu, elektrikli araç (EA) şarj altyapısını modern şehirciliğin ve ulusal enerji güvenliğinin merkezi bir bileşeni haline getirmiştir. Bu dönüşümün kalbinde, Şarj İstasyonları (CS) ile Şarj İstasyonu Yönetim Sistemleri (CSMS) arasındaki iletişimi sağlayan de facto standart olan Açık Şarj Noktası Protokolü (Open Charge Point Protocol - OCPP) yer almaktadır. Endüstri, erken benimseme aşamasından kitlesel yaygınlaşma evresine geçerken, bu sistemlerin siber güvenliği çevresel bir endişe olmaktan çıkıp kritik altyapı güvenliğinin temel taşı haline gelmiştir.

Bu rapor, OCPP tabanlı ekosistemlerin güvenlik duruşunun, stratejik bir SWOT (Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler) çerçevesi üzerinden gerçekleştirilen kapsamlı bir analizini sunmaktadır. Analiz, protokolün evrimsel sürecini, özellikle 2025 yılında yayınlanan OCPP 2.1 sürümünün getirdiği yenilikleri ve mevcut OCPP 1.6J altyapısının barındırdığı sistemik riskleri derinlemesine irdelemektedir. Ulaşım ve enerji sektörlerinin Araçtan Şebekeye (Vehicle-to-Grid - V2G) teknolojileri aracılığıyla yakınsaması, Yanıltıcı Veri Enjeksiyonu Saldırılarından (FDIA) şebeke istikrarını bozmayı hedefleyen botnet saldırılarına kadar uzanan yeni ve karmaşık saldırı vektörlerini ortaya çıkarmaktadır.

Aşağıdaki bölümlerde, akademik araştırmalar, endüstriyel teknik raporlar ve standart dokümantasyonlarından elde edilen veriler sentezlenerek, EA şarj güvenliğinin fiziksel, siber ve siber-fiziksel boyutları granüler bir düzeyde değerlendirilmiştir. Yapay Zeka (YZ) ve Blokzincir teknolojilerinin saldırı tespiti ve merkeziyetsiz güven mekanizmalarındaki potansiyel rolleri tartışılırken, organize siber suçlar ve devlet destekli tehdit aktörlerinin oluşturduğu riskler stratejik bir perspektifle ele alınmıştır.

1. Elektrikli Araç Şarj Ekosisteminin Mimari Temelleri ve Varlık Analizi

OCPP protokolünün güvenlik etkilerini tam olarak kavrayabilmek için, protokolün içinde çalıştığı mimariyi ve bu mimariyi oluşturan bileşenlerin birbirleriyle olan karmaşık etkileşimlerini yapıbozuma uğratmak gerekmektedir. Elektrikli araç şarj ekosistemi, ağır elektrik mühendisliği prensipleri ile sofistike bilgi teknolojilerinin entegrasyonunu gerektiren, çok katmanlı bir Siber-Fiziksel Sistem (CPS) olarak tanımlanmaktadır. Bu sistemin güvenliği, en zayıf halkasının güvenliği kadar güçlüdür ve bu halkalar fiziksel donanımdan bulut tabanlı yönetim panellerine kadar uzanmaktadır.

1.1 Çekirdek Varlıklar ve İletişim Yolları

OCPP tabanlı bir sistemin mimarisi, her biri güvenlik grafiğinde kritik bir düğümü temsil eden çeşitli varlıklar tarafından tanımlanır. Bu varlıkların her biri kendine özgü saldırı yüzeylerine ve koruma gereksinimlerine sahiptir.

Elektrikli Araç Tedarik Ekipmanı (EVSE), genellikle "şarj cihazı" veya "şarj ünitesi" olarak adlandırılan uç cihazdır. Fiziksel olarak elektrikli aracı şebekeye bağlayan arayüzdür. Modern uygulamalarda EVSE, sadece basit bir güç çıkışı değil, aynı zamanda enerji ölçümü yapan, kullanıcı kimlik doğrulaması gerçekleştiren, karmaşık algoritmalar çalıştıran ve sürekli veri iletimi sağlayan akıllı bir IoT cihazıdır.[1] Güvenlik açısından EVSE, fiziksel olarak halka açık alanlarda bulunması nedeniyle kurcalanmaya (tampering) en açık bileşendir.

Şarj İstasyonu (CS), bir veya daha fazla EVSE'yi yöneten merkezi birimdir. OCPP protokolünü kullanarak arka ofis sistemleriyle konuşan iletişim kontrolcüsünü barındırır. Şarj profillerinin uygulanması, yerel yetkilendirme önbelleklerinin yönetilmesi ve donanım yazılımı (firmware) güncellemelerinin işlenmesi CS'nin sorumluluğundadır. CS, yerel ağ ile geniş alan ağı (WAN) arasında bir köprü görevi görür ve bu nedenle ağ tabanlı saldırıların ilk hedefidir.

Şarj İstasyonu Yönetim Sistemi (CSMS), operasyonun merkezi beynidir. Genellikle bulut tabanlı olan CSMS, kullanıcı hesaplarını, faturalandırmayı, şarj oturumlarını ve şarj ağı genelindeki cihazların sağlığını yönetir. CSMS, OCPP aracılığıyla CS'ye komutlar gönderir. Bir CSMS'in ele geçirilmesi, ona bağlı binlerce şarj istasyonunun kontrolünün saldırganın eline geçmesi anlamına gelir ki bu, şebeke güvenliği için katastrofik sonuçlar doğurabilir.[1]

Enerji Yönetim Sistemi (EMS), akıllı şarj uygulamalarında kritik bir bileşendir. EMS, yerel şebeke kısıtlamalarını (örneğin, bir binanın veya trafonun maksimum yük kapasitesini) izler ve aşırı yüklenmeleri önlemek için dinamik şarj profilleri oluşturur. OCPP 2.1 ile birlikte EMS'nin rolü daha da belirginleşmiş, Dağıtık Enerji Kaynakları (DER) kontrolü kapsamında güneş panelleri ve batarya depolama sistemleri ile entegre çalışabilir hale gelmiştir.[3]

Dağıtım Sistemi Operatörü (DSO), elektriğin fiziksel teslimatından sorumlu olan kuruluştur. DSO, şebeke olaylarını, örneğin talep yanıtı gerektiren tepe yük uyarılarını bildirmek için CSMS ile (ve giderek artan bir şekilde doğrudan EMS ile) iletişim kurar.

1.2 Protokol Yığınında OCPP'nin Rolü ve İletişim Dinamikleri

OCPP, OSI modelinin uygulama katmanında çalışır ve temel işlevi CS ile CSMS arasındaki mesajlaşmayı standardize etmektir. Bu standardizasyon, farklı donanım üreticilerinin cihazlarının aynı yönetim sistemi altında çalışabilmesini sağlayan "birlikte çalışabilirlik" ilkesinin temelidir.

Protokolün yönettiği temel fonksiyonlar şunlardır:

- **Oturum Yönetimi:** Şarj işlemlerinin başlatılması ve sonlandırılması (StartTransaction, StopTransaction). Bu mesajlar, faturalandırma için kritik olan sayaç değerlerini ve kimlik bilgilerini taşır.
- **Cihaz Yönetimi:** Şarj cihazı parametrelerinin yapılandırılması (ChangeConfiguration), arıza teşhisi (diagnostics) ve donanım yazılımı güncellemeleri.
- **Akıllı Şarj:** Bir elektrikli aracın herhangi bir anda ne kadar güç çekebileceğini belirleyen şarj profillerinin iletilmesi (SetChargingProfile).

OCPP, alttaki taşıma katmanından bağımsız olsa da, pratikte TCP/IP protokol yığınına sıkı sıkıya bağlıdır. Erken sürümler (1.5 ve 1.6 SOAP) HTTP üzerinden Basit Nesne Erişim Protokolü (SOAP) kullanırken, modern ve baskın uygulamalar (1.6J, 2.0.1 ve 2.1) WebSockets (WSS) üzerinden JSON kullanmaktadır. WebSockets'e geçiş, sunucunun istemciye (şarj cihazına) güvenlik duvarlarını aşarak doğrudan komut gönderebilmesini sağladığı için ölçeklenebilirlik açısından hayati bir adım olmuştur. Ancak bu mimari değişim, güvenlik yükünü tamamen WebSocket uygulamasına ve alttaki TLS şifrelemesine kaydırmıştır.[1]

1.3 OCPP Protokolünün Evrimsel Güvenlik Süreci

OCPP'nin gelişim süreci, endüstrinin siber güvenlik risklerine karşı olgunlaşma sürecini yansıtmaktadır. Her yeni sürüm, önceki nesillerin güvenlik açıklarını kapatmayı hedefleyen özelliklerle donatılmıştır, ancak eski sürümlerin yaygınlığı "miras sistem" (legacy) sorununu derinleştirmektedir.

OCPP 1.6 (2015): Halen dünyadaki şarj istasyonlarının büyük çoğunluğunda kullanılan sürümdür.[6] Orijinal spesifikasyonda güvenlik, tasarımın bir parçası olmaktan ziyade sonradan eklenen bir düşünceydi. Güvenlik özellikleri, daha sonra yayınlanan "OCPP 1.6 Security Whitepaper" ile protokole yamanmıştır. Ancak, birçok 1.6J uygulaması hala güvenli WebSockets (wss://) yerine şifrelenmemiş WebSockets (ws://) kullanmakta, bu da trafiğin ağ üzerinde kolayca dinlenmesine ve manipüle edilmesine neden olmaktadır.[7]

OCPP 2.0.1 (2020): Güvenlik mimarisinde köklü bir değişiklik yapılmıştır. "Güvenlik Profilleri" kavramı getirilerek TLS kullanımı zorunlu hale getirilmiş ve güvenlik seviyeleri standartlaştırılmıştır. Ayrıca, güvenli donanım yazılımı güncellemeleri, güvenlik günlüğü tutma (logging) ve araç üzerinde kurulu sertifikalarla kimlik doğrulaması sağlayan ISO 15118 (Plug & Charge) desteği eklenmiştir.[1]

OCPP 2.1 (2025): Ocak 2025'te yayınlanan bu en yeni sürüm, V2X (Araçtan Her Şeye) teknolojisine odaklanmaktadır. Çift yönlü güç transferi ve Dağıtık Enerji Kaynakları (DER) kontrolü için yeni fonksiyonel bloklar eklenmiştir. OCPP 2.0.1 ile geriye dönük uyumlu olmakla birlikte, şebeke yönetimi ve enerji ticareti alanlarına genişlemesi, saldırı yüzeyini önemli ölçüde artırmakta ve daha sıkı güvenlik kontrollerini zorunlu kılmaktadır.[9] Özellikle yerel maliyet hesaplama ve güvenli dinamik QR kodları gibi özellikler, ödeme güvenliği açısından kritik yenilikler sunmaktadır.[12]

---

2. Güçlü Yönler (Strengths - İçsel Pozitif Faktörler)

SWOT analizinin "Güçlü Yönler" bileşeni, OCPP standardının, özellikle 2.0.1 ve 2.1 sürümlerinin, siber tehditlere karşı sunduğu yerleşik savunma mekanizmalarını ve mimari avantajlarını incelemektedir. Bu özellikler, Şarj Noktası Operatörlerine (CPO) dayanıklı bir altyapı inşa etmeleri için gerekli araç setini sağlamaktadır.

2.1 OCPP 2.0.1 ve 2.1'de Standartlaştırılmış Güvenlik Profilleri

Modern OCPP standartlarının en belirgin gücü, güvenliğin isteğe bağlı bir eklenti olmaktan

çıkarılıp zorunlu bir standart haline getirilmesidir. OCPP 1.6'nın aksine, OCPP 2.0.1 ve 2.1, uyumluluk için net bir yol haritası sunan üç farklı güvenlik profili tanımlar.[1]

Profil 1, TLS ile şifrelemeyi zorunlu kılar ancak uygulama katmanında temel kullanıcı adı/şifre kimlik doğrulamasına izin verir. Bu, en temel seviyede bile iletişimin şifrelenmesini sağlayarak pasif dinleme saldırılarını (eavesdropping) engeller. Profil 2, şarj istasyonunun sunucuyu (CSMS) sertifikalar aracılığıyla doğrulamasını sağlayarak sahte sunuculara bağlanma riskini azaltır.

Ancak asıl güç, **Profil 3 (TLS ile Karşılıklı Kimlik Doğrulama - mTLS)** ile ortaya çıkar. Bu profil, hem sunucunun hem de istemcinin (şarj cihazının) geçerli sertifikalar sunmasını zorunlu kılar. Bu Karşılıklı TLS (mTLS) yapısı, Ortadaki Adam (Man-in-the-Middle - MitM) saldırılarını ve cihaz taklitçiliğini (impersonation) etkili bir şekilde nötralize eder. Bir saldırgan, şarj cihazının özel anahtarına sahip olmadan CSMS'e bağlanamaz veya şarj cihazını sahte bir sunucuya yönlendiremez.[1] Bu katmanlı yaklaşım, operatörlerin risk ve maliyet dengesini gözeterek güvenlik seviyelerini belirlemelerine olanak tanır.

2.2 Kriptografik Olarak İmzalanmış Donanım Yazılımı Güncellemeleri

Donanım yazılımı (firmware) güncellemeleri, güvenlik açıklarının kapatılması için hayati öneme sahipken, aynı zamanda kötü amaçlı yazılım enjeksiyonu için de yüksek riskli bir vektördür. OCPP 2.0.1 ve sonrası sürümler, bu riski güçlü bir savunma mekanizmasına dönüştürür. Protokol, donanım yazılımı imajlarının üretici tarafından dijital olarak imzalanmasını zorunlu kılar. Şarj istasyonu, güncellemeyi yüklemeden önce bu dijital imzayı bir genel anahtar (public key) kullanarak doğrular. Eğer imza geçersizse veya imaj üzerinde herhangi bir değişiklik yapılmışsa (örneğin, bir saldırgan tarafından arka kapı eklenmişse), şarj istasyonu güncellemeyi reddeder.[1] Bu mekanizma, tedarik zinciri saldırılarına karşı kritik bir bariyer oluşturur.

2.3 Gelişmiş Cihaz Yönetimi ve Güvenlik İzleme

Güvenliğin ön koşulu görünürlüktür. OCPP 2.0.1 ve 2.1, şarj istasyonunun iç durumunun granüler bir şekilde izlenmesine olanak tanıyan sofistike bir Cihaz Modeli (Device Model) sunar. OCPP 1.6'nın düz yapısının aksine, hiyerarşik Cihaz Modeli, bileşenleri (fanlar, sensörler, kontrolcüler) ayrı değişkenler olarak ele alır. Bu yapı, CSMS'in belirli sağlık metriklerini ve güvenlik günlüklerini sorgulamasını sağlar.

Özellikle SecurityEvent bildirimleri, şarj cihazının bir kurcalama girişimi, başarısız oturum açma denemesi veya geçersiz sertifika sunumu gibi güvenlik ihlallerini tespit ettiği anda arka ofise bildirmesini sağlar.[9] Bu yetenek, şarj cihazını pasif bir enerji dağıtıcısından, güvenlik ağının aktif bir sensörüne dönüştürür ve Saldırı Tespit Sistemlerinin (IDS) etkinliğini artırır.

2.4 ISO 15118 (Plug & Charge) Entegrasyonu

ISO 15118 standardının entegrasyonu, kimlik doğrulama güvenliği açısından devrim niteliğinde bir adımdır. Geleneksel RFID tabanlı sistemlerde, kimlik doğrulama belirteci (kartın UID'si) kolayca kopyalanabilirken [1], ISO 15118'in "Tak ve Şarj Et" (Plug & Charge - PnC) mekanizması, fiziksel belirteçleri doğrudan araca yüklenen dijital sertifikalarla değiştirir. EA şarj kablosunu taktığında, araç ile şarj cihazı arasında bir TLS el sıkışması gerçekleşir ve araç sözleşme sertifikasını sunar. Bu otomatik ve kriptografik değişim, bir RFID kartını veya akıllı telefon uygulamasındaki QR kodunu taklit etmekten çok daha zordur. Kimlik doğrulamanın aracın güvenli donanımına gömülmesi, kullanıcı kimlik bilgilerinin çalınma riskini minimize eder.[10]

---

3. Zayıf Yönler (Weaknesses - İçsel Negatif Faktörler)

Yeni sürümlerdeki ilerlemelere rağmen, elektrikli araç şarj ekosistemi, özellikle eski altyapının yaygınlığı ve uygulama karmaşıklığından kaynaklanan önemli içsel zayıflıklar barındırmaktadır.

3.1 Miras Sistemin Tuzağı: OCPP 1.6J Hakimiyeti ve Güvensiz WebSocket'ler

Mevcut güvenlik manzarasının en belirgin zayıflığı, OCPP 1.6 sürümünün ezici hakimiyetidir. 2024 yılı itibarıyla dünyadaki 1.6 milyondan fazla hızlı şarj cihazının büyük çoğunluğu hala 1.6 veya daha eski sürümleri kullanmaktadır.[17] Bu durum, "miras tuzağı" olarak adlandırılabilecek sistemik bir risk yaratmaktadır.

OCPP 1.6J, WebSockets kullanımını standartlaştırmıştır, ancak birçok uygulamada bu wss:// (şifreli) yerine ws:// (şifresiz) olarak yapılandırılmaktadır. Bu konfigürasyon hatası, tüm komut akışını, kullanıcı fatura verilerini ve kimlik doğrulama etiketlerini, aynı ağ segmentindeki

herhangi biri tarafından araya girilerek (Man-in-the-Middle) dinlenmeye ve manipüle edilmeye açık hale getirir.[8] 1.6'dan 2.0.1 veya 2.1'e geçiş, basit bir yazılım güncellemesi değildir; genellikle TLS yükünü kaldırabilmek için daha fazla bellek ve işlemci gücü gerektiren donanım yükseltmelerini ve yazılım yığınının tamamen yeniden yazılmasını gerektirir.[18]

3.2 Açık Anahtar Altyapısı (PKI) Yönetiminin Karmaşıklığı

OCPP 2.0.1 (Profil 3) ve ISO 15118'in sunduğu güçlü güvenlik, büyük ölçüde Açık Anahtar Altyapısına (PKI) dayanır. Ancak PKI yönetimi, operasyonel açıdan son derece karmaşıktır ve uzmanlaşmış siber güvenlik ekiplerine sahip olmayan birçok CPO için önemli bir zayıflık oluşturur.

Sertifika yaşam döngüsü yönetimi, binlerce sertifikanın (her şarj cihazı ve sunucu için birer adet) verilmesini, yenilenmesini ve iptal edilmesini kapsar. Bir sertifikanın süresinin dolması, şarj cihazının devre dışı kalmasına neden olur. Daha kritiği, Sertifika İptal Listelerinin (CRL) veya OCSP (Online Certificate Status Protocol) yanıtlarının doğru şekilde güncellenmemesi veya kontrol edilmemesi durumunda, güvenliği ihlal edilmiş özel anahtarlara sahip saldırganlar, meşru varlıklar gibi davranmaya devam edebilir.[1] Güven zincirinin kökü olan Kök Sertifika Otoritesinin (Root CA) güvenliği, tüm ağın güvenliğinin tek noktada toplanması anlamına gelir ve bu anahtarların korunması yüksek maliyetli Donanım Güvenlik Modülleri (HSM) gerektirir.

3.3 Güç Hattı İletişimi (PLC) ve Yan Kanal Zayıflıkları

Elektrikli araç ile EVSE arasındaki iletişim (özellikle CCS standardı kullanan DC hızlı şarj için), Güç Hattı İletişimi (PLC) üzerinden gerçekleşir. Araştırmalar, PLC'nin yan kanal saldırılarına (side-channel attacks) karşı oldukça savunmasız olduğunu göstermektedir.

Şarj kablosu üzerinden iletilen PLC sinyali, kabloyu bir anten gibi kullanarak elektromanyetik radyasyon yayar. Saldırganlar, şarj cihazına fiziksel olarak dokunmadan, birkaç metre uzaktan bu kablosuz yan kanalı dinleyerek (eavesdropping) özel verileri, aracın MAC adresini ve ISO 15118 kimlik doğrulama mesajlarını ele geçirebilirler.[20] Bu zayıflık, kullanıcı mahremiyetinin ihlaline ve potansiyel fatura dolandırıcılığına kapı aralar. OCPP 2.0.1 şifrelemeyi desteklese de, alttaki fiziksel katman (HomePlug Green PHY) genellikle ilk el sıkışma (SLAC) sırasında açık metin olarak çalışır ve bu da bir güvenlik penceresi yaratır.

3.4 EMS Güvenlik Boşluğu ve ARP Spoofing Riski

Mevcut literatür ve anketler, Enerji Yönetim Sistemi (EMS) için standartlaştırılmış güvenlik önlemlerinin eksikliğini kritik bir zayıflık olarak işaret etmektedir. OCPP 2.0.1 ve 2.1, EMS'den gelen akıllı şarj girdilerini desteklese de, EMS'nin kendisinin nasıl korunacağını katı bir şekilde tanımlamamıştır.[1]

EMS genellikle yerel bir ağ üzerinde bulunur ve şarj cihazları, bina güç sayacı ve internet arasında bir köprü görevi görür. EMS'nin güvenliğinin ihlal edilmesi (ki genellikle CSMS kadar sıkı korunmaz), saldırganın şarj ağına sahte veriler enjekte etmesine olanak tanır. Ayrıca, yerel ağ üzerindeki iletişimde Adres Çözümleme Protokolü (ARP) sahteciliği (ARP Spoofing) riski yüksektir. Saldırganlar, ARP zehirlenmesi yoluyla kendilerini ağ geçidi veya meşru bir şarj istasyonu gibi göstererek trafiği kendi üzerlerine çekebilirler. Araştırmalar, ARP Spoofing'in OCPP trafiğini kesmek, değiştirmek veya DoS saldırıları düzenlemek için etkili bir yöntem olduğunu ve mevcut sistemlerde buna karşı yeterli önlem alınmadığını göstermektedir.[22]

---

4. Tehditler (Threats - Dışsal Negatif Faktörler)

Tehditler bileşeni, sistemin zayıflıklarını istismar eden dış aktörleri ve saldırı vektörlerini analiz eder. EA şarj güvenliği tehdit manzarası, basit enerji hırsızlığından, ulusal şebekeyi hedef alan sofistike devlet destekli operasyonlara kadar genişlemiştir.

4.1 Siber-Fiziksel Saldırılar ve Şebeke Destabilizasyonu

En ciddi tehdit, EA şarj altyapısının elektrik şebekesini istikrarsızlaştırmak için bir silah olarak kullanılmasıdır. Bu, tek bir şarj cihazını devre dışı bırakmanın ötesinde, binlerce şarj cihazına eş zamanlı saldırı düzenlemeyi (botnet) içerir.

Anahtarlama Saldırıları (Switching Attacks): Bir saldırgan, bir CPO'nun CSMS'ini ele geçirerek veya OCPP yayın mekanizmasındaki bir zafiyeti kullanarak, binlerce EA'nın aynı anda şarjı başlatıp durdurmasını sağlayabilir. Bu durum, şebekede büyük yük salınımları (rezonans) yaratır. Eğer bu anahtarlama frekansı, şebeke jeneratörlerinin elektromekanik salınım frekansı ile eşleşirse, voltaj dengesizliğine, trafo merkezlerinin devre dışı kalmasına ve zincirleme elektrik kesintilerine (blackout) yol açabilir.[1] Bu senaryo, EA'ların şebeke üzerindeki toplam

yükü arttıkça daha da kritik hale gelmektedir.

Güç Aşırı Yüklemesi: Saldırganlar, akıllı şarj mantığını manipüle ederek güvenlik sınırlarını devre dışı bırakabilir. Şarj cihazlarına, şebeke kullanımının en yoğun olduğu saatlerde maksimum güç çekmeleri talimatı verilirse (EMS'nin onları kısıtlama yeteneği baskılanarak), dağıtım trafoları patlatılabilir ve fiziksel hasara yol açılabilir.[1]

4.2 Finansal Dolandırıcılık ve "Quishing"

EA şarjının ücretli bir hizmete dönüşmesi, finansal suçları da beraberinde getirmiştir.

Quishing (QR Phishing): Düşük teknolojili ancak hızla yayılan bir tehdittir. Birçok halka açık AC şarj cihazında ekran bulunmaz ve ödeme için statik QR kod etiketleri kullanılır. Saldırganlar, meşru QR kodunun üzerine kendi sahte kodlarını yapıştırır. Kullanıcı bu kodu tarattığında, kimlik bilgilerini ve kredi kartı verilerini çalan sahte bir ödeme portalına yönlendirilir. Kullanıcı aracı şarj edemediğini fark edene kadar verileri çalınmış olur.[26]

Fatura Dolandırıcılığı: "Sayaç Baypas Etme" (Meter Bypassing) veya OCPP üzerinden gönderilen MeterValues mesajlarını manipüle etme yoluyla, bir saldırgan CSMS'i gerçekte tüketilenden daha az enerji harcandığına inandırabilir. Tersine, "Maskeleme" (Masquerading) saldırısında, bir saldırgan meşru bir kullanıcının aracının kimliğini taklit ederek, kurbanın hesabı üzerinden kendi aracını şarj edebilir.[1]

4.3 Yanıltıcı Veri Enjeksiyonu Saldırıları (FDIA)

FDIA, sistemin veri bütünlüğünü hedef alan sofistike bir tehdittir. Sensörlerin veya iletişim kanalının ele geçirilmesiyle, saldırganlar CSMS veya EMS'ye makul görünen ancak sahte veriler enjekte ederler.[1]

- **Şarj Durumu (SoC) Sahteciliği:** Saldırgan, bağlı araçların batarya durumunu manipüle edebilir. Sistem, dolu bataryaların boş olduğuna inanırsa, onlara şarj önceliği vererek diğer kullanıcıları mağdur edebilir veya şebeke üzerindeki yükü gereksiz yere artırabilir.
- **Şebeke Durumu Sahteciliği:** Sahte voltaj veya frekans okumaları enjekte etmek, akıllı şarj algoritmalarını kandırarak gereksiz yük atma (hizmet reddi) veya şebeke stres altındayken güç çekme (istikrarsızlık) kararları almasına neden olabilir.

4.4 Uzaktan Anahtarsız Giriş (RKE) Kopyalama ve Dijital Kimlik Hırsızlığı

Teknik olarak araca yönelik bir saldırı olan Uzaktan Anahtarsız Giriş (RKE) kopyalama, şarj ekosistemi için doğrudan sonuçlar doğurur. Saldırganlar, yazılım tanımlı radyolar kullanarak sürücünün anahtarlığından gelen kodları yakalar. Araca erişim sağladıklarında, aynı zamanda araç içinde saklanan "Tak ve Şarj Et" (Plug & Charge) kimlik bilgilerine de erişmiş olurlar. Bu, saldırganın sadece aracı çalmasına değil, aynı zamanda şarj hesabıyla ilişkili dijital kimliği de ele geçirerek, sertifikalar iptal edilene kadar çalıntı aracı sahibinin hesabından şarj etmesine olanak tanır.[1]

4.5 Tedarik Zinciri ve Donanım Yazılımı Arka Kapıları

Küresel donanım pazarı, tedarik zinciri risklerini beraberinde getirir. Son araştırmalar, bazı şarj cihazı üreticilerinin donanım yazılımlarında sabit kodlanmış (hard-coded) kimlik bilgileri ve arka kapılar tespit etmiştir. Bunlar arasında, kök erişimine izin veren "uyuyan" SSH hesapları veya belgelenmemiş web arayüzleri bulunmaktadır. Bir saldırgan (veya devlet destekli aktör) bunları keşfederse, üst katman OCPP güvenlik kontrollerini atlayarak tüm şarj filolarını anında ele geçirebilir.[2]

---

5. Fırsatlar (Opportunities - Dışsal Pozitif Faktörler)

Teknolojinin hızlı gelişimi, bu tehditleri hafifletmek için önemli fırsatlar sunmaktadır. Yapay Zeka ve Blokzincir gibi ileri teknolojilerin entegrasyonu, düzenleyici çerçevelerin olgunlaşmasıyla birleşerek daha güvenli bir ekosistemin yolunu açmaktadır.

5.1 Yapay Zeka ve Makine Öğrenimi (AI/ML) ile Gelişmiş Savunma

Yapay Zeka, siber-fiziksel saldırıların karmaşıklığına karşı güçlü bir karşı önlem sunar. Geleneksel kural tabanlı güvenlik duvarları, meşru protokol komutlarını kullanan ince mantık

saldırılarını (FDIA veya anahtarlama saldırıları gibi) tespit etmekte yetersiz kalır.

- **Anomali Tespiti (IDS):** YZ modelleri, tipik güç eğrileri, işlem süreleri ve mesaj frekansları gibi "normal" şarj davranışları için bir temel oluşturabilir. OCPP trafiğini sürekli izleyen bu modeller, bir saldırıyı işaret eden sapmaları tespit edebilir. Örneğin, tek bir konumdan gelen ani StartTransaction istekleri veya bağlı bataryanın fiziğine aykırı bir güç çekimi, anında alarm tetikleyebilir.[1]
- **Kestirimci Bakım:** YZ, donanım arızalarını veya kurcalamayı tahmin etmek için sensör verilerini analiz edebilir. Bir konektörün empedansındaki ani değişiklik, fiziksel bir kurcalama girişimini veya hırsızlar tarafından yerleştirilen bir "skimmer" cihazını işaret edebilir.[32]
- **Federe Öğrenme (Federated Learning):** Gizlilik endişelerini gidermek için Federe Öğrenme, şarj cihazlarının yerel verileri üzerinde saldırı tespit modellerini eğitmesini ve yalnızca model güncellemelerini (ham verileri değil) merkezi ağla paylaşmasını sağlar. Bu, tüm ağın, kullanıcı verilerini ifşa etmeden tek bir istasyona yapılan saldırıdan "ders çıkarmasına" olanak tanır.[22]

5.2 Blokzincir ve Dağıtık Defter Teknolojisi (DLT)

Blokzincir teknolojisi, merkezi güvenin ve tek hata noktalarının (Single Point of Failure) zayıflıklarını ele alır.

- **Merkeziyetsiz Açık Anahtar Altyapısı (DPKI):** Blokzincir, geleneksel PKI'ın yerini alabilir veya onu güçlendirebilir. Merkezi bir Sertifika Otoritesine güvenmek yerine, cihaz kimlikleri ve sertifikalar değiştirilemez bir defterde saklanabilir. Bu, bir saldırganın sahte bir sertifika oluşturmasını veya güven kökünü ele geçirmesini neredeyse imkansız hale getirir.[1]
- **Güvenli P2P Enerji Ticareti:** OCPP 2.1'in V2G yetenekleriyle birlikte, Blokzincir güvenli ve şeffaf eşler arası enerji ticaretini mümkün kılar. Akıllı sözleşmeler, EA ile şebeke arasındaki enerji işlemlerinin mutabakatını otomatikleştirerek, fatura verilerinin değiştirilememesini (fatura dolandırıcılığı tehdidini çözerek) ve ödemenin garanti altına alınmasını sağlar.[33]
- **Değiştirilemez Donanım Yazılımı Doğrulaması:** Donanım yazılımı özetlerinin (hash) bir blokzincirde saklanması, bir şarj cihazının, güncellemeyi yüklemeden önce bütünlüğünü merkeziyetsiz ve kurcalamaya karşı korumalı bir kayda göre doğrulamasını sağlar. Bu, merkezi güncelleme sunucusunun ele geçirildiği tedarik zinciri saldırılarını etkisiz hale getirir.[16]

5.3 V2X ve Şebeke Dayanıklılığı (Resilience)

V2X yeni tehditler getirse de, aynı zamanda şebeke dayanıklılığı için büyük bir fırsattır. Doğru şekilde güvence altına alınmış V2G, EA'ların merkeziyetsiz depolama birimleri olarak hareket etmesini sağlar. Merkezi bir enerji santraline yapılan siber saldırı durumunda, bir EA filosu (OCPP 2.1 aracılığıyla güvenli bir şekilde) şebekeye güç enjekte etmek üzere organize edilebilir. Bu filolar, frekansı ve voltajı dengelemek için devasa bir kesintisiz güç kaynağı (UPS) görevi görerek, EA'ları bir yükümlülükten kritik bir savunma varlığına dönüştürür.[11]

---

6. Detaylı SWOT Matrisi Analizi

Aşağıdaki tablo, yapılan analizi stratejik bir matris içinde sentezlemektedir.

GÜÇLÜ YÖNLER (İçsel)	**ZAYIF YÖNLER (İçsel)**
S1. Standartlaştırılmış Güvenlik Profilleri: OCPP 2.0.1+, TLS ve mTLS için net katmanlar (1-3) tanımlayarak belirsizliği ortadan kaldırır. **S2. Donanım Yazılımı Bütünlüğü:** Zorunlu dijital imzalama, kötü amaçlı kod enjeksiyonunu önler. **S3. Hiyerarşik Cihaz Modeli:** Bileşen sağlığının granüler görünürlüğü, daha iyi izleme sağlar. **S4. ISO 15118 Entegrasyonu:** Tak ve Şarj Et, kolayca kopyalanan RFID kartlarını ortadan kaldırarak güçlü istemci tarafı sertifikaları kullanır. **S5. Açık Yönetişim:** OCA topluluk denetimi, güvenlik açıklarının hızlı ifşasını ve yamanmasını sağlar.	**W1. Miras Yükü:** Güvensiz OCPP 1.6J'nin (şifresiz WebSockets) yaygın kullanımı. **W2. PKI Karmaşıklığı:** Sertifika yaşam döngüleri için yüksek yönetim yükü operasyonel risk yaratır. **W3. Yan Kanal Sızıntıları:** PLC iletişimi (CCS standardı), elektromanyetik radyasyon yoluyla veri sızdırır. **W4. EMS Güvenlik Boşluğu:** Enerji Yönetim Sistemi arayüzü için standartlaştırılmış güvenlik eksikliği ve ARP Spoofing riski. **W5. Fiziksel Zafiyet:** Halka açık portlar (USB/Ethernet) ve donanım üzerindeki JTAG arayüzleri.
FIRSATLAR (Dışsal)	**TEHDİTLER (Dışsal)**

O1. YZ/ML Entegrasyonu: Mantık saldırıları için anomali tespiti (IDS) ve kestirimci bakım. **O2. Blokzincir/DLT:** Merkeziyetsiz kimlik yönetimi (DPKI) ve güvenli P2P enerji mutabakatları. **O3. V2X Şebeke Dayanıklılığı:** EA filolarının saldırılar sırasında şebekeyi dengelemek için dağıtık depolama olarak kullanılması. **O4. Düzenleyici Zorunluluklar:** Hükümetlerin şarj cihazları için "Tasarım Gereği Güvenlik" ilkelerini zorunlu kılması. **O5. Federe Öğrenme:** CPO'lar arasında gizliliği koruyan tehdit istihbaratı paylaşımı.	**T1. Şebeke Destabilizasyonu:** Karartmalara neden olmak için anahtarlama/yük salınımı saldırıları düzenleyen botnetler. **T2. Organize Dolandırıcılık:** Quishing (QR phishing) ve organize enerji hırsızlığı. **T3. Devlet Destekli Sabotaj:** Kritik altyapıya yönelik hedefli saldırılar (örneğin, Ukrayna/Rusya çatışması örnekleri). **T4. Tedarik Zinciri İhlali:** Güvenilmeyen satıcılardan gelen donanımlarda sabit kodlanmış arka kapılar. **T5. RKE Kopyalama:** Araçların ve ilişkili Tak ve Şarj Et dijital kimliklerinin çalınması.

---

7. Stratejik Sentez ve Gelecek Öngörüleri

Bu raporun bulguları, elektrikli araç şarj güvenliğinin sadece bir teknoloji sorunu değil, aynı zamanda bir strateji ve yönetim sorunu olduğunu ortaya koymaktadır. OCPP 2.1'in 2025 yılında yayınlanmasıyla birlikte, sektör V2G yeteneklerine doğru büyük bir adım atmıştır, ancak bu adım güvenlik açıklarını da beraberinde getirmektedir.

7.1 Miras Sistemlerden Çıkış Stratejisi

OCPP 1.6'nın yarattığı "miras tuzağı", CPO'lar için en acil çözülmesi gereken sorundur. Donanım değişimi maliyetli olduğundan, ara çözümler hayati önem taşır. Şarj sahalarına **Güvenli Ağ Geçitleri (TLS Termination Proxies)** yerleştirilmesi, eski şarj cihazlarının yerel HTTP/TCP trafiğini alıp, CSMS'e güvenli WSS tünelleri üzerinden ileterek şifrelemesi, kısa vadeli ancak etkili bir mitigasyon stratejisidir.[8]

7.2 Sıfır Güven (Zero Trust) Mimarisinin Benimsenmesi

Mevcut mimarideki örtük güven (örneğin, "OCPP konuşuyorsa, o bir şarj cihazıdır") terk edilmelidir. Her varlık—şarj cihazı, araç, EMS, sunucu—kriptografik bir kimliğe sahip olmalıdır. OCPP 2.0.1 Profil 3'ün (mTLS) kritik altyapı için zorunlu hale getirilmesi kaçınılmazdır. Ayrıca, yetkilendirme oturum başında bir kez yapılan bir işlem olmaktan çıkıp, YZ destekli davranışsal analiz ile oturum boyunca sürekli doğrulanan bir süreç haline gelmelidir.

7.3 Siber-Fiziksel Güvenliğin Yakınsaması

Tehditler siber-fiziksel olduğu için, savunma da öyle olmalıdır. Endüstri, **Katmanlar Arası Saldırı Tespit Sistemleri (Cross-Layer IDS)** tasarımına geçmelidir. Güçlü bir savunma; fiziksel katmandaki voltaj/akım sensörlerini (kurcalama/FDIA tespiti), ağ katmanındaki trafik akışını (DoS tespiti) ve uygulama katmanındaki OCPP komutlarını (anahtarlama saldırıları tespiti) korele etmelidir. Ancak bu şekilde, meşru bir şebeke arızası ile siber saldırı birbirinden ayırt edilebilir.[23]

7.4 Sonuç

Yapılan SWOT analizi, Açık Şarj Noktası Protokolü'nün **2.0.1** ve **2.1** sürümleriyle sağlam ve güvenli bir standarda dönüştüğünü, ancak ekosistemin hala kırılgan olduğunu göstermektedir. Yeni protokollerin **Güçlü Yönleri**, devasa miras kurulum tabanının **Zayıf Yönleri** ve PKI uygulamasının karmaşıklığı tarafından gölgelenmektedir. **Tehditler**, basit dolandırıcılıktan şebeke istikrarını içeren ulusal güvenlik risklerine tırmanmaktadır.

Bununla birlikte, ilerleme yolu açıktır. Yapay Zeka ve Blokzincir tarafından sunulan **Fırsatlar**, güvenlik açığını kapatmak için gerekli araçları sunmaktadır. Paydaşlar için öncelik artık inovasyon değil, **göçtür (migration)**: OCPP 1.6'nın emekliye ayrılmasını hızlandırmak ve şebekenin fiziksel ucunu kaçınılmaz siber-fiziksel saldırı dalgasına karşı sertleştirmek. Geleceğin ulaşımını güçlendirecek olan kritik altyapının güvenliği, bu stratejik dönüşümün başarısına bağlıdır.

Alıntılanan çalışmalar

1. Electric_Vehicle_Charging_A_Survey_on_the_Security_Issues_and_Challenges_of_the_Open_Charge_Point_Protocol_OCPP.pdf
2. Vulnerabilities could let hackers remotely shut down EV chargers, steal electricity, erişim tarihi Kasım 22, 2025, https://cyberscoop.com/hack-electric-vehicle-chargers/
3. What's New OCPP 2.1 | Open Charge Alliance, erişim tarihi Kasım 22, 2025, https://openchargealliance.org/wp-content/uploads/2024/03/Whats-New-OCPP-2.1.pdf
4. OCPP 1.6 vs 2.0.1 - Key Differences & Updates - ChargePanel, erişim tarihi Kasım 22, 2025, https://www.chargepanel.com/ocpp-1-6-vs-ocpp-2-0-1-key-differencesupdates-and-functionality/
5. OCPP 2.0.1 vs. 1.6J: Security, V2G, and Device Management Deep Dive - LinkPower, erişim tarihi Kasım 22, 2025, https://www.elinkpower.com/news/ocpp-2-0-1-vs-1-6j-security-v2g-and-device-management-deep-dive/
6. The Complete Guide to OCPP 2.0.1 - S44 Energy, erişim tarihi Kasım 22, 2025, https://www.s44.team/resources/the-complete-guide-to-ocpp-201-yMS5iompvA7Aal
7. The Open Charge Point Protocol (OCPP) Version 1.6 Cyber Range A Training and Testing Platform - CORE Scholar, erişim tarihi Kasım 22, 2025, https://corescholar.libraries.wright.edu/etd_all/2788/
8. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - OSTI.GOV, erişim tarihi Kasım 22, 2025, https://www.osti.gov/servlets/purl/2431391
9. OCPP (Open Charge Point Protocol), erişim tarihi Kasım 22, 2025, https://openchargealliance.org/protocols/open-charge-point-protocol/
10. Understanding the differences between OCPP 1.6 & OCPP 2.0.1 - Current Eco AS, erişim tarihi Kasım 22, 2025, https://www.current.eco/resources/articles/understanding-the-differences-between-ocpp-1.6-ocpp-2.0.1
11. What Every CPO Needs to Know About OCPP 2.1 - AMPECO, erişim tarihi Kasım 22, 2025, https://www.ampeco.com/blog/what-every-cpo-needs-to-know-about-ocpp-2-1/
12. OCPP 2.1 is now available! - Open Charge Alliance, erişim tarihi Kasım 22, 2025, https://openchargealliance.org/ocpp-2-1-is-now-available/
13. Understanding OCPP Security Profiles: Securing the Future of EV Charging - eDRV, erişim tarihi Kasım 22, 2025, https://www.edrv.io/blog/understanding-ocpp-security-profiles
14. Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/1996-1073/15/11/3931

15. What is OCPP 2.0.1 and why does it matter? - Switch EV, erişim tarihi Kasım 22, 2025, https://www.switch-ev.com/blog/what-is-ocpp-2-0-1-and-why-does-it-matter
16. Blockchain-Based Secure Firmware Updates for Electric Vehicle Charging Stations in Web of Things Environments - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/2032-6653/16/4/226
17. Electric vehicle charging – Global EV Outlook 2025 – Analysis - IEA, erişim tarihi Kasım 22, 2025, https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-charging
18. OCPP 1.6 vs. OCPP 2.0: A Comprehensive Comparison - Ampcontrol, erişim tarihi Kasım 22, 2025, https://www.ampcontrol.io/post/ocpp-1-6-vs-ocpp-2-0-a-comprehensive-comparison
19. OCPP 1.6 vs 2.0 vs. 2.1 Comparing: Benefits, Limitations, and Adoption Trends, erişim tarihi Kasım 22, 2025, https://lembergsolutions.com/blog/ocpp-16-vs-20-vs-21-comparing-benefits-limitations-and-adoption-trends
20. Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP), erişim tarihi Kasım 22, 2025, https://openresearch.surrey.ac.uk/view/pdfCoverPage?instCode=44SUR_INST&filePid=13169250180002346&download=true
21. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging - USENIX, erişim tarihi Kasım 22, 2025, https://www.usenix.org/conference/usenixsecurity19/presentation/baker
22. Keywords: - arXiv, erişim tarihi Kasım 22, 2025, https://arxiv.org/html/2502.01569v1
23. Federated detection of open charge point protocol 1.6 cyberattacks - OAE Publishing Inc., erişim tarihi Kasım 22, 2025, https://www.oaepublish.com/articles/ces.2025.04
24. Cyber defense in OCPP for EV charging security risks - NTU > IRep, erişim tarihi Kasım 22, 2025, https://irep.ntu.ac.uk/id/eprint/54086/1/2477910_Brown.pdf
25. EV CPO Under Siege: A New Attack Exposed the Cybersecurity and Privacy Risks of EV Charging Networks - Upstream Security, erişim tarihi Kasım 22, 2025, https://upstream.auto/blog/cybersecurity-and-privacy-risks-of-ev-charging-networks/
26. 30 EV Ecosystem Statistics You Should Know About in 2025 - C2A Security, erişim tarihi Kasım 22, 2025, https://c2a-sec.com/30-ev-ecosystem-statistics-you-should-know-about-in-2024/
27. How to address the increasing threat of cyberattacks on EV charging stations - Virta, erişim tarihi Kasım 22, 2025, https://www.virta.global/blog/en/blog/how-to-address-the-increasing-threat-of-cyberattacks-on-ev-charging-stations
28. Cybersecurity Risk Analysis of Electric Vehicles Charging Stations - PMC - PubMed Central, erişim tarihi Kasım 22, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC10422437/

29. Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network - PMC, erişim tarihi Kasım 22, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11933351/
30. Ev Station Let Attackers Gain Unauthenticated network access - Cyber Press, erişim tarihi Kasım 22, 2025, https://cyberpress.org/ev-station-let-attackers/
31. Enhancing the Detection of Cyber-Attacks to EV Charging Infrastructures Through AI Technologies - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/2079-9292/14/21/4321
32. How AI is Shaping EVs and EV Charging - EVinfo.net, erişim tarihi Kasım 22, 2025, https://evinfo.net/2024/08/how-ai-is-shaping-evs-and-ev-charging/
33. Integrating AI and Blockchain in EV Charging: Innovations and Challenges - ResearchGate, erişim tarihi Kasım 22, 2025, https://www.researchgate.net/publication/381619413_Integrating_AI_and_Blockchain_in_EV_Charging_Innovations_and_Challenges
34. A Blockchain-Based Electric Vehicle Charging Cooperation Model - IEEE Xplore, erişim tarihi Kasım 22, 2025, https://ieeexplore.ieee.org/iel8/25/10910276/10746347.pdf