Mikrogird Ortamlarında OCPP v2.0.1 Güvenlik Değerlendirmesi: Alcaraz ve Ark. (2023) Kapsamlı İncelemesi ve SWOT Analizi

1. Yönetici Özeti

Elektrikli Araç (EA) ekosisteminin hızla genişlemesi, enerji sektörünü dijitalleşmiş ve merkeziyetsiz bir yapıya dönüştürmektedir. Bu dönüşüm, sadece ulaşım sektörünü değil, aynı zamanda elektrik şebekesinin operasyonel dinamiklerini de kökten değiştirmektedir. Endüstri 4.0 prensiplerinin enerji altyapılarına entegrasyonu ile birlikte, Şarj İstasyonları (CS) ve bunları yöneten merkezi sistemler (CSMS), kritik altyapı bileşenleri haline gelmiştir. Bu bağlamda, Açık Şarj Noktası Protokolü (OCPP), bu bileşenler arasındaki iletişimi sağlayan endüstri standardı olarak öne çıkmaktadır.

Bu rapor, Cristina Alcaraz, Jesus Cumplido ve Alicia Triviño tarafından kaleme alınan *"OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0"* (2023) başlıklı makaleyi merkeze alarak, modern elektrikli araç şarj altyapılarının (EVCI) güvenlik peyzajını derinlemesine analiz etmektedir.[1] Makale, özellikle mikroşebeke (microgrid) ortamlarına entegre edilmiş şarj istasyonlarında kullanılan en güncel protokol sürümü olan OCPP v2.0.1'in siber-fiziksel güvenlik açıklarını irdelemektedir.

Rapor, söz konusu akademik çalışmanın SWOT (Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler) analizini gerçekleştirmekle kalmayıp, aynı zamanda genişletilmiş literatür taraması ve sektörel veriler ışığında, protokolün uygulama zorluklarını, ortaya çıkan yeni tehdit vektörlerini (örneğin V2G saldırıları) ve önerilen karşı önlemlerin (Blokzincir, Yapay Zeka) pratik uygulanabilirliğini değerlendirmektedir. Alcaraz ve ekibinin önerdiği, STRIDE tehdit modelini enerji varlıklarını kapsayacak şekilde genişleten SD^{c+e} (STRIDE-DREAD+) metodolojisi, bu raporun analitik çerçevesini oluşturmaktadır.[1] Analizler, OCPP v2.0.1'in güvenlik profillerinde önemli iyileştirmeler sunmasına rağmen, özellikle fiziksel erişim, firmware manipülasyonu ve enerji dolandırıcılığı (spoofing) konularında ciddi risklerin devam ettiğini ortaya koymaktadır.

2. Endüstri 4.0 ve Elektrikli Araç Şarj Ekosisteminin Dönüşümü

2.1 Siber-Fiziksel Sistemlerin Yakınsaması ve Mikroşebekeler

Enerji sektörü, genellikle Enerji 4.0 olarak adlandırılan ve üretim, dağıtım ve tüketim süreçlerinin tam otomasyonunu hedefleyen bir devrim içerisindedir. Bu yeni paradigmada, Elektrikli Araç Şarj Altyapıları (EVCI), pasif yükler olmaktan çıkıp, akıllı şebeke (Smart Grid) veya mikroşebeke (Microgrid - MG) içerisinde aktif, yönetilebilir düğümler haline gelmiştir.[1] Bir mikroşebeke, ana şebeke ile senkronize çalışabilen ancak gerektiğinde "ada moduna" geçerek bağımsız enerji yönetimi sağlayabilen yerel bir enerji sistemidir.

Bu yapıda EA'lar, sadece enerji tüketen araçlar değil, aynı zamanda depolama kapasiteleri sayesinde Dağıtık Enerji Kaynakları (DER) olarak işlev gören unsurlardır. Ancak, bu entegrasyon derin bir siber bağımlılığı beraberinde getirmektedir. Mikroşebekenin voltaj ve frekans kararlılığı, güç dengesi ve ekonomik dağıtımı, artık tamamen iletişim protokollerinin bütünlüğüne bağlıdır.[1] Saldırganların bu siber katmanı manipüle etmesi, sadece veri ihlaline değil, aynı zamanda transformatörlerin aşırı yüklenmesi, bataryaların zarar görmesi veya bölgesel elektrik kesintileri gibi fiziksel sonuçlara yol açabilir. Bu durum, "Siber-Fiziksel Saldırılar" (Cyber-Physical Attacks) olarak adlandırılan yeni bir tehdit sınıfını doğurmuştur.

2.2 OCPP Protokolünün Stratejik Konumu ve Evrimi

Bu karmaşık etkileşimleri yönetmek için endüstri, Açık Şarj İttifakı (Open Charge Alliance - OCA) tarafından geliştirilen OCPP standardına güvenmektedir. Protokol, Şarj İstasyonu (donanım) ile Merkezi Yönetim Sistemi (CSMS - yazılım) arasındaki "lingua franca" (ortak dil) olarak işlev görür. Protokolün evrimi, güvenlik ihtiyaçlarının artışına paralel olarak şekillenmiştir:

- **OCPP 1.6:** Endüstride en yaygın kullanılan sürümdür. Başlangıçta güvenlik özellikleri sınırlıydı ve genellikle WebSocket uygulamalarındaki zafiyetler veya VPN kullanımına aşırı bağımlılık gibi sorunlarla eleştirilmiştir.[2] Güvenlik, protokolün çekirdeğine entegre edilmek yerine genellikle sonradan eklenen bir katman olarak düşünülmüştür.
- **OCPP 2.0.1:** Alcaraz ve arkadaşlarının çalışmasının odak noktası olan bu sürüm, cihaz ve

iletişim düzeyinde yerel güvenlik önlemleri içermektedir. ISO 15118 (Plug & Charge) desteği, güvenli firmware güncellemeleri, güvenlik olay günlükleri ve sıkı tanımlanmış güvenlik profilleri bu sürümün getirdiği temel yeniliklerdir.[1]

Bununla birlikte, v2.0.1'e geçiş süreci sancılıdır. Protokolün önceki sürümlerle geriye dönük uyumluluğunun olmaması, donanım ve yazılım tarafında kapsamlı güncellemeler gerektirmekte ve bu da "uygulama boşluğu" (implementation gap) riskini artırmaktadır.[4]

2.3 Paydaş Mimarisi ve Saldırı Yüzeyi

Tehdit analizi yapabilmek için Alcaraz ve ark. tarafından tanımlanan mimariyi ve paydaşları anlamak kritiktir.[1] Ekosistem çok katmanlıdır ve her katman ayrı bir saldırı vektörü sunar:

Paydaş / Bileşen	Rolü ve Kritikliği	Potansiyel Tehdit Vektörü
Şarj İstasyonu (CS/EVSE)	Fiziksel arayüz, güç aktarımı.	Fiziksel manipülasyon, Firmware zehirlenmesi.
Merkezi Sistem (CSMS)	Faturalama, yetkilendirme, yönetim.	Veritabanı enjeksiyonu, DDoS, Yetki yükseltme.
Enerji Yönetim Sistemi (EMS)	Mikroşebeke yük dengesi, DER kontrolü.	Enerji set-point manipülasyonu, Kararsızlık yaratma.
Dağıtım Sistemi Operatörü (DSO)	Şebeke kararlılığı.	Yanlış veri enjeksiyonu (FDI), Şebeke çökertme.
Son Kullanıcı (EV Sürücüsü)	Hizmet alıcısı, mobil uygulama kullanımı.	Kimlik hırsızlığı, Ödeme dolandırıcılığı.

Alcaraz ve ark., özellikle EMS ve CSMS arasındaki bağlantının kritik olduğunu vurgular. Eğer bir saldırgan OCPP bağlantısı üzerinden EMS'yi ele geçirirse, mikroşebekenin enerji profillerini değiştirerek fiziksel varlıklara zarar verebilir.[1] Bu, raporun temelini oluşturan "Enerji Tehditleri" kavramının merkezidir.

3. Metodolojik Çerçeve: SD^{c+e} Yaklaşımının Derinlemesine İncelemesi

İncelenen makalenin en önemli akademik katkısı, geleneksel yazılım tehdit modelleme metodolojilerini enerji sistemlerine uyarlamasıdır. Yazarlar, **STRIDE** ve **DREAD** modellerini birleştirerek ve genişleterek **SD^{c+e}** (STRIDE-DREAD for control and energy) adını verdikleri hibrit bir yaklaşım geliştirmişlerdir.[1]

3.1 STRIDE Modelinin Enerji Varlıklarına Genişletilmesi

Microsoft tarafından geliştirilen STRIDE, tehditleri altı kategoride sınıflandırır.[5] Alcaraz ve ark., bu kategorileri sadece yazılım (kontrol - c) varlıkları için değil, aynı zamanda fiziksel güç akışı (enerji - e) varlıkları için de tanımlamıştır.[1] Bu ayrım hayati önem taşır:

1. **Spoofing (Kimlik Yanıltma):**
   - *Kontrol (S_c):* Başkasının RFID kartını kopyalamak.
   - *Enerji (S_e):* Bir CS'nin sahte sayaç verisi göndererek tükettiğinden daha az veya çok enerji çekmiş gibi görünmesi (Enerji Dolandırıcılığı).
2. **Tampering (Veri Değiştirme):**
   - *Kontrol (T_c):* Log dosyalarını silmek.
   - *Enerji (T_e):* Şarj profillerini (OCPP Use Case K01) değiştirerek, mikroşebeke kapasitesinin üzerinde güç çekilmesini sağlamak ve fiziksel devre kesicilerin atmasına neden olmak.
3. **Repudiation (İnkar):**
   - *Enerji (R_e):* İmzalanmamış sayaç verileri nedeniyle, bir enerji transferinin gerçekleştiğinin veya miktarının inkar edilmesi.
4. **Information Disclosure (Bilgi İfşası):**
   - *Enerji (I_e):* Şarj alışkanlıklarından kullanıcının konum ve rutinlerinin çıkarılması (Gizlilik ihlali).
5. **Denial of Service (Hizmet Reddi):**
   - *Enerji (D_e):* Şarj işlemini durdurarak bataryanın dolmasını engellemek veya daha kritiği, şebeke frekans yanıtına katılmasını engelleyerek şebeke kararlılığını bozmak.
6. **Elevation of Privilege (Yetki Yükseltme):**
   - *Enerji (E_e):* Yetkisiz bir kullanıcının EMS üzerinde yönetici hakları kazanarak enerji akışını kontrol etmesi.

3.2 DREAD ile Risk Ölçümü ve Önceliklendirme

Sınıflandırmanın ötesine geçerek riskleri nicel hale getirmek için makale DREAD modelini kullanmaktadır. Her tehdit beş kriter üzerinden 1-10 arasında puanlanır: **Hasar (Damage)**, **Tekrarlanabilirlik (Reproducibility)**, **İstismar Edilebilirlik (Exploitability)**, **Etkilenen Kullanıcılar (Affected Users)** ve **Keşfedilebilirlik (Discoverability)**.

Makalenin analizi, **Tampering (T)** ve **Denial of Service (D)** tehditlerinin en yüksek risk puanlarına sahip olduğunu ortaya koymaktadır (Örn: "CS Spoofing" 8.0/10, "CS'ye DoS Saldırısı" 9.2/10).[1] Bu bulgu, endüstriyel kontrol sistemlerinde "Kullanılabilirlik" (Availability) ve "Bütünlük" (Integrity) ilkelerinin, geleneksel IT güvenliğindeki "Gizlilik" (Confidentiality) ilkesinden daha kritik olduğu gerçeğiyle örtüşmektedir.

3.3 Metodolojinin Eleştirisi ve Sınırlılıklar

Her ne kadar SD^{c+e} yaklaşımı sistematik bir çerçeve sunsa da, literatürdeki eleştiriler ve modelin doğasından kaynaklanan sınırlılıklar mevcuttur:

- **Sübjektiflik:** DREAD skorlaması, analistin uzmanlığına ve varsayımlarına aşırı derecede bağımlıdır.[5] Örneğin, bir saldırının "Tekrarlanabilirlik" puanı, saldırganın teknik becerisine göre değişebilir. Makale, bu puanların kesin değerler olduğunu ima etmekte ancak bir duyarlılık analizi sunmamaktadır.
- **Statik Yapı:** STRIDE ve DREAD, sistemin tasarım aşamasındaki bir anlık görüntüsüne odaklanır. Oysa siber tehdit peyzajı dinamiktir; bugün keşfedilmesi zor (Düşük Discoverability) olan bir açık, yarın yayınlanan bir araçla herkes tarafından kullanılabilir hale gelebilir.[5]
- **Fiziksel Etkileşimlerin Karmaşıklığı:** CPS (Siber-Fiziksel Sistemler) güvenliğinde, siber saldırıların fiziksel sonuçları (örneğin bir transformatörün aşırı ısınması) doğrusal olmayan süreçlerdir. DREAD'in lineer puanlama sistemi, düşük olasılıklı ancak felaket düzeyinde sonuçları olan "Siyah Kuğu" olaylarını (Black Swan events) yeterince temsil edemeyebilir.[7]

4. OCPP v2.0.1 Tehdit Analizi: Bulgular ve Gerçek Dünya Verileri

Alcaraz ve ark. (2023) çalışması, OCPP v2.0.1'in özelliklerini granüler düzeyde inceleyerek, protokolün güvenlik iyileştirmelerine rağmen devam eden zafiyetlerini ortaya koymaktadır. Bu bölüm, makalenin bulgularını dış kaynaklardan elde edilen gerçek dünya verileriyle sentezlemektedir.

4.1 Güvenlik Profilleri ve Kimlik Doğrulama Riskleri

OCPP v2.0.1 üç temel güvenlik profili tanımlar [3]:

1. **Profil 1:** Temel Kimlik Doğrulama ile Güvensiz İletim (HTTP + Parola).
2. **Profil 2:** Temel Kimlik Doğrulama ile TLS (Sadece Sunucu Sertifikası).
3. **Profil 3:** İstemci Tarafı Sertifikaları ile TLS (Karşılıklı TLS / mTLS).

Makale ve destekleyici araştırmalar, Profil 3 en güvenli seçenek olsa da, endüstrideki uygulamaların genellikle uyumluluk ve maliyet nedenleriyle daha düşük profillere yöneldiğini belirtmektedir.[8]

- **CS Spoofing (Şarj İstasyonu Taklidi):** Eğer Profil 1 veya 2 kullanılırsa, sistem güvenliği büyük ölçüde "Identity" ve "BasicAuthPassword" konfigürasyon değişkenlerine dayanır. Saldırganlar, genellikle kamuya açık ve fiziksel koruması zayıf olan CS'lere fiziksel erişim sağlayarak bu kimlik bilgilerini çalabilir. Makale bu tehdidi **Yüksek Risk (8.0)** olarak sınıflandırır.[1] Sahte bir CS, CSMS'e hatalı sayaç verileri göndererek fatura dolandırıcılığı yapabilir veya mikroşebeke yük hesaplamalarını bozabilir.
- **"Master Pass" Zafiyeti:** OCPP v2.0.1, kolluk kuvvetlerinin veya acil durum ekiplerinin herhangi bir şarj işlemini durdurabilmesi için bir "Master Pass" (Ana Anahtar) tanımlanmasına izin verir. Makale, bu özelliğin "Tek Hata Noktası" (Single Point of Failure) olduğunu tespit eder. Bu anahtar kopyalanırsa, saldırgan tüm aktif şarj işlemlerini aynı anda durdurarak (Use Case C16), kitlesel bir Hizmet Reddi (DoS) saldırısı gerçekleştirebilir.[1]

4.2 Firmware Yönetimi ve Kalıcılık

v2.0.1'deki en büyük iyileştirmelerden biri güvenli, imzalı firmware güncelleme sürecidir. Ancak makale, güncelleme mekanizmasının (Use Case L02) güven zincirinin kırılması durumunda hala istismar edilebileceğini belirtir.

- **Tampering Riskleri:** Eğer bir CS, Man-in-the-Middle (Ortadaki Adam) saldırısı ile kötü niyetli bir firmware indirmeye zorlanırsa (örneğin Profil 3 kullanılmıyorsa), saldırgan cihaz

üzerinde kalıcılık sağlar. Saldırgan, SmartChargingEnabled değişkenlerini devre dışı bırakarak EMS'nin güç sınırlamalarını yok sayabilir. Bu, şebeke varlıklarının fiziksel güvenliğini doğrudan tehdit ettiği için **Yüksek Risk (8.6)** puanına sahiptir.[1]

- **CVE-2024-37310 ve Arka Uç Zafiyetleri:** Teorik analizin ötesinde, gerçek dünyada keşfedilen zafiyetler riskin boyutunu doğrulamaktadır. Örneğin, Everest Core kütüphanesindeki CVE-2024-37310 zafiyeti, uygun kimlik doğrulama önlemleri alınmadığında saldırganların CSMS bağlantılarını manipüle edebileceğini göstermektedir.[9] Alcaraz makalesi, "CSMS Spoofing" tehdidini vurgulayarak bu tür yazılım hatalarının tüm şarj ağını etkileyebileceğini öngörmüştür.

4.3 Mikroşebeke Bağımlılığı ve Enerji Tehditleri

Çalışmanın en özgün katkısı, mikroşebekeyi hedef alan saldırı vektörlerinin analizidir.

- **Desenkronizasyon (TC-8):** Makale, saldırganların HeartbeatInterval veya zaman senkronizasyonunu (Use Case G02) manipüle etme riskini vurgular. Mikroşebekelerde talep tarafı yönetimi (Demand Response) milisaniyelik hassasiyet gerektirir. Zamanlaması bozulmuş bir şarj filosu, yük atma komutlarına yanlış zamanda yanıt vererek şebeke frekansını destabilize edebilir ve kesintilere yol açabilir.[1]
- **Ters Enerji Akışı ve V2G (TC-9):** ISO 15118 ve V2G (Vehicle-to-Grid) teknolojileriyle birlikte enerji akışı çift yönlü hale gelmiştir. Makale, saldırganların şarj/deşarj profillerini manipüle ederek şebekeye beklenmedik ve kitlesel miktarda enerji geri basması tehdidini tanımlar. Bu, yerel transformatörleri aşırı yükleyebilir ve güç elektroniği bileşenlerine zarar verebilir.[1]

5. Makalenin SWOT Analizi

Bu bölüm, kullanıcının temel talebi olan makalenin SWOT analizini, literatür ve sektörel gerçekler ışığında sunmaktadır.

5.1 Güçlü Yönler (Strengths)

1. **Metodolojik İnovasyon (SD^{c+e}):** Makalenin en güçlü yanı, STRIDE/DREAD modellerini "Enerji" varlıklarını kapsayacak şekilde genişletmesidir. Çoğu siber güvenlik

çalışması veriye odaklanırken, bu çalışma "Enerji Spoofing" veya "Enerji Tampering" kavramlarını literatüre kazandırarak, IT güvenliği ile Güç Sistemleri Mühendisliği arasındaki boşluğu doldurmuştur.[1]

2. **Güncel Odak (OCPP v2.0.1):** Literatürün çoğu v1.6 üzerine yoğunlaşmışken, bu çalışma v2.0.1'i analiz ederek önümüzdeki 5-10 yıllık altyapı yatırımları için geçerli bir kaynak oluşturmuştur. Özellikle ISO 15118 ve sertifika yönetimi gibi yeni özelliklerin analizi kritiktir.[10]
3. **Kapsamlı Tehdit Taksonomisi:** Makaledeki Tablo 9 ve 10, geliştiriciler ve denetçiler için paha biçilmez bir kontrol listesi sunmaktadır. Belirli Konfigürasyon Değişkenlerinin (örneğin AuthorizeRemoteStart) belirli tehditlerle (örneğin DoS) ilişkilendirilmesi, çalışmayı teoriden pratiğe taşımaktadır.[1]
4. **Bütüncül Mikroşebeke Bağlamı:** Şarj istasyonlarını izole cihazlar olarak değil, Akıllı Mikroşebeke'nin parçası olarak ele alması, siber saldırıların fiziksel etkilerini (şebeke kararsızlığı) doğru bir şekilde analiz etmesini sağlamıştır.

5.2 Zayıf Yönler (Weaknesses)

1. **Deneysel Doğrulama Eksikliği:** En belirgin zayıflık, çalışmanın tamamen teorik analize dayanmasıdır. Makale, bir test yatağı (testbed) kurulumu, sızma testi sonuçları veya saldırıların simülasyonunu içermemektedir. Risk puanları ampirik verilerle değil, analitik varsayımlarla türetilmiştir. Bu durum, donanım tabanlı simülasyonlar kullanan diğer çalışmalarla tezat oluşturmaktadır.[11]
2. **DREAD Puanlamasının Sübjektifliği:** DREAD modelinin doğası gereği, atanan puanlar (örneğin "Kullanıcı Spoofing için Tekrarlanabilirlik = 9") yazarın görüşüne bağlıdır ve uygulamanın kalitesine (örneğin 2FA var mı?) göre değişebilir. Makale, bu puanların belirsizliğini ele alan bir duyarlılık analizi sunmamaktadır.[6]
3. **Ekonomik Etki Analizinin Yokluğu:** Sonuçlar arasında "Ekonomik Zarar" (TC-3) listelenmiş olsa da, bu nicel olarak modellenmemiştir. Bir mikroşebeke operatörü için saldırının teknik detayları kadar maliyeti de önemlidir.
4. **Savunma Önerilerinin Geleneksel Olması:** Önerilen karşı önlemler (TLS, IPSec, IDS) standart IT çözümleridir. Makale, "fizik tabanlı anomali tespiti" (enerji tüketiminin fizik yasalarına uygunluğunun denetlenmesi) gibi daha alana özgü savunmaları yeterince derinleştirmemiştir.

5.3 Fırsatlar (Opportunities)

1. **Düzenleyici Çerçeveler İçin Taslak:** ABD (NIST) ve AB (Siber Güvenlik Yasası) gibi

otoritelerin EA güvenliğini düzenlemeye başladığı bir dönemde, bu makalenin taksonomisi, OCPP v2.0.1 uyumluluk denetimleri için bir temel oluşturabilir.[12]

2. **İleri Teknolojilerle Entegrasyon:** Makalenin tespit ettiği "İnkar Edilemezlik" riskleri (Risk puanı 3.6), blokzincir tabanlı değişmez kayıt defterleri ile çözülebilir. Makale, bu tür araştırmalar için bir zemin hazırlamaktadır.[13]
3. **V2G ve Kablosuz Şarj Genişlemesi:** Yazarlar, V2G ve kablosuz şarjı gelecek çalışma alanları olarak belirlemiştir.[1] Bu teknolojilerin olgunlaşmasıyla, SD^{c+e} modelinin endüktif şarjın elektromanyetik girişim (EMI) tehditlerine uyarlanması yeni bir araştırma fırsatıdır.

5.4 Tehditler (Threats)

1. **Teknolojik Eskime:** Siber tehditler akademik yayın döngülerinden daha hızlı evrilmektedir. Yapay zeka destekli saldırıların (Adversarial AI) IDS'leri atlatma yeteneği veya kuantum bilgisayarların şifreleme üzerindeki tehdidi, makaledeki risk puanlarını hızla geçersiz kılabilir.[15]
2. **Uygulama Boşluğu (Implementation Gap):** Makale protokolü analiz etmiştir ancak güvensizlik genellikle uygulamadan kaynaklanır. Şarj istasyonlarının %90'ının varsayılan şifrelerle veya eski Linux çekirdekleriyle sahaya sürülmesi durumunda, protokol seviyesindeki güvenliğin bir anlamı kalmayacaktır.[2]
3. **Maliyet Baskısı ve Operasyonel Felç:** Makale Karşılıklı TLS (mTLS) gibi güçlü önlemler önermektedir. Ancak milyonlarca IoT cihazı için PKI (Açık Anahtar Altyapısı) yönetmek pahalı ve zordur. Operatörler bu maliyetlerden kaçınırsa, makalenin önerileri kağıt üzerinde kalma riskiyle karşı karşıyadır.[8]

5.5 SWOT Özeti Tablosu

Güçlü Yönler (İçsel)	**Zayıf Yönler (İçsel)**
- **Metodoloji:** Enerji varlıklarını kapsayan yenilikçi SD^{c+e} modeli. - **Güncellik:** Modern OCPP v2.0.1 standardına odaklanma.	- **Doğrulama:** Deneysel/Test yatağı verisi eksikliği. - **Sübjektiflik:** DREAD puanlarının tahminlere dayanması.

- **Derinlik:** Konfigürasyon değişkenlerinin tehditlerle eşleştirilmesi. - **Bağlam:** EA-Mikroşebeke ekosisteminin bütüncül analizi.	- **Ekonomi:** Finansal etki modellemesinin yokluğu. - **Savunma:** Karşı önlemlerin standart IT çözümleriyle sınırlı kalması.
Fırsatlar (Dışsal)	**Tehditler (Dışsal)**
- **Düzenleme:** Hükümet/Endüstri uyumluluk denetimleri için temel. - **Teknoloji:** Blokzincir/YZ güvenlik katmanları için zemin. - **Genişleme:** V2G ve Kablosuz şarj alanlarına uygulanabilirlik. - **Eğitim:** CPS güvenliği müfredatı için kaynak.	- **Evrim:** YZ/Kuantum tehditlerinin hızlı yükselişi. - **Uygulama:** Güvenli protokol ile hatalı yazılım arasındaki uçurum. - **Maliyet:** Endüstrinin karmaşık PKI/mTLS yatırımlarına direnci. - **Standartlar:** Diğer şebeke protokollerinin (IEC 61850) rekabeti.

6. Genişletilmiş Perspektif ve Gelecek Teknolojiler

Alcaraz ve ark. çalışması, EVCI güvenliği bağlamında daha geniş teknolojik tartışmalar için bir sıçrama tahtası görevi görmektedir. Tespit edilen tehditler, özellikle inkar edilemezlik ve veri şeffaflığı sorunları, Blokzincir ve Yapay Zeka gibi tamamlayıcı teknolojilerin araştırılmasını zorunlu kılmaktadır.

6.1 Blokzincir: Bütünlük ve İnkar Edilemezlik İçin Bir Çözüm mü?

Makale, "İnkar Edilemezlik" (Repudiation) ve sayaç değerlerinin "Değiştirilmesi" (Tampering) risklerini tanımlamaktadır.[1] Blokzincir teknolojisi, merkezi olmayan yapısı sayesinde bu sorunlara potansiyel bir çözüm olarak görülmektedir. Şarj işlemlerinin dağıtık bir deftere kaydedilmesi, inkar edilemezliği matematiksel olarak garanti edebilir.[16]

- **Avantajlar:** Blokzincir, mikroşebeke içinde merkezi bir otoriteye (CSMS) ihtiyaç duymadan eşler arası (P2P) enerji ticaretini mümkün kılar. Bu, makalede belirtilen "CSMS Spoofing"

tehdidini ve tek hata noktasını ortadan kaldırabilir.[17]

- **Zorluklar ve Hesaplama Yükü:** Ancak, blokzincir entegrasyonu ciddi zorluklar barındırır. Konsensüs mekanizmalarının (Proof of Work/Stake) getirdiği işlem yükü ve gecikme süreleri (latency), gerçek zamanlı şebeke dengelemesi için engel teşkil edebilir.[13] Sınırlı işlemci gücüne sahip şarj istasyonu donanımlarına bir blokzincir katmanı eklemek, donanım maliyetlerini artırabilir ve "Hizmet Reddi" riskini, sistemin kendi kaynaklarını tüketmesi yoluyla ironik bir şekilde artırabilir.[13]

6.2 Yapay Zeka ve Dinamik Savunma

Alcaraz ve ark., Saldırı Tespit Sistemleri (IDS) kullanımını önermektedir. Endüstri 4.0 bağlamında modern IDS'ler, Yapay Zeka (YZ) ve Makine Öğrenmesi (ML) tabanlıdır.

- **Anomali Tespiti:** YZ, bir mikroşebekenin "normal" enerji tüketim modellerini öğrenebilir. Eğer manipüle edilmiş bir şarj profili, fizik kurallarına aykırı ani bir talep artışına neden olursa, YZ bunu siber trafik kurallarına uygun olsa bile (sentaktik olarak doğru OCPP mesajları) bir saldırı olarak işaretleyebilir.[15]
- **Adversarial AI (Düşman YZ):** Öte yandan, YZ'nin yükselişi iki ucu keskin bir kılıçtır. Saldırganlar, OCPP protokolünü "fuzzing" (rastgele veri enjeksiyonu) ile tarayarak sıfırıncı gün açıklarını insanlardan daha hızlı bulmak veya IDS'leri atlatmak için meşru kullanıcı davranışlarını taklit etmek amacıyla YZ'yi kullanabilir.[15]

6.3 V2G ve Genişleyen Saldırı Yüzeyi

Makale V2G'yi gelecek çalışma alanı olarak belirtse de, V2G risk profili şimdiden incelenmeyi hak etmektedir. V2G senaryosunda, EA sadece bir yük değil, bir jeneratördür.

- **Şebeke Destabilizasyonu:** Bir botnet tarafından kontrol edilen V2G özellikli araçlar, şebeke frekansıyla senkronize bir şekilde şarj/deşarj döngülerini osile edebilir. Bu "Salınım Saldırısı" (Oscillatory Attack), tüm güç sistemini dengesizleştirerek zincirleme arızalara yol açabilir.[18]
- **Batarya Bozunumu (Degradation):** V2G'nin kötü niyetli kontrolü, bataryayı agresif bir şekilde döngüye sokarak kullanıcının pahalı varlığına (araç bataryası) kalıcı hasar vermek için kullanılabilir. Bu durum, saldırının etkisini "Hizmet Reddi"nden "Mülkiyetin Tahribi"ne taşır.[18]

7. Stratejik Öneriler ve Sonuç

Alcaraz ve ark. makalesi ile destekleyici araştırmaların sentezi ışığında, bu rapor CSO'lar, DSO'lar ve politika yapıcılar için aşağıdaki stratejik önerileri sunmaktadır.

7.1 Stratejik Öneriler

1. **"Tasarım Yoluyla Güvenlik" (Secure-by-Design) Göçü:** Endüstri, OCPP 1.6'dan 2.0.1'e geçişi hızlandırmalıdır. Ancak bu geçiş, sadece bir sürüm yükseltmesi olmamalıdır. Arka uç sistemlerin mTLS (Profil 3) için Sertifika Otoritelerini (CA) destekleyecek şekilde yeniden mimarilendirilmesi şarttır. Halka açık altyapılarda Profil 1/2 kullanımı derhal sonlandırılmalıdır.[8]
2. **Fizik-Farkında Saldırı Tespiti:** Standart IT güvenlik duvarları mikroşebekeler için yetersizdir. Savunma sistemleri "fizik-farkında" (physics-aware) olmalıdır. Elektriksel parametreler (voltaj, akım, faz açısı) siber trafikle eşzamanlı izlenmelidir. Eğer bir siber komut (SetChargingProfile), yerel transformatörün fiziksel güvenlik limitleriyle çelişiyorsa, komut kriptografik olarak geçerli olsa bile yerel bir güvenlik mantığı tarafından engellenmelidir.[1]
3. **Fiziksel Güvenliğin Güçlendirilmesi:** Makale "CS Spoofing" tehdidini yüksek risk olarak tanımlar. Şarj istasyonları, kasa açıldığında anahtarları silen "anti-tamper" mekanizmaları ve anahtar depolama için Güvenli Elemanlar (Secure Elements / TPM) ile donatılmalıdır.[1]
4. **SD^{c+e} Metodolojisinin Standartlaştırılması:** Düzenleyiciler, risk değerlendirmeleri için Alcaraz ve arkadaşlarının SD^{c+e} metodolojisini bir standart olarak benimsemelidir. Operatörlerin sadece veri tehditlerini değil, "Enerji Tehditlerini" nasıl azalttıklarını kanıtlamaları zorunlu tutulmalıdır.

7.2 Sonuç

Cristina Alcaraz ve ekibinin *"OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0"* çalışması, kritik altyapı güvenliği literatüründe önemli bir kilometre taşıdır. Siber tehditler ile enerji varlıklarının kesişimini SD^{c+e} metodolojisi ile resmileştiren bu çalışma, modern mikroşebekelerdeki riskleri anlamak için gerekli çerçeveyi

sunmaktadır.

Gerçekleştirilen SWOT analizi ve genişletilmiş inceleme, OCPP v2.0.1'e geçişin gerekli ancak tek başına yeterli olmadığını göstermektedir. Fiziksel manipülasyondan sofistike enerji sahtekarlığına kadar uzanan tehdit yelpazesinin karmaşıklığı, bütüncül bir savunma stratejisi gerektirir. Bu strateji, güçlü kriptografik protokolleri (OCPP Güvenlik Profili 3), dinamik ve fizik-farkında tespit sistemlerini ve blokzincir gibi merkeziyetsiz doğrulama teknolojilerini birleştirmelidir.

Dünya elektrikli bir geleceğe doğru ilerlerken, şarj altyapısının güvenliği, enerji şebekesinin güvenliği ile eş anlamlı hale gelmiştir. Endüstri 4.0 çağında, siber güvenlik artık sadece verilerin korunması değil, fiziksel dünyanın ve enerjinin sürekliliğinin korunmasıdır. Gelecek, statik risk analizlerinin ötesine geçerek, dinamik, sürekli ve derinlemesine entegre edilmiş siber-fiziksel savunma mekanizmalarının inşasında yatmaktadır.

Alıntılanan çalışmalar

1. s10207-023-00698-8 (1).pdf
2. 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
3. What is new in OCPP 2.0.1 - Open Charge Alliance, erişim tarihi Kasım 22, 2025, https://openchargealliance.org/wp-content/uploads/2024/01/new_in_ocpp_201-v10.pdf
4. The challenges of migrating EV charging networks - Switch EV, erişim tarihi Kasım 22, 2025, https://www.switch-ev.com/blog/the-challenges-of-migrating-ev-charging-networks
5. Threat Modeling Methodology: STRIDE - IriusRisk, erişim tarihi Kasım 22, 2025, https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride
6. Modeling Threats to AI-ML Systems Using STRIDE - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/1424-8220/22/17/6662
7. Security Modelling for Cyber-Physical Systems: A Systematic Literature Review - arXiv, erişim tarihi Kasım 22, 2025, https://arxiv.org/html/2404.07527v3
8. 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
9. EVerest - Confluence - Atlassian, erişim tarihi Kasım 22, 2025, https://lf-energy.atlassian.net/wiki/display/EV/Cloud+Communication+WG
10. OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0 - ResearchGate, erişim tarihi Kasım 22, 2025, https://www.researchgate.net/publication/370558661_OCPP_in_the_spotlight_threats_and_countermeasures_for_electric_vehicle_charging_infrastructures_40
11. Cyber Resilience of Electric Vehicle Charging in Smart Grids: The Dutch Case - IEEE Xplore, erişim tarihi Kasım 22, 2025,

https://ieeexplore.ieee.org/iel8/6287639/10820123/11039783.pdf
12. Motivation and Design of the OCPP Security Service - Pacific Northwest National Laboratory, erişim tarihi Kasım 22, 2025, https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-35706.pdf
13. Optimizing demand response and load balancing in smart EV charging networks using AI integrated blockchain framework - PubMed Central, erişim tarihi Kasım 22, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11685539/
14. A Hybrid Blockchain Solution for Electric Vehicle Energy Trading: Balancing Proof of Work and Proof of Stake - MDPI, erişim tarihi Kasım 22, 2025, https://www.mdpi.com/1996-1073/18/7/1840
15. 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
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. The Role of Blockchain in Securing EV Charging Transactions | by AppVin Technologies, erişim tarihi Kasım 22, 2025, https://medium.com/@appvintechnologies/the-role-of-blockchain-in-securing-ev-charging-transactions-1d73460206ad
18. Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review - arXiv, erişim tarihi Kasım 22, 2025, https://arxiv.org/html/2503.15730v1