

Elektrikli Şarj İstasyonlarında Enerji Ölçüm Verisi Manipülasyonu ile Enerji Hırsızlığı

Anomali Senaryosu Raporu

HAZIRLAYAN : Mahmut DAĞAŞAN

ÖZET

Bu senaryoda, elektrikli araç şarj istasyonlarında kullanılan enerji ölçüm verilerinin (kWh) kötü niyetli kişiler tarafından manipüle edilmesi yoluyla gerçekleştirilen bir enerji hırsızlığı vakası ele alınmaktadır.

Saldırgan, şarj istasyonunun OCPP (Open Charge Point Protocol) üzerinden sisteme erişim sağlayarak, şarj oturumu sırasında ölçülen gerçek enerji tüketim değerlerini değiştirir. Böylece sistem, gerçekte verilen enerjiden daha az miktarı raporlar. Bu durum hem operatörün (CPO) gelir kaybına, hem de şebeke dengesinin bozulmasına neden olur.

Senaryoda; anormal enerji değerleri, sayaç geri dönüşleri (rollback), zaman damgası tutarsızlıkları ve log boşlukları gibi anomali göstergeleri analiz edilmiştir. Ayrıca saldırının tespit edilmesi ve önlenmesi için şifreleme, dijital imzalı firmware, güvenli kimlik doğrulama ve makine öğrenmesi tabanlı anomali izleme gibi önlemler önerilmektedir.

1. Giriş

Elektrikli araç (EV) kullanımının hızla artmasıyla birlikte, şarj istasyonları enerji altyapısının kritik bir parçası haline gelmiştir. Ancak bu sistemlerin artan dijitalleşmesi, beraberinde siber güvenlik risklerini de getirmektedir. Şarj istasyonları hem fiziksel hem de dijital saldırılara açık durumdadır.

Bu raporda, "Enerji Ölçüm Verisi Manipülasyonu ile Enerji Hırsızlığı" adlı anomali senaryosu ele alınmaktadır. Amaç, bu saldırının nasıl gerçekleştirilebileceğini, hangi verilerde anomalilerin gözlenebileceğini ve nasıl tespit edilebileceğini örnek bir vaka üzerinden açıklamaktır.

ENCS'nin (European Network for Cyber Security) "Security Threat Analysis for EV Charging Infrastructure" raporuna göre, şarj istasyonlarının %60'ından fazlası şifrelenmemiş veya zayıf kimlik doğrulamalı iletişim protokollerini kullanmaktadır. Bu durum, enerji ölçüm değerlerinin manipülasyonu riskini artırmaktadır [ENCS, 2022].

2. Senaryonun Tanımı

Bir saldırgan, uzaktan erişilebilen bir OCPP (Open Charge Point Protocol) bağlantısı üzerinden şarj istasyonunun yazılımına erişim sağlar. Bu istasyon, her şarj oturumunda tüketilen enerjiyi (kWh) sunucuya gönderir.

Saldırgan, bu ölçüm verisini manipüle ederek, istasyonun gerçekten verdiği enerji miktarını olduğundan daha düşük göstermektedir. Böylece:

- Operatör (CPO) faturalanması gereken enerjiyi eksik hesaplar,
- Kullanıcı gerçekte aldığı enerjidenden daha az ödeme yapar,
- Aradaki fark saldırgan tarafından kazanç olarak yönlendirilir.

Hamdare ve arkadaşlarının 2023 yılında *Sensors* dergisinde yayımlanan “Cybersecurity Risk Analysis of Electric Vehicles Charging Stations” adlı makalesinde belirtildiği gibi, bu tür saldırılar hem ekonomik kayıplara hem de şebeke güvenliği risklerine neden olabilir [Hamdare et al., 2023].

3. Saldırı Süreci (Aşamalar)

Aşama	Açıklama
1. Keşif (Reconnaissance)	Saldırgan, hedef şarj istasyonunun yazılım sürümü, ağ yapılandırması ve açık portlarını tarar.
2. Erişim Sağlama	Zayıf parola veya açık bir OCPP bağlantısı üzerinden yetkisiz erişim elde edilir.
3. Manipülasyon	Ölçüm verisi (örneğin <code>meter_value</code> veya <code>stop_transaction</code> parametreleri) değiştirilir. Gerçek değer 32.4 kWh iken sistem 26.1 kWh olarak kaydedeler.
4. İzleri Gizleme	Log kayıtları silinir veya zaman damgalarıyla oynanarak denetimlerde tutarlılık sağlanmaya çalışılır.

Benzer bir olay *Wired* dergisinin 2023 tarihli “EV Charger Hacking Poses a ‘Catastrophic’ Risk” haberinde raporlanmıştır. Bu haberde, uzaktan yönetilebilen şarj istasyonlarının kötü niyetli kişilerce topluca manipüle edilmesi halinde enerji dağıtım şebekesinde ciddi dengesizlikler oluşabileceği belirtilmiştir [Wired, 2023].

4. Veri Üzerindeki Anomaliler

Bu saldırının tespiti için analiz edilmesi gereken temel göstergeler şunlardır:

Gözlenen Anomali	Açıklama	Tespit Yöntemi
Beklenenden düşük kWh	Aynı model araç ve benzer sürelerde, ortalamanın %15 altında enerji raporlanması	Zaman serisi analizi / ortalama karşılaştırma
Meter değerinin azalması (rollback)	Sayaç değerinin bir anda geriye düşmesi	Sıralı veri kontrolü
Log boşlukları	Ölçüm aralıklarında kayıt eksikliği	Log zaman damgası analizi
Firmware değişikliği	Planlanmamış güncelleme veya versiyon değişimi	Sistem denetimi
Zaman uyumsuzluğu (timestamp skew)	Ölçüm ve işlem zamanları arasında olağanüstü fark	Zaman serisi bütünlük testi

Bu göstergeler, *IEEE Journal of Automation Sinica*'da yayımlanan "Energy Theft Detection in Smart Grids: Taxonomy and Techniques" makalesinde tanımlanan enerji hırsızlığı tespit yöntemleriyle de paralellik göstermektedir [IEEE, 2021].

5. Tespit ve Önleme Önerileri

Kısa vadede:

- Şarj istasyonlarından gelen ölçüm verileri için **doğrulama algoritması** uygulanmalıdır.
- "Firmware version change" ve "meter rollback" olayları için **otomatik alarm** mekanizması kurulmalıdır.
- Veri aktarımı sırasında **uçtan uca şifreleme (mutual TLS)** zorunlu hale getirilmeli.

Orta-uzun vadede:

- İstasyonlara **secure boot** ve **dijital imzalı firmware** sistemi entegre edilmeli.
- Anomalileri tespit etmek için **makine öğrenmesi tabanlı izleme sistemi** kurulmalı.
- Fiziksel saldırılarla veri manipülasyonunu ilişkilendirmek için **bölgesel olay korelasyonu** yapılmalı (örneğin kablo hırsızlığı raporları ile veri anomalileri

karşılaştırılmalı).

ElaadNL'nin 2023 tarihli “*Security Architecture for EV Charging Infrastructure*” raporunda, bu tür siber-fiziksel saldırıların önlenmesi için **sertifika tabanlı kimlik doğrulama ve periyodik firmware denetimi** önerilmektedir [ElaadNL, 2023].

6. Sonuç

Bu senaryo, elektrikli şarj altyapısında ölçüm verilerinin manipülasyonu yoluyla gerçekleştirilebilecek enerji hırsızlığının ciddi bir tehdit olduğunu göstermektedir.

Bu tür saldırılar sadece finansal kayıplara değil, aynı zamanda enerji şebekesinin güvenilirliğine ve kullanıcı güvenliğine de zarar verebilir. Etkin tespit için teknik, organizasyonel ve denetimsel önlemlerin birlikte uygulanması gerekmektedir.

7. Kaynakça

1. ENCS, *Security Threat Analysis for EV Charging Infrastructure*, 2022.
2. Hamdare, S. et al., *Cybersecurity Risk Analysis of Electric Vehicles Charging Stations, Sensors*, 2023.
3. *Wired*, “EV Charger Hacking Poses a ‘Catastrophic’ Risk”, 2023.
4. ElaadNL, *Security Architecture for EV Charging Infrastructure*, 2023.
5. *IEEE Journal of Automation Sinica*, “Energy Theft Detection in Smart Grids: Taxonomy and Techniques”, 2021.

SWOT ANALİZİ

Enerji Ölçüm Verisi Manipülasyonu ile Enerji Hırsızlığı

İç Faktörler (Kontrol Edilebilir)	Güçlü Yönler (Strengths - S)	Zayıf Yönler (Weaknesses - W)
Siber Güvenlik Altyapısı	S1. Güçlü Şifreleme: İletişim protokollerinin (OCPP) zorunlu TLS şifrelemesi kullanması, Veri Manipülasyonu riskini iletişim sırasında azaltır.	W1. Zayıf Kimlik Doğrulama: RFID kartlarının kolayca klonlanabilmesi veya mobil uygulama API'lerindeki zayıflıklar nedeniyle Enerji Hırsızlığına (Yetkisiz Sarja) açık olma.
	S2. Uzaktan Güncelleme (OTA): Yazılımların (firmware) uzaktan hızla güncellenecek yeni keşfedilen veri manipülasyonu açıklarının yanında kapatılabilmesi.	W2. Log ve Kayıt Tutma Eksikliği: Veri manipülasyonu girişimlerinin veya hırsızlık olaylarının takibini zorlaştıran yetersiz veya merkezi olmayan loglama sistemleri.
	S3. Merkezi Yönetim Yeteneği: Tüm istasyonların veri akışının tek bir noktadan izlenmesi, anormal şarj verilerinin ve hırsızlık girişimlerinin tespiti için altyapı sunması.	W3. Kullanıcı Arayüzü Güvenliği: Dokunmatik ekranlar ve fiziksel bağlantı noktaları gibi kullanıcı arayüzlerinin fiziksel kurcalama ve veri çalma girişimlerine karşı hassas olması.

Dış Faktörler (Kontrol Dışı)	Fırsatlar (Opportunities - O)	Tehditler (Threats - T)

Pazar Çevresi ve Tehditler	O1. Blockchain Teknolojisi: İşlemleri şeffaf ve değiştirilemez hale getiren blok zinciri tabanlı kimlik doğrulama/fatura sistemlerinin entegrasyon potansiyeli (Veri Bütünlüğünü artırma).	T1. Gelişmiş Hacker Teknikleri: Siber suçluların şarj istasyonlarını hedef alan gelişmiş yazılımlar ve teknikler kullanarak veri manipülasyonu (sayaç okumalarını değiştirme) girişimleri.
	O2. Siber Sigorta ve Standartlar: Şarj ağları için siber sigorta ürünlerinin ve zorunlu güvenlik standartlarının (ISO/IEC 27001 vb.) yaygınlaşması, yatırımcının güvenini artırma.	T2. Klonlama ve Taklit Kolaylığı: Piyasadaki ucuz ekipmanlarla Enerji Hırsızlığı amacıyla RFID kartlarının veya temel kimlik doğrulama tokenlarının kolayca klonlanabilmesi.
	O3. Yapay Zeka (YZ) Destekli Anomali Tespit: YZ sistemleri ile normal şarj seanslarından sapmaların (aşırı uzun şarj süreleri, anormal tüketimler) otomatik tespiti (Hırsızlığı önleme).	T3. Tedarik Zinciri Güvenlik Açıkları: İstasyon donanımının üçüncü taraf tedarikçilerden kaynaklanan ve manipülasyona olanak tanıyan arka kapılar (backdoor) içermesi.

Enerji Hırsızlığı ve Veri Manipülasyonuna Yönelik Stratejiler

Strateji Türü	Kombinasyon	Strateji Önerisi
SO Stratejisi	S3 + O3	Merkezi yönetim sistemi (S3) üzerinde YZ destekli anomali tespiti (O3) yazılımları kullanarak, veri manipülasyonu girişimlerini ve enerji hırsızlığına işaret eden anormal şarj paternlerini gerçek zamanlı olarak belirleme.
WO Stratejisi	W1 + O1	Zayıf kimlik doğrulama (W1) açığını kapatmak için, blok zinciri (O1) tabanlı veya tokenizasyon sistemleri gibi daha gügü ve klonlanması imkansız kimlik doğrulama yöntemlerine geçiş yapma.
ST Stratejisi	S1 + T1	Güçlü TLS şifrelemesini (S1) kullanarak, gelişmiş hacker tekniklerine (T1) karşı istasyon ile merkezi sistem arasındaki veri paketlerinin değiştirilmesini imkansız hale getirme.
WT Stratejisi	W2 + T2	Yetersiz loglama sistemini (W2) geliştirerek, klonlanmış kimliklerle (T2) yapılan yetkisiz şarj seanslarına dair tüm işlem kayıtlarını detaylı ve güvenli bir şekilde saklayarak yasal takibat için kanıt oluşturma.

