Electro-Mimetic Load Resonance Attack (EMLR) — Yük Rezonansı Taklitli Enerji Akışı Sabotajı

Ad-Soyad : Abdulselam Elahmed

No : 230541607

Anomali Tanımı

EMLR anomalisi, elektrikli araç şarj istasyonlarında (EVCS) saldırganın şarj yük profilini taklit ederek sistemde sahte rezonans dalgaları oluşturması sonucu enerji akışının düzensizleşmesine, yanlış tüketim ölçümlerine, ekipman zorlanmasına ve potansiyel fiziksel hasara yol açan gelişmiş bir sabotaj türüdür.
Bu anomali sırasında sahte yük dalgaları gerçek şarj yükü gibi algılandığı için sistem, enerji düzenleme algoritmalarını hatalı çalıştırır. Bu durum hem güvenlik hem de operasyonel stabilite için kritik tehdit oluşturur.

Olası Nedenler 🔍

Kategori	Olası Sebep	Açıklama
Sensör Manipülasyonu	Sahte rezonans sinyali enjeksiyonu	Saldırgan, akım/gerilim sensörlerine düşük genlikli fakat yüksek frekanslı sahte sinyaller gönderir.
Donanım Zafiyetleri	EMI zayıf filtreleme	Zayıf elektromanyetik filtreleme nedeniyle saldırganın ürettiği sinyaller sisteme karışabilir.
Protokol Açıkları	IEC 61851 güç modülasyon sapması	Protokolde sinyal bütünlüğü doğrulamasının olmaması saldırganın yük taklidi yapmasına izin verebilir.
Firmware Eksikleri	Rezonans tespit modülünün olmaması	Şarj cihazı içindeki kontrolör sahte rezonans frekanslarını ayırt edemez.
Siber Saldırı	Güç yönetimi algoritmalarının manipülasyonu	OCPP üzerinden gelen komutlar değiştirilerek yanlış yük tahmini yapılabilir.

Kategori	Olası Sebep	Açıklama
Çevresel Faktörler	EMI yoğunluğu	Yoğun elektromanyetik ortam, saldırı sinyallerinin gizlenmesini kolaylaştırır.
İç Tehditler	Bakım personeli tarafından port müdahalesi	Yetkili görünen bir iç kişi fiziksel portlara sinyal enjekte ederek saldırıyı başlatabilir.
Donanım Arızaları	Sensör kalibrasyon kayması	Sistem doğal hataları saldırı sinyaliyle karıştırarak yanlış enerji akışı hesaplaması yapabilir.

Olası Riskler ve Etkiler ⚠

- Şarj istasyonlarında **ani aşırı akım** algısı veya **düşük yük simülasyonu** nedeniyle yanlış enerji yönetimi.
- Ekipman bileşenlerinde **ısı artışı**, **işlemsel stres** ve uzun vadeli fiziksel hasar.
- Güç şebekesinde **mikro-destabilizasyon** ve senkron sapması.
- Yanlış enerji ölçümleri nedeniyle **fatura uyuşmazlıkları**, hukuki sorunlar ve müşteri şikayetleri.
- OCPP merkezinde hatalı kararlar sonucunda **yanlış yük dağıtımı**, **kesinti**, **hizmet durması**.
- Şarj istasyonlarının koruma devrelerinin yanlış tetiklenmesiyle **ani duruşlar**.
- V2G senaryolarında sahte yük nedeniyle **şebekeye yanlış güç geri beslemesi**.
- Uzun vadeli operasyonel maliyetlerde artış, bakım sürelerinin uzaması.

İlgili Standart Referans 📘

- **IEC 61851** – EV şarj protokollerinde güç sinyali uyumu.
- **IEC 62196** – Donanım port yapıları ve güvenlik gereksinimleri.
- **ISO 15118** – Yük profil yönetimi ve enerji veri bütünlüğü.
- **ISO/IEC 27001** – Bilgi güvenliği kontrol mekanizmaları.
- **NIST SP 800-82** – Endüstriyel kontrol sistemleri güvenlik kılavuzu.
- **NIST SP 800-30** – Risk değerlendirme metodolojisi.
- **NERC CIP** – Kritik altyapı elektrik güvenliği gereksinimleri.
- **EN 61000** – EMC (Electromagnetic Compatibility) standartları.

Çözüm Önerileri 🛠️

- **Rezonans Filtreleme:** Yüksek frekanslı sahte sinyaller için EMI filtreleri güçlendirilmeli.
- **Sinyal Bütünlüğü Doğrulama:** IEC 61851 güç sinyallerine kriptografik imza uygulanmalı.
- **Sensör Tamper Detection:** Sensörlere fiziksel müdahaleyi algılayan modüller eklenmeli.
- **OCPP Anomali Tespiti:** Gerçek yük verileriyle rezonans frekansları sürekli kıyaslanmalı.
- **Model Bazlı Tahmin:** Şarj istasyonunun beklenen yük davranışı tahminlenip anomali sapmaları işaretlenmeli.
- **Şebeke Seviyesi Takibi:** Birden fazla istasyonun senkron rezonans davranışı analiz edilmeli.
- **Firmware Güncellemeleri:** Rezonans tespit algoritmaları güncellenmeli.
- **Operasyonel Güvenlik:** Bakım personeli erişimi kayıt altına alınmalı.

Sonuç ve Değerlendirme 📄

EMLR anomalisi; modern şarj istasyonlarının hem elektriksel hem de siber katmanlarını hedefleyen karmaşık ve hibrit bir saldırı türüdür.
Yük rezonansı taklit edilerek sistemin doğal çalışma düzeni bozulur, enerji akışı yanlış hesaplanır ve fiziksel hasara yol açabilecek tehlikeli bir durum oluşur.

Bu nedenle:

- sürekli izleme,
- sinyal bütünlüğü doğrulama,
- EMI dayanım iyileştirmeleri
- ve OCPP tabanlı anomali tespiti

kritik öneme sahiptir.

EMLR'nin etkili şekilde yönetilmemesi, hem operasyonel hem de güvenlik açısından büyük ölçekli arızalara ve şebeke dengesizliğine yol açabilir.

Kaynakça 📚

- IEC 61851 – Electric Vehicle Conductive Charging System
- ISO 15118 – Vehicle-to-Grid Communication Interface
- NIST SP 800-82 – Industrial Control System Security

- EN 61000 – Electromagnetic Compatibility Requirements
- Whitman & Mattord, *Principles of Information Security*
- Debra Shinder, *Security Log Management*
- E. Stewart, *Power System Harmonics and Resonance*