ANOMALİ SENARYOSU SİMÜLASYON RAPORU

Elektrikli Araç Şarj İstasyonlarında Siber Güvenlik

Hazırlayan:	Oğuzhan Erdoğan
Senaryo Adı:	Sensör Verisi Zehirleme (Sensor Data Poisoning - SDP)
Tarih:	24 Aralık 2025
Kapsam:	Yapay Zeka Güvenliği, Model Drift, MitM Saldırıları

---

1. Senaryo Tanımı ve Teknik Arka Plan

Bu senaryo, şarj istasyonlarındaki (CP) enerji ölçümü yapan sensörlerin verilerinin istatistiksel olarak zehirlenmesi (poisoning) yoluyla, merkezi sistemdeki (CSMS) **yapay zekâ tabanlı anomali tespit sistemlerinin (IDS) yanıltılmasını** ele alır.

Makine öğrenmesi tabanlı IDS sistemleri, eğitildikleri veri ile güçlü bir ilişki gösterir. Eğer "öğrenme sürecine" kirli veri (poisoned data) enjekte edilirse, model zamanla **yanlış normal profiller** öğrenmeye başlar. Buna literatürde **"Model Drift"** veya **"Model Dejenerasyonu"** denir.

Simülasyonun Amacı

Sistemi aniden çökertmek değil; görüntülenen veriler üzerinde uzun süreli ve küçük manipülasyonlar yaparak güvenlik sistemini "körleştirmek" (Algoritmik Körlük) ve gelecekteki büyük saldırıları gizlemektir.

2. Saldırı Metodolojisi

Simülasyon ortamında, `EmuOCPP` altyapısı ve `MitM Proxy` kullanılarak aşağıdaki 4 aşamalı saldırı döngüsü gerçekleştirilmiştir:

1. **Keşif:** Saldırgan, hangi istasyonların telemetri verilerinin model eğitimine gönderildiğini belirler.
2. **İnce Müdahale (Subtle Manipulation):** Sensör verilerinde (MeterValues) ani değişiklikler yerine, modelin tolerans sınırları içinde kalan **%2-5 oranında küçük sapmalar** (±%2-5) enjekte edilir.
3. **Kümülatif Etki:** Zaman içinde bu küçük sapmalar birikir ve merkezi model, bu hatalı veriyi "yeni normal" olarak tanımlar.

4. **Fırsat:** Model zehirlendikten sonra, saldırgan büyük bir manipülasyon (örn. enerji hırsızlığı) yaptığında, IDS bunu artık bir anomali olarak algılamaz.

3. Simülasyon Bulguları

Gerçekleştirilen testte, Şarj İstasyonu ile Merkezi Sistem arasına yerleştirilen Proxy yazılımı, `MeterValues` paketlerini anlık olarak yakalamış ve değerleri sistematik olarak değiştirmiştir.

[BURAYA SİMÜLASYON EKRAN GÖRÜNTÜSÜNÜ YAPIŞTIRIN]

(Dosya: simülasyon.jpg)

İpucu: Sol tarafta Sunucu, ortada Saldırgan, sağda İstasyon terminali olmalı.

Şekil 1: Simülasyon sırasında alınan anlık veri akışı. Sağda CP (1000 Wh) üretirken, solda CSMS (1050 Wh) olarak kaydetmektedir.

Ekran görüntüsünde görüldüğü üzere:

- **CP (Kaynak):** 1000 Wh gerçek tüketim bildiriyor.
- **MitM (Saldırgan):** Veriyi yakalayıp %5 artırıyor (Zehirleme).
- **CSMS (Hedef):** Veriyi 1050 Wh olarak işliyor ve anomali uyarısı vermiyor.

4. Önlemler ve Azaltma Stratejileri

Bu tür "sinsi" saldırılara karşı alınması gereken teknik önlemler şunlardır:

- **Adversarial Training:** Model eğitiminde, bu tür zehirli veri örnekleri kullanılarak modelin dayanıklılığı artırılmalıdır.
- **Robust İstatistik:** Ortalama yerine Medyan tabanlı ve dışlanmış değerlere (outlier) dirençli metrikler (örn. MAD) kullanılmalıdır.

- **Veri Kaynağı Doğrulaması:** Telemetri zincirinde verinin kaynağının kriptografik olarak imzalanması (Data Signing) şarttır.

---

5. Sosyal Medya İletişim Planı (LinkedIn)

Bu teknik başarının, profesyonel ağlarda hem teknik yetkinliği göstermek hem de farkındalık yaratmak amacıyla paylaşılması planlanmıştır.

Önerilen Paylaşım Metni

Başlık: Elektrikli Araç Şarj Ağlarında "Sessiz" Tehdit: Sensör Verisi Zehirleme (SDP) Simülasyonu

Bugün Bilgi Sistemleri Güvenliği dersimiz kapsamında, elektrikli araç şarj istasyonlarına (EVSE) yönelik oldukça sofistike bir siber saldırı senaryosunu simüle ettik: **Sensör Verisi Zehirleme (SDP).**

Geleneksel siber saldırıların aksine, SDP sistemi çökertmeyi hedeflemiyor. Tam tersine, sistemin **"öğrenme sürecini"** hedef alıyor.

Simülasyon Detayları:
Geliştirdiğimiz Python tabanlı simülasyon ortamında, şarj istasyonundan (CP) merkezi sisteme (CSMS) giden enerji verilerini "Man-in-the-Middle" (MitM) yöntemiyle yakaladık. Veriler üzerinde ani değişimler yapmak yerine, sadece **%2-5 oranında, sistematik ve küçük sapmalar** ekledik.

Sonuç:
Merkezi sistemdeki Yapay Zeka tabanlı Anomali Tespit Sistemi (IDS), bu küçük sapmaları "normal varyasyon" olarak algıladı. Ancak zamanla bu manipülasyonlar birikerek modelin "normal" algısını kaydırdı (Model Drift). Sonuç olarak, sistem büyük enerji hırsızlıklarını artık tehdit olarak görmemeye başladı.

Bu çalışma, siber güvenlikte sadece ağın değil, **verinin bütünlüğünün (Data Integrity)** ve yapay zeka modellerinin güvenliğinin (Adversarial ML) ne kadar kritik olduğunu bize gösterdi.

Simülasyon altyapısında emeği geçen ekip arkadaşlarıma teşekkürler!

#CyberSecurity #ElectricVehicles #OCPP #AIsecurity #Simulation #DataPoisoning #InfoSec #Engineering