ANOMALİ SENARYO RAPORU: AŞIRI ISINMA VE TERMİNALE ZARAR

Ders: Bilgi Sistemleri Güvenliği

Proje: Şarj İstasyonlarının Güvenliği

Tarih: 01.11.2025

Hazırlayan: Kadir Başer (Takım 1)

1. 📝 Özet ve Tanım

Saldırganın, şarj istasyonunun kritik termal sensörlerinden gelen veriyi **yazılımsal olarak manipüle etmesi (veri sahtekarlığı / spoofing)** sonucu, istasyonun veya araç bataryasının (Battery Management System - BMS) soğutma mekanizması (fanlar / pompalar) devreye girmez.

Bu durum, özellikle **DC hızlı şarj** sırasında çekilen yüksek akımın neden olduğu ısının kontrolsüz bir şekilde yükselmesine; kabloların ve güç modüllerinin erimesine ve potansiyel olarak **yangın riskine** yol açar.

Normal Akış (Beklenen)

Sistemin sıcaklık yönetiminde beklenen süreç:

Aşama	Olay	Mekanizma
Başlatma	Şarj başlar, yüksek akım çekimi başlar.	Sistem sürekli sıcaklık ölçümü yapar.
Koruma	Sıcaklık eşik değere (T_{ESIK}, örn: $70^{\circ}C$) ulaşır.	Kontrol birimi soğutmayı açar veya şarj akımını düşürür (derate).
Güvenli Durdurma	Sıcaklık kritik eşiği (T_{KRITIK}, örn: $90^{\circ}C$) aşarsa.	Şarj tamamen durdurulur.

Anomali Tanımı (Gözlenen)

Şarj istasyonu veya araç kritik sıcaklık eşiklerini aşmış olmasına rağmen:

- Soğutma aktüatörleri (fan / pompa) çalışmıyor veya düşük hızda kalıyor.

- Şarj istasyonu, aşırı ısınan kabloya rağmen akım düşürme veya şarjı durdurma eylemi gerçekleştirmiyor.
- Log kayıtlarında, ortam ve akım yüksek görünse bile, kritik sensör değerleri **anormal derecede düşük** raporlanıyor (örn. sensör değeri $30^{\circ}C$ gösteriyor).

Etki Analizi

- **Güvenlik (Kritik):** Kontrolsüz aşırı ısınma, **termal kaçağa (yangın / patlama riski)** yol açabilir.
- **Ekipman Hasarı:** Güç dönüştürücüleri ve kablolar yanarak **kalıcı donanım arızası** oluşturabilir.
- **Operasyonel:** Fiziksel hasar nedeniyle uzun süreli hizmet kesintisi ve yüksek onarım maliyetleri.

2. 🛡️ Tespit Kuralları ve Risk Azaltma

Tespit Kuralları (Teorik IF/THEN Mantığı)

Bu tip bir sahtekarlığı/sensör tutarsızlığını tespit etmek için kullanılacak temel mantık kuralları:

- KURAL-1 (Temel Spoofing Tespiti):

$$IF \ (AKIM > A\_HIGH) \ AND \ (KRITIK\_SICAKLIK < T\_SAFE) \ AND \ (SOGUTMA = OFF) \ THEN \ RAISE \ ALARM$$

- KURAL-2 (Çevresel Tutarsızlık):

$$IF \ (AKIM > A\_HIGH) \ AND \ (KRITIK\_SICAKLIK < T\_SAFE) \ AND \ (ORTAM\_SICAKLIGI > T\_ORTA) \ THEN \ RAISE \ ALARM$$

- KURAL-3 (Akım / Sıcaklık Korelasyonu):

$$IF \ (AKIM \ ani \ olarak \ artıyor) \ AND \ (KRITIK\_SICAKLIK \ sabit \ veya \ tepki \ vermiyor) \ THEN \ RAISE \ ALARM$$

Risk Azaltma Önerileri

- **Korelasyon Analizi:** Kritik sensör verilerini çekilen akım, ortam sıcaklığı ve donanım telemetrisi ile sürekli **çapraz doğrulayın**.

- **Donanımsal Yedekleme:** Yazılımla manipüle edilemeyen, tamamen donanıma dayalı **termal kesiciler ve sigortalar** kullanın.
- **Veri Bütünlüğü:** Kritik sensör verilerine **dijital imza** veya benzeri bütünlük kontrolleri ekleyin.
- **İzleme & Alarm:** Threshold tabanlı ve **istatistiksel anomali tabanlı (ML destekli)** tespit sistemleri kurun; alarm durumunda otomatik güvenli durdurma mekanizmaları olsun.

3. 🎯 Proje Hedefleri: SMART Metodu

Bu senaryoya karşı geliştirilecek savunma mekanizmasını ölçmek için belirlenen hedefler:

SMART Kriteri	Hedef Açıklaması
S (Specific)	Geliştirilen Güvenlik Uygulaması, **DC Hızlı Şarj** sırasında termal sensör verisi sahtekarlığı kaynaklı sıcaklık anomalisini, **çapraz korelasyon analizi** kullanarak tespit etmelidir.
M (Measurable)	Anomali başlatıldıktan sonra sistem, T_{ESIK} değerine ulaşılmadan ve **maksimum 500 milisaniye** içinde alarm vermeli ve şarjı durdurmalıdır.
A (Achievable)	Simüle edilen termal saldırı senaryosuna karşı, **%98 oranında doğru tespit (True Positive)** başarısı elde edilmelidir.
R (Relevant)	Bu savunma çözümü, hem donanımı **yangın/erime riskine** karşı koruyarak can güvenliğini sağlamalı hem de operasyonel kesintileri önlemelidir.
T (Time-bound)	Savunma uygulaması ve otomatik engelleme mekanizması (IPS) **[10. Hafta - Final Teslimi]** itibarıyla entegre sistemde başarıyla test edilmiş olmalıdır.

4. 🔎 Anomali Analizi: SWOT

Bu senaryoya özel saldırı ve savunma yaklaşımlarının değerlendirilmesi:

Kategoriler	Açıklama
Güçlü Yönler (Strengths) 💪	

S1. Protokol Bilgisi: OCPP komut ve veri akışı bilgisine sahip olmak, **özelleştirilmiş, protokole duyarlı tespit kuralları** yazmayı kolaylaştırır.	
S2. Korelasyon İmkanı: Tespiti için sadece bir sensöre değil, **akım (A), voltaj (V) ve ortam sıcaklığı** gibi birden fazla veri noktasına dayalı güçlü korelasyon analizi geliştirme potansiyeli vardır.	
S3. Kritikalite: Bu anomali, **en yüksek güvenlik riskini (yangın)** taşıdığı için, projenin sektörel değeri yüksektir.	
Zayıf Yönler (Weaknesses) 😟	
W1. Gerçek Donanım Kısıtlaması: Simülasyon ortamında gerçek bir termal sensör manipülasyonunun karmaşıklığını tam olarak taklit etmek zordur; **gerçek dünyada test edilebilirlik sınırlıdır**.	
W2. Hız Gereksinimi: Termal kaçak çok hızlı gelişebileceğinden, tespit ve otomatik müdahale (IPS) mekanizmasının **gecikmesinin (latency) çok düşük** olması gerekir.	
Fırsatlar (Opportunities) ✨	
O1. Sektörel İhtiyaç: EVCS güvenliğinde **donanım tabanlı fiziksel riske** odaklanan çözümler (özellikle yangın önleme) büyük bir pazar ihtiyacına cevap verir.	
O2. Entegrasyon Fırsatı: Geliştirilen Korelasyon/IPS modülü, doğrudan bir **OCPP Güvenlik Ağ Geçidi (Security Gateway)** ürününe entegre edilebilir.	
Tehditler (Threats) 💀	
T1. Saldırganın Erişim Metodu: Saldırgan, sensör verisini sadece iletişim katmanında değil, doğrudan şarj istasyonunun **yerel kontrol birimi** içinden manipüle ederse, uzaktan tespit mekanizmanız etkisiz kalır.	
T2. Pasif Hasar: Saldırganın aktif manipülasyonu sona erse bile, yüksek ısı nedeniyle **geriye dönük hasar** devam edebilir ve yangın başlayabilir.	