ELEKTRİKLİ ARAÇ ŞARJ İSTASYONLARINDA ANOMALİ TESPİTİ VE SİBER-FİZİKSEL ZAFİYET ANALİZİ — GENEL PROJE RAPORU

1. Giriş

Elektrikli araç şarj altyapıları günümüzde akıllı ulaşım sistemlerinin kritik bir bileşenine dönüşmüş durumda. Şarj istasyonları; OCPP (Open Charge Point Protocol), ISO 15118 gibi haberleşme standartlarına dayanarak merkezi yönetim sistemleri (CSMS) ile haberleşir. Bu alt yapı; faturalama, enerji yönetimi, kimlik doğrulama, operasyonel güvenlik ve şebeke istikrarı açısından kritik veriler üretir.

Bu ders kapsamında amaç; elektrikli araç şarj altyapılarında ortaya çıkabilecek güvenlik açıklarını simüle ederek **gerçek dünya siber-fiziksel tehditlerinin** nasıl işlediğini anlamak, bu tehditleri analiz etmek, tespit yöntemlerini tartışmak ve her öğrenci tarafından belirlenen farklı bir anomaliyi teknik olarak incelemektir.

Her öğrenci kendi anomalisini tanımlamış, teknik analizini yapmış ve simülasyon/kanıt-of-concept çalışması hazırlamıştır. Bu rapor, tüm anomalileri bütünleştiren genel bir değerlendirme niteliğindedir.

2. Projede İncelenen Anomalilerin Genel Özeti

Proje kapsamında incelenen anomaliler, protokol zafiyetlerinden donanımsal sorunlara, finansal manipülasyonlardan zaman senkronizasyon saldırılarına kadar geniş bir çeşitliliğe sahiptir. Aşağıdaki tablo projeye dâhil edilen tüm anomali türlerini özetler.

2.1. Diferansiyel Gecikme Enjeksiyonu (DLI) – Gizli Enerji Hırsızlığı

Bu anomali, şarj istasyonundan CSMS'e gönderilen sayaç verilerinin zaman damgalarının manipüle edilmesiyle oluşur. Raporlar geciktirilerek enerji tüketiminin bir kısmı sistemden kaçırılır. Fark edilmesi zor, uzun vadeli finansal kayba yol açan bir saldırıdır.

2.2. Bellek Sızıntısı (Memory Leak) – Donanım Kaynak Tükenmesi

Şarj istasyonunun kontrol yazılımındaki hatalar nedeniyle RAM sürekli artar ve istasyon bir süre sonra hizmet dışı kalabilir. Bu bir *hizmet reddi (DoS)* türüdür ve operasyonel sürekliliği etkiler.

2.3. OCPP Üzerinden Finansal Manipülasyon (Tampering)

StopTransaction mesajına düşük sayaç değeri enjekte edilerek fatura tutarı düşürülür. OCPP'nin TLS zorunlu olmaması bu saldırıyı mümkün kılar.

2.4. Ghost RFID Event – Fiziksel Kart Olmadan Yetkisiz Oturum

RFID okuyucu elektromanyetik parazit, firmware hatası veya replay saldırısı nedeniyle "hayalet" kart görür. Fiziksel kart okutulmadan oturum başlatılabilir.

2.5. GPS Spoofing – Konum Sahtekarlığı ve Tarife Arbitrajı

OCPP mesajlarındaki koordinat manipülasyonu ile istasyon farklı bir coğrafi bölgede gösterilir. Bu durum bölgesel tarife farklarından yararlanılarak finansal kazanç elde edilmesine yol açabilir.

2.6. Phantom Fleet – V2G Piyasa Manipülasyonu

Gerçekte var olmayan araçlardan V2G enerji katkısı raporlanır. Şebeke operatörü, fiziksel olarak mevcut olmayan sanal bir filoya ödeme yapar. Kritik altyapı seviyesinde etkisi büyük olan bir saldırıdır.

2.7. Session Fork / Oturum Çatallama Saldırısı

Saldırgan, aynı istasyon kimliğini kullanarak ikinci bir WebSocket bağlantısı açar. CSMS aynı ID ile iki istasyonu ayırt edemediği için sahte StopTransaction mesajları kabul edebilir.

2.8. StopTransaction Bastırılması – Zombi Şarj Oturumu

Saldırgan StopTransaction mesajını MITM ile düşürür. Şarj fiilen bitse bile CSMS oturumu aktif sanır. Bu durum fatura kaymalarına, enerji hırsızlığına ve veri tutarsızlıklarına yol açar.

2.9. Yetkilendirme Token/Nonce Replay Anomalisi

Önceden yakalanmış bir yetkilendirme token/nonce yeniden oynatılarak yetkisiz şarj oturumları başlatılabilir. Token'ın tek kullanımlık olmaması temel zafiyettir.

3. Anomalilerin Ortak Temaları ve Risk Kümeleri

Yukarıdaki anomaliler farklı teknik yöntemlere sahip olsa da, tamamı ortak bazı güvenlik zayıflıklarını işaret etmektedir.

3.1. Protokol Güvenliği Eksiklikleri

Çoğu saldırı OCPP 1.6'nın aşağıdaki kısıtlarından doğmaktadır:

- TLS şifrelemesi zorunlu değildir
- CP kimliği yeterince doğrulanmaz
- Mesaj imzalama yoktur
- Session tekilliği garanti edilmez

Bu nedenle MitM, spoofing, sahte mesaj enjeksiyonu ve replay saldırıları kolaylaşır.

3.2. Zaman Senkronizasyonu ve Log Tutarsızlıkları

Özellikle DLI (gecikme enjeksiyonu) ve Zombi Oturum gibi saldırılar, zaman damgası manipülasyonlarından doğar. Kritik altyapılarda 2 ms hassasiyetle zaman uyumu gereklidir.

3.3. Kimlik Doğrulama Zayıflıkları

- RFID sistemleri parazite açıktır
- Token/nonce mekanizması yetersizdir
- CP-ID doğrulaması sadece WebSocket yoluna bağlıdır

Bunlar Ghost RFID, Token Replay ve Session Fork gibi saldırılara kapı açar.

3.4. Siber-Fiziksel Ayrışma

Bazı anomaliler (Phantom Fleet, GPS Spoofing) tamamen **siber** tarafta yaratılan yalan verilerin **fiziksel** gerçeklikle uyuşmaması sorununu ortaya koyar.

Bu saldırılar:

- Şebeke istikrarını
- Faturalama bütünlüğünü

- Operasyonel şeffaflığı

ciddi şekilde etkiler.

4. Ortak Etki Analizi

Anomalilerin sınıflandırılmış etkileri:

4.1. Finansal Etkiler

- Enerji hırsızlığı (DLI, StopTx bastırma, Token Replay)
- Yanlış faturalama (Tampering, GPS Spoofing)
- Piyasa manipülasyonu (Phantom Fleet)

4.2. Operasyonel Etkiler

- İstasyonun hizmet dışı kalması (Memory Leak)
- Birbirine giren oturumlar (Session Fork)
- Kullanıcı mağduriyeti (Ghost RFID)

4.3. Güvenlik & Siber-Fiziksel Etkiler

- Trafik manipülasyonu ile güvenlik riskleri
- Gerçek güç akışının yanlış raporlanması (V2G saldırıları)
- Sistem kaynaklarının tüketilmesi

5. Tespit ve Korunma Mekanizmaları (Genel Öneriler)

Proje çalışmalarının ortak çıktıları, elektrikli araç şarj altyapılarının aşağıdaki savunma mekanizmalarıyla güçlenebileceğini göstermektedir:

- **TLS/mTLS zorunluluğu**
- **Mesaj imzalama (HMAC/ECDSA)**
- **Token/nonce tek kullanımlık sistemi**
- **Session-lock mekanizması**
- **Anomali tabanlı IDS**

- **Zaman senkronizasyonu otomatizasyonu (NTP/GPS/5G)**
- **RFID'de challenge-response tabanlı kimlik doğrulama**
- **IP-coğrafi konum çapraz doğrulama (GPS spoofing'e karşı)**
- **Bellek profilleme ve kaynak yönetimi**

6. Projenin Genel Sonucu

Bu proje, elektrikli araç şarj altyapılarının aslında beklenenden çok daha fazla siber ve fiziksel riske açık olduğunu göstermiştir. Her öğrenci tarafından incelenen anomali, bu ekosistemin farklı katmanlarındaki zayıflıkları ortaya çıkarmıştır:

- İletişim protokolleri
- Donanım sürücüleri
- Kimlik doğrulama sistemi
- Zaman yönetimi
- Piyasa entegrasyonu
- Veri bütünlüğü

Sonuç olarak:

Elektrikli araç şarj altyapıları, yalnızca bir enerji dağıtım sistemi değil, aynı zamanda karmaşık bir siber-fiziksel bütünlük gerektiren kritik altyapıdır. Proje, bu sistemlerdeki güvenlik açıklarının hem teknik hem de ekonomik sonuçlar doğurabileceğini başarılı simülasyonlarla göstermiştir.

7. Kaynakça (Genel)

Her rapordaki kaynaklar korunmuş olup, öğrencilerin kendi dosyalarında belirtilen makalelere dayanır.
Bu rapor, yüklenen tüm proje dokümanlarının referanslarına dayalı bütünleşik bir özet niteliğindedir.