PROJE SENARYO ANALİZ RAPORU

Konu: OCPP Kimlik Doğrulama Atlatma (Authentication Bypass) Anomalisi ve PoC Test Sonuçları

Ad Soyad: Emin TÖRE

Öğrenci No: 235541022

1. SENARYO TANIMI

Senaryo: OCPP Kimlik Doğrulama Atlatma (Authentication Bypass)

Açıklama: Saldırgan (Man-in-the-Middle), şarj istasyonu ile merkezi sistem arasındaki iletişimi manipüle ederek, geçerli bir kimlik doğrulama (Authorize) işlemi olmadan sahte bir "Şarjı Başlat" (StartTransaction) komutu gönderir. Amaç, sisteme yetkisiz erişim sağlamak ve enerji hırsızlığı yapmaktır.

2. SMART HEDEFLER

S (Specific): OCPP protokolündeki Authorize ve StartTransaction mesajları arasındaki zaman farkını ve sıralamayı izleyerek, aradaki "yetkisiz başlatma" girişimlerini tespit etmek.

M (Measurable): Yetkisiz bir Start komutu ağa düştükten sonra en geç 1 saniye içinde (Test sonucu: <0.5 sn) tespit etmek ve RemoteStop komutuyla şarjı kesmek.

A (Achievable): Python ve UDP Multicast mimarisi kullanılarak, durum bazlı (stateful) analiz yöntemiyle bu saldırıyı yakalamak teknik olarak başarılmıştır.

R (Relevant): Bu senaryo, projenin ana problemlerinden olan "Enerji Hırsızlığı" ve "Yetkisiz Erişim" sorununa doğrudan, donanımsal bir çözüm sunar.

T (Time-bound): Saldırı başladığı an (t=0), güvenlik sistemi gerçek zamanlı olarak devreye girer ve işlemi anında durdurur.

GÜÇLÜ YÖNLER (Strengths)

1. Proaktif Müdahale: Saldırıyı sadece raporlamakla kalmayıp, STOP komutu göndererek eylemi fiziksel olarak engeller.
2. Hız ve Performans: Python tabanlı hafif mimari sayesinde milisaniyeler içinde tepki verir.
3. Protokol Bağımsızlığı: Markadan bağımsız olarak, standart OCPP mesajlaşmasını kullanan tüm şarj istasyonlarında çalışır.

ZAYIF YÖNLER (Weaknesses)

1. Şifreleme (TLS) Engeli: Gerçek dünyada OCPP trafiği TLS (WSS) ile şifrelenmişse, araya girmek için sertifika yönetimi gerekir.
2. Ağ Gecikmesi (Lag): İnternet bağlantısı çok kötü olan istasyonlarda, gerçek 'Authorize' mesajı geç gelirse sistem bunu yanlışlıkla saldırı sanabilir.

FIRSATLAR (Opportunities)

1. Eski Cihazlara Güvenlik: Güvenlik güncellemesi almayan eski şarj istasyonlarına harici bir 'Güvenlik Modülü' olarak entegre edilebilir.
2. Edge Computing: İnternet kesilse bile yerel ağda çalıştığı için istasyonu korumaya devam eder.

TEHDİTLER (Threats)

1. Zaman Damgası Saldırısı: Çok gelişmiş saldırganlar, sahte mesajın zaman damgasını değiştirerek algoritmayı kandırmayı deneyebilir.
2. Fiziksel Sabotaj: Saldırgan, dedektör cihazımızın ağ kablosunu keserse koruma devre dışı kalır.