🏛 PROJE RAPORU

OCPP Kimlik Doğrulama Atlatma (Authentication Bypass) Anomalisi

Ad Soyad: Emin Töre
Öğrenci No: 235541022
Sınıf: Gece-B

📝 1. Senaryo Kapsamı

Senaryo: OCPP Kimlik Doğrulama Atlatma (Authentication Bypass) Anomalisi

Açıklama: Kötü niyetli bir kullanıcı, şarj istasyonu ile merkezi yönetim sistemi arasındaki iletişimi manipüle eder. Bu manipülasyonla, geçerli bir RFID kart veya mobil uygulama onayı olmaksızın, sahte bir "Yetkilendirildi" (Authorized) mesajı üreterek veya eski bir meşru mesajı yeniden oynatarak (Replay Attack) ücretsiz şarj seansı başlatır. Bu durum, projemizin anomali tespit sistemi tarafından proaktif olarak tespit edilmelidir.

🔬 2. Teknik Arka Plan ve Anomali Tehdidi

Şarj istasyonları, bir seansı başlatmak için OCPP (Open Charge Point Protocol) `Authorize` (Yetkilendir) mesajını kullanır. İstasyon, bu isteği merkezi sisteme gönderir ve merkezi sistemden olumlu bir yanıt ({ "status": "Accepted" }) almadan şarjı başlatmamalıdır.

Ancak, projemizde ele aldığımız "zayıf şifreleme" ve "Man-in-the-Middle (Ortadaki Adam) saldırıları" bu süreci savunmasız bırakır. Araştırdığımız makalelerde de vurgulandığı gibi, "authentication bypass" (kimlik doğrulama atlatma), EV şarj altyapısındaki en yaygın siber tehditlerden biridir. Saldırgan, istasyon ile merkezi sistem arasına girerek sahte bir "Accepted" yanıtı oluşturabilir ve sistemi kandırabilir.

🔍 3. Anomali Kaynakları ve Gözlenen Belirtiler

Bu senaryo, projemizin temel problemlerinden olan "Yetkisiz Erişim" konusuna odaklanır. Anomali tespit sisteminin izleyeceği temel belirtiler:

1. Yetkisiz `StartTransaction`: Aktif bir şarj seansının (`StartTransaction` mesajı) başlaması, ancak bu seansın hemen öncesinde merkezi sistemden gelen meşru ve ilişkili bir `Authorize` kaydının bulunmaması.

2. Yeniden Oynatma (Replay) Deseni: Daha önce (örn. 3 saat önce) kullanılmış geçerli bir `Authorize` mesajının ağda tekrar tespit edilmesi ve yeni bir seans başlatmak için kullanılması.

3. Sahte Yanıt: Şarj istasyonuna gelen `Authorize` yanıt paketinin, merkezi sisteme ait olmayan (veya şüpheli) bir kaynaktan gelmesi (Bu, klasik bir MitM saldırı belirtisidir).

🧠 4. Anomali Tespiti Süreci

Bu kısım, projemizin "%95 doğruluk" hedefi olan anomali tespit sistemi ile doğrudan bağ kurar:

4. Veri Toplama: Yapay zeka sistemi, tüm OCPP ağ trafiğini (özellikle `Authorize` ve `StartTransaction` mesajlarını) ve iletişim kaynaklarını izler.

5. Durum Bazlı (Stateful) Analiz: Geliştirilecek yapay zeka modeli, sadece tekil paketlere bakmak yerine seansın "durumunu" (state) takip eder. "Şarj seansı başladı" (`StartTransaction`) durumuna geçiş için geçerli bir "Kimlik doğrulandı" durumundan gelme zorunluluğunu bilir.

6. Tetikleme: Model, Bölüm 3'teki belirtilerden birini (örn. geçerli `Authorize` olmadan `StartTransaction`'ın başlaması) algıladığında, bu durumu yüksek doğrulukla "Anomali" olarak işaretler ve otomatik müdahale sürecini tetikler.

📉 5. Etki ve Risk Değerlendirmesi

* Etki (Negatif): Bu anomali (yetkisiz erişim) tespit edilemezse, doğrudan finansal kayba (ücretsiz şarj), yetkisiz şebeke erişimine ve istasyonun operasyonel bütünlüğünün bozulmasına yol açar.

* Risk (Yanlış Pozitif): Sistem, merkezi sistem ile istasyon arasındaki aşırı ağ gecikmesini (network lag) yanlışlıkla bir anomali olarak yorumlayabilir. `Authorize` yanıtı gecikirse, sistem `StartTransaction`'ı "yetkisiz" sanabilir. Bu, yapay zeka modelinin geliştirilmesinde dikkate alınması gereken bir zorluktur.

🛡️ 6. Çok Katmanlı Doğrulama ve Müdahale

Projemiz, bu tür "Yetkisiz Erişim" anomalilerine karşı çok katmanlı bir savunma önermektedir:

7. Çapraz Kontrol (Merkezi Sistem Doğrulaması): Yapay zeka modeli, bir seans başladığında, merkezi sistem veritabanını da kontrol ederek bu seansın orada da "yetkilendirilmiş" olarak görünüp görünmediğini teyit eder.

8. Kaynak Doğrulaması: MitM saldırılarını engellemek için sistem, merkezi sistemden gelen yanıtların sadece bilinen ve güvenli bir kaynaktan veya dijital sertifikadan gelmesini bekler.

9. Gerçek Zamanlı Müdahale: Anomali kesinleştiğinde, sistem (30 saniye içinde müdahale hedefimiz kapsamında) istasyona derhal bir `RemoteStopTransaction` (Uzaktan Seansı Durdur) komutu göndermeyi ve ilgili seansı "Şüpheli" olarak işaretlemeyi içerir.

⚖️ 7. Sonuç (Anomali Odaklı)

Bu senaryo, projemizin ana problemlerinden olan "Yetkisiz Erişim" tehdidini ve incelediğimiz makalede belirtilen "Authentication Bypass" açığını doğrudan ele alır. Geliştirilecek yapay zeka sistemi, OCPP protokolünün durumunu analiz ederek bu tür gelişmiş saldırıları tespit edebilen proaktif bir savunma mekanizması olarak çalışacaktır.

📚 8. Kaynakça

* Proje Tanıtım Dokümanı (Hedef 1, Hedef 4, Problemler: Yetkisiz Erişim, MitM)
* Securing the Electrified Future: A Systematic Review of Cyber Attacks, Intrusion and Anomaly Detection, and Authentication in Electric Vehicle Charging Infrastructure. (MDPI, 2024) https://www.mdpi.com/1996-1073/18/18/4847

Belge Oluşturma Tarihi: 2025-11-03 12:40:33