ANOMALI SENARYOSU: REPLAY (TEKRAR OYNATMA) SALDIRISI

Hazırlayan: [Melik Fırat Çenber]

Tarih: 7.11.2025

Konu: Elektrikli Araç Şarj İstasyonlarında Kimlik Doğrulama Manipülasyonu

---

1. Amaç ve Kapsam

Bu teknik rapor, Elektrikli Araç Şarj İstasyonu (EVCS) ile Merkezi Yönetim Sistemi (CSMS) arasındaki OCPP (Open Charge Point Protocol) haberleşmesinde meydana gelebilecek **Replay (Tekrar Oynatma)** saldırısını analiz etmek amacıyla hazırlanmıştır.

Senaryo, kötü niyetli bir aktörün (saldırganın), yetkili bir kullanıcının kimlik doğrulama verilerini ağ trafiği üzerinden ele geçirip, daha sonra bu veriyi tekrar kullanarak yetkisiz enerji temin etmesini ve bu durumun sistem kayıtlarında oluşturduğu anomalileri kapsamaktadır.

2. Saldırı Yöntemi (Teknik Detay)

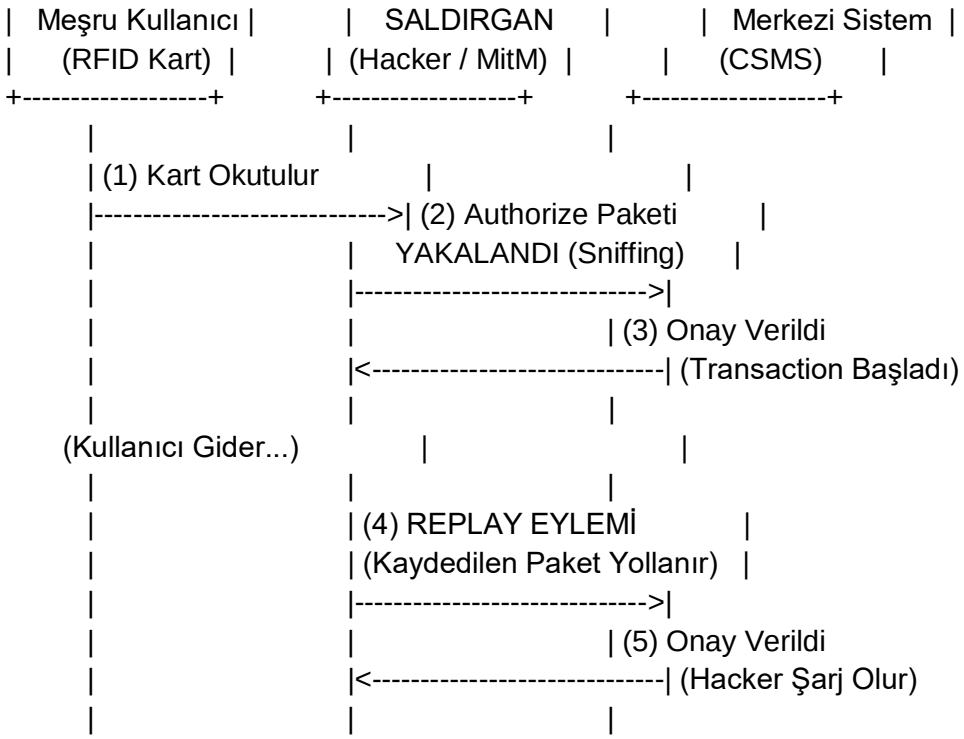
Saldırı, iletişim hattının şifrelenmediği veya zayıf güvenlik protokollerinin kullanıldığı durumlarda, "Man-in-the-Middle" (Ortadaki Adam) yöntemiyle gerçekleştirilir. Süreç üç aşamada işler:

1. **İzleme ve Yakalama (Sniffing):** Saldırgan, şarj istasyonunun bağlı olduğu yerel ağa (LAN) sızar. Wireshark vb. araçlar kullanarak istasyon ile sunucu arasındaki veri paketlerini dinler.
2. **Veri Hırsızlığı:** Meşru bir kullanıcı kartını okuttuğunda, istasyonun sunucuya gönderdiği `Authorize` mesajını (içinde `idTag` kimlik bilgisini barındıran JSON paketi) kopyalar.
3. **Tekrar Oynatma (Replay):** Meşru kullanıcı ayrıldıktan sonra saldırgan kendi aracını bağlar. Daha önce kaydettiği geçerli `Authorize` paketini, sanki istasyon gönderiyormuş gibi sunucuya tekrar gönderir. Sunucu bu paketi geçerli sandığı için şarjı başlatır.

3. Saldırı Akış Şeması (Görsel Analiz)

Aşağıdaki diyagram, saldırganın araya girerek paketi nasıl kopyaladığını ve tekrar kullandığını göstermektedir:

Plaintext
+------------------+ +------------------+ +------------------+



[Şekil 1: Replay Saldırısı Akış Diyagramı]

4. Saldırının Etkileri (Impact Analysis)

Bu anomali gerçekleştiğinde sistem ve operasyon üzerinde aşağıdaki kritik etkiler gözlemlenir:

- **Finansal Kayıp ve Hatalı Faturalandırma:** Saldırganın tükettiği enerji bedeli, kimlik bilgisi çalınan masum müşteriye fatura edilir. Bu durum müşteri şikayetlerine ve tazminat süreçlerine yol açar.
- **Veri Bütünlüğü İhlali:** CSMS veritabanında, aynı kullanıcının fiziksel olarak bulunmasının imkansız olduğu zaman aralıklarında işlem yaptığına dair tutarsız kayıtlar (loglar) oluşur.
- **Yetkisiz Erişim:** Saldırgan, herhangi bir fiziksel karta ihtiyaç duymadan sistemi manipüle ederek enerji hırsızlığı gerçekleştirir.

5. Zafiyet Analizi ve Nedenler

Sistemin bu saldırıya açık olmasının temel nedenleri şunlardır:

- **Şifreleme Eksikliği:** İletişimin TLS (Transport Layer Security) olmadan, düz metin (Plaintext/HTTP) olarak yapılması verilerin okunmasını sağlar.
- **"Nonce" Kullanılmaması:** Mesajların benzersizliğini sağlayan rastgele sayı (Nonce) veya zaman damgası (Timestamp freshness) kontrollerinin protokol seviyesinde zorunlu tutulmaması.

6. Tespit ve Savunma Önlemleri

Bu tehdidi bertaraf etmek için aşağıdaki güvenlik katmanları uygulanmalıdır:

- **OCPP Güvenlik Profili 3 (TLS with Client Certificates):** Tüm haberleşme şifreli (WSS) yapılmalı ve karşılıklı sertifika doğrulaması kullanılmalıdır.
- **Mesaj Benzersizliği (Uniqueness):** Her mesaj için benzersiz bir ID kullanılmalı ve sunucu daha önce işlenmiş bir ID'ye sahip mesajı "Replay" girişimi olarak algılayıp reddetmelidir.
- **Anomali Tespit Sistemi (IDS):** Merkezi yazılımda, "Co-traveler" (İmkansız Seyahat) kuralları tanımlanmalıdır. Örneğin; bir kart İstanbul'da kullanıldıktan 5 dakika sonra Ankara'da işlem görüyorsa sistem bunu bloke etmelidir.