STOPTRANSACTION BASTIRILMASIYLA ZOMBİ ŞARJ OTURUMU VE ENERJİ HIRSIZLIĞI ANOMALİSİ

Hazırlayan: Ali Yalçın
Okul No: 230541153

1. Giriş

Elektrikli araç şarj istasyonları (EVSE), genellikle bir **Merkezi Şarj Yönetim Sistemi (CSMS)** ile **OCPP (Open Charge Point Protocol)** üzerinden haberleşir. Tipik bir şarj oturumu, üç temel mesaj etrafında döner:

1. **StartTransaction** / TransactionEvent (başlatma)
2. **MeterValues** / ölçüm verileri (süreç boyunca)
3. **StopTransaction** / TransactionEvent (bitiş)

CSMS, faturayı ve enerji tüketimini "başlangıç → ölçümler → bitiş" akışına göre hesaplar. Bu zincirin son halkası olan **StopTransaction**, oturumun sona erdiğinin resmî kanıtı niteliğindedir.

Bu raporda, **StopTransaction mesajının kötü niyetli olarak bastırılması** sonucu ortaya çıkan ve literatürde enerji hırsızlığı ile ilişkili tehdit sınıfına giren **"zombi şarj oturumu"** anomalisi tanımlanmakta ve etkileri tartışılmaktadır.

2. Anomali Tanımı

Önerilen anomali senaryosu özetle şu şekildedir:

Şarj işlemi fiilen bittiği hâlde, **StopTransaction mesajı CSMS'e ulaşmaz veya kasıtlı olarak bastırılır**. Böylece şarj oturumu mantıksal olarak "açık" kalır, faturalama ve oturum yönetimi anormal bir duruma geçer. Bu durum; **enerji hırsızlığı, fatura uyuşmazlığı ve hizmet kesintisi** gibi sonuçlara yol açabilir.

Bu anomali iki farklı teknik yolla ortaya çıkabilir:

1. **MITM (Man-in-the-Middle) bastırma senaryosu**
    - Saldırgan, şarj istasyonu ile CSMS arasındaki OCPP trafiğine araya girer.
    - StartTransaction ve MeterValues mesajlarını olduğu gibi iletir.
    - Ancak StopTransaction mesajını **yakalar ve CSMS'e iletmez** (drop / suppress).

- Sonuç: CSMS açısından oturum hiç sonlanmamış gibi görünür; istasyon tarafında fiziksel olarak kablo çekilmiş ya da araç ayrılmış olsa bile mantıksal oturum "zombi" hâle gelir.

2. **Yanlış/istismar edilen konfigürasyon senaryosu**
   OCPP 2.0.1'de tanımlı bazı konfigürasyon değişkenleri (Configuration Variables) yanlış ayarlandığında da benzer anomaliler oluşabilir. Örneğin:

   - **StopTxOnInvalidId**: "Yetkisiz ID tespit edildiğinde oturumu durdur" anlamına gelen bir değişkendir. **FALSE** olarak ayarlandığında, yetkisiz bir kullanıcıyla başlayan oturum, CSMS tarafından onaylanmasa bile devam edebilir. Bu, makalede doğrudan **enerji hırsızlığı (Energy theft)** riski olarak sınıflandırılmaktadır.

   - **MaxEnergyOnInvalidId** değişkeninin yüksek bir değere ayarlanması da, yetkisiz kullanıcıya verilebilecek enerjinin sınırını yükselterek benzer bir enerji hırsızlığı riskini artırır.

Bizim anomali senaryomuzda, bu konfigürasyon zafiyetleri ile **StopTransaction bastırma** birleştiğinde, istasyon tarafında fiili durum ile CSMS tarafındaki mantıksal durum **tamamen kopar** ve "zombi oturum" oluşur.

3. Saldırı Modeli ve Olay Akışı

Bu anomalinin tipik bir saldırı akışı aşağıdaki adımlarla açıklanabilir:

1. **Oturum Başlangıcı**
   - Kullanıcı, kart/etiket veya uygulama ile şarj oturumunu başlatır.
   - İstasyon, CSMS'e `StartTransaction` (veya OCPP 2.0.1'de `TransactionEvent` başlangıç olayı) gönderir.
   - CSMS bu mesajı alır, oturumu veri tabanına kayıt eder.
2. **Normal Ölçüm Süreci**
   - Araç şarj olurken istasyon düzenli aralıklarla `MeterValues` mesajları gönderir.
   - Bu mesajlar, toplam enerji tüketiminin CSMS tarafında kademeli olarak güncellenmesini sağlar.
3. **MITM Kurulumu**
   - Saldırgan, örneğin sahte bir Wi-Fi AP veya yönlendirici üzerinden OCPP trafiğine **araya girer**. OCPP için TLS kullanılmayan veya zayıf yapılandırılmış bir ortamda bu daha kolay gerçekleşir.

- Bilimsel çalışmalarda OCPP üzerindeki MitM saldırılarıyla `meterValues` değiştirerek **enerji hırsızlığı**yapılabildiği açıkça belirtilmektedir.

- Biz bu senaryoda doğrudan MeterValues içeriğini değil, **StopTransaction mesajının akışını** hedef alıyoruz.

4. **Fiziksel Bitiş – Mantıksal Devam (Zombi Oturum)**
   - Kullanıcı kabloyu çıkarır, araç ayrılır. İstasyon kendi tarafında oturumu bitirip **StopTransaction** mesajını üretir.
   - Bu mesaj CSMS'e gitmek üzere yola çıkarken MITM tarafından **yakalanır ve düşürülür** (drop).
   - CSMS, StopTransaction almadığı için oturumu hâlâ **"aktif"** sanır.
   - Eğer istasyon tarafında ek güvenlik kontrolü yoksa, aynı soket üzerinde yeni kullanıcıya izin verilebilir veya enerji tüketim kaydı anormal uzun süre "açık" kalabilir.
5. **Sonuç Durum – Anomali**
   - Veri tabanında sonlanmayan, olağandışı uzun süreli, hatta **çakışan zaman damgalarına sahip "aktif oturumlar"** görünür.
   - Fatura karşılaştırıldığında; kullanıcı ve işletmeci, tüketilen enerji/fiyat tutarsızlığı veya **faturalanmamış enerji** ile karşılaşabilir.
   - Çok sayıda zombi oturum biriktiğinde sistem tarafında ek kayıt yükü, bağlantı yönetiminde karmaşa ve potansiyel **hizmet kesintisi** riski doğar.

4. Anomali Belirtileri

Bu saldırı sonucunda gözlenebilecek anomali belirtileri şunlardır:

- **Tamamlanmamış işlem kayıtları:**
  `StartTransaction` ve birden fazla `MeterValues` kaydı bulunurken **StopTransaction kaydı yoktur**.
- **Olağan dışı uzun oturum süreleri:**
  Normalde birkaç saat süren oturumlar, sistemde günlerce "aktif" görünebilir.
- **Fatura / sayaç tutarsızlığı:**
  - Kullanıcının kendi uygulamasında gördüğü ücret ile CSMS tarafındaki fatura uyuşmayabilir.
  - İstasyonun fiziksel sayaç değeri ile CSMS'te hesaplanan toplam tüketim arasında fark oluşabilir.

- **Kritik sistemlerde erişilebilirlik etkisi:**
  Çok sayıda zombi oturum, CSMS ve bağlı modüllerde gereksiz kaynak tüketimi, bağlantı sınırlarının dolması ve sonuçta **kısmi DoS etkisi** yaratabilir. Bu, OCPP risk analizinde DoS ve bütünlük ihlali kategorileriyle uyumludur.

Bu belirtiler, anomali tabanlı saldırı tespit sistemleri (IDS) için güçlü özellikler sunar. Nitekim literatürde şarj istasyonlarına özel **anomali tespiti sistemlerinin** geliştirildiği ve bu sistemlerin özellikle **beklenmeyen işlem örüntülerini** yakalamak üzere tasarlandığı gösterilmektedir.

5. Etki Analizi

Bu anomali, uluslararası literatürde tanımlanan tehdit sınıflarıyla (ör. **STRIDE** ve enerji odaklı **TC-7: Energy Theft**, **TC-2/TC-3: DoS**) doğrudan ilişkilidir.

Başlıca etkiler:

1. **Enerji Hırsızlığı ve Finansal Kayıp**
   - StopTransaction'ın bastırılması, belirli bir oturuma ait enerjinin yanlış veya eksik faturalandırılmasına sebep olabilir.
   - StopTxOnInvalidId ve MaxEnergyOnInvalidId gibi değişkenlerin saldırgan lehine ayarlanmasıyla birleştiğinde sistemden bilinçli olarak enerji çekilebilir.

2. **Hukuki ve Operasyonel Riskler**
   - Fatura uyuşmazlıkları, kullanıcı şikâyetleri ve olası hukuki süreçler ortaya çıkabilir.
   - İşletmeci tarafında hangi enerji kime ait, hangi oturum gerçekten ne zaman sonlandı gibi sorular belirsizleşir.

3. **Hizmet Sürekliliği ve Güven Sorunu**
   - Zombi oturumlar biriktiğinde CSMS kaynak tüketimi artar; bu durum literatürde vurgulanan **hizmet sürekliliği (availability)** gereksinimiyle çelişir.
   - Kullanıcıların sisteme güveni azalır; özellikle akıllı şebeke ve mikroşebeke (MG) senaryolarında bu tür anomaliler, enerji yönetimi algoritmalarını da yanıltarak daha geniş etkiler doğurabilir.

5.1 SWOT Analizi

(Bu bölüm, StopTransaction bastırılması anomalisi için sistemin güçlü ve zayıf yönlerini, fırsatlarını ve tehditlerini bütünsel şekilde değerlendirmektedir.)

Strengths (Güçlü Yönler)

- Literatürde doğrudan karşılığı olan gerçekçi bir saldırı modeli sunar.
- Simülasyon ortamında kolaylıkla yeniden üretilebilir ve gözlemlenebilir.
- Enerji hırsızlığı gibi somut etkileri görünür kılar.
- OCPP 2.0.1 konfigürasyon zafiyetleriyle uyumludur.

Weaknesses (Zayıf Yönler)

- Gerçek şarj istasyonlarında denenmesi teknik ve hukuki olarak zordur.
- TLS kullanılan modern kurulumlarda saldırının uygulanabilirliği azalabilir.
- Simülasyonda güvenilir sonuç almak için doğru mesaj zamanlaması gerekir.
- Güçlü log/timeout mekanizmaları olan sistemlerde saldırı etkisi sınırlı kalabilir.

Opportunities (Fırsatlar)

- EV şarj altyapılarında güvenlik geliştirme çalışmalarına temel oluşturur.
- IDS, makine öğrenmesi ve blokzincir gibi teknolojilerle birleştirilebilir.
- Akademik ve sektörel araştırmalar için güncel ve önemli bir problem alanıdır.
- Enerji yönetimi algoritmalarında daha güvenli tasarımlar yapılmasına katkı sağlar.

Threats (Tehditler)

- Enerji hırsızlığına ve finansal kayıplara yol açabilir.
- Fatura ve kayıt tutarsızlıkları müşteri güvenini sarsar.
- Birden fazla zombi oturum, CSMS üzerinde DoS etkisi oluşturabilir.
- Konfigürasyon zafiyetleriyle birleştiğinde çok daha geniş ölçekli saldırılara yol açabilir.
- Akıllı şebekelerde yanlış enerji verisinin yayılması zincirleme sistem hatalarına sebep olabilir.

6. Tespit ve Karşı Önlemler

Bu anomalinin tespiti ve önlenmesi için önerilebilecek bazı yaklaşım başlıkları:

1. **İşlem Akışı Tutarlılık Kontrolleri**
    - Her `StartTransaction` için mutlaka bir `StopTransaction` bekleyen, maksimum oturum süresi sınırı içeren kurallar tanımlanabilir.
    - Belirli bir süre içinde StopTransaction gelmeyen oturumlar "şüpheli" etiketiyle işaretlenip IDS'e bildirilir.
2. **Anomali Tabanlı IDS ve İşbirlikçi Tespit**
    - Literatürde şarj istasyonlarına özel **işbirlikçi anomali tespiti sistemleri** önerilmektedir. Bu sistemler, birden fazla istasyonda gözlenen normal ve anormal oturum desenlerini karşılaştırarak saldırıları daha etkin biçimde yakalayabilir.
3. **Kriptografik Koruma ve İmza / Hash Kullanımı**
    - OCPP mesajlarının TLS ile korunması MitM saldırılarını zorlaştırır; ancak tek başına yeterli değildir.
    - Mesaj bütünlüğü ve doğruluğu için **dijital imza, hash fonksiyonları** ve **blokzincir tabanlı kayıt** kullanımı, hem araç içi ağlar hem de şarj altyapısı için literatürde önerilen yöntemler arasındadır.
4. **Konfigürasyon Değişkenlerinin Güvenli Yönetimi**
    - StopTxOnInvalidId, MaxEnergyOnInvalidId, MessageAttempts, HeartBeatInterval gibi kritik OCPP konfigürasyonları için güvenlik odaklı varsayılan değerler ve değişiklik denetimi (audit) uygulanmalıdır.

7. Sonuç

StopTransaction mesajının bastırılması sonucu oluşan "zombi şarj oturumu" ve buna bağlı enerji hırsızlığı / fatura anomalisi.

Bu senaryo, hem **iletişim bütünlüğünün (integrity)** ihlali hem de **hizmet sürekliliği (availability)** açısından kritik bir zafiyetin göstergesidir. OCPP protokolüne ilişkin güncel makaleler, özellikle konfigürasyon değişkenleri ve MitM saldırıları üzerinden bu tür risklerin gerçekçi ve ciddiye alınması gereken tehditler olduğunu vurgulamaktadır.

Bu anomali, proje kapsamında geliştirilecek **simülasyon ortamında**;

- normal oturum akışı ile
- StopTransaction bastırılan saldırı senaryosu

karşılaştırılarak açık şekilde gösterilebilir. Bu da hem teorik hem pratik açıdan güçlü bir proje çıktısı sunar.

KAYNAKÇA

[1] A., “Machine Learning–Driven Intrusion Detection Systems for Automotive Networks,” *Journal of Autonomous Intelligent Systems*, vol. 3, no. 7, pp. 1–17, 2023.

[2] C. K. T. Chan, W. H. Ip, C. C. Cheung, and Y. K. Wong, “Trustworthy and Practical OCPP Security Implementation for Electric Vehicle Charging Infrastructures,” *Sensors*, vol. 22, no. 21, pp. 1–25, 2022.

[3] Open Charge Alliance, *Open Charge Point Protocol 2.0.1 – Specification*, 2020.

[4] J. Petit and S. E. Shladover, “Potential Cyberattacks on Automated Vehicles,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[5] M. Müslim, H. M. Al-Mrashdeh, A. M. Alsmirat, and Y. Jararweh, “Collaborative Anomaly Detection System for Electric Vehicle Charging Stations,” *Proc. 2022 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pp. 1–6, 2022.

[6] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway,” *WIRED*, Jul. 2015.

[7] S. Checkoway et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” in *Proc. USENIX Security Symp.*, 2011, pp. 1–15.

[8] Open Charge Alliance, *OCPP 2.0.1 Security Whitepaper*, 2021.