Yapan : Şerif Miraç GÖGEBAKAN - 230541126

Anomali: Diferansiyel Gecikme Enjeksiyonu (DLI) – Gizli Enerji Hırsızlığı Anomalisi

1. Anomali Tanımı

Diferansiyel Gecikme Enjeksiyonu (DLI), elektrikli araç şarj istasyonlarında kullanılan sayaçtaki verileri hedef alan gizli bir hiledir. Bu saldırı, şarj istasyonu ile fatura sistemi arasındaki iletişimin zaman aralığını manipüle eder.

Nasıl Çalışıyor? Şarj istasyonu, şarj edilen enerji miktarını düzenli olarak mesela her istasyon 10 saniyede bi faturalama sistemine rapor yollar saldırgan bu raporları faturalama sistemine ulaşmadan önce yakalar ve iki hileden birini yapar:

1. **Gecikme Yaratma:** Raporu kasıtlı olarak çok geç gönderecek
2. **Zaman Kaydırma:** Raporun içindeki zaman damgasını ileri kaydırır (sanki rapor daha erken gönderilmiş gibi gösterir).

Bu hile, faturalama sisteminin aracın gerçekte tükettiği toplam enerji miktarının bir kısmını (örneğin %5'ini) gözden kaçırmasına, yani faturalandırılmamasına neden olur. Sonuç, **sahte enerji tüketimi** veya enerji hırsızlığıdır.[1]

2. Olası Nedenler

Olası Nedenler	Olası Sebep	Açıklama
İletişim Güvenliği	Eski OCPP yazılımlarının zayıf güvenliği	Şarj istasyonu ve merkezi sistem arasındaki iletişimin şifrelenmemesi ,saldırganın araya girip mesajları değiştirmesini kolaylaştırabilir.[4]
Zamanlama Hataları	saat senkronizasyonu	Şarj istasyonu ve merkezi sistemin saatlerinin çok hassas bir şekilde (2 milisaniye hassasiyetinde) senkronize edilememesi, saldırganın küçük zaman kaymalarını gizlemesini sağlar.[7]
Raporlama Kuralı İhlali	Düzenli raporlama kuralının atlanması	İstasyonun, enerji miktarını bildirme aralığını (örneğin 10 saniye) kasten uzatması (örneğin 30 saniye), bu arada tüketilen enerjinin faturalama kaydına girmemesine neden olur.[9]
Fiziksel Müdahale	Cihaza doğrudan erişim	Saldırganın doğrudan şarj istasyonunun içine girerek (fiziksel müdahale) zararlı yazılım yüklemesi; bu durumda cihazın açıldığına dair kayıtların [11] silinmesi gerekir.

3. Olası Riskler ve Etkiler

- **Yüksek Gizlilik :** Bu saldırı, büyük bir arıza veya hizmet kesintisi yaratmak yerine, çok küçük zaman kaymaları yarattığı için fark edilmesi zordur. Sistem loglarında bu durum, masum bir ağ yavaşlaması veya geçici bağlantı hatası gibi görünür.[7]
- **Finansal Kayıp:** Saldırı, tek bir seferde büyük bir hırsızlık yapmaz, ancak her şarj seansında küçük bir miktar enerji çalar. Bu durum, yüzlerce şarj istasyonu üzerinde tekrarlandığında, İşletmeciler için yıllar içinde biriken çok ciddi gelir kaybına neden olur.[12]
- **Veri Güvenilirliği Sorunu:** Şebeke yönetimi ve faturalama için kullanılan temel enerji verileri güvenilirliğini kaybeder. Faturalanan enerji ile gerçek tüketim uyuşmaz.[15]
- **Siber-Fiziksel Saldırı:** Bu, sadece bir bilgisayar korsanlığı değil, aynı zamanda fiziksel dünyada karşılığı olan (gerçek elektrik enerjisi hırsızlığı) bir eylemdir.[16]

4. İlgili Standartlar ve Kurallar

- **OCPP (Open Charge Point Protocol):** Şarj istasyonu ve merkezi yönetim arasındaki konuşma dilini belirleyen protokoldür. Sayaç Değerleri raporlaması bu protokolün ana konusudur.[17]
- **ISO 15118:** Aracın şarj istasyonuyla doğrudan güvenli iletişim kurmasını sağlayan kural setidir (örneğin, şarj kablosunu takınca otomatik tanıma).[18]
- **Zaman Senkronizasyonu Kuralları:** Kritik altyapıların, olayları doğru tespit edebilmesi için saatlerini çok hassas bir şekilde (2 milisaniye) uluslararası saate (UTC) göre ayarlamasını gerektiren kurallardır.[8]
- **Sıfır Güven (Zero Trust):** Güvenlik modelidir. "Asla güvenme, her zaman kontrol et" prensibini benimser. Yani bir cihaz ağa bağlı olsa bile, her hareketinin doğrulanmasını gerektirir.[21]

5. Simülasyon Sonuçları

Burada benim yaptığım VS Code üzerinde sümülasyon kurarrak gerçekleştirdiğim Diferansiyel Gecikme Enjeksiyonu (DLI) saldırısının sonuçları vardır. Burada anomali tespit metriklerinin pratik uygulanabilirliğini göstermekte

Anomali Log Kayıtları : Tabloda, DLI saldırısı sırasında 2 saniyelik eşiği aşarak anomali olan örnek sayaç raporları var

Alınma Zamanı (sunucunun) mesajı aldığı zaman)	**Yollanma Zamanı (raporlanan zaman)**	**Enerji Değeri (kWh)Rapolanan enerji miktarları**	**İstemci (Yollayan şarj istasyonu)**	**Gecikme süresi(az-yz farkı)**
2025-11-06 07:50:55.568372	2025-11-06 07:50:50.566007	0.717	EVSE1	5.002365
2025-11-06 07:51:15.577661	2025-11-06 07:51:10.577203	1.301	EVSE1	5.000458
2025-11-06 07:51:25.591607	2025-11-06 07:51:20.590849	0.694	EVSE1	5.000758
2025-11-06 07:51:35.595899	2025-11-06 07:51:30.595430	1.277	EVSE1	5.000469
2025-11-06 07:51:45.597549	2025-11-06 07:51:40.597168	0.900	EVSE1	5.000381

- ---

  1. Log Analizi Metriği (Zaman Farkını Bulma - TDD): Merkezi sistemin tuttuğu loglarda, bir sayaç raporunun ulaştığı an ile raporun içindeki zaman damgası arasındaki fark (gecikme) sürekli ölçülmelidir. Yukarıdaki test sonuçlarında görüldüğü gibi, normal ağ gecikmesinin üzerine çıkan tutarlı sapmalar (ortalama 5 saniye) alarm vermelidir.[22]
- **2. Log Analizi Metriği (Enerji/Süre Tutarlılığı - ESC):** Şarj seansının toplam süresi ile bu sürede faturalanan enerji miktarı arasındaki normal ilişki (ortalama güç) sürekli kontrol

edilmelidir. DLI saldırısında ortalama gücün [23] sürekli olarak beklenenden düşük çıkması, hırsızlığın kanıtıdır. Bu, Basit Hareketli Ortalama (SMA) [24] gibi yöntemlerle tespit edilebilir.

- **3. Saldırı Ortamı Kurulumu (PoC):** Düşük maliyetli donanımlar (örneğin Raspberry Pi) kullanılarak EVSE ve CSMS simülasyonu yapan bir test ortamı [25] kurulabilir. Bu ortamda, yazılımlar modifiye edilerek kasıtlı gecikme enjeksiyonu gerçekleştirilmeli ve yukarıdaki 1. ve 2. maddede belirtilen log verileri toplanmalıdır.

Sistem Geliştirme Odaklı Öneriler:

- **Sürekli Saat Ayarı:** Şarj istasyonları , uydu (GPS) vb farklı bir kaynaktan sürekli zaman ayarı almalı ve bu hassasiyeti (2 ms) korumalıdır.[8]
- **Tüm İletişimi Şifreleme:** Şarj istasyonu ile faturalama sistemi arasındaki tüm iletişimin şifrelenmesi zorunlu olmalıdır. Bu, saldıran tarafın mesajları değiştirmesini veya okumasını engeller.[4]

6. Sonuç ve Değerlendirme

Diferansiyel Gecikme Enjeksiyonu (DLI), elektrikli araç şarj sektöründe ortaya çıkan, finansal bütünlüğü tehdit eden, yeni nesil gizli siber-fiziksel saldırı türüdür. Bu saldırı, geleneksel güvenlik önlemlerini aşarak, sistemin zamanlama hassasiyetindeki zayıflıkları kullanır.

Bu ders projesi kapsamında, DLI saldırı uygulamasının ve yukarıdaki test kayıtlarında gösterilen **5 saniyelik kasıtlı gecikme** ile bu saldırının izlerinin ortaya çıkarılması hedeflenmiştir. Elde edilen log kayıtları ve istatistiksel sapmalar, DLI'nın hem uygulanabilir hem de basit istatistiksel analizlerle (TDD ve ESC) tespit edilebilir bir anomali olduğunu kanıtlamaktadır. Bu tür zamansal anormalliklerin tespiti, şarj altyapılarının sadece fiziksel hasarlara değil, aynı zamanda gizli mali kayıplara karşı da korunması için hayati önem taşır.[12]

7. Kaynaklar

Alıntılanan çalışmalar

1. OCPP Protocol: Security Threats and Challenges - NICS Lab, erişim tarihi Kasım 5, 2025, https://www.nics.uma.es/pub/papers/AlcarazLopezWolthusen2017.pdf
2. Federated detection of open charge point protocol 1.6 cyberattacks - OAE Publishing Inc., erişim tarihi Kasım 5, 2025,

https://www.oaepublish.com/articles/ces.2025.04
3. Detection Methods in Smart Meters for Electricity Thefts: A Survey - Yang Xiao, erişim tarihi Kasım 5, 2025, https://yangxiao.cs.ua.edu/Detection_Methods_in_Smart_Meters_for_Electricity_Thefts_A_Survey.pdf
4. OCPP Security and Security Profiles - Ampcontrol, erişim tarihi Kasım 5, 2025, https://www.ampcontrol.io/product-details/ocpp-security-and-security-profiles
5. Disrupting EV Charging Sessions and Gaining Remote Code Execution with DoS, MITM, and Code Injection Exploits using OCPP 1.6 - - INL Research Library Digital Repository - Idaho National Laboratory, erişim tarihi Kasım 5, 2025, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65949.pdf
6. CIC EV charger attack dataset 2024 (CICEVSE2024) - University of New Brunswick, erişim tarihi Kasım 5, 2025, https://www.unb.ca/cic/datasets/evse-dataset-2024.html
7. Reducing Latency in EV Charging: Observability and Smart Backend... - Zaptec, erişim tarihi Kasım 5, 2025, https://www.zaptec.com/info-hub/industry-news/thoughts-about-latency-observability-and-backend-systems-for-charging-infrastructure
8. Time Synchronization Techniques in the Modern Smart Grid: A Comprehensive Survey, erişim tarihi Kasım 5, 2025, https://www.mdpi.com/1996-1073/18/5/1163
9. Charging Session Integration | EV Charge Web Docs | Tridens Technology, erişim tarihi Kasım 5, 2025, https://tridenstechnology.com/ev-charge-web-docs/integrations/charging-session-integration/
10. Test case document OCTT for OCPP 1.6 - Open Charge Alliance, erişim tarihi Kasım 5, 2025, https://openchargealliance.org/wp-content/uploads/2024/07/CompliancyTestTool-TestCaseDocument.pdf
11. EV-201-2019 - Security architecture for electric vehicle charging infrastructure - ElaadNL, erişim tarihi Kasım 5, 2025, https://elaad.nl/wp-content/uploads/2022/05/security-architecture-for-ev-charging-infrastructure.pdf
12. Detecting electricity theft via meter tampering using statistical methods - Google Patents, erişim tarihi Kasım 5, 2025, https://patents.google.com/patent/US9600773B2/en
13. "Ideologically motivated:" Vandalism and theft a growing problem for EV charging stations, erişim tarihi Kasım 5, 2025, https://thedriven.io/2025/10/15/ideologically-motivated-vandalism-and-theft-a-growing-problem-for-ev-charging-stations/
14. EV Cable Theft Calculator for Charge Point Operators | Formula Space, erişim tarihi Kasım 5, 2025, https://formula-space.com/blog/ev-cable-theft-calculator-the-impact-on-charge-point-operators/
15. OCPP Security ⟶ Area - Prism ⟶ Sustainability Directory, erişim tarihi Kasım 5, 2025, https://prism.sustainability-directory.com/area/ocpp-security/

16. Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network - PubMed Central, erişim tarihi Kasım 5, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11933351/
17. OCPP 2.0.1: Part 0 - Introduction - Regulations.gov, erişim tarihi Kasım 5, 2025, https://downloads.regulations.gov/FHWA-2022-0008-0404/attachment_3.pdf
18. ISO-15118 Açıklaması - Sektör Haberleri - Haberler - Teison Elektrikli Araç Şarj Çözümleri, erişim tarihi Kasım 5, 2025, https://tr.evj1772.com/news/iso-15118-explained-80163800.html
19. ISO 15118 Nedir? - Teison Energy Technology Co.,Ltd., erişim tarihi Kasım 5, 2025, https://tr.teison.com/news/industry_news/what_is_iso_15118_.html
20. Smart Metering Technology for EVSE - Analog Devices, erişim tarihi Kasım 5, 2025, https://www.analog.com/en/solutions/energy/ev-charging-solutions/smart-metering-technology-evse.html
21. The Design and Evaluation of Zero Trust Architecture for Electric Vehicle Charging Infrastructure: EVs @ Scale Series on EV Charging Station Cybersecurity | Report - Pacific Northwest National Laboratory, erişim tarihi Kasım 5, 2025, https://www.pnnl.gov/publications/design-and-evaluation-zero-trust-architecture-electric-vehicle-charging-infrastructure
22. Online Machine Learning for Intrusion Detection in Electric Vehicle Charging Systems, erişim tarihi Kasım 5, 2025, https://www.mdpi.com/2227-7390/13/5/712
23. Machine Learning for Anomaly Detection in Electric Transportation Networks - E3S Web of Conferences, erişim tarihi Kasım 5, 2025, https://www.e3s-conferences.org/articles/e3sconf/pdf/2024/41/e3sconf_amgse2024_01039.pdf
24. Anomaly detection and prediction of charging station failure - Munich Data Science Institute, erişim tarihi Kasım 5, 2025, https://www.mdsi.tum.de/fileadmin/w00cet/di-lab/pdf/TUM-DI-LAB___BMW_WS2022_Final_Report.pdf
25. Development of a Hardware-in-the-Loop Testbed for a Decentralized, Data-Driven Electric Vehicle Charging Control Algorithm - National Renewable Energy Laboratory, erişim tarihi Kasım 5, 2025, https://research-hub.nrel.gov/en/publications/development-of-a-hardware-in-the-loop-testbed-for-a-decentralized
26. Methodology for Detecting Energy Anomalies due to Multi-Replay Attacks on Electric Vehicle Charging Infrastructure - arXiv, erişim tarihi Kasım 5, 2025, https://arxiv.org/html/2504.00319v1
27. A Scriptable OCPP Chargepoint Simulator for OCPP 1.6J. Client and Server. - GitHub, erişim tarihi Kasım 5, 2025, https://github.com/oglimmer/scriptable-ocpp-chargepoint-simulator
28. ocppjs - An experimental OCPP Simulator - GIR, erişim tarihi Kasım 5, 2025, http://www.gir.fr/ocppjs/
29. anomaly_report.txt