EV Şarj Altyapısında OCPP-CANbus Etkileşimine Dayalı Anomali Senaryoları ve Tehdit Analizi

Giriş: Yeni Nesil Tehdit Vektörü - Siber-Fiziksel Yakınsama

Elektrikli Araç (EV) şarj altyapısı, modern enerji ve ulaşım ekosistemlerinin vazgeçilmez bir bileşeni haline gelmiştir. Bu altyapının hızla yaygınlaşması, onu siber saldırganlar için giderek daha cazip bir hedef haline getirmektedir. Geleneksel Bilgi Teknolojileri (IT) sistemlerinden farklı olarak, EV şarj istasyonları (Charge Point - CP), siber ve fiziksel dünyaların kesiştiği karmaşık siber-fiziksel sistemlerdir. Bu sistemlerin kalbinde, iki temel iletişim protokolü arasındaki kritik etkileşim yatmaktadır: Şarj istasyonunu merkezi bir yönetim sistemine (Charge Station Management System - CSMS) bağlayan Open Charge Point Protocol (OCPP) ve istasyonun iç donanım bileşenlerini (güç elektroniği, röleler, sensörler) yöneten Controller Area Network (CAN-bus).

OCPP, yönetimsel ve işlemsel komutları (örn. şarjı başlat/durdur, faturalandırma verilerini gönder) ileten bir ağ protokolü iken, CAN-bus bu komutları fiziksel eylemlere (örn. bir röleyi kapat, akım seviyesini ayarla) dönüştüren bir operasyonel teknoloji (OT) protokolüdür. Bu iki protokol arasındaki mantıksal bağlantıyı sağlayan "köprü" bileşeni, yani şarj noktasının ana denetleyicisi (CP Main Controller), benzersiz ve kritik bir saldırı yüzeyi oluşturmaktadır. Bir OCPP zafiyeti, artık sadece bir veri ihlali veya faturalandırma hatasıyla sınırlı kalmamakta; doğrudan fiziksel donanımın manipülasyonuna, araç bataryalarının hasar görmesine ve hatta elektrik şebekesinin istikrarının tehlikeye atılmasına yol açabilecek bir potansiyel taşımaktadır.[1]

Bu raporun temel amacı, EV şarj altyapısındaki bu siber-fiziksel yakınsama noktasını derinlemesine analiz etmektir. Rapor, OCPP ve CAN-bus arasındaki mantıksal ilişkiyi, bu etkileşimden doğan zafiyetleri ve bu zafiyetlerin istismar edilebileceği somut anomali senaryolarını sistematik bir şekilde ortaya koymaktadır. Metodoloji olarak, endüstri standardı tehdit modelleme çerçeveleri olan STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) ve DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) kullanılarak kapsamlı bir risk analizi yapılmıştır.[1] Bu çalışma, geliştiriciler, üreticiler, operatörler ve güvenlik araştırmacıları için bu yeni nesil tehditlere karşı etkili tespit ve savunma stratejileri geliştirmelerine yönelik temel bir kaynak olmayı hedeflemektedir.

Bölüm 1: Siber-Fiziksel Etkileşim Mimarisi: OCPP ve CAN-bus Arasındaki Mantıksal Köprü

EV şarj altyapısının güvenliğini anlamak, onu oluşturan temel iletişim katmanlarının ve bu katmanlar arasındaki etkileşimin doğru bir şekilde analiz edilmesini gerektirir. Bu mimarinin merkezinde, yönetimsel niyetleri fiziksel eylemlere dönüştüren OCPP ve CAN-bus protokolleri arasındaki mantıksal köprü yer alır.

1.1. Protokollerin Rol Ayrımı ve İşlevsel Alanları

Sistemin güvenli ve verimli çalışması, her protokolün kendi alanında uzmanlaşmış görevleri yerine getirmesine dayanır.

- OCPP (Open Charge Point Protocol): Yönetim ve İşlem Katmanı
  OCPP, bir şarj istasyonu (CP) ile merkezi bir yönetim sistemi (CSMS) arasındaki iletişimi standartlaştıran bir uygulama katmanı protokolüdür. Temel görevi, şarj operasyonlarının uzaktan yönetimi ve izlenmesidir. Bu protokol, sistemin "ne yapacağını" belirleyen stratejik katmanı temsil eder. Başlıca işlevleri arasında kullanıcı yetkilendirme (Authorize), şarj işlemlerini uzaktan başlatma ve durdurma (RemoteStartTransaction, RemoteStopTransaction), faturalandırma için enerji tüketim verilerini periyodik olarak raporlama (MeterValues) ve şarj istasyonunun çeşitli parametrelerini yapılandırma (SetVariables, SetChargingProfile) bulunur.1 İletişim genellikle WebSocket üzerinden JSON formatında mesajlarla sağlanır ve güvenliği TLS (Transport Layer Security) ile sağlanmaya çalışılır.
- CAN-bus (Controller Area Network): Operasyonel ve Kontrol Katmanı
  CAN-bus, şarj istasyonunun içindeki çeşitli Elektronik Kontrol Üniteleri (ECU'lar) arasında yüksek güvenilirlikli, gerçek zamanlı iletişimi sağlayan bir mesaj tabanlı protokoldür. Bu protokol, OCPP tarafından belirlenen stratejik komutların "nasıl yapılacağını" icra eden operasyonel katmandır. Görevleri arasında güç kontaktörlerini (röleleri) fiziksel olarak açıp kapatmak, güç elektroniği modülüne (invertör/konvertör) hedef akım ve voltaj seviyelerini iletmek, batarya yönetim sisteminden (BMS) gelen sıcaklık ve durum verilerini okumak ve akıllı sayaçtan (smart meter) anlık tüketim verilerini almak yer alır.1 Ancak CAN-bus, doğası gereği kimlik doğrulama, şifreleme veya mesaj bütünlüğü gibi temel güvenlik mekanizmalarından yoksundur. Bu durum, ağa fiziksel veya mantıksal olarak erişim sağlayan bir saldırganın mesaj enjeksiyonu, sahtecilik ve tekrar saldırıları gerçekleştirmesine olanak tanır, bu da onu iç tehditlere karşı son derece savunmasız kılar.1

1.2. "Köprü" Bileşeni Analizi: Şarj Noktası Ana Denetleyicisi (CP Main

Controller)

OCPP ve CAN-bus arasındaki boşluğu dolduran ve bu iki farklı dünyayı birbirine bağlayan bileşen, şarj noktasının ana denetleyicisidir. Genellikle bir Mikrodenetleyici Ünitesi (MCU) veya Çip Üzerinde Sistem (SoC) olan bu bileşen, şarj istasyonunun beyni olarak işlev görür. Üzerinde bir OCPP istemci yazılımı çalıştırır ve bir CAN alıcı-verici (transceiver) donanımı aracılığıyla fiziksel CAN-bus hattına bağlanır.[1]
Bu denetleyicinin en kritik görevi, soyut, metin tabanlı OCPP komutlarını, donanım tarafından anlaşılabilecek somut, ikili (binary) CAN çerçevelerine "çevirmektir". Bu çeviri süreci, siber saldırıların fiziksel etkilere dönüştüğü birincil noktadır. Örnek bir çeviri akışı şu şekildedir:

1. CSMS'ten bir OCPP RemoteStartTransaction JSON mesajı, güvenli bir WebSocket tüneli üzerinden CP'nin ana denetleyicisine ulaşır.
2. Ana denetleyici üzerindeki OCPP istemci yazılımı, bu JSON mesajını ayrıştırır (parse eder) ve içindeki parametreleri (örn. connectorId, idTag) doğrular.
3. Denetleyici, ilgili uygulama mantığını çalıştırır: Konektörün durumu uygun mu? Kullanıcı yetkilendirmesi geçerli mi?
4. Tüm kontroller başarılıysa, denetleyici, güç elektroniği ECU'suna şarj işlemini başlatması için spesifik bir CAN çerçevesi oluşturur ve CAN-bus üzerine gönderir. Bu çerçeve, önceden tanımlanmış bir yapıya sahip olabilir; örneğin, CAN ID 0x200 ve veri yükü (payload) olarak `` gibi bilgileri içerebilir.[1]

1.3. Saldırı Yüzeyinin Genişlemesi ve Kaskad Etkisi

İzole sistemlerde, bir OCPP zafiyeti (örn. zayıf parola) yalnızca yönetimsel sorunlara (yanlış faturalandırma gibi) yol açarken, bir CAN-bus zafiyeti (örn. fiziksel erişimle mesaj enjeksiyonu) yalnızca yerel ve anlık manipülasyonla sonuçlanırdı. Ancak bu entegre mimaride, zafiyetler birbirini tetikleyerek bir kaskad etkisi yaratır.
Bu mimari, "güven sınırı ihlali" olarak adlandırılabilecek bir durum oluşturur. Sistem, katmanlar arasında örtük bir güven varsayımı üzerine kurulmuştur:

- CP ana denetleyicisi, doğası gereği CSMS'ten gelen ve TLS ile korunan OCPP mesajlarına **güvenir**.
- Güç elektroniği ECU'su ve diğer alt sistemler, aynı şekilde, ana denetleyiciden gelen CAN çerçevelerine **güvenir**.

Bir saldırgan, bu güven zincirindeki tek bir halkayı, genellikle internete en açık olan OCPP kanalını, kırmayı başarırsa (örneğin zayıf bir TLS uygulaması, çalınmış CSMS kimlik bilgileri veya bir MitM saldırısı ile), tüm sistemi ele geçirebilir.[1] Saldırgan, meşru bir CSMS gibi davranarak CP'ye kötü niyetli bir komut gönderdiğinde, CP'nin "köprü" yazılımı bu komutu sorgusuzca güvenilir bir CAN çerçevesine çevirir. Bu çevrilmiş komut, CAN-bus üzerindeki diğer ECU'lar tarafından meşru bir iç komut olarak algılanır ve icra edilir. Böylece, basit bir ağ tabanlı zafiyetin etkisi katlanarak artar ve doğrudan fiziksel donanımı, bağlı aracı ve hatta elektrik

şebekesini tehlikeye atabilecek bir siber-fiziksel saldırıya dönüşür.[2] Bu durum, saldırı yüzeyinin sadece toplanarak değil, çarpılarak genişlediği bir senaryo yaratır.
Aşağıdaki tablo, bu mimarideki ana bileşenleri, işlevlerini ve ilişkili potansiyel zafiyetleri özetleyerek bütünsel bir bakış açısı sunmaktadır.

Tablo 1: Bileşen-Zafiyet Matrisi

Bileşen Adı	Katman	Birincil İşlevi	Bilinen Zafiyetler / Saldırı Vektörleri
CSMS	Yönetim	Şarj noktalarını merkezi olarak yönetme, yetkilendirme, faturalandırma.	Zayıf parola politikaları, web uygulama zafiyetleri (SQLi, XSS), yetkisiz erişim.
İnternet Bağlantısı (TLS/VPN)	Yönetim	CP ve CSMS arasında güvenli iletişim kanalı sağlama.	Zayıf TLS şifreleme paketleri, süresi dolmuş sertifikalar, MitM saldırıları, VPN kimlik bilgisi hırsızlığı.[3]
CP Ana Denetleyici (MCU/SoC)	Köprü	OCPP mesajlarını işleme ve CAN çerçevelerine çevirme.	Firmware zafiyetleri, güvenli olmayan firmware güncelleme mekanizmaları, mantık hataları, arabellek taşması.
OCPP İstemci Yazılımı	Yönetim	CSMS ile OCPP iletişimini yönetme.	Zayıf hata yönetimi, gelen verilerin yetersiz doğrulanması, DoS zafiyetleri.
CAN Alıcı-Vericisi	Operasyonel	Mantıksal sinyalleri CAN-bus için fiziksel elektrik sinyallerine dönüştürme.	Fiziksel dinleme (eavesdropping), sinyal bozucular (jamming).
Güç Elektroniği ECU'su	Operasyonel	AC/DC dönüşümünü ve şarj akımını/voltajını kontrol etme.	Gelen CAN komutlarını doğrulamama, donanım limitlerini aşan komutları uygulama.
Akıllı Metre ECU'su	Operasyonel	Enerji tüketimini ölçme ve ana denetleyiciye raporlama.	Ölçüm verilerinin manipülasyonu (fiziksel müdahale), sahte veri enjeksiyonu.
Röle Kontrol ECU'su	Operasyonel	Güç kontaktörlerini açıp kapatma.	"Fail-safe" mekanizmalarının

			eksikliği, sahte açma/kapama komutlarına karşı savunmasızlık.

Bölüm 2: Bütünleşik Tehdit Modeli: STRIDE Çerçevesinin Uygulanması

OCPP-CANbus etkileşiminden kaynaklanan tehditleri sistematik olarak analiz etmek için, potansiyel saldırganları, motivasyonlarını ve kullanabilecekleri yöntemleri tanımlayan yapılandırılmış bir tehdit modeli gereklidir. Bu bölümde, tehdit aktörleri profillendirilmekte ve STRIDE çerçevesi, bu spesifik siber-fiziksel mimariye uyarlanarak tehditler sınıflandırılmaktadır.

2.1. Tehdit Aktörleri ve Motivasyonları

Saldırıların doğasını ve potansiyel etkilerini anlamak için, bu saldırıları gerçekleştirebilecek aktörleri ve hedeflerini belirlemek kritik öneme sahiptir.

- **Fırsatçı Saldırgan (Örn: EV Sahibi):** Bu aktörün temel motivasyonu kişisel kazançtır. Hedefleri arasında ücretsiz şarj etmek veya aracını standart limitlerden daha hızlı şarj etmek bulunur. Teknik yetenekleri genellikle düşüktür ve genellikle halka açık arayüzlerdeki (örn. mobil uygulamalar) zayıflıkları veya basit donanım müdahalelerini (örn. RFID klonlama) kullanırlar.
- **Siber Suçlu / Organize Gruplar:** Bu aktörler finansal kazanç odaklıdır. Geniş ölçekli faturalandırma sahtekarlığı yapmak, şarj ağını fidye yazılımı ile kilitlemek veya kullanıcıların kişisel ve finansal verilerini çalmak gibi hedefleri vardır. Yüksek teknik yeteneklere sahiptirler ve karmaşık ağ saldırıları (Man-in-the-Middle), tersine mühendislik ve özel zararlı yazılımlar geliştirebilirler.
- **İç Tehdit (Örn: Kötü Niyetli Bakım Teknisyeni/Operatör):** Bu aktörler, sisteme meşru erişimi olan kişilerdir. Motivasyonları sabotaj, intikam, endüstriyel casusluk veya finansal kazanç olabilir. Sisteme fiziksel erişimleri, potansiyel olarak yönetici seviyesinde kimlik bilgileri ve sistemin iç işleyişine dair derin bilgileri nedeniyle en tehlikeli aktör gruplarından biridir.
- **Devlet Destekli Aktörler / Gelişmiş Kalıcı Tehditler (APT'ler):** Bu aktörlerin birincil motivasyonu jeopolitiktir. Hedefleri, bir ülkenin kritik altyapısını, özellikle de elektrik şebekesini, istikrarsızlaştırmaktır. En yüksek seviyede teknik yeteneklere, kaynaklara ve zamana sahiptirler. Sıfır gün zafiyetlerini keşfedebilir, tedarik zinciri saldırıları düzenleyebilir ve çok sayıda şarj istasyonunu eş zamanlı olarak kontrol ederek şebeke düzeyinde büyük kesintilere yol açabilirler.[4]

2.2. STRIDE Kategorilerine Göre Tehditlerin Sınıflandırılması

STRIDE tehdit modelleme çerçevesi, yazılım ve sistemlerdeki potansiyel güvenlik tehditlerini altı kategoride sınıflandırmak için kullanılır.[1] Bu çerçeve, OCPP-CANbus köprüsü bağlamında şu şekilde uygulanabilir:

- **Spoofing (Sahtecilik):** Bir varlığın, başka bir varlığın kimliğine bürünmesidir.
  - *OCPP-CANbus Bağlamı:* Bir saldırganın, CP'ye kendisini meşru bir CSMS olarak tanıtması veya CP içindeki bir saldırgan cihazın, kendisini ana denetleyici gibi tanıtarak güç elektroniği ECU'suna sahte komutlar göndermesi.
- **Tampering (Kurcalama):** Verilerin veya mesajların yetkisiz olarak değiştirilmesidir.
  - *OCPP-CANbus Bağlamı:* CP ve CSMS arasındaki OCPP mesajlarının (örn. MeterValues veya SetChargingProfile) yolda değiştirilmesi veya CP içindeki CAN-bus üzerinde akan çerçevelerin içeriğinin manipüle edilmesi.
- **Repudiation (İnkar):** Bir eylemin gerçekleştirildiğinin inkar edilmesidir.
  - *OCPP-CANbus Bağlamı:* Bir saldırganın, şebekeyi istikrarsızlaştıracak bir SetChargingProfile komutu gönderdikten sonra, yetersiz loglama ve dijital imza eksikliği nedeniyle bu eylemin kaynağının tespit edilememesi ve saldırganın eylemi inkar edebilmesi.
- **Information Disclosure (Bilgi İfşası):** Hassas bilgilerin yetkisiz kişilere ifşa edilmesidir.
  - *OCPP-CANbus Bağlamı:* Şifrelenmemiş veya zayıf şifrelenmiş OCPP trafiğini dinleyerek kullanıcı kimliklerini (idTag), şarj alışkanlıklarını, konum verilerini veya CP'nin firmware sürümü gibi teknik detayları öğrenmek.
- **Denial of Service (Hizmet Reddi):** Bir hizmetin veya kaynağın meşru kullanıcılar için erişilemez hale getirilmesidir.
  - *OCPP-CANbus Bağlamı:* CP'nin CSMS ile olan ağ bağlantısını keserek şarj hizmetini uzaktan yönetilemez hale getirmek veya CP'nin iç CAN-bus'ını yüksek öncelikli anlamsız mesajlarla kilitleyerek (bus-off durumu) istasyonu tamamen işlevsiz kılmak.
- **Elevation of Privilege (Ayrıcalık Yükseltme):** Düşük ayrıcalıklı bir kullanıcının, daha yüksek ayrıcalıklara (örn. yönetici) sahip olmasıdır.
  - *OCPP-CANbus Bağlamı:* Normal bir kullanıcı yetkisiyle başlatılan bir saldırının sonucunda, CP'nin yapılandırma değişkenlerini (SetVariables) değiştirebilme veya doğrudan CAN-bus'a rastgele çerçeveler gönderebilme yetkisinin elde edilmesi.

Bu sınıflandırma, bir sonraki bölümde detaylandırılacak olan spesifik anomali senaryoları için yapısal bir temel oluşturur ve her bir saldırının hangi temel güvenlik ilkesini ihlal ettiğini netleştirir.

Bölüm 3: Detaylı Anomali Senaryoları Kataloğu

Bu bölüm, teorik tehdit modelini, OCPP-CANbus köprüsünün zafiyetlerini istismar eden somut,

adım adım ilerleyen anomali senaryolarına dönüştürür. Her senaryo, bir saldırının başlangıcından nihai fiziksel etkisine kadar olan tüm zinciri detaylandırarak, siber ve fiziksel dünyalar arasındaki etkileşimi gözler önüne serer. Aşağıdaki özet matris, bu bölümde incelenecek senaryolara hızlı bir genel bakış sunar.

Tablo 2: Anomali Senaryoları Özet Matrisi

Senaryo Kodu	Senaryo Adı	STRIDE Kategorisi	Etkilenen Varlık(lar)	DREAD Risk Skoru (Ortalama)	Özet Etki
S-01	Sahte CSMS ile Ücretsiz Şarj	Spoofing	CP, CSMS, Kullanıcı	Orta (6.2)	Enerji hırsızlığı, faturalandırma kaybı.
T-01	MitM ile MeterValues Manipülasyonu	Tampering	CSMS, Kullanıcı	Orta (7.4)	Finansal sahtekarlık, gelir kaybı.
T-02	SetChargingProfile ile Aşırı Yükleme	Tampering	EV Bataryası, CP Donanımı, Elektrik Şebekesi	Yüksek (8.6)	Batarya hasarı, yangın riski, şebeke istikrarsızlığı.
D-01	CAN-bus Mesaj Yoğunluklu Saldırı	Denial of Service	CP Donanımı (Tüm ECU'lar)	Yüksek (9.2)	Şarj istasyonunun tamamen hizmet dışı kalması.
E-01	Çevrimdışı Yetkilendirme İstismarı	Elevation of Privilege	CP, Kullanıcı	Orta (6.8)	Yetkisiz erişim, enerji hırsızlığı.

Not: DREAD risk skorları[1]'deki Tablo 13'ten alınan benzer tehditlerin değerlendirmelerine dayanarak niteliksel olarak tahmin edilmiştir ve belirli bir uygulama bağlamında değişiklik gösterebilir.

3.1. Sahtecilik (Spoofing) Senaryoları

Senaryo S-01: Sahte CSMS ile RemoteStartTransaction Komutu Göndererek Ücretsiz Şarj

Bu senaryo, bir saldırganın kendisini meşru bir CSMS olarak tanıtarak, yetkilendirme sürecini atlatıp ücretsiz enerji elde etmesini içerir.

- **Saldırı Vektörü:** Zayıf yapılandırılmış bir ağda DNS sahteciliği (DNS spoofing) veya zayıf

TLS sertifika doğrulaması nedeniyle gerçekleştirilen bir Man-in-the-Middle (MitM) saldırısı.[3]

- **Adım-Adım Akış:**
    1. Saldırgan, şarj istasyonunun bulunduğu yerel ağa (örneğin, halka açık bir Wi-Fi) sızar ve CP'nin CSMS'e olan ağ trafiğini kendi kontrolündeki bir sunucuya yönlendirmek için ARP zehirlenmesi veya DNS sahteciliği gibi teknikler kullanır.
    2. CP açıldığında veya yeniden başlatıldığında, standart prosedür gereği CSMS'e bir BootNotification mesajı gönderir. Bu mesaj, saldırganın sahte CSMS sunucusuna ulaşır.
    3. Saldırganın sunucusu, meşru bir CSMS gibi davranarak, geçerli bir zaman damgası ve kabul durumu içeren bir BootNotification yanıtı gönderir. CP, bu sahte CSMS ile başarılı bir şekilde bağlantı kurduğunu varsayar.
    4. Saldırgan, elektrikli aracını şarj istasyonuna bağlar.
    5. Sahte CSMS, geçerli bir kullanıcı kimliği (idTag) belirtmeden veya önceden çalınmış/klonlanmış bir kimlik kullanarak CP'ye bir RemoteStartTransaction komutu gönderir.
- **OCPP Gözlemleri:** Saldırganın sunucu loglarında, CP'den gelen BootNotification, StatusNotification ve Heartbeat mesajları görülür. CP'ye ise sahte CSMS'ten gönderilen bir BootNotification onayı ve yetkisiz bir RemoteStartTransaction mesajı ulaşır. Gerçek CSMS loglarında ise bu CP'nin çevrimdışı olduğu veya hiç bağlanmadığı görülür.
- **CAN-bus Gözlemleri:** CP ana denetleyicisi, sahte CSMS'ten gelen RemoteStartTransaction komutunu aldığında, bunu meşru bir talep olarak işler. Röle kontrol ECU'suna gücü bağlaması için bir CAN çerçevesi (örneğin, ID 0x200, Payload:) gönderir. Ardından, akıllı metre ECU'su enerji tüketimini ölçmeye ve bu veriyi periyodik olarak ana denetleyiciye raporlamaya başlar (örneğin, ID 0x300 ile).
- **Nihai Etki:** Enerji hırsızlığı. Şarj işlemi, gerçek CSMS'in bilgisi ve kaydı dışında gerçekleştiği için, tüketilen enerji için herhangi bir faturalandırma yapılamaz. Bu durum, şarj operatörü için doğrudan finansal kayıp anlamına gelir.

3.2. Kurcalama (Tampering) Senaryoları

Senaryo T-01: MitM ile OCPP MeterValues Mesajlarının Değiştirilerek Faturalandırma Sahtekarlığı

Bu senaryo, saldırganın şarj sırasında iletilen enerji tüketim verilerini manipüle ederek ödeyeceği fatura tutarını düşürmesini hedefler.

- **Saldırı Vektörü:** Güvenli olmayan, şifrelenmemiş WebSocket (ws://) bağlantılarının kullanılması veya zayıf TLS uygulamaları (eski protokol sürümleri, zayıf şifreleme takımları) üzerinden gerçekleştirilen bir MitM saldırısı.[1]

- **Adım-Adım Akış:**
    1. Saldırgan, CP ile CSMS arasındaki ağ trafiğinin geçtiği bir noktaya (örneğin, bir ağ anahtarı veya yönlendirici) kendisini bir proxy olarak konumlandırır. mitmproxy gibi araçlar bu amaçla kullanılabilir.
    2. Meşru bir kullanıcı (saldırganın kendisi veya başka bir kurban) normal bir şarj işlemi başlatır.
    3. CP, şarj süresince düzenli aralıklarla, o ana kadar tüketilen toplam enerjiyi içeren MeterValues mesajlarını CSMS'e gönderir. Örnek mesaj: {"meterValue":}]} (15 kWh).
    4. Saldırganın proxy'si, bu giden mesajı yolda yakalar, "value" alanındaki değeri gerçek değerden daha düşük bir değerle (örneğin, "1500") değiştirir ve manipüle edilmiş mesajı CSMS'e iletir.
- **OCPP Gözlemleri:** CSMS'in veritabanı ve loglarında, şarj işlemi boyunca kaydedilen enerji tüketim değerleri, aracın batarya kapasitesi ve şarj süresi göz önüne alındığında mantıksız derecede düşük görünür.
- **CAN-bus Gözlemleri:** Bu saldırı türünde CAN-bus seviyesinde herhangi bir anomali gözlemlenmez. Akıllı metre ECU'su (ID 0x300), gerçek ve doğru tüketim verilerini CP ana denetleyicisine göndermeye devam eder. Manipülasyon, veriler CAN-bus'tan alınıp OCPP mesajına dönüştürüldükten sonra, yani "köprü" bileşeninden sonraki ağ katmanında meydana gelir.
- **Nihai Etki:** Şarj operatörü için finansal kayıp. CSMS, manipüle edilmiş düşük verilere dayanarak faturalandırma yapacağından, tüketilen enerjinin yalnızca küçük bir kısmı için ödeme alınır.

Senaryo T-02: SetChargingProfile Komutunun Manipüle Edilerek Bataryaya Aşırı Yükleme veya Şebekeyi Destabilize Etme

Bu, siber bir eylemin doğrudan kinetik ve geniş alanlı fiziksel hasara yol açabileceği en tehlikeli senaryolardan biridir.

- **Saldırı Vektörü:** Ele geçirilmiş bir CSMS yönetici hesabı, CSMS'teki bir zafiyet veya Senaryo S-01'deki gibi bir MitM saldırısı ile sahte bir CSMS üzerinden komut gönderme.[1]
- **Adım-Adım Akış:**
    1. Saldırgan, devam eden meşru bir şarj işlemi sırasında hedef CP'ye bir SetChargingProfile komutu gönderme yetkisi elde eder.
    2. Saldırgan, komutun chargingProfile nesnesi içindeki chargingSchedule listesinde yer alan limit değerini, hem aracın batarya yönetim sisteminin (BMS) hem de şarj istasyonunun güç elektroniğinin güvenli operasyonel limitlerinin çok üzerine ayarlar. Örneğin, 32 Amper kapasiteli bir istasyon için 80 Amper gibi bir değer belirler.
    3. CP, CSMS'ten geldiği için bu profile güvenir ve geçerli kabul eder. "Köprü" yazılımı, bu tehlikeli akım limitini belirten yeni bir CAN çerçevesi oluşturur.
- **OCPP Gözlemleri:** CSMS'ten CP'ye, donanım limitlerini aşan, tehlikeli derecede yüksek

akım veya güç limitleri içeren bir SetChargingProfile mesajı gönderildiği loglanır.
- **CAN-bus Gözlemleri:** CP ana denetleyicisi, OCPP komutunu işledikten sonra, güç elektroniği ECU'suna yeni akım limitini ayarlaması için bir CAN çerçevesi gönderir (örneğin, ID 0x210, Payload:). Güç elektroniği ECU'su, bu komutu alarak çıkış akımını artırmaya çalışır.
- **Nihai Etki:**
    - **Araç ve İstasyon Seviyesi:** Eğer istasyonun veya aracın donanım korumaları (sigortalar, yazılımsal limitler) bu komutu engelleyemezse, sonuçlar felaket olabilir. EV bataryasında aşırı ısınma, hücrelerin kalıcı hasar görmesi (degradasyon) ve en kötü senaryoda kontrolsüz bir kimyasal reaksiyon olan termal kaçak (thermal runaway) meydana gelebilir, bu da yangın ve patlama riski yaratır. Şarj istasyonunun güç elektroniği bileşenleri de aşırı yüklenerek yanabilir.
    - **Şebeke Seviyesi (Silahlaştırılmış Altyapı):** Bu senaryonun gerçek tehlikesi, ölçeklendirilebilirliğinde yatmaktadır. Devlet destekli bir aktör veya sofistike bir siber suç grubu, binlerce şarj istasyonunu aynı anda ele geçirip bu saldırıyı eş zamanlı olarak gerçekleştirirse, yerel bir elektrik trafosu veya hatta bölgesel bir alt istasyon üzerinde ani ve kitlesel bir yük artışı yaratabilir. Bu durum, frekans ve voltaj dengesizliklerine, koruma rölelerinin atmasına ve geniş çaplı elektrik kesintilerine (blackout) yol açabilir.[4] Bu noktada, EV şarj istasyonları sadece enerji tüketen cihazlar olmaktan çıkar ve aktif olarak şebekeye zarar vermek için kullanılabilecek dağıtık bir siber silaha dönüşür. Bir siber komut manipülasyonu, geniş alanlı bir fiziksel etkiye dönüşerek ulusal güvenlik sorunu haline gelir.

3.3. Hizmet Reddi (Denial of Service) Senaryoları

Senaryo D-01: CAN-bus'ın Arbitrasyon Mekanizmasını İstismar Ederek Mesaj Yoğunluklu Saldırı (Bus-Off)

Bu saldırı, şarj istasyonunun iç iletişim omurgasını hedef alarak onu tamamen işlevsiz hale getirir.

- **Saldırı Vektörü:** CP'nin kasasına fiziksel erişim sağlayarak CAN-bus hattına zararlı bir cihaz bağlamak veya daha önce ele geçirilmiş firmware aracılığıyla ana denetleyiciyi bu saldırıyı gerçekleştirmesi için programlamak.[2]
- **Adım-Adım Akış:**
    1. Saldırgan, CP'nin içindeki CAN-bus'a (genellikle CAN-H ve CAN-L pinlerine) erişim sağlar.
    2. Saldırganın cihazı, CAN protokolünde mümkün olan en yüksek önceliğe sahip olan 0x000 ID'li CAN çerçevelerini sürekli ve çok yüksek bir hızda (flood) bus'a göndermeye başlar.

3. CAN protokolünün tahkim (arbitration) mekanizması gereği, daha düşük ID değerine sahip mesajlar her zaman daha yüksek ID'li mesajlara göre öncelik kazanır. Bu nedenle, saldırganın 0x000 ID'li mesajları, bus üzerindeki diğer tüm meşru mesajlara (güç durumu, sıcaklık, sayaç verileri vb.) baskın çıkar.
4. Güç elektroniği, akıllı metre ve röle kontrolü gibi kritik ECU'lar, bus'a kendi mesajlarını gönderemez hale gelirler. Bir süre sonra, sürekli olarak tahkimi kaybettikleri ve hata sayaçları dolduğu için kendilerini korumak amacıyla "bus-off" durumuna geçerek iletişimden tamamen çekilirler.

- **OCPP Gözlemleri:** CP ana denetleyicisi, iç ECU'lardan kritik durum güncellemelerini (metre değerleri, güç durumu vb.) alamaz hale gelir. Sonuç olarak, CSMS'e StatusNotification mesajları aracılığıyla InternalError veya OtherError gibi hata kodları göndermeye başlar. Bir süre sonra, ana denetleyici de kilitlenebilir ve CSMS'e Heartbeat mesajı göndermeyi tamamen durdurarak ağda çevrimdışı görünür.
- **CAN-bus Gözlemleri:** Bir CAN analizörü ile bus dinlendiğinde, 0x000 ID'li çerçevelerin anormal derecede yüksek bir frekansta ve sürekli olarak tekrarlandığı görülür. Diğer tüm meşru ID'lerin (örn. 0x200, 0x210, 0x300) frekansı sıfıra düşer. Bus yükü (bus load) %100'e yaklaşır.
- **Nihai Etki:** Şarj istasyonu tamamen işlevsiz hale gelir. Devam eden şarj işlemleri aniden kesilir ve yeni işlemler başlatılamaz. İstasyon, fiziksel bir müdahale (yeniden başlatma ve saldırgan cihazın sökülmesi) olmadan kurtarılamaz.

3.4. Ayrıcalık Yükseltme (Elevation of Privilege) Senaryoları

Senaryo E-01: CP'nin Çevrimdışı Yetkilendirme Mekanizmalarını İstismar Ederek Yetkisiz Erişim

Bu senaryo, bir hizmet reddi saldırısını, zayıf bir yapılandırma ile birleştirerek yetkisiz erişim ve enerji hırsızlığına yol açan karmaşık bir saldırı zincirini gösterir.

- **Saldırı Vektörü:** İki aşamalı bir saldırıdır: İlk olarak CP'nin ağ bağlantısına yönelik bir DoS saldırısı, ardından CP'nin zayıf çevrimdışı mod yapılandırmasının istismar edilmesi.[1]
- **Adım-Adım Akış:**
    1. Saldırgan, CP ile CSMS arasındaki iletişimi kesintiye uğratmak için bir ağ tabanlı DoS saldırısı başlatır. Bu, CP'nin bulunduğu ağa yönelik bir UDP/TCP flood saldırısı veya CP'nin internet bağlantısını fiziksel olarak kesmek şeklinde olabilir.
    2. CP, CSMS'e ulaşamadığını anladığında, önceden yapılandırılmış olan "çevrimdışı mod"a geçer.
    3. Saldırgan, CP'nin zayıf bir şekilde yapılandırıldığını varsayar. Özellikle, OfflineTxForUnknownIdEnabled yapılandırma değişkeninin true olarak ayarlandığını hedefler. Bu ayar, CP'nin çevrimdışıyken, daha önce hiç görmediği

veya yerel listesinde bulunmayan herhangi bir kimliği otomatik olarak kabul etmesine neden olur.[1]

4. Saldırgan, aracını istasyona bağlar ve herhangi bir geçersiz veya sahte RFID kartını/token'ını okutur.
5. CP, CSMS'e danışamadığı ve yapılandırması "bilinmeyen kimlikleri kabul et" dediği için, bu geçersiz kimliği yerel olarak yetkilendirir ve şarj işlemini başlatır.

- **OCPP Gözlemleri:** Saldırının ilk aşamasında, CSMS logları CP'den gelen Heartbeat mesajlarının kesildiğini ve CP'nin çevrimdışı olarak işaretlendiğini gösterir. Ağ bağlantısı yeniden kurulduğunda, CP, CSMS'e daha önce çevrimdışıyken gerçekleşmiş olan ve bilinmeyen/geçersiz bir idTag'e ait bir TransactionEvent (şarj işlemi detayı) gönderir. Bu, CSMS tarafında bir anomali olarak tespit edilebilir.
- **CAN-bus Gözlemleri:** CAN-bus seviyesindeki trafik, normal bir şarj işlemindeki trafikle tamamen aynıdır. Röleler kapanır, güç akışı başlar ve sayaç verileri akar. Anomali, CAN seviyesinde değil, ana denetleyicinin uygulama mantığı ve yetkilendirme katmanında meydana gelir.
- **Nihai Etki:** Yetkisiz erişim ve enerji hırsızlığı. Bu senaryo, bir siber saldırının (DoS), bir mantık zafiyetini (zayıf yapılandırma) tetikleyerek nasıl doğrudan fiziksel bir kazanca (ücretsiz enerji) dönüştüğünü göstermesi açısından önemlidir.

Bölüm 4: Anomali Tespiti ve Savunma Stratejileri

Önceki bölümde detaylandırılan karmaşık siber-fiziksel tehditlere karşı koymak, tek bir güvenlik çözümüne dayanmak yerine, çok katmanlı ve bütünsel bir yaklaşım gerektirir. Bu bölümde, anomali tespiti için kullanılabilecek mekanizmalar ve "Derinlemesine Savunma" (Defense-in-Depth) ile "Sıfır Güven" (Zero Trust) gibi modern güvenlik mimarilerinin OCPP-CANbus köprüsünü korumak için nasıl uygulanabileceği ele alınmaktadır.

4.1. Kural Tabanlı ve İstatistiksel Tespit Mekanizmaları (IDS)

Anomali Tespiti Sistemleri (Intrusion Detection Systems - IDS), normal sistem davranışından sapmaları tespit ederek saldırıları proaktif olarak belirlemeyi amaçlar.

- **CAN-IDS (CAN-bus Anomali Tespiti Sistemi):** Bu sistem, genellikle CP ana denetleyicisi üzerinde çalışır ve iç CAN-bus trafiğini sürekli olarak izler.
    - **İstatistiksel Yöntemler:** Sistemin normal çalışma koşulları altında (farklı şarj senaryolarında) bir temel davranış profili oluşturulur. Bu profil, her bir CAN ID'sinin beklenen frekansını (saniyedeki mesaj sayısı), periyodik mesajlar arasındaki zaman aralıklarını ve bus yükünü içerir. Senaryo D-01'de olduğu gibi, 0x000 ID'sinin frekansında ani ve ezici bir artış veya kritik ECU ID'lerinin (örn. güç elektroniği durum mesajı) aniden kaybolması, bu temel profilden bir sapma olarak anında tespit edilir ve bir alarm tetiklenir.[1]

    - **Zamanlama Analizi:** Güç elektroniği ECU'sundan gelen periyodik durum mesajları gibi kritik mesajlar arasındaki zaman aralıkları (inter-arrival time) takip edilir. Bu aralıklarda beklenmedik gecikmeler veya tam tersi, mesajların çok sık gelmesi (flood), bus üzerindeki bir anormalliğin veya bir ECU'nun arızalandığının/ele geçirildiğinin bir göstergesi olabilir.
- **OCPP Mesaj Akışı Analizi:** Bu analiz, CSMS tarafında gerçekleştirilir ve her bir CP'den gelen OCPP mesajlarının sırasını, içeriğini ve zamanlamasını izler.
    - **Kural Tabanlı Tespit:** Belirli mantıksal kurallar tanımlanır. Örneğin, bir CP'den gelen MeterValues mesajındaki enerji artış hızı, o CP için daha önce gönderilen SetChargingProfile komutundaki akım limitiyle tutarlı olmalıdır. Senaryo T-02'deki gibi, düşük bir akım limiti belirlenmesine rağmen enerji tüketiminde anormal derecede hızlı bir artış raporlanması, bir tutarsızlık ve potansiyel bir saldırı belirtisidir.
    - **Durum Makinesi Analizi:** Bir CP'nin durumu (örn. Available, Charging, Faulted) ve bu durumlar arasındaki geçişler izlenir. Bir CP'nin çok sık bir şekilde çevrimdışı ve çevrimiçi durumları arasında gidip gelmesi, ağ bağlantısında bir soruna veya potansiyel bir DoS saldırısına işaret edebilir.

4.2. Derinlemesine Savunma (Defense-in-Depth) Mimarisi

"Derinlemesine Savunma" stratejisi, tek bir güvenlik katmanının başarısız olması durumunda sistemin tamamen savunmasız kalmasını önlemek için birden fazla, birbiriyle örtüşen koruma katmanı oluşturmayı hedefler.[1]

- **Katman 1 (Ağ Güvenliği - Çevre Koruma):** Bu katman, CP'nin dış dünya ile olan iletişimini güvence altına alır.
    - **Zorunlu Karşılıklı TLS (mTLS):** OCPP iletişimi için standart TLS yerine mTLS kullanılmalıdır. mTLS, sadece CSMS'in kendi kimliğini CP'ye kanıtlamasını değil, aynı zamanda CP'nin de kendi kimliğini (bir istemci sertifikası kullanarak) CSMS'e kriptografik olarak kanıtlamasını gerektirir. Bu, sahte bir CP'nin veya sahte bir CSMS'in ağa dahil olmasını neredeyse imkansız hale getirerek Senaryo S-01 gibi sahtecilik ve MitM saldırılarını büyük ölçüde engeller.[1]
- **Katman 2 ("Köprü" / Gateway Güvenliği - İç Kontrol):** Bu katman, OCPP komutlarının CAN çerçevelerine çevrildiği kritik noktayı korur.
    - **İzin Listesi (Allow-List) Filtresi:** CP ana denetleyicisi üzerindeki çeviri mantığı, bir "sağduyu filtresi" gibi davranmalıdır. Örneğin, CSMS'ten gelen bir SetChargingProfile komutu, CAN-bus'a çevrilmeden önce içeriği doğrulanmalıdır. Komutla istenen akım limiti, şarj istasyonunun donanımının fiziksel olarak desteklediği maksimum değerle (örn. 32A) karşılaştırılır. Eğer istenen değer bu güvenli limiti aşıyorsa, komut reddedilir ve CSMS'e bir hata mesajı gönderilir. Bu, Senaryo T-02'deki gibi tehlikeli komutların fiziksel donanıma ulaşmasını engeller.[1]
- **Katman 3 (Yazılım Bütünlüğü - Uç Nokta Koruması):** Bu katman, CP'nin üzerinde

çalışan yazılımın güvenilir ve değiştirilmemiş olmasını sağlar.
    - **Güvenli Önyükleme (Secure Boot) ve Firmware İmzalama:** CP'nin donanımı, yalnızca üretici tarafından kriptografik olarak imzalanmış bir firmware'i çalıştıracak şekilde tasarlanmalıdır. Cihaz her açıldığında, önyükleyici (bootloader) firmware imzasını doğrular. İmza geçersizse veya firmware değiştirilmişse, cihaz çalışmayı reddeder. Bu, saldırganların cihaza zararlı veya değiştirilmiş bir firmware yüklemesini engelleyerek kalıcı tehditlerin önüne geçer.[1]
- **Katman 4 (CAN-bus Segmentasyonu - Ağ İzolasyonu):** Bu katman, bir ihlalin yayılma alanını sınırlar.
    - CP'nin iç ağı, mantıksal segmentlere ayrılabilir. Örneğin, şarj işleminin kritik kontrolünü yürüten (güç elektroniği, BMS iletişimi) CAN-bus segmenti, daha az kritik olan (kullanıcı arayüzü, LED göstergeler) segmentten bir ağ geçidi (gateway) ile ayrılır. Bu ağ geçidi, segmentler arasında yalnızca önceden tanımlanmış, güvenli mesajların geçişine izin verir. Böylece, kullanıcı arayüzü gibi daha kolay erişilebilir bir bileşenin ele geçirilmesi durumunda, saldırganın kritik güç kontrol sistemlerine ulaşması engellenir.

4.3. Sıfır Güven (Zero Trust) Yaklaşımının Entegrasyonu

"Sıfır Güven" mimarisi, geleneksel "içerisi güvenli, dışarısı tehlikeli" anlayışını reddeder ve ağ içindeki hiçbir varlığa veya isteğe varsayılan olarak güvenilmemesi gerektiğini savunur.[1] Bu paradigma, OCPP-CANbus mimarisine şu şekilde uygulanabilir:

- **"Asla Güvenme, Her Zaman Doğrula" İlkesi:**
    - CSMS'ten gelen bir RemoteStartTransaction komutu, sadece mTLS ile doğrulanmakla kalmaz. CP, bu komutu alırken ek bağlamsal kontroller de yapar: Bu komut, bu CP'nin normalde iletişim kurduğu CSMS IP adresinden mi geliyor? Günün bu saatinde bu tür bir istek normal mi? İstenen şarj parametreleri, aracın daha önceki şarj seanslarıyla tutarlı mı? Bu çok faktörlü doğrulama, sadece kimliğe değil, aynı zamanda davranışa da odaklanarak daha sofistike saldırıları tespit edebilir.
    - Benzer şekilde, CP ana denetleyicisi, güç elektroniği ECU'sundan gelen bir "aşırı sıcaklık" uyarısını körü körüne kabul etmez. Bu uyarıyı, akıllı metreden gelen akım çekiş verisi ve soğutma fanı ECU'sundan gelen durum bilgisi gibi diğer sensör verileriyle karşılaştırır. Eğer yüksek akım çekişi yoksa ve fan normal çalışıyorsa, sıcaklık uyarısının sahte bir sensör verisinden veya bir saldırıdan kaynaklanabileceği ihtimali değerlendirilir. Bu, siber-fiziksel bir sistemde "asla güvenme, her zaman doğrula" ilkesinin pratik bir uygulamasıdır.

Sonuç ve Gelecek Çalışmalar

Bu rapor, Elektrikli Araç (EV) şarj altyapısının siber güvenliğinde, genellikle göz ardı edilen ancak kritik öneme sahip bir alanı, yani OCPP yönetim protokolü ile CAN-bus operasyonel kontrol protokolü arasındaki siber-fiziksel köprüyü, detaylı bir şekilde analiz etmiştir. Yapılan analizler, bu etkileşim noktasının, sofistike ve yüksek etkili saldırılar için verimli bir zemin oluşturduğunu net bir şekilde ortaya koymuştur.

Raporun temel bulguları şu şekilde özetlenebilir:

1. **Kritik "Köprü" Zafiyeti:** Şarj istasyonunun ana denetleyicisi, soyut OCPP komutlarını somut CAN-bus eylemlerine çevirerek, siber saldırıların doğrudan fiziksel sonuçlar doğurmasına olanak tanıyan bir "kaskad etkisi" yaratmaktadır. Bu, saldırı yüzeyini ve potansiyel hasarı katlanarak artırmaktadır.
2. **Siber-Fiziksel Etkilerin Gerçekliği:** Geliştirilen anomali senaryoları, bir ağ mesajının (SetChargingProfile) manipülasyonunun, bir aracın bataryasına fiziksel hasar verebileceğini (termal kaçak riski) ve çok sayıda istasyonda koordine edildiğinde elektrik şebekesinde istikrarsızlığa yol açabileceğini göstermiştir. Bu durum, EV şarj altyapısı güvenliğinin bir ulusal altyapı güvenliği meselesi olduğunu kanıtlamaktadır.
3. **Katmanlı Savunmanın Zorunluluğu:** Tek bir güvenlik önleminin (örneğin, sadece TLS şifrelemesi) yetersiz olduğu açıktır. Etkili bir koruma, ağ güvenliğinden (mTLS), ağ geçidi mantığına (izin listeleri), yazılım bütünlüğüne (güvenli önyükleme) ve iç ağ segmentasyonuna kadar uzanan bir "Derinlemesine Savunma" stratejisi gerektirmektedir. "Sıfır Güven" ilkelerinin benimsenmesi ise bu savunmayı daha da güçlendirecektir.

Bu çalışma, mevcut tehdit ortamına dair bir anlık görüntü sunmakla birlikte, EV teknolojisi ve altyapısı geliştikçe yeni tehditlerin ortaya çıkacağı kaçınılmazdır. Bu bağlamda, gelecekteki araştırma ve geliştirme çabalarının aşağıdaki alanlara odaklanması önerilmektedir:

- **ISO 15118 ve V2G (Vehicle-to-Grid) Tehditleri:** Araçtan şebekeye enerji akışını sağlayan ISO 15118 standardı, saldırganların sadece enerji çalmasına veya hizmeti engellemesine değil, aynı zamanda şebekeye aktif olarak "enerji enjekte ederek" onu destabilize etmesine olanak tanıyabilecek yeni ve karmaşık saldırı vektörleri sunmaktadır.[5] Bu çift yönlü etkileşimin güvenlik analizi acil bir önceliktir.
- **Yapay Zeka ve Makine Öğrenmesi Tabanlı Adaptif IDS:** Bu raporda bahsedilen istatistiksel anomali tespit yöntemleri, bilinen saldırı kalıpları için etkili olsa da, sıfır gün saldırılarına ve karmaşık, yavaş ilerleyen tehditlere karşı yetersiz kalabilir. Şarj seanslarının çok boyutlu verilerini (OCPP mesajları, CAN-bus trafiği, güç parametreleri, kullanıcı davranışları) analiz eden yapay zeka tabanlı adaptif tespit sistemleri, daha önce görülmemiş anomalileri tespit etme potansiyeline sahiptir.
- **Blokzincir Tabanlı Güvenlik ve Denetlenebilirlik:** Özellikle faturalandırma, yetkilendirme ve şarj profili komutları gibi kritik işlemlerin güvenliği ve inkar edilemezliği için blokzincir teknolojisinin kullanımı araştırılabilir. Dağıtık ve değiştirilemez bir kayıt defteri, işlemlerin bütünlüğünü garanti altına alabilir ve sahtekarlık girişimlerini zorlaştırabilir.[1]

Sonuç olarak, EV şarj altyapısının güvenliği, sadece bir teknoloji sorunu değil, aynı zamanda sistemik bir mimari ve strateji sorunudur. Siber ve fiziksel dünyalar arasındaki sınırların giderek belirsizleştiği bu yeni ekosistemde, güvenliği en başından tasarıma dahil eden, proaktif ve çok

katmanlı yaklaşımlar, sürdürülebilir ve güvenli bir elektrikli ulaşım geleceği için hayati öneme sahiptir.

Alıntılanan çalışmalar

1. BİLGİ NOTU.pdf
2. CANAttack: Assessing Vulnerabilities within Controller Area Network, erişim tarihi Ekim 27, 2025, https://www.mdpi.com/1424-8220/23/19/8223
3. MitM Cyber Risk Analysis in OCPP enabled EV ... - NTU > IRep, erişim tarihi Ekim 27, 2025, https://irep.ntu.ac.uk/id/eprint/54419/1/2478037_Brown.pdf
4. (PDF) Uncovering Covert Attacks on EV Charging Infrastructure ..., erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/377183224_Uncovering_Covert_Attacks_on_EV_Charging_Infrastructure_How_OCPP_Backend_Vulnerabilities_Could_Compromise_Your_System
5. Securing the Charge: Hidden Risks in ISO 15118 - VicOne, erişim tarihi Ekim 27, 2025, https://cdn.vicone.com/files/research-papers/EN/vicone_securing_the_charge_hidden_risks_in_iso15118.pdf
6. Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review - arXiv, erişim tarihi Ekim 27, 2025, https://arxiv.org/html/2503.15730v1