# Gelişmiş EV Şarj Ekosistemlerinde Siber-Fiziksel Anomali Senaryoları Kataloğu

## Giriş: OCPP'den Araçtan Şebekeye (V2G) Genişleyen Saldırı Yüzeyi

Elektrikli Araç (EV) şarj altyapısı, artık izole cihazların bir koleksiyonu olarak değil, siber ve fiziksel dünyaların iç içe geçtiği, genişleyen ve birbirine bağlı bir siber-fiziksel ekosistem olarak değerlendirilmelidir. Bu karmaşık yapının merkezinde, soyut komutları kinetik eylemlere dönüştüren kritik bir bileşen olan Şarj Noktası (Charge Point - CP) ana denetleyicisi yer almaktadır.1 Bu denetleyici, bir "siber-fiziksel pivot noktası" olarak işlev görür; Merkezi Yönetim Sisteminden (CSMS) gelen bir Open Charge Point Protocol (OCPP) mesajını alır ve bunu, aracın bataryasına güç sağlayan röleleri ve güç elektroniğini kontrol eden somut bir Controller Area Network (CAN-bus) komutuna çevirir.1

Ancak bu model, tehdit manzarasının yalnızca başlangıcını temsil etmektedir. ISO 15118 standardının getirdiği "Tak ve Şarj Et" (Plug & Charge) otomasyonu ve Araçtan Şebekeye (Vehicle-to-Grid - V2G) teknolojilerinin ortaya çıkışıyla birlikte, bu pivot noktası konsepti radikal bir şekilde genişlemiştir.2 Artık sadece şarj istasyonu değil, V2G yetenekli her bir elektrikli araç, potansiyel bir siber-fiziksel pivot noktasına dönüşmüştür. Bu durum, tek bir zafiyetin potansiyel etkisini yerel bir kesintiden, tüm elektrik şebekesini istikrarsızlaştırabilecek sistemik bir tehdide dönüştürmektedir.4 Saldırı yüzeyi artık sadece şarj istasyonlarının sayısıyla değil, şebekeye bağlı araçların sayısıyla katlanarak artmaktadır.

Bu raporun amacı, bu gelişen ekosistemdeki paydaşlara, daha dirençli sistemler inşa etmelerine yardımcı olacak yapılandırılmış ve teknik olarak detaylı bir anomali senaryoları kataloğu sunmaktır. Bu katalog, tehdit modellemesi, güvenlik kontrollerinin doğrulanması ve sızma testi (red team) tatbikatlarının planlanması için temel bir kaynak olarak tasarlanmıştır. Aşağıdaki Ana Anomali Senaryo Matrisi, raporda detaylandırılan tehdit manzarasına hızlı bir genel bakış sağlamaktadır.

## Ana Anomali Senaryo Matrisi

Bu matris, raporda incelenen 20 senaryonun tamamına ilişkin üst düzey bir özet sunarak, güvenlik mimarlarının, analistlerin ve karar vericilerin tehditleri önceliklendirmesine ve kaynakları etkin bir şekilde tahsis etmesine olanak tanır.

| **Senaryo Kodu** | **Senaryo Adı** | **Birincil Hedef** | **Anahtar Protokol(ler)** | **STRIDE Kategorisi** | **Tehdit Aktörü Profili** | **Etki Şiddeti** |
| --- | --- | --- | --- | --- | --- | --- |
| **OCPP-01** | Kalıcı CAN Enjektörü Oluşturmak İçin Güvenli Olmayan Firmware Manipülasyonu | CP Donanımı | OCPP 1.6, CAN | Tampering | Siber Suçlu | Yüksek |
| **OCPP-02** | Uzaktan Log Kurcalama ile İnkar (Repudiation) Saldırısı | Adli Kanıtlar | OCPP 1.6 | Repudiation | Gelişmiş Kalıcı Tehdit (APT) | Orta |
| **CAN-01** | Sensör Arızasını Taklit Etmek ve Acil Durdurmayı Tetiklemek İçin Hassas CAN Enjeksiyonu | Hizmet Sürekliliği | CAN | Spoofing | İç Tehdit | Orta |
| **CAN-02** | Sahte Şarj Kayıtları Oluşturmak İçin CAN Tekrar Saldırısı ile "Hayalet EV" Saldırısı | CPO Geliri (Promosyonlar) | CAN, OCPP 1.6 | Spoofing | Fırsatçı Saldırgan | Düşük |
| **LOGIC-01** | OCPP-CAN Çeviri Mantığında Yarış Durumu (Race Condition) İstismarı | CP Yazılım Stabilitesi | OCPP 1.6, CAN | Denial of Service | Siber Suçlu | Orta |
| **ISO-01** | EV Parmak İzi ve CPO'lar Arası Kullanıcı Takibi | Kullanıcı Gizliliği | ISO 15118 | Information Disclosure | Devlet Destekli Aktör | Yüksek |
| **ISO-02** | "EVExchange" Röle Saldırısı ile Enerji Hırsızlığı | CPO Geliri, Kullanıcı | ISO 15118 | Spoofing | Siber Suçlu | Yüksek |
| **OCPP-03** | Dinamik Fiyatlandırmayı İstismar Etmek İçin "Zaman Kaydırmalı" MeterValues Saldırısı | CPO Geliri | OCPP 1.6 | Tampering | Fırsatçı Saldırgan | Orta |
| **PKI-01** | Sahte Araç Kontrat Sertifikaları Düzenlemek İçin eMSP Alt-CA'sının Ele Geçirilmesi | Güven Altyapısı | ISO 15118 | Spoofing | Organize Suç Grubu | Kritik |
| **DATA-01** | CSMS Web Uygulaması Zafiyeti ile Bilgi İfşası | Kullanıcı PII/Finansal Verileri | HTTP/S | Information Disclosure | Siber Suçlu | Yüksek |
| **DOS-01** | Hatalı OCPP SetChargingProfile Komutları ile "Uykucu Şarj Cihazı" Saldırısı | Hizmet Sürekliliği | OCPP 1.6 | Denial of Service | Siber Suçlu | Orta |
| **DOS-02** | PLC Sinyal Bozma (Jamming) ile CCS İletişiminin Kablosuz Olarak Kesintiye Uğratılması | Hizmet Sürekliliği | ISO 15118 (PLC) | Denial of Service | Fırsatçı Saldırgan | Yüksek |
| **NET-01** | Bir CPO Ağının DNS Ele Geçirilmesi (Hijacking) | Tüm Şarj Ağı | DNS, OCPP | Denial of Service | Organize Suç Grubu | Kritik |
| **PHYS-01** | Dahili Ağ Anahtarına Kötü Niyetli Donanım Kurmak İçin Fiziksel Kurcalama | Ağ Güvenliği | Ethernet | Elevation of Privilege | İç Tehdit | Yüksek |
| **RANSOM-01** | CSMS Zafiyeti Üzerinden Koordineli Fidye Yazılımı Saldırısı | Tüm Şarj Ağı | OCPP 1.6 | Denial of Service | Organize Suç Grubu | Kritik |
| **V2G-01** | Şebeke Frekansını Bozmak İçin Koordineli Filo Deşarjı | Elektrik Şebekesi | V2G (ISO 15118-20) | Tampering | Devlet Destekli Aktör | Kritik |
| **V2G-02** | Faz Desenkronizasyonu ile Kötü Niyetli Enerji Enjeksiyonu | Şebeke Donanımı | V2G (ISO 15118-20) | Tampering | Devlet Destekli Aktör | Kritik |
| **V2G-03** | Enerji Piyasası Tahminlerini Manipüle Etmek İçin Sahte Veri Enjeksiyonu Saldırısı | Enerji Piyasası | V2G, OCPP | Tampering | Gelişmiş Kalıcı Tehdit (APT) | Yüksek |
| **V2G-04** | Hızlı ve Değişken Şarj/Deşarj Komutları ile "Şebeke Titremesi" Saldırısı | Şebeke Stabilitesi | V2G (ISO 15118-20) | Tampering | Gelişmiş Kalıcı Tehdit (APT) | Yüksek |
| **V2G-05** | Toplayıcı (Aggregator) Kontrollerini Atlamak İçin ISO 15118-20 V2G İletişiminin İstismarı | Şebeke Kontrolü | V2G (ISO 15118-20) | Elevation of Privilege | Siber Suçlu | Yüksek |

## Bölüm 1: Çekirdek OCPP-CANbus Köprüsünün İstismarı

Bu bölüm, tek bir şarj istasyonu içindeki Bilgi Teknolojileri (IT) ve Operasyonel Teknolojiler (OT) alanları arasındaki temel etkileşimden kaynaklanan zafiyetlere odaklanmaktadır. Bu senaryolar, EV şarj ekipmanlarına yönelik "klasik" siber-fiziksel saldırıları temsil eder ve bu saldırıların temelinde, CP Ana Denetleyicisi olarak adlandırılan "köprü" bileşeninin doğrulama yapmadan duyduğu güven yatar.1 Bu bileşen, TLS ile korunan bir oturumdan gelen ve sözdizimsel olarak doğru olan herhangi bir OCPP komutunun meşru olduğunu ve güvenli bir şekilde bir CAN komutuna çevrilebileceğini varsayar. Bu bölümde incelenen senaryoların tamamı, bu hatalı güven varsayımını farklı yöntemlerle istismar etmektedir. Saldırganların her iki protokolü de kırmasına gerek yoktur; güven zincirindeki tek bir halkayı (genellikle CSMS'i taklit ederek) kırmaları yeterlidir ve sistemin kendi mantığı, kötü niyetli talimatı güven sınırının ötesine, fiziksel dünyaya sadakatle yayacaktır.

### OCPP-01: Kalıcı CAN Enjektörü Oluşturmak İçin Güvenli Olmayan Firmware Manipülasyonu

Bu senaryo, 1'daki Tablo 1'de belirtilen firmware zafiyetleri konseptini genişleterek, bir şarj istasyonunu uzaktan kontrol edilebilen bir CAN-bus saldırı aracına dönüştürmeyi hedefler.

* **Saldırı Akışı:**
  1. Bir saldırgan, bir CSMS platformundaki bir zafiyeti (örneğin, zayıf kimlik bilgileri veya bir web uygulama açığı) istismar ederek, bir şarj istasyonu filosuna kötü niyetli bir firmware güncellemesi gönderme yetkisi elde eder.
  2. Saldırgan, meşru bir üretici güncellemesi gibi görünen, ancak içinde bir arka kapı (backdoor) barındıran bir firmware paketi hazırlar. Bu paketi, CSMS'in UpdateFirmware OCPP komutunu kullanarak hedef şarj istasyonlarına gönderir.
  3. Hedef şarj istasyonlarının önyükleyicisi (bootloader), gelen firmware'in kriptografik imzasını düzgün bir şekilde doğrulamadığı için (veya imza doğrulama mekanizması hiç olmadığı için), kötü niyetli yazılımı kabul eder ve kurar.1
  4. Yeni firmware, şarj istasyonunun normal işlevlerini sürdürürken, aynı zamanda saldırganın kontrolünde olan özel, belgelenmemiş bir OCPP mesajını dinleyen bir arka kapı içerir.
  5. Saldırgan, bu özel mesaj aracılığıyla şarj istasyonunun ana denetleyicisine doğrudan CAN çerçeveleri gönderme komutu verebilir. Örneğin, saldırgan {"vendorSpecificCommand": "sendCan", "canId": "0x18FEF100", "payload": "0102030405060708"} gibi bir mesaj göndererek, istasyonun CAN-bus'ına istediği herhangi bir veriyi enjekte edebilir.
* **Etki:** Bu saldırı, saldırgana şarj istasyonunun donanımı üzerinde kalıcı ve düşük seviyeli bir kontrol sağlar. Saldırgan, standart OCPP komut mantığını tamamen atlayarak, güç elektroniği, röleler veya bağlı olan aracın BMS'i ile doğrudan iletişim kurabilir. Şarj istasyonu, artık sadece bir kurban değil, aynı zamanda daha karmaşık saldırılar için bir sıçrama tahtası haline gelir.

### OCPP-02: Uzaktan Log Kurcalama ile İnkar (Repudiation) Saldırısı

Bu senaryo, STRIDE modelindeki "İnkar" (Repudiation) kategorisini ele alır ve sofistike bir saldırganın, yüksek etkili bir saldırı gerçekleştirdikten sonra adli soruşturmayı nasıl engelleyebileceğini gösterir.1

* **Saldırı Akışı:**
  1. Bir saldırgan, T-02 senaryosundaki gibi bir aracı aşırı şarj etmek veya V2G-01'deki gibi şebekeye zarar vermek amacıyla bir saldırı gerçekleştirir.
  2. Saldırının hemen ardından, saldırgan ele geçirdiği CSMS yönetici hesabını kullanarak hedef CP'ye bir dizi SetVariables OCPP komutu gönderir. Bu komutlarla, LoggingVerbosity veya LogUploadInterval gibi yapılandırma anahtarlarını değiştirerek loglamayı en aza indirir veya tamamen devre dışı bırakır.
  3. Daha sonra, saldırgan GetLog komutunu kullanarak mevcut teşhis loglarını kendi sistemine çeker. Bu log dosyası içinde, saldırıyı gösteren (örneğin, tehlikeli SetChargingProfile komutunun alındığına dair) tüm satırları siler.
  4. Son olarak, saldırgan CP'nin teşhis betiklerinde (diagnostic scripts) bulunan bir komut enjeksiyonu zafiyetini veya belgelenmemiş bir dosya yükleme özelliğini kullanarak, temizlenmiş log dosyasını şarj istasyonuna geri yükler ve orijinal, suçlayıcı log dosyasının üzerine yazar.
* **Etki:** Bu saldırı, adli bilişim (forensics) sürecini sabote eder. Yetersiz loglama ve dijital imza eksikliği nedeniyle, saldırının gerçekleştiğini veya kaynağını kanıtlamak imkansız hale gelir.1 Saldırgan, eylemini inkar edebilir ve CPO, ne olduğunu veya sistemlerinin nasıl ele geçirildiğini asla tam olarak anlayamaz. Bu, gelecekteki benzer saldırılara karşı savunma geliştirme yeteneğini de baltalar.

### CAN-01: Sensör Arızasını Taklit Etmek ve Acil Durdurmayı Tetiklemek İçin Hassas CAN Enjeksiyonu

Bu saldırı, D-01 senaryosundaki gürültülü "bus-off" saldırısının aksine, şarj istasyonunun iç mantığını hedef alan gizli ve hassas bir hizmet reddi saldırısıdır. CAN-bus'ın doğası gereği kimlik doğrulama veya mesaj bütünlüğü mekanizmalarından yoksun olması bu saldırıyı mümkün kılar.1

* **Saldırı Akışı:**
  1. Bir iç tehdit (örneğin, kötü niyetli bir bakım teknisyeni) veya fiziksel erişim sağlayan bir saldırgan, şarj istasyonunun kasasını açarak CAN-bus hattına (CAN-H ve CAN-L pinleri) bir CAN enjeksiyon cihazı (örneğin, bir CANtact veya Raspberry Pi ile CAN kalkanı) bağlar.
  2. Saldırgan, ilk olarak pasif bir şekilde CAN-bus trafiğini dinleyerek (reconnaissance) güç elektroniği modülündeki sıcaklık sensörüne ait olan CAN ID'sini tespit eder. Örneğin, bu ID'nin 0x4A2 olduğunu belirler.
  3. Saldırgan, daha sonra bu ID'yi kullanarak sahte CAN çerçeveleri enjekte etmeye başlar. Bu çerçevelerin veri yükü (payload), kademeli olarak artan ve gerçekçi olmayan sıcaklık değerleri içerir (örneğin, 70°C, 85°C, 100°C).
  4. CP Ana Denetleyicisi, bu sahte sensör verilerini alır ve donanımın gerçekten aşırı ısındığına inanır. Kendi kendini koruma mantığı gereği, denetleyici şarj işlemini derhal durdurur ve bir "acil durum" hatası (fault state) tetikler.
* **Etki:** Bu, hedeflenmiş ve gizli bir Hizmet Reddi (Denial of Service) saldırısıdır. Sistem loglarında saldırı, bir siber olay olarak değil, bir donanım arızası olarak görünür. Bu durum, CPO'nun gereksiz ve maliyetli bakım teknisyeni ziyaretleri yapmasına neden olur. Saldırgan cihaz sökülmediği sürece, istasyon her şarj denemesinde aynı "arıza" ile karşılaşarak hizmet dışı kalmaya devam eder.

### CAN-02: Sahte Şarj Kayıtları Oluşturmak İçin CAN Tekrar Saldırısı ile "Hayalet EV" Saldırısı

Bu senaryo, ana denetleyicinin alt sistemlere (özellikle akıllı sayaca) duyduğu güveni istismar eden yenilikçi bir dolandırıcılık yöntemidir. Amaç enerji çalmak değil, CPO'nun promosyon veya sadakat programlarını kötüye kullanmaktır.

* **Saldırı Akışı:**
  1. Kötü niyetli bir EV sahibi, aracının CAN ağ geçidini (gateway) modifiye eder veya şarj fişine bağlanan özel bir cihaz kullanır.
  2. Bu kullanıcı, meşru bir şarj seansının başlangıcındaki CAN-bus iletişim dizisini (bir aracın bağlandığını, şarj talep ettiğini ve akıllı sayacın enerji akışını raporladığını gösteren CAN çerçevelerini) kaydeder.
  3. Daha sonra, saldırgan *araç bağlı değilken* cihazını bir şarj istasyonuna bağlar.
  4. Cihaz, önceden kaydedilmiş CAN çerçevelerini CAN-bus üzerine tekrar oynatır (replay attack). Bu çerçeveler, CP Ana Denetleyicisine bir aracın bağlı olduğunu ve şarj olduğunu düşündürür. Akıllı sayaçtan gelmesi beklenen enerji tüketim verilerini taklit eden çerçeveler de bu tekrarın bir parçasıdır.
  5. Ana denetleyici, bu sahte verilere dayanarak bir şarj seansının gerçekleştiğini varsayar ve CSMS'e periyodik olarak MeterValues mesajları gönderir.
* **Etki:** Finansal dolandırıcılık. Bu saldırı, CPO'ların sunduğu "ilk 30 dakika ücretsiz şarj" gibi promosyonları veya "her şarj seansı için puan kazan" gibi sadakat programlarını istismar etmek için kullanılır. Saldırgan, hiç enerji tüketmeden yüzlerce sahte şarj seansı oluşturarak haksız kazanç elde edebilir. Ayrıca, bu sahte veriler CPO'nun kullanım istatistiklerini kirleterek gelecekteki altyapı planlaması için yanıltıcı bilgilere yol açar.

### LOGIC-01: OCPP-CAN Çeviri Mantığında Yarış Durumu (Race Condition) İstismarı

Bu senaryo, "köprü" bileşeninin kendisindeki bir yazılım mantığı hatasını hedef alan daha sofistike bir saldırıdır. Donanım veya protokollerin kendisinden ziyade, bu ikisi arasındaki çeviri katmanının zayıf kodlanmasını istismar eder.

* **Saldırı Akışı:**
  1. Bir CSMS üzerinde kontrol sahibi olan veya bir Man-in-the-Middle (MitM) pozisyonunda bulunan bir saldırgan, hedef şarj istasyonuna çok hızlı bir şekilde birbiriyle çelişen OCPP komutları gönderir.
  2. Örneğin, saldırgan bir RemoteStartTransaction komutu gönderir. Bundan sadece birkaç milisaniye sonra bir RemoteStopTransaction komutu ve hemen ardından tekrar bir RemoteStartTransaction komutu gönderir.
  3. Düzgün bir durum yönetimi (state management) veya kilitleme (locking) mekanizmasına sahip olmayan, kötü yazılmış bir denetleyici firmware'i, bu komutları sıralı olarak işleyemeyebilir.
  4. Örneğin, denetleyici ilk Start komutunu alıp "röleyi kapat" CAN komutunu gönderebilir. Ancak bu komutun fiziksel olarak uygulanmasını beklemeden veya kendi iç durumunu "Şarj Ediyor" olarak güncellemeden, Stop komutunu işleyebilir. Bu noktada mantıksal durumu "Durduruldu" olarak güncellerken, röle kontrol ECU'su hala ilk komutu işlemektedir. Ardından gelen ikinci Start komutu ise tamamen göz ardı edilebilir veya bir hataya neden olabilir.
* **Etki:** Bu saldırı, şarj istasyonunun mantıksal durumu (OCPP katmanında bilinen) ile fiziksel durumu (CAN-bus katmanında gerçek olan) arasında bir desynchronizasyon yaratır. Bu durum, öngörülemeyen davranışlara yol açabilir. En olası sonuç, faturalandırma mantıksal duruma bağlıysa, röleler kapalıyken ve araç enerji çekerken sistemin şarjı durmuş olarak görmesi ve bu sayede enerji hırsızlığına olanak tanımasıdır. Daha kötü bir senaryoda, bu durum denetleyicinin çökmesine veya kilitlenmesine neden olarak bir hizmet reddi saldırısına yol açar ve cihazın yeniden başlatılmasını gerektirir.1

## Bölüm 2: Kimlik Doğrulama, Faturalandırma ve Veri Bütünlüğüne Yönelik Saldırılar

Bu bölüm, temel OCPP-CAN köprüsünün ötesine geçerek, ekosistemin iş ve veri katmanlarına yönelik daha karmaşık saldırıları ele almaktadır. ISO 15118 "Tak ve Şarj Et" standardının getirdiği yeni zafiyetlere odaklanarak, finansal dolandırıcılık, gizlilik ihlali ve kimlik yönetimi başarısızlıklarını inceler. Bu standardın getirdiği otomatik, sertifika tabanlı kimlik doğrulama, saldırı yüzeyini basit fiziksel token (RFID kart) kopyalamadan, çok daha soyut ve karmaşık olan Açık Anahtar Altyapısı (Public Key Infrastructure - PKI) yönetimi ve protokol seviyesindeki gizlilik sızıntılarına kaydırmıştır.2 Saldırganların artık bir kartı kopyalamak için fiziksel olarak orada bulunmalarına gerek yoktur; bunun yerine, güven altyapısının kendisine uzaktan saldırabilir veya tek bir ücretsiz şarj seansından çok daha değerli olan meta verileri pasif olarak toplayabilirler. Bu, tehdit manzarasının olgunlaştığını ve ATM kartı kopyalamadan büyük ölçekli finansal veri ihlallerine geçişe benzer bir evrimi temsil ettiğini göstermektedir. Saldırganlar için "yatırımın geri dönüşü", artık fiziksel otoparkta değil, siber uzaydadır; tek bir RFID kartını kopyalamaktansa, binlerce sahte kontrat sertifikası düzenlemek için bir e-Mobilite Hizmet Sağlayıcısının (eMSP) alt-CA'sını ele geçirmek çok daha kârlıdır.10

### ISO-01: EV Parmak İzi ve CPO'lar Arası Kullanıcı Takibi

Bu senaryo, 11'de A2 saldırısı olarak tanımlanan ve ISO 15118'in getirdiği bir gizlilik zafiyetini istismar eden bir saldırıdır.

* **Saldırı Akışı:**
  1. Kötü niyetli bir CPO veya geniş ağ görünürlüğüne sahip bir devlet aktörü, ISO 15118 oturum anlaşması sırasında EV'lerden gelen ilk TLS el sıkışma (handshake) parametrelerini pasif olarak toplar. Bu parametreler, aracın desteklediği şifreleme takımlarını (cipher suites), TLS uzantılarını ve diğer konfigürasyon detaylarını içerir.
  2. Saldırgan, JA3/JARM gibi araçları kullanarak, bu parametrelerden her bir EV için benzersiz bir "parmak izi" oluşturur.11 Bu parmak izi, aracın işletim sistemi ve TLS kütüphanesinin spesifik uygulamasına dayanır ve genellikle araç modeli ve yazılım sürümüyle ilişkilidir.
  3. Aracın kontrat sertifikası (ve dolayısıyla eMAID'si) zamanla değişse bile, bu temel TLS parmak izi büyük olasılıkla aynı kalacaktır.
  4. Saldırgan, farklı şarj istasyonları ve hatta farklı CPO'lar arasında bu parmak izlerini zaman içinde ilişkilendirerek, belirli bir aracın (ve dolayısıyla kullanıcısının) hareketlerini, şarj alışkanlıklarını ve günlük rutinlerini detaylı bir şekilde profiller.
* **Etki:** Bu, ciddi bir gizlilik ihlalidir. Saldırı, bir kullanıcının anonimliğini ortadan kaldırarak, onun nerede yaşadığı, nerede çalıştığı ve ne zaman seyahat ettiği gibi hassas bilgilerin ortaya çıkmasına neden olur. Bu bilgiler, yüksek profilli kişilerin fiziksel takibi, hedefli reklamcılık veya diğer kötü niyetli faaliyetler için kullanılabilir.

### ISO-02: "EVExchange" Röle Saldırısı ile Enerji Hırsızlığı

Bu senaryo, 16'da teorik olarak açıklanan ve ISO 15118'in güvenli olduğu varsayılan kimlik doğrulama sürecini fiziksel olarak atlatan pratik bir saldırıdır.

* **Saldırı Akışı:**
  1. Bu saldırı iki kişi ve özel donanım gerektirir. Saldırgan A ("sülük"), kimliği doğrulanmamış EV'sini bir şarj istasyonuna park eder. Saldırgan B ("hayalet"), meşru bir kurbanın ISO 15118 Plug & Charge seansını başlattığı başka bir şarj istasyonunun yakınına konumlanır.
  2. Kurban aracını şarj cihazına taktığında, Saldırgan B, kurbanın aracı ile şarj cihazı arasındaki tüm iletişimi (güvenli TLS el sıkışması ve sertifika değişimi dahil) yakalayan bir cihaz kullanır.
  3. Bu iletişim akışı, ayrı bir kablosuz kanal (örneğin, 4G veya Wi-Fi) üzerinden gerçek zamanlı olarak Saldırgan A'nın ekipmanına aktarılır.
  4. Saldırgan A'nın ekipmanı, bu rölelenmiş verileri kendi şarj cihazına iletir. Şarj cihazı, aslında kurbanın aracıyla konuştuğunu düşünür.
  5. Kimlik doğrulama süreci tamamlandığında, kurbanın aracı, Saldırgan A'nın bulunduğu şarj cihazını başarıyla doğrulamış olur. Sonuç olarak, Saldırgan A'nın aracı enerji almaya başlar, ancak fatura kurbanın hesabına kesilir.
* **Etki:** Bu, tespit edilmesi son derece zor olan doğrudan bir enerji hırsızlığı ve finansal dolandırıcılıktır. CSMS ve CPO'nun bakış açısından, her şey kriptografik olarak geçerli ve güvenli bir oturum gibi görünür. Saldırı, protokolün kendisini kırmak yerine, iletişim kanalını fiziksel olarak uzatarak güven mekanizmasını aldatır.

### OCPP-03: Dinamik Fiyatlandırmayı İstismar Etmek İçin "Zaman Kaydırmalı" MeterValues Saldırısı

Bu, 1'daki T-01 senaryosunun daha sofistike bir versiyonudur ve saldırganın sadece fatura tutarını düşürmekle kalmayıp, aynı zamanda CPO'nun dinamik fiyatlandırma stratejisini kendi lehine kullanmasını sağlar.

* **Saldırı Akışı:**
  1. Bir saldırgan, CP ile CSMS arasında bir MitM saldırısı gerçekleştirir. Bu, zayıf TLS uygulamaları veya güvenli olmayan ağlar üzerinden yapılabilir.1
  2. Saldırgan, elektrik tarifesinin en yüksek olduğu bir "yoğun saat" (peak pricing) diliminde aracını şarj etmeye başlar.
  3. Şarj sırasında CP, düzenli aralıklarla tüketilen enerji miktarını içeren MeterValues mesajlarını CSMS'e gönderir.
  4. Saldırgan, bu giden mesajları yakalar ve basitçe değerini düşürmek yerine, onları bir arabellekte (buffer) biriktirir.
  5. Elektrik tarifesi, fiyatın daha düşük olduğu bir "yoğun olmayan saat" (off-peak) dilimine geçtiğinde, saldırgan biriktirdiği tüm MeterValues mesajlarını, muhtemelen zaman damgalarını da manipüle ederek, CSMS'e toplu olarak gönderir.
* **Etki:** Finansal dolandırıcılık. CSMS, enerji tüketiminin tamamının ucuz tarife diliminde gerçekleştiğini varsayarak faturalandırma yapar. Sonuç olarak, kullanıcı pahalı olan yoğun saat enerjisini tüketir, ancak ucuz olan yoğun olmayan saat tarifesi üzerinden faturalandırılır. Bu, CPO için doğrudan gelir kaybına neden olur.

### PKI-01: Sahte Araç Kontrat Sertifikaları Düzenlemek İçin eMSP Alt-CA'sının Ele Geçirilmesi

Bu senaryo, ISO 15118'in karmaşık PKI güven zincirinin en zayıf halkasını hedefler.10 Bu, tüm Plug & Charge ekosisteminin temelini tehdit eden, yüksek etkili bir saldırıdır.

* **Saldırı Akışı:**
  1. Sofistike bir siber suç grubu, genellikle bir otomotiv OEM'i veya büyük bir CPO'dan daha az güvenlik bütçesine ve uzmanlığına sahip olan bir e-Mobilite Hizmet Sağlayıcısını (eMSP) hedefler.
  2. Saldırganlar, eMSP'nin ağına sızarak, şarj işlemlerini yetkilendiren kontrat sertifikalarını (contract certificates) düzenlemekten sorumlu olan alt Sertifika Otoritesinin (sub-CA) özel anahtarını (private key) ele geçirir.
  3. Bu özel anahtarla, saldırganlar artık kriptografik olarak tamamen geçerli, sınırsız sayıda sahte kontrat sertifikası üretebilir.
  4. Bu sahte sertifikaları, "ömür boyu ücretsiz şarj" vaadiyle karanlık ağda (dark web) satabilir veya büyük ölçekli bir V2G saldırısı için bir araç filosunu yetkilendirmek amacıyla kullanabilirler.
* **Etki:** Kimlik doğrulama modelinin sistem genelinde çökmesi. Sahte ancak kriptografik olarak geçerli olan bu kontratları kabul etmek zorunda kalan CPO'lar için devasa finansal kayıplar. Bu saldırı, kullanıcıların ve operatörlerin Plug & Charge sistemine olan güvenini tamamen yok edebilir ve tüm ekosistemin sürdürülebilirliğini tehlikeye atabilir.

### DATA-01: CSMS Web Uygulaması Zafiyeti ile Bilgi İfşası

Bu senaryo, EV ekosistemine uygulanan klasik bir web uygulaması saldırısını temsil eder ve 1 (Tablo 1) ile 3'te belirtilen tehditlere dayanır.

* **Saldırı Akışı:**
  1. Bir saldırgan, bir CPO tarafından kullanılan CSMS'in web portalında bir SQL Enjeksiyonu (SQL Injection) veya Siteler Arası Betik Çalıştırma (Cross-Site Scripting - XSS) zafiyeti keşfeder.1
  2. Bu zafiyeti istismar ederek, saldırgan arka uç veritabanına erişim sağlar.
  3. Veritabanı, kayıtlı her kullanıcı için Kişisel Tanımlayıcı Bilgiler (Personally Identifiable Information - PII) içerir. Bu bilgiler arasında isimler, adresler, fatura bilgileri, kredi kartı verileri ve detaylı şarj geçmişleri (konum, zaman, süre) bulunur.3
  4. Saldırgan, bu veritabanının tamamını kendi sistemine kopyalar.
* **Etki:** Büyük ölçekli bir veri ihlali. Bu durum, CPO için GDPR gibi düzenlemeler kapsamında ağır para cezalarına, müşteri güveninin kaybına ve ciddi itibar zedelenmesine yol açar. Ayrıca, çalınan veriler, kullanıcıların ne zaman evde olmadıklarını (araçlarını başka bir yerde şarj ederken) analiz ederek ev soygunları düzenlemek veya şantaj gibi daha hedefli saldırılar için kullanılabilir.

## Bölüm 3: Hizmet Reddi ve Altyapının Kesintiye Uğratılması

Bu bölümdeki saldırıların birincil amacı hırsızlık veya veri sızıntısı değil, şarj altyapısını kullanılamaz hale getirmektir. Bu saldırılar, tek bir şarj cihazını etkileyen gizli mantık saldırılarından, bütün bir bölgenin şarj kapasitesini devre dışı bırakabilen büyük ölçekli ağ saldırılarına kadar çeşitlilik gösterir. EV ekosistemindeki bir hizmet reddi (Denial of Service - DoS) saldırısının gerçek dünya etkisi, geleneksel bir IT DoS saldırısına kıyasla orantısız derecede yüksektir. Erişilemeyen bir web sitesi bir rahatsızlık iken, erişilemeyen bir şarj ağı sürücüleri yolda mahsur bırakabilir, lojistik ve ulaşım filolarını aksatabilir ve EV'lerin benimsenmesine yönelik kamu güvenini sarsabilir. Dolayısıyla, bir DoS saldırısının "maliyeti" sadece kaybedilen gelir değil, aynı zamanda kritik bir altyapı geçişine duyulan kamu güveninin kaybıdır. Bu durum, teknik bir saldırıyı toplumsal ve politik sonuçları olan stratejik bir soruna dönüştürür.

### DOS-01: Hatalı OCPP SetChargingProfile Komutları ile "Uykucu Şarj Cihazı" Saldırısı

Bu, gürültülü ağ trafiği oluşturmaktan kaçınan, bunun yerine şarj istasyonunun kendi mantığını ona karşı kullanan gizli bir DoS saldırısıdır.

* **Saldırı Akışı:**
  1. Bir saldırgan, ele geçirilmiş bir CSMS hesabı veya MitM pozisyonu aracılığıyla bir şarj istasyonuna SetChargingProfile OCPP komutu gönderir.
  2. Bu komutun içindeki chargingSchedule nesnesinde, limit değerini 0 Amper olarak ve duration değerini ise son derece uzun bir süre (örneğin, 315,360,000 saniye, yani 10 yıl) olarak ayarlar.
  3. Gelen profilin parametrelerini (örneğin, sürenin makul olup olmadığını) düzgün bir şekilde doğrulamayan bir şarj istasyonu, bu profili kabul eder ve uygular.
  4. Şarj istasyonu ağda çevrimiçi kalır, CSMS'e düzenli olarak Heartbeat mesajları gönderir ve sistem monitörlerinde "sağlıklı" ve "kullanılabilir" (Available) olarak görünür. Ancak, herhangi bir araç bağlandığında, şarj limiti kalıcı olarak sıfır olduğu için asla güç sağlamaz.
* **Etki:** Bu, teşhis edilmesi zor olan, gizli ve kalıcı bir DoS saldırısıdır. Tipik ağ veya donanım arızası alarmlarını tetiklemediği için, operatörler sorunun ne olduğunu anlamakta zorlanabilir. Tek çözüm, CSMS'in bir ClearChargingProfile komutu göndermesidir, ancak saldırgan bu komutu periyodik olarak yeniden göndererek istasyonu hizmet dışı tutmaya devam edebilir.

### DOS-02: PLC Sinyal Bozma (Jamming) ile CCS İletişiminin Kablosuz Olarak Kesintiye Uğratılması

Bu senaryo, 6'te açıklanan saldırıya ve 13'da belirtildiği gibi Birleşik Şarj Sistemi (Combined Charging System - CCS) standardında Güç Hattı İletişimi (Power Line Communication - PLC) kullanımına dayanmaktadır.

* **Saldırı Akışı:**
  1. CCS standardı, ISO 15118 gibi üst düzey iletişim protokolleri için şarj kablosunun kontrol pilotu pini üzerinden PLC (özellikle HomePlug Green PHY) teknolojisini kullanır.13
  2. Bir saldırgan, bir yazılım tanımlı radyo (Software-Defined Radio - SDR) veya özel bir PLC cihazı kullanarak, HPGP tarafından kullanılan spesifik frekans bandında (2 MHz ile 28 MHz arası) radyo frekansı (RF) gürültüsü üretir.
  3. Saldırgan, bu gürültüyü yakındaki bir konumdan (örneğin, kurbanın yanına park edilmiş bir arabadan veya yakındaki bir binadan) yayınlayarak, şarj kablosu üzerindeki PLC iletişimini bozar.
  4. Bu parazit, EV ile şarj cihazının bir oturum anlaşması yapmasını engeller. Hatta halihazırda devam eden bir şarj seansını bile aniden sonlandırabilir.
* **Etki:** Bu, fiziksel temas gerektirmeyen, kablosuz ve etki alanına sahip bir DoS saldırısıdır. Tek bir saldırgan, bir otoparktaki veya servis alanındaki birden fazla DC hızlı şarj cihazını aynı anda devre dışı bırakabilir. Saldırının kaynağının tespiti zordur ve altyapıya kalıcı bir hasar vermediği için tekrarlanması kolaydır.6

### NET-01: Bir CPO Ağının DNS Ele Geçirilmesi (Hijacking)

Bu, tekil istasyonları değil, bir operatörün tüm ağını hedef alan büyük ölçekli bir altyapı saldırısıdır.

* **Saldırı Akışı:**
  1. Bir saldırgan, bir CPO'nun alan adı kayıt kuruluşu (domain registrar) hesabını ele geçirir (örneğin, oltalama veya kimlik bilgisi hırsızlığı yoluyla).
  2. Saldırgan, CPO'nun CSMS uç noktasına ait DNS A kayıtlarını (örneğin, ocpp.cpo-ornek.com) kendi kontrolündeki bir IP adresine (bir sinkhole sunucusuna) yönlendirir.
  3. Ağdaki şarj istasyonları yeniden başlatıldıkça veya DNS önbellekleri sona erdikçe, meşru CSMS yerine saldırganın sunucusuna bağlanmaya çalışırlar.
  4. Saldırganın sunucusu bağlantı taleplerini reddeder veya yanıtsız bırakır. Sonuç olarak, CPO'nun tüm şarj ağı kademeli olarak çevrimdışı olur.
* **Etki:** Bir CPO için ülke çapında veya küresel ölçekte katastrofik bir kesinti. CPO, filosu üzerindeki tüm izleme ve kontrol yeteneklerini kaybeder. Binlerce kullanıcı hizmet alamaz ve şirketin geliri ile itibarı ciddi şekilde zarar görür.

### PHYS-01: Dahili Ağ Anahtarına Kötü Niyetli Donanım Kurmak İçin Fiziksel Kurcalama

Bu senaryo, 14'deki gerçek dünya değerlendirmesinde tespit edilen tehdidin pratik bir uygulamasıdır ve fiziksel güvenliğin siber güvenliğin temel bir parçası olduğunu vurgular.

* **Saldırı Akışı:**
  1. Birçok şarj sahası, şarj cihazlarını internete bağlayan ağ anahtarları (switches) gibi ekipmanları kilitsiz veya zayıf güvenlikli dolaplarda barındırır.14
  2. Bir saldırgan, bu dolaplardan birine kısa süreli fiziksel erişim sağlar.
  3. Saldırgan, anahtarın boş bir portuna küçük, kötü niyetli bir cihaz (örneğin, bir ağ dinleyicisi olarak yapılandırılmış bir Raspberry Pi veya bir "throwable LAN tap") takar.
  4. Bu cihaz, saldırgana yerel ağa kalıcı bir uzaktan giriş noktası sağlar. Bu sayede saldırgan, güvenlik duvarlarını (firewalls) atlayabilir, şarj cihazları ile CSMS arasındaki tüm trafiği dinleyebilir (MitM saldırıları) veya doğrudan şarj cihazlarına yönelik saldırılar başlatabilir.
* **Etki:** Saha seviyesindeki ağ güvenliğinin tamamen tehlikeye atılması. Bu, saldırgana daha sonraki ve daha yıkıcı saldırılar için bir köprübaşı sağlar. Örneğin, bu erişim noktasını kullanarak ağdaki tüm şarj cihazlarına fidye yazılımı yayabilir veya V2G saldırıları için bir botnet oluşturabilirler.

### RANSOM-01: CSMS Zafiyeti Üzerinden Koordineli Fidye Yazılımı Saldırısı

Bu senaryo, geleneksel kurumsal fidye yazılımı saldırı modelini EV şarj ekosistemine uygular ve en kötü durum senaryolarından birini temsil eder.

* **Saldırı Akışı:**
  1. Bir siber suç grubu, yaygın olarak kullanılan bir CSMS yazılım platformunda sıfır gün (zero-day) bir zafiyet keşfeder.
  2. Bu zafiyeti kullanarak, CSMS'ten bağlı tüm şarj cihazlarına yayılan bir solucan (worm) geliştirirler.
  3. Şarj cihazlarına bulaşan yük (payload), dosyaları şifrelemek yerine, cihazın ekranını bir fidye notu gösterecek şekilde değiştirmek için bir SetVariables OCPP komutu kullanır. Ardından, güç elektroniğini devre dışı bırakmak için bir CAN komutu gönderir.
  4. Eş zamanlı olarak, CSMS'in web arayüzü de bir fidye talebiyle kilitlenir.
  5. CPO, hem merkezi yönetim sistemine hem de tüm şarj istasyonu filosuna erişimini kaybeder. Fidye ödenene kadar tüm operasyonları durur.
* **Etki:** Bir CPO'nun operasyonlarının tamamen durması. Kesintiden ve potansiyel fidye ödemesinden kaynaklanan devasa finansal kayıp. Müşteri verilerinin de ele geçirilme riski ve şirket itibarının geri döndürülemez şekilde zarar görmesi.

## Bölüm 4: Şebeke Seviyesinde İstikrarsızlaştırma ve V2G'nin Silah Olarak Kullanılması

Bu son ve en kritik bölüm, EV şarj altyapısının elektrik şebekesinin kendisine saldırmak için bir silah olarak kullanıldığı senaryoları açıklamaktadır. Bu senaryolar, Araçtan Şebekeye (V2G) teknolojisinin çift yönlü enerji akışından yararlanır ve çok sayıda EV'nin koordineli kontrolünü gerektirir. Bu tehditler, bireysel cihazların güvenliğinin ihlal edilmesinden ulusal güvenlik sorununa dönüşen en yüksek etki seviyesini temsil eder. V2G teknolojisi, elektrik şebekesinin tehdit modelini temelden değiştirmektedir. Elektrik tüketicileri ile üreticileri arasındaki geleneksel, iyi tanımlanmış sınırı ortadan kaldırır. Milyonlarca mobil, internete bağlı ve çift yönlü güç kaynağı (EV'ler) yaratarak, V2G şebekeyi etkili bir şekilde "sınırsızlaştırır" ve kritik şebeke stabilizasyon fonksiyonlarını tüm sistemin en az güvenli uç noktalarına dağıtır.5 Başarılı bir saldırı sadece bir elektrik kesintisi değil, geleceğin akıllı şebekesinin temel mimarisinin kendisine karşı döndürülebileceğinin bir kanıtıdır. Şebekenin istikrarı artık milyonlarca tüketiciye ait, karmaşık yazılımlar çalıştıran, halka açık ağlar üzerinden bağlanan ve OEM'ler, CPO'lar ve eMSP'lerden oluşan parçalanmış bir ekosistem tarafından yönetilen cihazların güvenliğine bağlıdır. Saldırı yüzeyi artık birkaç düzine enerji santrali değil, ülkedeki V2G özellikli her arabadır.

### V2G-01: Şebeke Frekansını Bozmak İçin Koordineli Filo Deşarjı

Bu, 5 ve 7'de açıklanan kanonik V2G saldırısıdır ve bir siber saldırının geniş alanlı bir fiziksel etkiye nasıl dönüşebileceğini gösterir.

* **Saldırı Akışı:**
  1. Büyük bir CSMS'i ele geçirmiş veya kötü amaçlı yazılımla (Senaryo OCPP-01 aracılığıyla) enfekte edilmiş bir EV filosuna sahip olan devlet destekli bir aktör, on binlerce V2G özellikli araç üzerinde kontrol sağlar.
  2. Şebeke talebinin yüksek olduğu bir anda (örneğin, sıcak bir yaz gününde akşam saatlerinde), saldırgan kontrolündeki tüm araçlara aynı anda bataryalarını maksimum güçte şebekeye deşarj etme komutu verir.
  3. Bu komut, ISO 15118-20 V2G iletişim protokolü üzerinden araçlara iletilir.
* **Etki:** Beklenmedik, anlık ve devasa bir güç üretimi dalgası. Bu durum, şebeke frekansının (nominal olarak 50 Hz veya 60 Hz) tehlikeli bir şekilde yükselmesine neden olur. Şebeke koruma sistemleri (röleler), bu anormalliği algılayarak ekipmanı korumak için şebekenin bazı kısımlarını otomatik olarak ayırmaya başlar. Bu, zincirleme arızalara (cascading failures) ve potansiyel olarak bölgesel bir elektrik kesintisine (blackout) yol açar.6

### V2G-02: Faz Desenkronizasyonu ile Kötü Niyetli Enerji Enjeksiyonu

Bu, basit bir güç boşaltmasından daha teknik ve yıkıcı bir şebeke saldırısıdır ve doğrudan fiziksel hasar vermeyi amaçlar.

* **Saldırı Akışı:**
  1. Saldırgan, coğrafi olarak yoğunlaşmış bir alandaki (örneğin, büyük bir elektrikli otobüs deposu) çok sayıda V2G şarj cihazının kontrolünü ele geçirir.
  2. Saldırgan, şarj cihazlarının invertörlerinin firmware'ini manipüle eder. Normalde, bir invertör şebekeye güç verirken, ürettiği AC gücünün sinüs dalgasını şebekenin sinüs dalgasıyla mükemmel bir şekilde senkronize (in-phase) eder.
  3. Saldırgan, filoya deşarj komutu verdiğinde, manipüle edilmiş firmware, invertörlere şebekenin kendi sinüs dalgasından hafifçe faz dışı (out-of-phase) AC gücü enjekte etme talimatı verir.
* **Etki:** Bu, yerel şebeke ekipmanı için son derece tehlikelidir. Faz uyuşmazlığı, yerel transformatörler ve diğer dağıtım donanımları üzerinde muazzam bir stres yaratır. Bu stres, ekipmanın aşırı ısınmasına, arızalanmasına ve en kötü durumda fiziksel olarak patlamasına neden olabilir. Bu, altyapıya kalıcı ve maliyetli fiziksel hasar vermek için tasarlanmış kinetik bir saldırıdır.

### V2G-03: Enerji Piyasası Tahminlerini Manipüle Etmek İçin Sahte Veri Enjeksiyonu Saldırısı

Bu saldırı, şebekeyi yöneten ekonomik ve kontrol sistemlerini hedef alır ve 17 ile 8'te bahsedilen Sahte Veri Enjeksiyonu Saldırılarının (False Data Injection Attacks - FDIA) bir V2G versiyonudur.

* **Saldırı Akışı:**
  1. V2G sistemleri, ne zaman şarj veya deşarj yapacaklarına karar vermek için piyasa sinyallerine ve yük tahminlerine güvenir.
  2. Bir saldırgan, bir toplayıcı (aggregator - bir V2G araç filosunu yöneten şirket) ile şebeke operatörü arasındaki iletişim kanalını ele geçirir.
  3. Saldırgan, şebeke operatörüne sahte telemetri verileri enjekte eder. Bu veriler, toplayıcının filosunun gerçekte olduğundan çok daha fazla (veya daha az) enerji kapasitesine sahip olduğunu gösterir.
  4. Şebeke operatörü, bu yanlış verilere dayanarak operasyonel kararlar alır. Örneğin, kritik bir anda var olmayan bir "hayalet" güç rezervini kullanmaya çalışabilir veya toplayıcıya sağlayamadığı bir hizmet için ödeme yapabilir.
* **Etki:** Enerji piyasasının istikrarsızlaşması. Yanlış şebeke operatörü kararları, şebeke dengesizliklerine yol açabilir. Ayrıca, bu durum büyük ölçekli finansal dolandırıcılığa neden olur ve V2G'nin bir şebeke dengeleme aracı olarak güvenilirliğini baltalar.

### V2G-04: Hızlı ve Değişken Şarj/Deşarj Komutları ile "Şebeke Titremesi" Saldırısı

Bu, 6'te açıklanan saldırının bir varyantıdır ve şebekenin otomatik kontrol sistemlerini karıştırmak için tasarlanmıştır.

* **Saldırı Akışı:**
  1. Saldırgan, bir V2G araç filosunu ele geçirir.
  2. Sürekli bir şarj veya deşarj komutu vermek yerine, araçlara maksimum şarj ve maksimum deşarj arasında hızla geçiş yapmaları için komutlar gönderir (örneğin, her saniyede bir durum değiştirerek).
  3. Bu, yerel şebeke üzerinde hızlı ve şiddetli güç talebi salınımları yaratır.
* **Etki:** Bu "titreme" (jitter), şebekenin bu kadar hızlı yük değişimlerine yanıt vermek için tasarlanmamış olan otomatik düzenleme ve kontrol sistemlerini karıştırabilir. Voltaj ve frekans istikrarsızlığına neden olabilir, transformatörlerdeki kademe değiştiriciler gibi mekanik bileşenleri yıpratabilir ve potansiyel olarak koruyucu röleleri tetikleyerek yerel elektrik kesintilerine yol açabilir.

### V2G-05: Toplayıcı (Aggregator) Kontrollerini Atlamak İçin ISO 15118-20 V2G İletişiminin İstismarı

Bu saldırı, komuta zincirini kırmak için protokolün kendisinden yararlanır ve V2G kontrol hiyerarşisindeki bir zafiyeti hedefler.

* **Saldırı Akışı:**
  1. Tipik bir V2G kurulumunda, şebeke operatörü toplayıcı ile, toplayıcı CSMS ile, CSMS ise OCPP ve ISO 15118 aracılığıyla EV ile iletişim kurar. Bu uzun bir komuta zinciridir.
  2. Bir saldırgan, EV'nin bilgi-eğlence (infotainment) sistemi üzerinde çalışan ve aracın V2G kontrol ECU'sunu doğrudan manipüle edebilen kötü niyetli bir uygulama geliştirir.
  3. Toplayıcı, bu uzun zincir üzerinden EV'ye deşarjı *durdurması* için meşru bir sinyal gönderdiğinde, kötü niyetli uygulama bu komutu aracın içinde yakalar ve V2G kontrol ECU'suna deşarja *devam etmesi* talimatını verir.
  4. Araç, meşru komutu görmezden gelerek şebekeye güç basmaya devam eder.
* **Etki:** Şebeke operatörü ve toplayıcı, V2G kaynaklarının bir kısmı üzerindeki kontrolünü kaybeder. Bu, V2G'nin bir şebeke stabilizasyon aracı olarak güvenilirliğini temelden sarsar. Mevcut bir şebeke acil durumunu daha da kötüleştirebilecek "haydut" EV'lerin ortaya çıkmasına neden olabilir. Bu senaryo, güvenliğin sadece iletişim kanalında değil, aynı zamanda komutların uygulandığı son noktada da sağlanması gerektiğini göstermektedir.

#### Alıntılanan çalışmalar

1. EV Şarj İstasyonu Siber Güvenlik Anomali Senaryoları.pdf
2. Securing the Charge: Hidden Risks in ISO 15118 - VicOne, erişim tarihi Ekim 30, 2025, <https://cdn.vicone.com/files/research-papers/EN/vicone_securing_the_charge_hidden_risks_in_iso15118.pdf>
3. POWERING PROGRESS IN EV CHARGING - Addressing Cybersecurity Risks, Ensuring Compliance and Driving Adoption - DigiCert, erişim tarihi Ekim 30, 2025, <https://www.digicert.com/content/dam/digicert/pdfs/whitepaper/ev-charging-whitepaper-en.pdf>
4. arxiv.org, erişim tarihi Ekim 30, 2025, <https://arxiv.org/abs/2509.13393#:~:text=A%20critical%20analysis%20of%20cybersecurity,%2C%20and%20quantum%2Dresistant%20cryptography.>
5. Why Is Cybersecurity Crucial for V2G Systems? - Energy → Sustainability Directory, erişim tarihi Ekim 30, 2025, <https://energy.sustainability-directory.com/question/why-is-cybersecurity-crucial-for-v2g-systems/>
6. The Power Grid Must Be Protected, But Are EV Charging Stations Secure?, erişim tarihi Ekim 30, 2025, <https://upstream.auto/blog/are-ev-charging-stations-secure/>
7. Local Power Grids at Risk – An Experimental and Simulation-based Analysis of Attacks on Vehicle-To-Grid Communication - ResearchGate, erişim tarihi Ekim 30, 2025, <https://www.researchgate.net/publication/366017368_Local_Power_Grids_at_Risk_-_An_Experimental_and_Simulation-based_Analysis_of_Attacks_on_Vehicle-To-Grid_Communication>
8. Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review - arXiv, erişim tarihi Ekim 30, 2025, <https://arxiv.org/html/2503.15730v1>
9. ISO15118 Plug&Charge vs. Traditional EV Charging: Key Differences - iocharger, erişim tarihi Ekim 30, 2025, <https://www.iocharger.com/iso15118-plugcharge-vs-traditional-ev-charging/>
10. Self-Sovereign Identity for Electric Vehicle Charging - arXiv, erişim tarihi Ekim 30, 2025, <https://arxiv.org/html/2403.06632v1>
11. Enhancing Anonymity for Electric Vehicles in the ISO 15118 Plug-and-Charge - SciTePress, erişim tarihi Ekim 30, 2025, <https://www.scitepress.org/Papers/2025/135717/135717.pdf>
12. EV and Charging | Plug&Charge. V2G Security | ISO 15118 | AUTOCRYPT, erişim tarihi Ekim 30, 2025, <https://autocrypt.io/solutions/ev-charging/>
13. Current Affairs: A Security Measurement Study of CCS EV Charging Deployments - arXiv, erişim tarihi Ekim 30, 2025, <https://arxiv.org/html/2404.06635v2>
14. Cybersecurity Lessons Learned from Vehicle to Grid Engagement - OSTI.GOV, erişim tarihi Ekim 30, 2025, <https://www.osti.gov/servlets/purl/2429955>
15. [Literature Review] Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review, erişim tarihi Ekim 30, 2025, <https://www.themoonlight.io/en/review/cybersecurity-in-vehicle-to-grid-v2g-systems-a-systematic-review>
16. Security Weaknesses in ISO 15118-Based CCS2 Charging - ResearchGate, erişim tarihi Ekim 30, 2025, <https://www.researchgate.net/publication/396531741_Security_Weaknesses_in_ISO_15118-Based_CCS2_Charging>
17. Cybersecurity in Vehicle-to-Grid (V2G) Systems: A Systematic Review - ResearchGate, erişim tarihi Ekim 30, 2025, <https://www.researchgate.net/publication/390038852_Cybersecurity_in_Vehicle-to-Grid_V2G_Systems_A_Systematic_Review>