ANOMALİ SENARYO RAPORU: Koordineli "Siren" Saldırısı: V2G Protokol Manipülasyonu Yoluyla Mikroşebeke Destabilizasyonu

Ders: Bilgi Sistemleri Güvenliği (BSG)

Hazırlayan : Mehmet Sait DÜNDAR

Tarih: 02.11.2025

1.0 YÖNETİCİ ÖZETİ

Bu rapor, Elektrikli Araç (EV) şarj altyapılarına yönelik, özellikle Araçtan Şebekeye (Vehicle-to-Grid - V2G) teknolojisini hedef alan, yüksek etkili ve siber-fiziksel bir anomali senaryosunu analiz etmektedir. "Siren Saldırısı" olarak adlandırılan bu senaryo, incelenen mevcut proje konuları arasında yer almayan, özgün bir konsepti ele almaktadır. Mevcut senaryolar daha çok faturalama manipülasyonu ("Fatura Yönlendirme Hilesi"), oturum tutarsızlıkları ("Anomali_Raporu_Yetim_Seans") veya tekil kapasite sahtekarlığı ("Kapasite Sahtekarlığı (Phantom SoC Report)") gibi konulara odaklanırken, bu rapor doğrudan enerji şebekesinin fiziksel kararlılığını hedef alan kolektif bir sabotaj eylemini incelemektedir.

Saldırı, birden fazla V2G özellikli EV'nin bir botnet aracılığıyla ele geçirilmesine dayanır. Bu "hayalet filo", bir Mikroşebeke (MG) içerisindeki Enerji Yönetim Sistemi'ne (EMS) toplu olarak sahte (spoofed) V2G deşarj kapasitesi raporlar. EMS, bu "Sanal Enerji Santrali"ne (Virtual Power Plant - VPP) güvenerek şebeke dengeleme operasyonlarını (örn. talep-yanıt) planlar. Saldırgan, önceden belirlenmiş kritik bir anda, tüm botnete eş zamanlı ve maksimum güçte deşarj (şebekeye enerji basma) komutu vererek şebekede ani bir aşırı gerilim ve frekans çöküşü (destabilizasyon) yaratır.

Bu senaryonun STRIDE analizi, ana tehdit vektörlerini **Spoofing** (sahte kapasite raporlama) ve **Tampering** (EMS'nin operasyonel şebeke modelini manipüle etme) olarak tanımlamaktadır. Nihai etki ise **Denial of Service (DoS)** olarak ortaya çıkmaktadır; ancak bu DoS, dijital bir hizmet kesintisinden ziyade, akademik literatürde de belirtilen (TC-9) "büyük ölçekte enerjinin geri basılması" (revert power on a massive scale) sonucu oluşan fiziksel bir çöküş (blackout) ve ekipman hasarı (I-1, I-2) ile sonuçlanır.

Saldırının temel zafiyetleri, protokol düzeyinde (ISO 15118 ve OCPP'nin EV'nin *fiziksel kapasitesini* değil, sadece *kriptografik kimliğini* doğrulaması) ve mimari düzeyde (EMS'nin toplu verilere "körlemesine" güvenmesi) yatmaktadır. Bu "körlemesine güven" durumu, modern güvenlik paradigmaları tarafından eleştirilen ve "Sıfır Güven Mimarisi"nin (Zero Trust Architecture) tam tersi olan bir yaklaşımdır.

Tespit ve önleme yöntemleri, şebeke düzeyinde (PMU verisi ile OCPP verisinin çapraz doğrulanması) ve araç düzeyinde (Telematik ve Batarya Yönetim Sistemi arasında Güvenilir Yürütme Ortamı - TEE - kullanımı) gibi çok katmanlı bir "Derinlemesine Savunma" (Defense-in-Depth) stratejisi gerektirmektedir.

2.0 SENARYO TANIMI, AMACI VE KAPSAMI

2.1 Anomali Tanımı: "Siren" Saldırısı

Anomali, siber ve fiziksel alanlar arasındaki temel bir tutarsızlık üzerine inşa edilmiştir. Bu tutarsızlık, dijital olarak raporlanan bir *taahhüt* ile fiziksel dünyadaki *kabiliyet* arasındaki farktan kaynaklanır:

- **Normal Operasyon:** Bir EV'nin şebekeye V2G yoluyla X MWh enerji sunma *taahhüdü* (dijital sinyal), o EV'nin fiziksel olarak X MWh enerji sunma *kabiliyetine* (fiziksel durum) dayanır. Sistem, bu ikisinin eşit olduğunu varsayar.
- **Anomalili Durum (Saldırı):** Binlerce EV'den oluşan bir botnet, kolektif olarak Y MWh enerji sunma *taahhüdünde* bulunur (dijital sinyal), ancak bu sırada gerçek fiziksel kabiliyetleri 0'dır (veya bu taahhütten tamamen bağımsızdır). Saldırı anında ise, bu dijital taahhüdün tam tersi bir zamanda (örn. şebeke talebi düşükken), Z MWh'lik ani ve koordineli bir deşarj (beklenmedik fiziksel eylem) gerçekleştirirler.

Saldırıya "Siren" adının verilmesi, mitolojideki sirenlerin denizcileri cezbedici sesleriyle (sahte vaatler) tuzağa çekip felakete sürüklemesine bir göndermedir. Saldırgan botnet, EMS'yi yüksek kapasiteli bir VPP vaadiyle (cezbedici ses) "kandırır" ve şebekeyi bu hayali kapasiteye bağımlı hale getirir, ardından koordineli deşarj ile şebekeyi "kayalara çarptırır" (fiziksel çöküş).

2.2 Saldırının Amacı ve Motivasyonu

Saldırının motivasyonu, basit bir enerji hırsızlığından çok daha yıkıcıdır:

- **Birincil Amaç (Fiziksel Sabotaj):** Ana amaç, kritik altyapıya yönelik fiziksel bir sabotaj eylemidir. Literatürde açıkça belirtildiği gibi, "farklı şarj istasyonları üzerinde senkronize saldırı vektörleri" kullanarak "büyük ölçekte enerjiyi geri basmak" (TC-9) ve "önemli yerel çöküşlere veya elektrikli ekipman hasarına" (I-1, I-2) neden olmaktır. Hedef, mikroşebeke transformatörleri, koruma röleleri ve şarj istasyonlarının güç elektroniği devreleridir.

- **İkincil Amaç (Finansal Manipülasyon):** Gelişmiş enerji piyasalarında, şebeke frekansını stabilize etmek için anlık kapasite (Frekans Tepki Piyasaları - FCR) alınıp satılır. Saldırgan, şebekede kasıtlı olarak bir dengesizlik yaratarak ve bu dalgalanma üzerine önceden finansal pozisyon alarak (örn. açığa satış) büyük bir finansal kazanç elde edebilir.

2.3 Benzersizlik ve Kapsam

Bu senaryo, listesindeki diğer anomalilerden temelden farklıdır. Örneğin, Grup 5 tarafından listelenen "Kapasite Sahtekarlığı (Phantom SoC Report)" , muhtemelen *daha hızlı* veya *daha ucuz* şarj alabilmek için (örn. şarj önceliği) aracın mevcut şarj durumunu (SoC) düşük göstermeye odaklanan, bireysel ve bencil bir saldırıdır.

"Siren" saldırısı ise tam tersine;

1. **Kolektif bir eylemdir** (botnet vs. tekil araç).
2. **Kapasiteyi yüksek gösterir** (V2G deşarj kapasitesi).
3. **Hedefi şebekenin kendisidir** (bireysel kazanç değil, sistemsel çöküş).

Bu rapor, belgesindeki Şekil 1'de gösterilen tam entegre mimariyi, yani EV, Şarj İstasyonu (CS), Merkezi Yönetim Sistemi (CSMS), Enerji Yönetim Sistemi (EMS) ve Mikroşebeke (Microgrid) arasındaki tüm siber-fiziksel etkileşimleri kapsamaktadır.

3.0 SİBER-FİZİKSEL ARKA PLAN VE NORMAL OPERASYON

Saldırının nasıl çalıştığını anlamak için, öncelikle V2G özellikli bir mikroşebekenin "Sanal Enerji Santrali" (VPP) olarak nasıl normal bir şekilde çalıştığını anlamak zorunludur.

3.1 Ekosistem Bileşenleri ve İlişkileri

- **Microgrid (MG) ve EMS:** Mikroşebeke, Dağıtılmış Enerji Kaynaklarını (DERs - örn. güneş panelleri) ve yükleri (EV'ler dahil) yöneten otonom bir yerel şebekedir. EMS (Enerji Yönetim Sistemi), bu şebekenin "beynidir". 'de belirtildiği gibi, "şebeke kararlılığını, güvenilirliğini ve verimliliğini" sağlamak için "gelişmiş kontrol algoritmalarını" çalıştırır.

- **CSMS ve OCPP:** CSMS (Şarj İstasyonu Yönetim Sistemi), sahadaki tüm şarj istasyonlarını (CS) yöneten operasyonel merkezdir. EMS, CSMS ile entegre çalışır. EMS'nin şebeke dengeleme (Akıllı Şarj) kararları, 'deki Tablo 9'da (UC K01: Set charging profile) görüldüğü gibi, CSMS üzerinden OCPP `SetChargingProfile` mesajları olarak CS'lere iletilir.

- **CS ve ISO 15118:** CS, EV ile gelişmiş V2G iletişimi için ISO 15118 protokolünü kullanır. Bu protokol, EV'nin batarya durumunu (SoC), ne kadar enerji alabileceğini veya daha önemlisi, ne kadar enerji *verebileceğini* (deşarj kapasitesi) CS'ye bildirmesini ve müzakere etmesini sağlar.

3.2 Normal Operasyon: V2G Olarak "Sanal Enerji Santrali" (VPP)

Normal ve meşru bir V2G operasyonu şu adımları izler:

1. **Bağlantı ve Müzakere:** Bir V2G özellikli EV, bir CS'ye bağlanır. ISO 15118 protokolü aracılığıyla kimliğini (örn. "Plug & Charge" sertifikası ile) ve V2G kabiliyetini, mevcut SoC seviyesini ve batarya sağlığını (SoH) CS'ye bildirir.
2. **Veri Toplama (Aggregation):** CS, bu bilgiyi (örn. 50 kWh deşarj kapasitesi mevcut) bir OCPP `TransactionEvent` veya `MeterValues` mesajı ile CSMS'e iletir.

3. **VPP Oluşturma:** CSMS, yönetimindeki (örn. 1000 adet) V2G özellikli EV'den gelen bu verileri toplar (aggregate) ve EMS'ye "Şu anda şebekeye 50 MWh (1000 arac¸ ×50 kWh) kapasite sunabilirim" şeklinde bir VPP bilgisi sağlar.
4. **Talep-Yanıt (Demand-Response):** EMS, şebeke talebi aniden arttığında (örn. bir bulutun güneş tarlasının üzerini kapatmasıyla güneş enerjisi üretimi aniden düştüğünde), bu 50 MWh'lik VPP'ye "devreye gir" komutu verir.
5. **Fiziksel Eylem:** Bu komut, CSMS üzerinden OCPP `SetChargingProfile` (negatif güç/akım değerleri içeren, örn. −11 kW) olarak CS'lere iletilir. CS, bu profili ISO 15118 üzerinden EV'ye iletir. EV'ler, şebekeye enerji vererek (deşarj olarak) ani talep pikini dengeler.

Bu mimarinin verimliliği, tek bir kritik varsayıma dayanır: *Güven*. EMS, CSMS'in VPP olarak raporladığı 50 MWh kapasitenin *gerçek* ve *kullanılabilir* olduğuna güvenmek zorundadır. Bu "körlemesine güven" (blind trust) modeli, 'da bahsedilen "Sıfır Güven Mimarisi"nin (Zero Trust Architecture) tam tersidir ve Siren Saldırısı'nın temel mimari zafiyetini oluşturur.

4.0 HEDEF VARLIKLAR VE SALDIRI YÜZEYİ

Saldırı, ekosistemin tamamını kapsayan hem siber hem de fiziksel varlıkları hedefler.

4.1 Siber Varlıklar

- **EMS Karar Destek Modülü:** Şebeke dengeleme algoritmaları ve VPP kapasite tahmin motoru (saldırının mantıksal hedefi).
- **CSMS Veritabanı:** Toplu kapasite verilerinin ve `ChargingProfile` şablonlarının saklandığı yer.
- **Protokol Kanalları:** OCPP (CS-CSMS) ve ISO 15118 (EV-CS) iletişim kanalları.
- **EV Telematik Kontrol Ünitesi (TCU):** 'daki (Miller & Valasek) çalışmasında da gösterildiği gibi, aracın dış dünya (4G/5G) ile iletişim kuran ve araç içi CAN-Bus ağına bağlı olan birimi. Bu, botnet oluşturmak için birincil giriş noktasıdır (saldırı yüzeyi).

4.2 Fiziksel Varlıklar

- **Mikroşebeke Altyapısı:** Yerel transformatörler, frekans regülatörleri ve koruma röleleri (saldırının fiziksel hedefi).
- **CS Güç Elektroniği:** EV'nin DC batarya gücünü şebekenin AC gücüne dönüştüren V2G çift yönlü inverterleri (saldırının fiziksel hedefi).

4.3 Siber-Fiziksel Köprü

Saldırının "köprüsü", Şarj İstasyonunun (CS) ana kontrolcüsüdür. Bu kontrolcü, siber ve fiziksel dünyalar arasında bir tercüman görevi görür.

1. **Siber Alan (Giriş):** CSMS'ten dijital bir OCPP komutu (`SetChargingProfile`) alır.

• • **Fiziksel Alan (Çıkış):** Bu komutu, EV'nin Batarya Yönetim Sistemine (BMS) ve güç inverterlerine ileten fiziksel bir CAN-Bus (veya ISO 15118) komutuna çevirir (örn. `CAN ID 0x210, payload [profile_id, max_current]`).

Siren Saldırısı, bu köprünün her iki tarafını da manipüle eder: (1) EMS'nin, sahte VPP verilerine dayanarak hatalı bir OCPP komutu (`SetChargingProfile`) üretmesini sağlar (Spoofing/Tampering yoluyla). (2) Daha da kötüsü, ele geçirdiği EV'nin bu komut *olmaksızın* deşarjı tetiklemesini sağlar (Botnet C2 komutası yoluyla).

5.0 İLİŞKİLİ TEMEL ZAFİYETLER

Bu sofistike saldırı, tek bir hatadan ziyade, birbiriyle ilişkili üç temel zafiyetin birleşiminden yararlanır:

5.1 Zafiyet 1: Kapasite Doğrulaması Eksikliği (Protokol Zafiyeti)

ISO 15118 ve OCPP 2.0.1, V2G için tasarlanmış olsalar da, birincil güvenlik odak noktaları *kimlik doğrulama* (Authentication) ve *faturalandırma* (Billing) doğruluğudur.

- **Doğrulanan Şey:** Bir EV, ISO 15118 "Plug & Charge" (PnC) özelliği ile kimliğini kriptografik bir sertifika kullanarak kanıtlayabilir. Sistem, "Bu araç *gerçekten* X plakalı araç mı?" sorusunu yüksek güvenilirlikle doğrular.
- **Doğrulanmayan Şey:** Sistem, "Bu araç *gerçekten* %80 SoC'ye ve deşarj için 50 kWh sağlıklı kapasiteye sahip mi?" sorusunu *fiziksel olarak doğrulamaz*. Bu bilgiye *güvenir*.
- **Zafiyetin Sömürülmesi:** 'te ("Hareket Halinde Şarj") sunulan senaryonun gösterdiği gibi, bir aracın CAN-Bus verileri (hız, vites durumu) içeriden manipüle edilebiliyorsa, aynı mantıkla BMS'in SoC ve SoH (State of Health) verileri de manipüle edilebilir. EV'nin TCU'su (Telematik) veya BMS'i ele geçirilmişse, ISO 15118 üzerinden "güvenli" bir kanaldan *sahte* fiziksel durum verileri göndermesi engellenemez.

5.2 Zafiyet 2: Merkezi Kör Güven Modeli (Mimari Zafiyet)

, modern güvenlik paradigmaları olarak "Sıfır Güven Mimarisi"ni (Zero Trust Architecture) güçlü bir şekilde vurgulamaktadır. VPP mimarisi, doğası gereği bu paradigmanın tam zıttıdır.

- **Zafiyet:** EMS, binlerce dağınık ve potansiyel olarak güvenilmeyen uç noktadan (EV'ler) gelen verileri *toplayan* (aggregate) tek bir "güvenilir" varlığa (CSMS) *körlemesine güvenir*.
- **Sömürülmesi:** Bu toplulaştırma (aggregation), bireysel anomalileri gizler. Tek bir EV'nin sahte kapasite bildirmesi istatistiksel bir "aykırı değer" (outlier) olarak tespit edilebilir. Ancak, 'teki "Veri Zehirleme" (Data Poisoning) konseptinde olduğu gibi, binlerce EV'nin *hafifçe* sahte kapasite bildirmesi veya kolektif olarak hareket etmesi, EMS'nin "normal" operasyonel modelini kaydırır ve bu durum "yeni normal" olarak kabul edilerek tespit edilemez hale gelir.

5.3 Zafiyet 3: Güvensiz Araç Telematik ve Araç İçi Ağlar (Uç Nokta Zafiyeti)

Saldırının "Aşama 1"inin (Botnet oluşturma) fizibilitesi, bu zafiyete dayanır.

- **Zafiyet:** , araç içi ağların (CAN-Bus) "tasarım gereği güvenlik mekanizmalarından yoksun" olduğunu ve şifreleme, kimlik doğrulama gibi temel önlemleri içermediğini belirtir.

- **Sömürülmesi:** 'daki (Miller & Valasek) ve (Koscher vd.) gibi temel akademik çalışmalar, telematik (TCU) ve bilgi-eğlence (infotainment) sistemlerindeki zafiyetler üzerinden hücresel ağ (4G) aracılığıyla CAN-Bus'a uzaktan erişimin ve fren, motor gibi kritik fonksiyonların manipüle edilebildiğinin kanıtıdır. V2G deşarj inverterini kontrol etmek, bu vektör üzerinden benzer şekilde mümkündür. ("Hareket Halinde Şarj"), bu tür bir CAN-Bus sahteciliğinin pratik bir örneğini sunmaktadır.

6.0 SALDIRI SENARYOSUNUN STRIDE ANALİZİ

Bu bölümde, 'de (Tablo 1) tanımlanan ve diğer öğrenci raporlarında uygulanan STRIDE tehdit modelleme metodolojisi, "Siren Saldırısı" senaryosuna uygulanacaktır.

Spoofing (Kimlik Sahteciliği)

- **Açıklama:** Saldırgan, V2G kabiliyetli bir EV'nin kimliğine bürünür *veya* daha önemlisi, meşru bir EV'nin Batarya Yönetim Sistemi'nin (BMS) kimliğine bürünerek onun *kapasite* (SoC, SoH) ve *durum* verilerini taklit eder.
- **Vektör:** Ele geçirilmiş EV'nin TCU'su , BMS'den geliyormuş gibi sahte CAN mesajları oluşturur. Bu sahte fiziksel durum verileri, ISO 15118 ve OCPP protokolleri üzerinden EMS'ye kadar "meşru" veri olarak akar.

- **Etki:** EMS'nin şebeke modelinin, var olmayan "Hayali Kapasite" (Phantom Capacity) üzerine inşa edilmesine neden olur.

Tampering (Veri Manipülasyonu)

- **Açıklama:** Bu, saldırının "Güven Oluşturma" (Aşama 3) aşamasıdır. Saldırgan, EMS'nin şebeke operasyonlarına ilişkin *algısını* ve *karar verme modelini* aktif olarak manipüle eder.
- **Vektör:** 'teki "Yavaş Faz" (Data Poisoning) konseptinin bir varyasyonu olarak, botnet, EMS'nin "güvenini kazanmak" için küçük, "başarılı" ve kontrollü V2G işlemleri gerçekleştirir. Bu işlemler, EMS'nin VPP algoritmasını bu "güvenilir" kaynağa daha fazla operasyonel ağırlık vermesi için "eğitir".

- **Etki:** EMS'nin VPP botnetine olan operasyonel bağımlılığını artırır ve gerçek, sağlıklı enerji kaynaklarının (örn. gaz türbinleri) bekleme moduna alınmasına veya daha az kullanılmasına yol açar.

Repudiation (İnkâr)

- **Açıklama:** Saldırı sonrasında, saldırganın eylemlerini veya saldırıya katılan botların eylemlerini inkâr etmesi.

- **Vektör:** Fiziksel çöküş gerçekleştikten sonra, botnet'teki her bir EV, "CS'den hiçbir zaman deşarj komutu almadım" (OCPP/ISO 15118 loglarını silme) veya "Yerel bir voltaj dalgalanması algıladım ve güvenlik protokolü gereği kendimi kapattım" (sahte hata logları oluşturma) iddiasında bulunabilir.
- **Etki:** Kök neden analizi (RCA) ve adli bilişim (forensics) süreçlerini son derece karmaşık hale getirir ve saldırının kaynağını gizler.

Information Disclosure (Bilgi İfşası)

- **Açıklama:** Saldırının "Keşif" (Aşama 1) aşaması. Saldırgan, saldırıyı planlamak ve zamanlamak için kritik operasyonel verileri toplar.
- **Vektör:** Botnet'teki EV'ler, şarja bağlandıklarında pasif dinleyiciler olarak hareket eder. EMS'nin VPP'yi ne zaman (hangi talep/fiyat eşiğinde) devreye aldığını, şebekenin normal frekans ve voltaj aralıklarını, ataletini (inertia) ve tepki sürelerini (response times) öğrenirler.
- **Etki:** Saldırının *zamanlamasının* (Aşama 4) maksimum fiziksel hasarı verecek (örn. şebekenin en kırılgan olduğu, en az atalete sahip olduğu bir an) şekilde ayarlanmasını sağlar.

Denial of Service (Hizmet Reddi)

- **Açıklama:** Saldırının nihai hedefi ve fiziksel yükü (payload).
- **Vektör:** (p. 18, TC-9) tarafından açıkça tanımlanan "büyük ölçekte enerjinin geri basılması" (revert power on a massive scale). Saldırgan, C2 sunucusu aracılığıyla tüm botnet'e *aynı milisaniye içinde* (zaman senkronizasyonu ile) maksimum deşarj komutunu gönderir.

• • **Etki (Fiziksel DoS):** Şebeke frekansı (örn. 50Hz) ve voltajı, regülasyon limitlerinin (örn. ±5%) çok dışına çıkar. Koruma röleleri, transformatörler gibi pahalı ekipmanları korumak için devreyi açar (trip) ve bu da 'de (I-1) belirtilen "aşırı yük/karartma" (overload/blackout) ile sonuçlanır.

Elevation of Privilege (Yetki Yükseltme)

- **Açıklama:** Saldırganın, düşük ayrıcalıklı bir konumdan (tek bir araç sahibi) yüksek ayrıcalıklı bir etkiye (şebeke operatörü) ulaşması.
- **Vektör:** Normalde bir EV kullanıcısı, sadece kendi aracının şarjını kontrol etme yetkisine (User-level privilege) sahiptir.
- **Etki:** Saldırgan, binlerce hesabı koordine ederek, fiili olarak bir *şebeke operatörü* (Grid Operator-level privilege) yetkisine yükselir ve tüm bir mikroşebekenin "fişini çekme" kabiliyetini elde eder.

7.0 SALDIRI ADIMLARI (ADIM ADİM SİMÜLASYON)

"Siren Saldırısı", üç ana aşamada gerçekleştirilen, sabır gerektiren ve metodik bir operasyondur.

Aşama 1: Keşif ve Silahlanma (EV Botnet Oluşturma)

1. **Hedef Belirleme:** Saldırgan, yüksek V2G adaptasyon oranına sahip bir mikroşebeke bölgesini (örn. belirli bir kargo şirketinin EV filosunun bulunduğu veya bir araç paylaşım servisinin yoğun olarak kullanıldığı bir lojistik merkezi) hedefler.
2. **Sızma:** 'da atıfta bulunulan telematik (TCU) zafiyetlerini (örn. 4G/5G modemindeki veya bilgi-eğlence sistemindeki bir uzaktan kod çalıştırma - RCE zafiyeti) kullanarak, araçların ağına sızar.

• • **Kalıcılık ve Yükseltme:** TCU'ya bir rootkit yerleştirir. Buradan, ve 'te açıklandığı gibi, BMS ve güç elektroniği inverterleri ile konuşan güvenilmeyen CAN-Bus ağına tam yazma/okuma erişimi sağlar.

3. **Komuta-Kontrol (C2):** Ele geçirilen tüm araçlar (botlar), gizli bir C2 sunucusuna (örn. Tor üzerinden veya DNS tünelleme ile) bağlanarak sessizce komut beklemeye başlar.

Aşama 2: Güven Oluşturma ("Siren" Aşaması - Kavramsal Zehirleme)

1. **Pasif Dinleme (Information Disclosure):** Botnet, EMS'nin VPP taleplerini (OCPP `ChargingProfile` mesajları olarak gelir) birkaç hafta boyunca dinler. EMS'nin güven tröstlerini, talep desenlerini ve fiyat eşiklerini öğrenir.
2. **Aktif Sahtecilik (Spoofing):** Botnet, C2 komutuyla, EMS'ye kolektif olarak "100 MWh kapasite sunmaya hazırız" (gerçek kapasiteleri 0 veya 10 MWh olabilir) şeklinde sahte ISO 15118/OCPP durum verileri göndermeye başlar.
3. **Güven "Eğitimi" (Tampering):** EMS, bu 100 MWh'lik "sanal" kapasiteyi "görür". EMS'nin otomatik dengeleme sistemi, bu 100 MWh'lik "güvenilir" ve "ucuz" kaynağa güvenerek, diğer (daha pahalı veya kirli) kaynakların (örn. gaz jeneratörü) bekleme süresini artırır veya devreye alınmasını geciktirir. 'teki "Model Kayması" konsepti burada şebeke düzeyinde gerçekleşir: Şebeke artık *operasyonel olarak* bu hayali kapasiteye bağımlı hale gelir.

Aşama 3: Destabilizasyon (Koordineli Fiziksel Saldırı)

1. **Tetikleme Anı:** Saldırgan, şebekenin en kırılgan olduğu (örn. talep düşük, şebeke ataleti düşük olduğu için frekans oynamalarına karşı hassas olan gece yarısı) veya en yüksek hasarı vereceği (örn. yüksek talep anında, EMS'nin VPP'ye en çok güvendiği anda) bir zamanı seçer.
2. **Saldırı Komutu:** C2 sunucusu, tüm botnet'e tek bir, zaman senkronize komut gönderir: `EXECUTE_DISCHARGE_MAX_NOW`.
3. **Fiziksel Eylem (DoS):** Binlerce EV, aynı anda, EMS'den bir `SetChargingProfile` komutu *gelmese bile*, Aşama 1'de elde edilen CAN-Bus erişimi üzerinden V2G inverterlerine doğrudan komut vererek şebekeye maksimum güçte (örn. her biri 11 kW) enerji basar.

• Sonuç : Şebekeye anlık olarak basılan +50 MWh'lik bu ani ve beklenmedik enerji, şebeke voltajını ve frekansını felaket düzeyde sapmasına (transient) neden olur. Koruma röleleri,

şebekeyi ve bağlı ekipmanları (transformatörler, vb.) korumak için tüm bölgenin enerjisini keser (blackout). 'de (I-2) belirtilen "ekipman hasarı" meydana gelir.

7.1 Alternatif Saldırı Vektörü: CSMS/EMS Kompromizesi

Bu raporda odaklanılan EV botnet (bottom-up, uç noktadan merkeze) yaklaşımı yerine, saldırgan (top-down, merkezden uç noktaya) bir yaklaşım da benimseyebilir.

Bu alternatifte, saldırgan 'de ("SSRF Zafiyeti") gösterildiği gibi, CSMS platformunun kendisine (veya EMS'ye) ait bir web zafiyetini (SSRF, SQL Injection vb.) kullanarak sunucuyu ele geçirir. Sunucu üzerinde tam kontrole sahip olan saldırgan, Aşama 1'e (botnet oluşturma) gerek duymaz. CSMS'in *meşru* özel anahtarlarını ve veritabanı erişimini kullanarak, *meşru* OCPP `SetChargingProfile` komutlarını tüm istasyonlara *aynı anda* göndererek aynı koordineli deşarjı tetikleyebilir. Bu vektör, botnet oluşturma ihtiyacını ortadan kaldırır ve çok daha hızlı gerçekleştirilebilir.

8.0 ETKİ VE RİSK ANALİZİ (DREAD MODELİ)

Bu bölümde, 'de (Tablo 12) kullanılan DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) risk değerlendirme modeli temel alınarak "Siren Saldırısı"nın riski değerlendirilecektir.

Damage (Hasar): 10/10

- **Gerekçelendirme:** Hasar, veri kaybının veya 'deki gibi faturalama sahteciliğinin çok ötesindedir. 'de (TC-9, I-1, I-2) açıkça belirtildiği gibi, saldırı doğrudan "ekipman hasarı" (yanan transformatörler, patlayan V2G inverterleri) ve "büyük ölçekli karartma" (blackout) hedefler. Bu, bir mikroşebeke için en yüksek ve geri dönülmez hasar seviyesidir.

Reproducibility (Tekrarlanabilirlik): 6/10

- **Gerekçelendirme:** Saldırının kendisi (Aşama 3 - koordineli deşarj komutu) yüksek oranda tekrarlanabilirdir. Ancak, Aşama 1 (botnet oluşturma) için 'da bahsedilen spesifik telematik zafiyetlerinin bulunması ve sömürülmesi gerekir. Bu, hedefe özel (target-specific) bir çaba gerektirir ancak imkansız değildir. Alternatif vektör kullanılırsa bu puan artar.

Exploitability (Sömürülebilirlik): 7/10

- **Gerekçelendirme:** Saldırı, çoklu protokol (TCU/CAN, ISO 15118, OCPP) ve sistem (EV, CS, CSMS, EMS) bilgisi gerektiren sofistike bir saldırıdır. *Ancak,* 'de (Tablo 7) belirtildiği gibi, mevcut altyapıların birçoğu hala zayıf güvenlik profilleri

kullanmaktadır. 'da belirtilen araç içi güvenlik açıkları da yaygındır. Bu "zayıf halkalar" sömürülebilirliği artırmaktadır.

-

Affected Users (Etkilenen Kullanıcılar): 10/10

- **Gerekçelendirme:** Saldırı, tek bir kullanıcıyı, istasyonu veya 'deki gibi tek bir grubu hedef almaz. Tüm bir mikroşebekeyi (bir yerleşim alanı, bir hastane kampüsü, bir endüstriyel bölge) etkiler ve tüm kullanıcılara yönelik tam bir hizmet reddine (blackout) neden olur.

-

Discoverability (Keşfedilebilirlik): 3/10

- **Gerekçelendirme:** Aşama 1 ve 2 (botnet oluşturma ve güven kazanma) son derece gizlidir (stealthy). 'teki gibi, yavaş ve düşük seviyeli veri manipülasyonları, şebeke gürültüsünden (normal operasyonel gürültü) ayırt edilemez. Saldırı, yalnızca Aşama 3'te (fiziksel deşarj) keşfedilir, ancak bu noktada hasar zaten verilmiş ve çok geç kalınmıştır.

Genel Risk Değerlendirmesi: KRİTİK

- **Sonuç:** Ortalama puan (7.2) yüksek olsa da, *Damage* ve *Affected Users* metriklerinin 10/10 olması, bu senaryoyu basit bir siber suçun ötesinde, ulusal güvenlik düzeyinde kritik bir altyapı tehdidi olarak konumlandırmaktadır.

9.0 TESPİT YÖNTEMLERİ (DETECTION)

Başarılı bir tespit, 'da belirtilen "Derinlemesine Savunma" (Defense in Depth) ve /'de görülen "fiziksel-dijital durum tutarlılığı" ilkelerine dayanmalıdır. Tespit, ekosistemin dört katmanında da uygulanmalıdır:

9.1 Katman 1: Şebeke Düzeyi (EMS) - Makro Anomali Tespiti

- **Yöntem:** Yüksek frekanslı, *fiziksel* şebeke verileri (örn. PMU'lardan - Phasor Measurement Units - gelen voltaj ve frekans verileri) ile CSMS'ten gelen *dijital* toplu VPP kapasite verileri arasında gerçek zamanlı çapraz tutarlılık kontrolü.
- **Kural:** `IF (CSMS_Aggregated_VPP_Capacity > X MWh) AND (PMU_Measured_Grid_Draw < Y MWh) FOR T seconds THEN ALARM (Siren_Spoofing_Detected)`
- **İçgörü:** Bu mantık, 'deki "Yetim Seans" tespit kuralı ("plug_state=false iken status=Charging ise ALARM") ile temelde aynıdır: Fiziksel durum ile dijital durum arasındaki tutarsızlığın tespiti. Buradaki fark, bu mantığın şebeke ölçeğinde (makro) uygulanmasıdır. Bu yöntem, saldırının "Aşama 2"sini (Güven Oluşturma) yakalayabilir.

9.2 Katman 2: Merkezi Sistem (CSMS) - Davranışsal Analiz

- **Yöntem:** 'teki AI/ML konseptini kullanarak, tekil EV'lerin ve filoların V2G davranış profillerini modelleme.

- **Anomali:** Normal EV'ler ve filolar, V2G'ye katılımda *istatistiksel rastgelelik* (statistical randomness) gösterir (kullanıcı davranışları, SoC seviyeleri, bağlantı süreleri farklıdır). Saldırganın botnet'i ise *mükemmel bir koordinasyon* (perfect synchronization) ve *homojen bir davranış* gösterir.
- **Kural:** `IF (Standard_Deviation(V2G_Response_Time) < Threshold) AND (Fleet_Size > N) THEN ALARM (Botnet_Behavior_Detected)`
- **İçgörü:** Binlerce aracın, farklı yerlerde, farklı batarya durumlarına sahip olmalarına rağmen, aynı anda, mükemmel bir senkronizasyonla "deşarja hazırım" demesi istatistiksel bir anormalliktir.

9.3 Katman 3: Şarj İstasyonu (CS) - Siber-Fiziksel Köprü Tespiti

- **Yöntem:** 'te açıklanan "Gateway" (Ağ Geçidi) veya "CP main controller" üzerinde akıllı güvenlik mantığı uygulama.

- **Kural:** CS kontrolcüsü, hem OCPP (CSMS'ten gelen talep) hem de ISO 15118 (EV'den gelen eylem) arasındaki güç akışını sürekli izler. `IF (EV_Deşarj_Gücü > EMS_Talep_Gücü + Tolerans) THEN ALARM (Local_Override_Attack)`
- **İçgörü:** Bu, "Aşama 3"ü (izinsiz deşarj) yakalayabilir. CS, EMS'den bir deşarj profili *almadıysa* ancak EV yine de şebekeye enerji basmaya *çalışıyorsa*, CS bu işlemi derhal (fiziksel röleyi açarak) kesmeli ve CSMS'e kritik bir alarm göndermelidir.

9.4 Katman 4: Araç İçi (EV) - Uç Nokta Tespiti

- **Yöntem:** (Tablo 1) "Güvenilir Yürütme Ortamı" (TEE) ve "Sıfır Güven" ilkelerinin araç içine uygulanması.

• • **Mimari:** Telematik Ünitesi (TCU - "güvensiz" dış dünya) ve Batarya Yönetim Sistemi (BMS - "kritik" güç kontrolü) donanımsal olarak izole edilmelidir.

• **Kural:** BMS, *sadece* kriptografik olarak imzalanmış ve TEE içinde doğrulanmış komutları kabul etmelidir. `IF (TCU_Komutu_İmzasız_Veya_Geçersiz) THEN REJECT_COMMAND`

• **İçgörü:** Bu, 'teki CAN-Bus spoofing saldırısını ve "Siren" saldırısının "Aşama 1"ini (botnet oluşturma) temelden engeller veya en azından zorlaştırır.

10.0 ÖNLEME VE AZALTMA YÖNTEMLERİ (MITIGATION)

Tespit yöntemleri saldırıyı bildirirken, önleme (prevention) ve azaltma (mitigation) yöntemleri saldırının başarılı olmasını engeller.

10.1 Protokol Düzeyinde Güçlendirme (Kısa Vade)

- **OCPP Güvenliği:** (Tablo 8) ve 'da (s. 43) belirtildiği gibi, tüm CS-CSMS iletişimi için "OCPP 2.0.1 Güvenlik Profili 3" zorunlu kılınmalıdır. Bu, sadece sunucu tarafı TLS değil, *karşılıklı TLS kimlik doğrulamasını* (mutual TLS) içerir ve CS'ler için donanım tabanlı sertifikaların (HSM) kullanılmasını gerektirir. Bu, sahte CS veya MitM saldırılarını engeller.

- **ISO 15118 Güvenliği:** "Plug & Charge" (PnC) özelliği, her EV'nin V2G işlemlerine başlamadan önce kendi kimliğini (ve ideal olarak kapasite durumunu da içeren bir "batarya sağlık sertifikası"nı) kriptografik olarak kanıtlamasını zorunlu kılmalıdır.

10.2 Mimari Düzeyde Güçlendirme (Orta Vade): Sıfır Güven Doğrulaması

- **EMS Güveni:** EMS, 'da savunulan "Sıfır Güven Mimarisi"ni benimsemelidir. EMS, CSMS'ten gelen toplu VPP kapasite raporuna "körlemesine güvenmemelidir".

- **Azaltma Yöntemi: Rastgele Örneklem ile Doğrulama (Randomized Sampling Verification):** Bu, saldırıyı önlemenin en etkili yoludur. EMS, 50 MWh'lik VPP kapasitesini şebeke dengeleme planına dahil etmeden önce, filodan rastgele seçilmiş bir alt kümeye (örn. filonun %1'i) küçük, anlık bir deşarj/şarj testi (`SetChargingProfile`) göndermelidir.
- **Sonuç:** Eğer botnet *gerçekten* var olmayan bir kapasiteyi raporluyorsa, bu test fiziksel olarak başarısız olur (EV'ler enerji basamaz). EMS, bu VPP'nin tamamını "güvenilmez" olarak işaretler ve saldırının "Aşama 2"sini (Güven Oluşturma) tamamen boşa çıkarır.

10.3 Donanım Düzeyinde Güçlendirme (Uzun Vade): Fiziksel Savunma

- **Araç İçi (EV):** (Tablo 1) "TEE" ve donanım güvenlik modüllerinin (HSM'ler) araçlarda standart hale gelmesi. Bu, TCU'nun ele geçirilmesi durumunda bile BMS'in kontrol edilememesini (veya sadece imzalı komutları çalıştırmasını) sağlar.

- **Şarj İstasyonu (CS):** 'teki "Gateway" konseptinin fiziksel olarak uygulanması. CS, EMS'den gelen OCPP `ChargingProfile` ile fiziksel olarak ölçülen deşarj gücünü milisaniye düzeyinde karşılaştıran ve sapma durumunda devreyi kesen donanımsal bir "rate limiter" veya "siber-fiziksel güvenlik duvarı" içermelidir. Bu, saldırının "Aşama 3"ünün fiziksel etkisini (DoS) büyük ölçüde sınırlar.

11.0 SONUÇ

Bu rapor, 'de listelenen standart anomalilerin dışında, benzersiz ve yüksek etkili bir siber-fiziksel anomali olan "Siren Saldırısı"nı analiz etmiştir. Bu saldırı, V2G teknolojisinin siber-fiziksel doğasını (hem bir yük hem de bir kaynak olma özelliği) nasıl bir silaha dönüştürebileceğini somut bir şekilde göstermektedir.

Saldırı, EV telematik sistemlerinin ve araç içi ağların (CAN-Bus) zafiyetlerinden başlayarak, bu zafiyetleri ISO 15118 ve OCPP protokollerini manipüle etmek için bir sıçrama tahtası olarak kullanır. Saldırının en sofistike yönü, EMS'nin operasyonel modelini 'teki "veri zehirleme" benzeri bir yöntemle "eğiterek" şebekeyi hayali bir kapasiteye bağımlı hale getirmesidir. Nihai etki, 'de (TC-9) öngörüldüğü gibi, koordineli bir fiziksel deşarj yoluyla şebekede geri dönülmez ekipman hasarı ve karartmadır.

Bu analiz, sadece protokol düzeyinde kriptografik çözümlerin (TLS gibi) tek başına yetersiz olduğunu; çünkü saldırının, *doğrulanmış* bir kanaldan *sahte içerik* (spoofed capacity) göndererek güven mekanizmasını aştığını ortaya koymuştur. Çözüm, EMS düzeyinde "Sıfır Güven" (Sıfır Güven Mimarisi) ve "Rastgele Örneklemle Doğrulama" gibi proaktif test mekanizmalarının ve araç/istasyon düzeyinde donanım tabanlı izolasyonun (TEE) zorunlu olduğu çok katmanlı bir savunma stratejisi gerektirmektedir.