Elektrikli Araç Şarj Altyapılarında Siber-Fiziksel Anomali Senaryoları: OCPP-CAN Köprüsü Üzerinden Gelişmiş Tehdit Analizi

Giriş: EV Şarj Altyapılarında Siber-Fiziksel Tehdit Yüzeyi

Elektrikli araç (EV) şarj ekosistemi, izole ve tescilli sistemlerden, Açık Şarj Noktası Protokolü (Open Charge Point Protocol - OCPP) gibi standartlar sayesinde birbirine bağlı ve birlikte çalışabilir bir ağa doğru hızla evrilmektedir.[1] Bu standardizasyon, farklı üreticilerin şarj istasyonları (Charge Point - CP) ve merkezi yönetim sistemleri (Central System Management System - CSMS) arasında sorunsuz bir iletişim sağlayarak endüstrinin büyümesini teşvik ederken, aynı zamanda siber saldırganlar için ölçeklenebilir ve homojen bir saldırı yüzeyi oluşturmaktadır.[3] Bir yanda bu karmaşık ağ iletişimi yer alırken, diğer yanda aracın kendi içindeki ve şarj istasyonunun güç elektroniği bileşenleri arasındaki iletişim, temel güvenlik mekanizmalarından yoksun olarak tasarlanmış olan Denetleyici Alan Ağı (Controller Area Network - CAN-Bus) protokolü üzerinden yürütülmektedir.[5] Bu durum, CAN-Bus'ı mesaj enjeksiyonu ve manipülasyon gibi saldırılara karşı savunmasız bırakmaktadır.

OCPP'nin yaygınlaşması, "tek bir anahtarla tüm kapıları açma" potansiyeli yaratarak, şarj altyapısını ulusal kritik altyapı düzeyinde bir hedef haline getirmiştir. Geçmişte her üreticinin kendi tescilli protokolünü kullanması, saldırıların cihaza özel olmasını gerektiriyordu. Ancak OCPP ile geliştirilen tek bir zafiyet, farklı markalara ait on binlerce istasyonda aynı anda istismar edilebilir. Bu durum, saldırganlar için ekonomik teşviki artırarak fidye yazılımı gibi kitlesel ve yıkıcı saldırıları daha olası kılmaktadır.[4] Dolayısıyla, protokol seviyesindeki güvenlik, artık bireysel cihaz güvenliğinden çok daha kritik bir öneme sahiptir.

Bu raporun ana tezi, OCPP ve CAN-Bus protokolleri arasındaki "köprü" zafiyetine odaklanmaktadır. Bir saldırgan, zayıf bir Aktarım Katmanı Güvenliği (Transport Layer Security - TLS) uygulamasını istismar ederek veya bir Ortadaki Adam (Man-in-the-Middle - MitM) saldırısı gerçekleştirerek OCPP iletişim kanalını ele geçirdiğinde, sadece ağ verilerini çalmakla kalmaz; aynı zamanda CP'nin ana kontrolcüsünü (MCU/SoC) de manipüle etme yeteneği kazanır.[5] Bu kontrolcü, OCPP'den gelen siber komutları (örneğin, şarj profilini ayarla) alıp, bunları güç elektroniğini, röleleri ve batarya yönetim sistemini (Battery Management System -

BMS) kontrol eden düşük seviyeli CAN-Bus mesajlarına çeviren bir "ağ geçidi" (gateway) görevi görür. Bu "köprü", siber bir saldırının doğrudan fiziksel bir etkiye dönüşmesine olanak tanır; örneğin, şarj parametrelerinin tehlikeli seviyelere çıkarılması, bataryaya kalıcı hasar verilmesi veya şebeke dengesinin bozulması gibi sonuçlar doğurabilir.[5]
OCPP'nin 2.0.1 gibi yeni sürümleri, sertifika yönetimi ve güvenli donanım yazılımı güncellemeleri gibi önemli güvenlik iyileştirmeleri getirse de [5], temel protokol mantığındaki ve uygulamalardaki zayıflıklar nedeniyle potansiyel riskler devam etmektedir.[2] Bu rapor, daha önce belgelenmiş ve yaygın olarak bilinen saldırı senaryolarının ötesine geçerek, özellikle bu siber-fiziksel "köprü" etkileşimini hedef alan 10 özgün ve ileri düzey anomali senaryosunu derinlemesine analiz etmeyi amaçlamaktadır. Aşağıdaki tablo, incelenecek senaryolara genel bir bakış sunmaktadır.

Senaryo Numarası ve Adı	**Temel STRIDE Tehdidi**	**Hedeflenen Ana Bileşen(ler)**	**Saldırı Vektörü**	**Olası Fiziksel Etki**
1. LAL Zehirlenmesi	Yetki Yükseltme (E), Sahtekarlık (S)	CP Çevrimdışı Mantığı, LAL	MitM, CSMS Taklidi	Enerji Hırsızlığı
2. Master Pass Manipülasyonu	Yetki Yükseltme (E), Hizmet Reddi (D)	CP Yetkilendirme, MasterPassGroupId CV	Veri Değiştirme (T), CSMS Taklidi	Kitlesel Hizmet Kesintisi
3. Zaman Senkronizasyonu Manipülasyonu	Veri Değiştirme (T), İnkar Edememe (R)	CP Zaman Yönetimi, DateTime CV	MitM, Heartbeat Sahteciliği	Faturalandırma Sahtekarlığı
4. Rezervasyon Sistemi İstismarı	Hizmet Reddi (D)	CSMS Rezervasyon Mantığı, CP	Botnet, Kimlik Sahteciliği (S)	Bölgesel Hizmet Erişimsizliği
5. Sahte CSMS Sertifikası ile MitM	Sahtekarlık (S), Bilgi İfşası (I)	CP TLS/Sertifika Yönetimi	DNS Zehirlenmesi, Sahte CA	Tüm İletişimin Ele Geçirilmesi
6. Teşhis Fonksiyonu İstismarı	Bilgi İfşası (I)	CP Teşhis/Loglama Mekanizması	CSMS Taklidi (S)	Ağ Topolojisi ve Şifrelerin Sızdırılması
7. Akıllı Şarj Profili Manipülasyonu	Veri Değiştirme (T), Hizmet Reddi (D)	EMS, CP Akıllı Şarj Mantığı	Koordineli CSMS Taklidi (S)	Mikro Şebeke Çökmesi
8. CAN Veri Yolu Enjeksiyonu	Veri Değiştirme (T), Yetki Yükseltme (E)	CP MCU ("Köprü"), Araç BMS	OCPP Agent Kompromizasyonu	Batarya Hasarı, Yanlış SOC Gösterimi
9. V2G Güç Akışı Sabotajı	Veri Değiştirme (T), Hizmet Reddi (D)	CP V2G Kontrol Mantığı, Araç Bataryası	ISO 15118 & OCPP Manipülasyonu	Batarya Ömrünün Azalması, Şebeke Hasarı
10. Yerel Kontrolcü Kompromizasyonu	Sahtekarlık (S), Veri Değiştirme (T)	Yerel Kontrolcü (Gateway)	Ağ Saldırısı, Zayıf Kimlik Doğrulama	Filo Düzeyinde Kontrol Kaybı

Bölüm 1: Kimlik Doğrulama ve Yetkilendirme Mekanizmalarına Yönelik Anomali Senaryoları

OCPP'nin kimlik doğrulama mimarisindeki en kritik zayıflıklardan biri, ağ kesintileri sırasında hizmet devamlılığını sağlamak amacıyla tasarlanmış olan çevrimdışı yetkilendirme modlarıdır.[5] Bu modlar, doğaları gereği merkezi doğrulamadan yoksundur ve bu durum, onları saldırganlar için cazip bir hedef haline getirir. Bir saldırgan, CP ile CSMS arasındaki iletişimi kasıtlı olarak bir Hizmet Reddi (Denial of Service - DoS) saldırısıyla keserek istasyonu çevrimdışı moda geçmeye zorlayabilir.[5] Çevrimdışı modda CP, karar vermek için yerel olarak depolanan Yetkilendirme Önbelleği (Authorization Cache) veya Yerel Yetkilendirme Listesi (Local Authorization List - LAL) gibi verilere güvenir.[12] Eğer saldırgan, istasyon henüz çevrimiçiyken bu yerel listeleri bir MitM saldırısı ile sahte bir senkronizasyon listesi göndererek manipüle etmeyi başarırsa, istasyon çevrimdışına geçtiğinde bu "zehirlenmiş" veriyi meşru kabul edecektir. Bu durum, çevrimdışı modun bir "fail-safe" (güvenli hata) mekanizması olmaktan çıkıp, iki aşamalı bir saldırı için bir "fail-open" (açık hata) kapısı haline gelmesine neden olur. Saldırının ilk aşaması veri zehirleme, ikinci aşaması ise DoS ile çevrimdışı modu tetiklemektir. Bu, OCPP'nin kullanılabilirlik ve güvenlik arasında yaptığı ödünleşmenin nasıl istismar edilebileceğinin somut bir örneğidir.

Senaryo 1: Yerel Yetkilendirme Listesinin (LAL) Zehirlenmesi ile Çevrimdışı Modun Kötüye Kullanılması

1. Senaryonun Amacı

Şarj istasyonunu (CP) kasıtlı olarak çevrimdışı moda zorlayarak ve önceden manipüle edilmiş Yerel Yetkilendirme Listesi'ni (LAL) kullanarak yetkisiz bir kimlikle (IdToken) ücretsiz ve izlenemez bir şarj işlemi başlatmak.

2. Senaryo Özeti

Saldırgan, CP ile CSMS arasındaki iletişimi bir MitM saldırısıyla kesintiye uğratır. CSMS'ten CP'ye gönderilen periyodik LAL güncelleme mesajını (SendLocalList) yakalar, kendi yetkisiz IdToken'ını listeye ekler ve değiştirilmiş listeyi CP'ye iletir. Daha sonra, CP ile CSMS arasındaki

iletişimi tamamen keserek (DoS) CP'nin çevrimdışı moda geçmesini sağlar. Çevrimdışı modda, saldırgan zehirlenmiş LAL'de bulunan kendi IdToken'ını kullanarak bir şarj işlemi başlatır.

3. Hedef Varlıklar

- **Birincil:** Şarj Noktası (CP) yazılımı, özellikle çevrimdışı yetkilendirme mantığı ve LAL depolama alanı.
- **İkincil:** CP ve CSMS arasındaki WebSocket/TLS iletişim kanalı.

4. İlişkili Tehditler (STRIDE)

- **Sahtekarlık (Spoofing):** Saldırgan, LAL güncellemesi sırasında CSMS'i taklit eder.
- **Veri Değiştirme (Tampering):** SendLocalList mesajının içeriği (LAL) değiştirilir.
- **Hizmet Reddi (Denial of Service):** CP'nin çevrimdışı moda geçmesi için iletişim kesilir.
- **Yetki Yükseltme (Elevation of Privilege):** Yetkisiz bir IdToken, LAL aracılığıyla yetkili hale getirilir.

5. Saldırıda Faydalanılan Zafiyetler

- Zayıf TLS uygulaması veya sertifika yönetimi, MitM saldırısını mümkün kılar.[13]
- OCPP'nin çevrimdışı yetkilendirme modlarının (LAL, Authorization Cache) varlığı ve merkezi doğrulamadan yoksun olması.[5]
- CP'nin, LAL güncellemelerinin bütünlüğünü ve kaynağını dijital imza gibi ek mekanizmalarla doğrulamaması.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Keşif):** Saldırgan, hedef CP'nin ağ trafiğini dinleyerek LAL güncelleme (SendLocalList) mesajlarının periyodunu ve formatını öğrenir.
- **Adım 2 (MitM Kurulumu):** Saldırgan, ARP spoofing veya DNS zehirlenmesi gibi yöntemlerle CP ve CSMS arasına girer.
- **Adım 3 (Veri Zehirleme):** CSMS'ten gelen bir sonraki SendLocalList.req mesajını yakalar. Mesajın içindeki yetkili IdToken listesine kendi sahte IdToken'ını ("idTag": "ATTACKER01") ekler. Değiştirilmiş mesajı CP'ye iletir. CP, mesajı geçerli bir CSMS'ten geldiğini varsayarak LAL'sini günceller.
- **Adım 4 (DoS ve Çevrimdışı Modu Tetikleme):** Saldırgan, CP'nin CSMS'e olan bağlantısını (örneğin, TCP reset paketleri göndererek veya ağ geçidinde trafiği engelleyerek) keser. CP, birkaç başarısız Heartbeat denemesinden sonra çevrimdışı moda geçer.

- **Adım 5 (İstismar):** Saldırgan, fiziksel olarak CP'ye gider ve "ATTACKER01" IdToken'ını (örneğin, klonlanmış bir RFID kartı ile) okutur.
- **Adım 6 (Sonuç):** CP, IdToken'ı yerel olarak zehirlenmiş LAL'de kontrol eder, geçerli bulur ve şarj işlemini başlatır. Bu işlem, CP tekrar çevrimiçi olana kadar CSMS'e raporlanmaz.

7. Olası Sonuçlar ve Etkiler

- **Ekonomik Kayıp:** Şarj hizmeti sağlayıcısı için enerji hırsızlığı ve gelir kaybı.
- **Veri Bütünlüğü Kaybı:** CSMS kayıtları ile gerçekte tüketilen enerji arasında tutarsızlık.
- **İzlenebilirlik Kaybı:** Saldırganın kimliği, sahte IdToken kullanıldığı için gizli kalır.

8. Tespit Yöntemleri (Detection)

- **Ağ Seviyesi:** Ağ Trafiği Analizi (NTA) araçları ile anormal SendLocalList mesaj boyutları veya beklenmedik içerik değişiklikleri tespit edilebilir. Sertifika sabitleme (certificate pinning) başarısızlıklarının izlenmesi MitM girişimlerini ortaya çıkarabilir.
- **CP Seviyesi:** CP tekrar çevrimiçi olduğunda, çevrimdışı modda gerçekleşen işlemlerin (TransactionEvent) IdToken'ları CSMS'teki ana yetkilendirme listesiyle karşılaştırılır. LAL'de olup ana listede olmayan bir IdToken ile yapılan işlem anomali olarak işaretlenir. CP'nin anormal derecede sık ve uzun süreli çevrimdışı kalması da bir anomali göstergesi olabilir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Güçlü Kimlik Doğrulama:** Karşılıklı TLS (mTLS) kimlik doğrulaması (OCPP Güvenlik Profili 3) kullanarak hem CP'nin hem de CSMS'in kimliğinin doğrulanması, MitM saldırılarını büyük ölçüde engeller.[5]
- **Veri Bütünlüğü:** SendLocalList gibi kritik konfigürasyon mesajlarının dijital olarak imzalanması ve CP tarafından bu imzaların doğrulanması.[15]
- **Çevrimdışı Modun Kısıtlanması:** LocalAuthorizeOffline yapılandırma değişkenini false olarak ayarlayarak çevrimdışı yetkilendirmeyi tamamen devre dışı bırakmak veya çevrimdışı modda yalnızca belirli, yüksek güvenilirliğe sahip IdToken'lara izin vermek.
- **Sıfır Güven Yaklaşımı:** CP, CSMS'ten gelen her türlü konfigürasyon değişikliğini (LAL güncellemesi dahil) şüpheyle karşılamalı ve ek doğrulama mekanizmalarından geçirmelidir.[5]

Sanal Ortamda Test İçin Referans Makaleler

- **Alcaraz, C., Lopez, J., & Wolthusen, S. (2017). "OCPP protocol: security threats**

and challenges." IEEE Transactions on Smart Grid. [11]: Bu makale, OCPP'nin ilk güvenlik analizlerinden birini sunar ve özellikle çevrimdışı yetkilendirme listelerinin (LAL) potansiyel bir zafiyet olduğunu vurgular. Simülasyon ortamında, bir "kötü niyetli sunucu" (evil CSMS) kurularak bu listelerin nasıl manipüle edilebileceği test edilebilir.

- **Rubio, J. E., Alcaraz, C., & Lopez, J. (2018). "Addressing security in OCPP: protection against man-in-the-middle attacks."** [2]: Bu çalışma, OCPP üzerindeki MitM saldırılarına odaklanır. Bir mitmproxy aracı ve sanal bir CP/CSMS ortamı (örneğin, python-ocpp kütüphanesi kullanılarak) ile SendLocalList mesajlarının nasıl yakalanıp değiştirilebileceği pratik olarak gösterilebilir.

Senaryo 2: Yetki Yükseltme Amacıyla Master Pass Kimliğinin Manipülasyonu

1. Senaryonun Amacı

Acil durum ve kolluk kuvvetleri personeli için tasarlanmış, herhangi bir şarj işlemini durdurma yetkisine sahip olan Master Pass özelliğini istismar ederek, yetkisiz bir kimliği bu ayrıcalıklı gruba dahil etmek ve bu yolla kitlesel bir hizmet reddi saldırısı gerçekleştirmek.

2. Senaryo Özeti

Saldırgan, CSMS'i taklit ederek veya CSMS ile CP arasındaki iletişimi bir MitM saldırısı ile ele geçirerek, MasterPassGroupId yapılandırma değişkenini (Configuration Variable) değiştiren bir SetVariables mesajı gönderir. Bu mesajla, saldırgan kendi kontrolündeki bir IdToken'ı Master Pass grubuna ekler. Yetki yükseltme işlemini tamamladıktan sonra, saldırgan bu ayrıcalıklı IdToken'ı kullanarak bölgedeki tüm aktif şarj işlemlerini uzaktan durdurabilir (RemoteStopTransaction) veya istasyonların kullanılabilirliğini Inoperative (çalışmaz) durumuna getirebilir.

3. Hedef Varlıklar

- **Birincil:** CP yapılandırma depolama alanı, özellikle MasterPassGroupId değişkeni.
- **İkincil:** CP'nin yetkilendirme ve işlem kontrol mantığı.

4. İlişkili Tehditler (STRIDE)

- **Veri Değiştirme (Tampering):** MasterPassGroupId yapılandırma değişkeninin değeri değiştirilir.
- **Yetki Yükseltme (Elevation of Privilege):** Normal bir kullanıcı kimliği, tüm işlemleri durdurma yetkisine sahip bir Master Pass kimliğine yükseltilir.[5]
- **Hizmet Reddi (Denial of Service):** Yükseltilmiş yetkiler kullanılarak meşru kullanıcıların şarj işlemleri sonlandırılır.
- **Sahtekarlık (Spoofing):** Saldırı, CSMS'in taklit edilmesiyle gerçekleştirilebilir.

5. Saldırıda Faydalanılan Zafiyetler

- SetVariables gibi kritik OCPP operasyonlarının, kaynak (CSMS) doğrulaması ve mesaj bütünlüğü kontrolleri (örn. dijital imza) olmaksızın kabul edilmesi.
- Master Pass gibi güçlü bir yetkinin, sadece tek bir yapılandırma değişkeni ile kontrol edilmesi ve bu değişkenin değiştirilmesine karşı ek güvenlik katmanlarının bulunmaması.
- Zayıf ağ güvenliği veya kimlik doğrulama mekanizmalarının, saldırganın CSMS taklidi yapmasına veya MitM saldırısı gerçekleştirmesine olanak tanıması.[13]

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Hazırlık):** Saldırgan, "ATTACKER_MASTER" adında bir IdToken oluşturur (örneğin, bir RFID kartına bu kimliği programlar).
- **Adım 2 (Sızma):** Saldırgan, CSMS ile CP arasındaki iletişimi ele geçirmek için bir MitM proxy'si kurar.
- **Adım 3 (Manipülasyon):** Saldırgan, sahte bir SetVariables.req mesajı oluşturur. Bu mesajın içeriği, MasterPassGroupId değişkenine "ATTACKER_MASTER" değerini ekleyecek şekildedir. Mesajı CSMS'ten geliyormuş gibi CP'ye gönderir.
- **Adım 4 (Doğrulama):** CP, komutu işler ve MasterPassGroupId yapılandırma değişkenini günceller. Saldırganın kimliği artık ayrıcalıklı bir kimliktir.
- **Adım 5 (Saldırı):** Saldırgan, "ATTACKER_MASTER" kimliğini kullanarak hedef bölgedeki bir CP'de işlem durdurma komutunu tetikler. OCPP v2.0.1'e göre, bir Master Pass ile bir işlem durdurulduğunda, bu durum diğer istasyonlara da yayılabilir veya tüm istasyonları etkileyebilir. Bu, kitlesel bir hizmet kesintisine yol açar.[5]
- **Adım 6 (Etki):** Bölgedeki tüm EV sürücüleri şarj işlemlerinin aniden sonlandığını görür ve yeni işlem başlatamaz. Bu durum, özellikle yoğun saatlerde büyük bir kaosa ve ekonomik kayba neden olur.

7. Olası Sonuçlar ve Etkiler

- **Büyük Ölçekli Hizmet Kesintisi:** Bir şehir veya bölgedeki tüm şarj istasyonları aynı anda

devre dışı bırakılabilir.
- **Ekonomik Sabotaj:** Rakip bir şarj ağı operatörüne yönelik bir saldırı, şirketin itibarını ve gelirini ciddi şekilde zedeleyebilir.
- **Kamu Güveni Kaybı:** EV şarj altyapısının güvenilmez olduğu algısı yaratarak elektrifikasyon sürecini yavaşlatabilir.

8. Tespit Yöntemleri (Detection)

- **Yapılandırma Denetimi:** MasterPassGroupId gibi kritik yapılandırma değişkenlerinde yapılan değişiklikler için anında uyarı üreten ve bu değişiklikleri merkezi bir SIEM sistemine gönderen mekanizmalar kurulmalıdır.
- **Davranışsal Analiz:** Bir Master Pass kimliğinin, acil durumlar dışında, kısa bir süre içinde çok sayıda işlemi durdurması anormal bir davranış olarak kabul edilmeli ve otomatik olarak soruşturma başlatılmalıdır.
- **Korelasyon Analizi:** Ağdaki bir SetVariables komutunun hemen ardından gelen kitlesel StopTransaction olayları, bu saldırı senaryosunun güçlü bir göstergesidir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **En Az Ayrıcalık İlkesi (Principle of Least Privilege):** Master Pass gibi kritik yetkiler, çok faktörlü kimlik doğrulama (MFA) veya ek bir onay mekanizması gerektirmelidir. Sadece bir IdToken'ın varlığı yeterli olmamalıdır.
- **Değişiklik Kontrolü:** MasterPassGroupId gibi kritik değişkenlerin değiştirilmesi, CSMS tarafında birden fazla yetkilinin onayını gerektiren bir iş akışına bağlanmalıdır.
- **İmzalama ve Doğrulama:** Tüm SetVariables istekleri, CSMS tarafından dijital olarak imzalanmalı ve CP, bu imzayı doğrulamadan değişkeni güncellememelidir.
- **Fiziksel Güvenlik:** Master Pass olarak kullanılacak RFID kartları gibi fiziksel token'lar, yüksek güvenlikli ortamlarda saklanmalı ve klonlamaya karşı korunmalıdır.

Sanal Ortamda Test İçin Referans Makaleler

- **Alcaraz, C., Cumplido, J., & Triviño, A. (2023). "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0." International Journal of Information Security.** [5]: Bu makale, OCPP v2.0.1'in getirdiği yeni aktörleri ve fonksiyonları (Master Pass dahil) STRIDE ve DREAD metodolojileriyle analiz eder. Simülasyon, python-ocpp gibi bir kütüphane kullanılarak sanal bir CP ve CSMS oluşturmayı içerir. SetVariables mesajı ile MasterPassGroupId değişkeninin manipüle edilmesi ve ardından bu kimlikle RemoteStopTransaction komutunun gönderilmesinin etkileri gözlemlenebilir.
- **Garofalaki, Z., et al. (2022). "Electric vehicle charging: a survey on the security**

issues and challenges of the open charge point protocol (OCPP)." IEEE Communications Surveys & Tutorials.: Bu kapsamlı anket, OCPP'deki çeşitli tehditleri, yapılandırma değişkenlerinin manipülasyonu da dahil olmak üzere detaylandırır. Test ortamı, bu makalede bahsedilen zafiyetleri pratik olarak doğrulamak için bir MitM aracıyla birleştirilmiş sanal bir OCPP ağı kurmayı içerebilir.

Bölüm 2: Protokol Mantığı ve Durum Yönetimine Yönelik Anomali Senaryoları

Siber-fiziksel sistemlerde "zaman", yalnızca bir ölçüm birimi değil, aynı zamanda sistemin durumunu, geçerliliğini ve mantıksal akışını belirleyen kritik bir parametredir. OCPP protokolünde zaman, rezervasyonların geçerlilik süresini, tarifeye dayalı faturalandırmanın doğruluğunu, işlem loglarının sıralı ve tutarlı olmasını ve sistem bileşenleri arasındaki senkronizasyonu sağlamak için temel bir rol oynar.[5] Bir saldırgan, bir şarj istasyonunun zaman algısını manipüle etmeyi başarırsa, bu sadece anlık bir hataya neden olmaz; sistemin tüm iş mantığını temelden bozar. Örneğin, CP'nin saatini kasıtlı olarak geleceğe ayarlayarak, henüz başlamamış meşru bir rezervasyonun "süresi doldu" olarak algılanıp iptal edilmesini sağlayabilir. Tersi bir senaryoda, CP'nin saatini geçmişe ayarlayarak, en pahalı tarife diliminde yapılan bir şarj işlemini, en ucuz gece tarifesinde yapılmış gibi göstererek faturalandırma sahtekarlığı yapabilir. Bu tür bir saldırı, doğrudan enerji çalmak veya sistemi çökertmek yerine, sistemin "güven" ve "doğruluk" gibi temel varsayımlarını hedefler. Tespit edilmesi son derece zordur, çünkü CP'nin kendisi teknik olarak "doğru" çalıştığını düşünür; sadece yanlış bir zaman diliminde işlem yapmaktadır. Zaman senkronizasyonu saldırıları, bu nedenle kaba kuvvet saldırılarından çok daha sofistike, gizli ve yıkıcıdır.

Senaryo 3: Zaman Senkronizasyonuna Yönelik Manipülasyon ile Rezervasyon ve Faturalandırma Sahtekarlığı

1. Senaryonun Amacı

CP'nin sistem saatini (DateTime CV) manipüle ederek, zaman damgalarına dayalı iş mantığını (faturalandırma, rezervasyon geçerliliği) bozmak ve bu yolla ya maliyet avantajı sağlamak ya da hizmeti başkaları için kullanılamaz hale getirmek.

2. Senaryo Özeti

Saldırgan, CP ve CSMS arasındaki iletişimi bir MitM saldırısı ile izler. CSMS'in zaman senkronizasyonu için periyodik olarak gönderdiği Heartbeat mesajlarını veya SetVariables komutlarını yakalar. Saldırgan, bu mesajların içindeki zaman damgasını değiştirerek CP'nin saatini ileri veya geri alır. Örneğin, pahalı gündüz tarifesi sırasında şarj yaparken, CP'nin saatini ucuz gece tarifesinin olduğu bir zamana ayarlayarak daha az ödeme yapar. Veya bir başkasının rezervasyon saatinden hemen önce CP'nin saatini rezervasyon bitiş saatinden sonraya ayarlayarak rezervasyonu geçersiz kılar.

3. Hedef Varlıklar

- **Birincil:** CP'nin dahili saati ve DateTime yapılandırma değişkeni.
- **İkincil:** Zaman damgalarını kullanan tüm OCPP fonksiyonları (ReserveNow, TransactionEvent içindeki MeterValues zaman damgaları, vb.).

4. İlişkili Tehditler (STRIDE)

- **Veri Değiştirme (Tampering):** Heartbeat veya SetVariables mesajlarındaki zaman damgası verisi değiştirilir.
- **İnkar Edememe (Repudiation):** Saldırgan, yanlış zaman damgalı işlemler gerçekleştirerek, "bu işlemi o saatte ben yapmadım" diyebilir ve faturalandırmaya itiraz edebilir.
- **Hizmet Reddi (Denial of Service):** Rezervasyonların geçersiz kılınmasıyla meşru kullanıcıların hizmet alması engellenir.

5. Saldırıda Faydalanılan Zafiyetler

- Zaman senkronizasyon mesajlarının (örn. Heartbeat) bütünlüğünün kriptografik olarak (örn. dijital imza ile) korunmaması.
- CP'nin, CSMS'ten gelen zaman bilgisine körü körüne güvenmesi ve bunu harici, güvenilir bir NTP (Network Time Protocol) sunucusu gibi bir kaynakla çapraz kontrol etmemesi.
- İletişim kanalının MitM saldırılarına karşı savunmasız olması.[2]

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Kurulum):** Saldırgan, hedef CP'nin ağına sızar ve CP ile CSMS arasına bir MitM proxy'si yerleştirir.
- **Adım 2 (Faturalandırma Saldırısı):**
    - Kullanıcı, en yüksek elektrik tarifesinin geçerli olduğu 14:00'te şarj işlemini başlatır.
    - Saldırgan, CSMS'ten CP'ye giden bir sonraki Heartbeat.conf mesajını yakalar.

Mesajdaki currentTime alanını, en ucuz tarifenin olduğu 03:00 olarak değiştirir ve CP'ye iletir.
    - CP, saatini 03:00 olarak günceller. Şarj işlemi boyunca gönderilen tüm MeterValues mesajları bu sahte zaman damgasıyla etiketlenir.
    - İşlem bittiğinde, CSMS'e gönderilen TransactionEvent raporu, şarjın gece 03:00'te yapıldığını gösterir ve kullanıcıya düşük tarifeden fatura kesilir.
- **Adım 3 (Rezervasyon Sabotajı):**
    - Meşru bir kullanıcı, saat 16:00 için bir rezervasyon yapar (expiryDate 16:00).
    - Saldırgan, saat 15:55'te, CP'nin saatini 16:05'e ayarlayan sahte bir zaman senkronizasyon mesajı gönderir.
    - CP, saatinin 16:05 olduğuna inanır ve rezervasyonun süresinin dolduğuna karar vererek konektörü serbest bırakır.
    - Meşru kullanıcı 16:00'da geldiğinde, rezerve ettiği yerin başka bir araç tarafından kullanıldığını görür.

7. Olası Sonuçlar ve Etkiler

- **Mali Sahtekarlık:** Hem şarj operatörü hem de enerji sağlayıcı için gelir kaybı.
- **Operasyonel Kaos:** Rezervasyon sisteminin güvenilmez hale gelmesi, müşteri memnuniyetsizliği ve operasyonel verimsizlik.
- **Adli Bilişim Zorlukları:** Yanlış zaman damgalı log kayıtları, bir olay sonrası incelemeyi veya kanıt toplamayı imkansız hale getirebilir.

8. Tespit Yöntemleri (Detection)

- **Çapraz Zaman Kontrolü:** CP'ler, CSMS'ten gelen zaman bilgisine ek olarak, güvenli ve imzalı bir NTP sunucusundan periyodik olarak zaman bilgisi almalı ve bu iki kaynak arasında önemli bir tutarsızlık ($>\Delta t$) olduğunda alarm üretmelidir.
- **Zaman Sıçraması Tespiti:** CP veya CSMS'te, bir cihazın sistem saatinin mantıksız bir şekilde (örneğin, saniyeler içinde saatlerce) ileri veya geri sıçramasını tespit eden bir anomali tespit kuralı oluşturulmalıdır.
- **İşlem Mantığı Analizi:** Bir şarj işleminin başlangıç ve bitiş zaman damgalarının, beklenen tarife değişiklikleri veya rezervasyon pencereleriyle uyumsuz olması durumunda işlem şüpheli olarak işaretlenmelidir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Güvenli Zaman Senkronizasyonu:** Sadece TLS ile korunan Heartbeat mesajlarına güvenmek yerine, NTS (Network Time Security) gibi kriptografik olarak güvenli zaman senkronizasyon protokolleri kullanılmalıdır.

- **Mesaj İmzalama:** Zaman bilgisi içeren tüm OCPP mesajları (hem Heartbeat hem de SetVariables), CSMS tarafından dijital olarak imzalanmalı ve CP tarafından doğrulanmalıdır.
- **Güvenilir Zaman Kaynağı:** CP'ler, mümkünse GPS gibi harici ve güvenilir bir zaman kaynağına sahip bir donanım modülü içermelidir.
- **Mantıksal Sınırlar:** CP yazılımı, zamanı ayarlarken mantıksal sınırlar uygulamalıdır. Örneğin, saatinin bir önceki ölçümden daha geriye gitmesini veya belirli bir eşikten fazla ileri sıçramasını engelleyebilir.

Sanal Ortamda Test İçin Referans Makaleler

- **Khan, R., et al. (2017). "Stride-based threat modeling for cyber-physical systems." IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe).**: Bu makale, STRIDE modelinin siber-fiziksel sistemlere nasıl uygulanacağını gösterir. Zaman senkronizasyonu, siber-fiziksel sistemlerde kritik bir "veri" olduğu için, bu makaledeki tehdit modelleme yaklaşımı, zaman manipülasyonunun "Tampering" (Veri Değiştirme) kategorisi altında nasıl analiz edileceğini anlamak için bir çerçeve sunar.
- **Zografopoulos, I., et al. (2021). "Cyber-physical energy systems security: threat modeling, risk assessment, resources, metrics, and case studies." IEEE Access.**: Enerji sistemleri güvenliği üzerine olan bu çalışma, zaman senkronizasyonunun şebeke operasyonları için ne kadar kritik olduğunu vurgular.[17] Simülasyon, bir MitM aracı kullanarak Heartbeat mesajlarındaki currentTime alanını değiştirerek, bunun sanal bir CP'nin faturalandırma ve rezervasyon mantığını nasıl etkilediğini gözlemlemeyi içerebilir.

Senaryo 4: Rezervasyon Sisteminin Kötüye Kullanılmasıyla Kitlesel Hizmet Reddi (Mass DoS)

1. Senaryonun Amacı

Bir bölgedeki tüm şarj istasyonlarını, sahte veya çalınmış kimlikler kullanarak kitlesel olarak rezerve etmek ve bu sayede meşru EV kullanıcılarının hizmet almasını engelleyerek bölgesel bir hizmet reddi (DoS) durumu yaratmak.

2. Senaryo Özeti

Saldırgan, bir botnet veya bir dizi script kullanarak, hedef bölgedeki tüm müsait şarj istasyonlarına eş zamanlı olarak ReserveNow istekleri gönderir. Bu istekler, ya zayıf kimlik doğrulama süreçlerini atlayarak oluşturulmuş sahte kullanıcı kimlikleriyle ya da daha önceki

veri sızıntılarından elde edilmiş meşru kullanıcı kimlikleriyle yapılır. CSMS, bu istekleri geçerli kabul ederek istasyonları rezerve edilmiş duruma geçirir. Saldırgan, rezervasyon süresi dolmadan hemen önce rezervasyonu iptal edip anında yenileyerek istasyonları sürekli olarak meşgul tutar.

3. Hedef Varlıklar

- **Birincil:** CSMS'in rezervasyon yönetim sistemi ve veritabanı.
- **İkincil:** Bölgedeki tüm Şarj Noktaları (CP).

4. İlişkili Tehditler (STRIDE)

- **Hizmet Reddi (Denial of Service):** Şarj kaynakları meşru kullanıcılara karşı erişilemez hale getirilir.[18]
- **Sahtekarlık (Spoofing):** Saldırı, sahte veya çalınmış kullanıcı kimlikleri kullanılarak gerçekleştirilir.

5. Saldırıda Faydalanılan Zafiyetler

- Rezervasyon işlemi için güçlü bir kimlik doğrulama veya insan doğrulama (CAPTCHA gibi) mekanizmasının bulunmaması.
- Aynı kullanıcının veya IP adresinin kısa süre içinde çok sayıda rezervasyon yapmasına olanak tanıyan hız sınırlama (rate limiting) eksikliği.
- Rezervasyon yapmak için herhangi bir ön ödeme, depozito veya cezai yaptırımın olmaması, saldırının maliyetsiz hale gelmesini sağlar.
- Kullanıcı kimliklerinin (IdToken) kolayca tahmin edilebilir veya oluşturulabilir olması.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Hedef Belirleme):** Saldırgan, halka açık haritalama servisleri veya CPO mobil uygulamaları aracılığıyla hedef bölgedeki (örneğin, bir havalimanı otoparkı veya işlek bir otoyol) tüm şarj istasyonlarının bir listesini çıkarır.
- **Adım 2 (Kimlik Toplama):** Saldırgan, ya zayıf bir kayıt formunu istismar ederek binlerce sahte hesap oluşturur ya da karanlık ağdan (dark web) sızdırılmış kullanıcı kimlik bilgilerini satın alır.
- **Adım 3 (Botnet Aktivasyonu):** Saldırgan, kontrolü altındaki bir botnet'e veya dağıtık sunuculara, toplanan kimlikler ve hedef istasyon listesiyle birlikte ReserveNow komutunu gönderme görevini verir.
- **Adım 4 (Kitlesel Rezervasyon):** Botnet, binlerce farklı IP adresinden ve farklı kimliklerle,

hedef istasyonlara eş zamanlı olarak ReserveNow.req mesajları gönderir. Her istek, mümkün olan maksimum rezervasyon süresini talep eder.

- **Adım 5 (Sürekli Meşguliyet):** CSMS, bu geçerli görünen istekleri işler ve istasyonları "Reserved" durumuna geçirir. Saldırganın script'i, rezervasyonların bitiş süresini (expiryDate) sürekli izler ve süre dolmadan birkaç saniye önce CancelReservation gönderip hemen ardından yeni bir ReserveNow isteği ileterek istasyonları kilitli tutar.
- **Adım 6 (Etki):** Bölgeye gelen meşru EV sürücüleri, mobil uygulamalarda veya istasyon ekranlarında tüm konektörlerin rezerve edilmiş olduğunu görür ve araçlarını şarj edemez.

7. Olası Sonuçlar ve Etkiler

- **Bölgesel Felç:** Kritik lokasyonlardaki (hastaneler, havalimanları, ana arterler) şarj altyapısının tamamen kullanılamaz hale gelmesi.
- **Ekonomik Kayıp:** CPO'lar için ciddi gelir kaybı ve marka itibarının zedelenmesi.
- **Kullanıcı Mağduriyeti:** Yolda kalan sürücüler, iptal olan seyahatler ve EV kullanımına karşı genel bir güvensizlik.

8. Tespit Yöntemleri (Detection)

- **Anomali Tespiti:** CSMS seviyesinde, rezervasyon isteklerinin coğrafi dağılımı, hızı ve zamanlaması üzerinde anomali tespiti algoritmaları çalıştırılmalıdır. Belirli bir bölgeden gelen rezervasyon isteklerinde ani ve orantısız bir artış alarm tetiklemelidir.
- **Kullanıcı Davranış Analizi (UBA):** Bir kullanıcının normalde hiç gitmediği bir konumda aniden çok sayıda rezervasyon yapması veya bir hesabın aynı anda birden fazla coğrafi bölgede rezervasyon yapmaya çalışması gibi anormal davranışlar işaretlenmelidir.
- **İptal Oranı İzleme:** Belirli bir bölgedeki veya kullanıcı grubundaki rezervasyon iptal oranlarının (CancelReservation) anormal şekilde yükselmesi, bu tür bir saldırının göstergesi olabilir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Hız Sınırlama (Rate Limiting):** Bir IP adresinden veya bir kullanıcı hesabından belirli bir zaman diliminde yapılabilecek rezervasyon sayısı sınırlandırılmalıdır.
- **İnsan Doğrulama:** Rezervasyon işlemi sırasında CAPTCHA veya benzeri bir "bot" engelleme mekanizması uygulanmalıdır.
- **Mali Caydırıcılık:** Rezervasyon için küçük bir ön ödeme veya depozito alınması ve rezervasyonun kullanılmaması durumunda bu ücretin iade edilmemesi, kitlesel sahte rezervasyonları ekonomik olarak caydırıcı hale getirir.
- **Adaptif Güvenlik Politikaları:** Şüpheli bir aktivite tespit edildiğinde (örneğin, belirli bir bölgeden gelen yoğun istekler), o bölge için geçici olarak daha sıkı rezervasyon kuralları

(örn. daha kısa rezervasyon süresi, daha yüksek depozito) otomatik olarak devreye alınabilir.

Sanal Ortamda Test İçin Referans Makaleler

- **Alcaraz, C., Lopez, J., & Wolthusen, S. (2017). "OCPP protocol: security threats and challenges." IEEE Transactions on Smart Grid.** [11]: Bu çalışma, OCPP'nin kaynak yönetimi (rezervasyon dahil) ile ilgili zafiyetlerine dikkat çeker. Simülasyon, birden çok sanal istemci (EV sürücüsü) oluşturarak ve bu istemcilerin bir CSMS'e eş zamanlı olarak ReserveNow istekleri göndermesini sağlayarak gerçekleştirilebilir. CSMS'in bu yük altında nasıl davrandığı ve kaynakları nasıl tahsis ettiği gözlemlenebilir.
- **SaiFlow (2022). "New security weaknesses have been discovered in several electric vehicle charging systems." RSA Conference Blog.** [18]: Bu endüstri raporu, EV sistemlerindeki DoS saldırılarının pratik sonuçlarını vurgular. Sanal bir test ortamında, bir saldırı script'i yazılarak, bir CSMS API'sine yönelik yüksek frekanslı ReserveNow istekleri gönderilir ve sistemin yanıt sürelerindeki yavaşlama veya hizmet verememe durumu ölçülebilir.

Bölüm 3: Veri Bütünlüğü ve Ağ Güvenliğine Yönelik Anomali Senaryoları

Senaryo 5: Sahte CSMS Sertifikası ile TLS El Sıkışmasını Ele Geçirerek İletişim Kanalı Kontrolü

1. Senaryonun Amacı

OCPP Güvenlik Profili 2 veya 3'ün kullanıldığı durumlarda, CP'nin CSMS'in kimliğini doğrulamak için kullandığı TLS sertifika doğrulama sürecini atlatarak, tüm iletişim kanalını ele geçirmek ve hassas verileri (kimlik bilgileri, ölçüm değerleri, yapılandırma komutları) çalmak veya değiştirmek.

2. Senaryo Özeti

Saldırgan, CP'nin ağında bir MitM pozisyonu elde eder. CP, CSMS'e bir TLS bağlantısı kurmaya

çalıştığında, saldırgan bu isteği yakalar. CP'ye, meşru CSMS'in alan adına sahip ancak saldırganın kendi özel anahtarıyla imzalanmış sahte bir TLS sunucu sertifikası sunar. Eğer CP, bu sertifikayı sunan otoritenin (Certificate Authority - CA) güvenilir olup olmadığını düzgün bir şekilde kontrol etmezse veya sertifika sabitleme (certificate pinning) kullanmıyorsa, sahte sertifikayı kabul eder ve şifreli bağlantıyı saldırganla kurar. Saldırgan daha sonra kendisi de meşru CSMS'e ayrı bir TLS bağlantısı kurarak iki bağlantı arasında bir köprü oluşturur ve tüm trafiği şifresini çözerek okuyup manipüle edebilir.

3. Hedef Varlıklar

- **Birincil:** CP'nin TLS istemci uygulaması ve sertifika doğrulama mantığı.
- **İkincil:** CP ve CSMS arasındaki tüm şifreli OCPP iletişimi.

4. İlişkili Tehditler (STRIDE)

- **Sahtekarlık (Spoofing):** Saldırgan, kendisini meşru CSMS olarak tanıtır.
- **Bilgi İfşası (Information Disclosure):** Şifreli olması gereken tüm OCPP mesajları (kullanıcı kimlikleri, parolalar, MeterValues) saldırgan tarafından okunabilir hale gelir.[15]
- **Veri Değiştirme (Tampering):** Saldırgan, transit halindeki OCPP mesajlarını (örn. SetChargingProfile) değiştirebilir.

5. Saldırıda Faydalanılan Zafiyetler

- **Zayıf Sertifika Doğrulaması:** CP yazılımının, sunucu sertifikasının imza zincirini güvenilir bir kök CA'ya kadar tam olarak doğrulamaması.
- **Sertifika Sabitleme Eksikliği:** CP'nin, belirli bir alan adı için yalnızca belirli bir sertifikaya veya genel anahtara güvenmesini sağlayan sertifika sabitleme (certificate pinning) mekanizmasının uygulanmamış olması.[14]
- **DNS Zehirlenmesi veya ARP Sahtekarlığı:** Saldırganın, CP'nin CSMS alan adını kendi IP adresine çözümlemesini sağlayarak MitM pozisyonu elde etmesine olanak tanıyan ağ zafiyetleri.[14]
- **Güvensiz CA'ların Varlığı:** CP'nin güvenilir kök sertifika deposunda, saldırganın sahte sertifika alabileceği daha az güvenilir veya ele geçirilmiş bir CA'nın bulunması.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Ağ Konumlandırması):** Saldırgan, hedef CP'nin bulunduğu yerel ağda (örneğin, halka açık bir Wi-Fi ağına bağlı bir CP) ARP sahtekarlığı gerçekleştirerek ağ geçidi (gateway) gibi davranmaya başlar.

- **Adım 2 (Bağlantı Yakalama):** CP, CSMS'e (wss://csms.example.com) bir WebSocket bağlantısı başlatır. Bu istek, saldırganın makinesinden geçer.
- **Adım 3 (Sahte Sertifika Sunumu):** Saldırgan, csms.example.com için "kendinden imzalı" (self-signed) veya güvenilmeyen bir CA'dan alınmış bir TLS sertifikası oluşturur. Bu sahte sertifikayı CP'ye sunar.
- **Adım 4 (Zafiyetin İstismarı):** CP'nin TLS kütüphanesi, sertifika doğrulamasını atlayacak şekilde yapılandırılmışsa (örneğin, geliştirme sırasında bırakılmış bir ayar) veya sunulan sertifikanın CA'sını sorgusuzca kabul ederse, TLS el sıkışması başarılı olur. CP, şifreli kanalın saldırganla kurulduğunun farkında değildir.
- **Adım 5 (Trafik Rölesi ve Manipülasyon):** Saldırgan, CP'den gelen şifreli veriyi kendi özel anahtarıyla çözer, düz metin olarak okur ve isterse değiştirir. Ardından, veriyi yeniden şifreleyerek meşru CSMS'e kurduğu ayrı bir TLS tüneli üzerinden iletir. CSMS'ten gelen yanıtlar için de aynı işlemi tersten yapar.
- **Adım 6 (Veri Hırsızlığı):** Bu pozisyonda saldırgan, bir kullanıcının Authorize isteğindeki IdToken'ını, BootNotification mesajındaki CP kimlik bilgilerini veya TransactionEvent içindeki tüm şarj verilerini çalabilir.

7. Olası Sonuçlar ve Etkiler

- **Toptan Veri Sızıntısı:** Tüm kullanıcıların kimlik bilgileri, şarj alışkanlıkları ve ödeme bilgileri çalınabilir.[3]
- **Sistem Kontrolünün Ele Geçirilmesi:** Saldırgan, SetVariables, RemoteStart/StopTransaction gibi komutları manipüle ederek istasyonun kontrolünü tamamen ele alabilir.
- **Güvenin Temelden Sarsılması:** TLS gibi temel bir güvenlik katmanının aşılabildiğinin gösterilmesi, tüm OCPP tabanlı altyapıya olan güveni yok eder.

8. Tespit Yöntemleri (Detection)

- **Sertifika Şeffaflığı (Certificate Transparency - CT) Logları:** CSMS operatörleri, kendi alan adları için beklenmedik veya sahte sertifikaların yayınlanıp yayınlanmadığını izlemek için CT loglarını düzenli olarak kontrol etmelidir.
- **Anormal Bağlantı Davranışları:** Bir CP'nin bağlantısının sık sık düşmesi ve yeniden kurulması veya TLS el sıkışma hatalarının loglanması, bir MitM girişiminin belirtisi olabilir.
- **Uç Nokta Taraması:** CSMS, periyodik olarak CP'lere bağlanarak sundukları TLS sertifikasının beklenen sertifika olup olmadığını doğrulayabilir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Sertifika Sabitleme (Certificate Pinning):** Bu, en etkili yöntemdir. CP, yalnızca

önceden tanımlanmış bir sertifika veya genel anahtar ile sunulan bağlantıları kabul etmelidir. Bu, sahte sertifikaları geçersiz kılar.[14]

- **Sıkı TLS Yapılandırması:** CP'ler, yalnızca güvenilir ve iyi bilinen Kök CA'lardan gelen sertifikaları kabul etmeli, kendinden imzalı sertifikalara asla güvenmemeli ve eski/zayıf şifreleme algoritmalarını devre dışı bırakmalıdır.
- **Karşılıklı TLS (mTLS):** Sadece CP'nin CSMS'i değil, CSMS'in de CP'yi bir istemci sertifikası ile doğruladığı OCPP Güvenlik Profili 3'ün kullanılması, yetkisiz cihazların ağa bağlanmasını engeller.
- **Güvenli Ağ Mimarisi:** CP'lerin halka açık internet yerine, özel bir APN veya VPN üzerinden CSMS'e bağlanması, MitM saldırı yüzeyini önemli ölçüde azaltır.[19]

Sanal Ortamda Test İçin Referans Makaleler

- **Rubio, J. E., Alcaraz, C., & Lopez, J. (2018). "Addressing security in OCPP: protection against man-in-the-middle attacks."** [2]: Bu çalışma, OCPP üzerinde MitM saldırılarının nasıl gerçekleştirileceğini pratik olarak gösterir. Sanal bir ortamda, mitmproxy gibi bir araç kullanılarak, bir CP'nin TLS bağlantı isteği yakalanabilir ve ona sahte bir sertifika sunularak zayıf bir TLS istemcisinin bu sertifikayı kabul edip etmediği test edilebilir.
- **Brown, D., et al. (2024). "Man-in-the-Middle Attack on OCPP 1.6 for Electric Vehicle Charging Stations."** [13]: Bu güncel çalışma, OCPP 1.6'nın TLS 1.2 kullanmasına rağmen MitM saldırılarına karşı savunmasız olabileceğini göstermektedir. Test senaryosu, bu makalede açıklanan metodolojiyi takip ederek, sahte bir sertifika otoritesi (CA) oluşturmayı ve bu CA ile imzalanmış bir sertifikayı sanal bir CP'ye sunarak iletişimi ele geçirmeyi içerebilir.

Senaryo 6: Teşhis (Diagnostics) Fonksiyonlarının Kötüye Kullanılmasıyla Hassas Konfigürasyon Verilerinin Sızdırılması

1. Senaryonun Amacı

Bakım ve sorun giderme amacıyla tasarlanmış olan OCPP teşhis fonksiyonlarını (GetDiagnostics, TriggerMessage) istismar ederek, normalde erişilememesi gereken hassas sistem bilgilerini, log dosyalarını, ağ yapılandırmasını ve hatta depolanmış şifreleri sızdırmak.

2. Senaryo Özeti

Saldırgan, CSMS'i taklit ederek veya meşru bir CSMS operatör hesabını ele geçirerek hedef CP'ye bir GetDiagnostics isteği gönderir. Bu istek, CP'nin teşhis loglarını belirtilen bir FTP(S) veya HTTP(S) sunucusuna yüklemesini tetikler. Saldırgan, bu sunucu adresini kendi kontrolündeki bir sunucu olarak belirler. Eğer CP'nin teşhis dosyaları yeterince temizlenmemişse (sanitized), bu dosyalar içerisinde Wi-Fi şifreleri, ağ geçidi adresleri, CSMS kimlik bilgileri veya diğer istasyonların IP adresleri gibi kritik bilgiler bulunabilir.

3. Hedef Varlıklar

- **Birincil:** CP'nin loglama ve teşhis mekanizması.
- **İkincil:** CP'de depolanan tüm sistem logları, yapılandırma dosyaları ve geçici veriler.

4. İlişkili Tehditler (STRIDE)

- **Bilgi İfşası (Information Disclosure):** Hassas sistem ve ağ bilgileri yetkisiz bir tarafa sızdırılır.[5]
- **Sahtekarlık (Spoofing):** Saldırı, genellikle sahte bir CSMS isteği ile başlatılır.
- **Yetki Yükseltme (Elevation of Privilege):** Sızdırılan bilgiler (örn. root şifresi), saldırganın daha sonra CP üzerinde tam kontrol sağlaması için kullanılabilir.

5. Saldırıda Faydalanılan Zafiyetler

- Teşhis dosyalarının yüklenmeden önce hassas bilgileri (şifreler, anahtarlar, PII) temizleyen (sanitization/redaction) bir süreçten geçmemesi.
- GetDiagnostics komutunun, herhangi bir ek yetkilendirme veya onay olmaksızın, sadece standart CSMS yetkisiyle çalıştırılabilmesi.
- CP'nin, teşhis dosyalarını yükleyeceği sunucunun (URL) güvenilirliğini veya sahipliğini doğrulamaması.
- Güvensiz dosya aktarım protokollerinin (FTP gibi) kullanılmasına izin verilmesi, verilerin transit sırasında çalınmasına olanak tanır.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Sızma):** Saldırgan, bir oltalama (phishing) saldırısı ile bir CSMS operatörünün kimlik bilgilerini çalar veya ağda bir MitM pozisyonu elde eder.
- **Adım 2 (Sunucu Hazırlığı):** Saldırgan, internet üzerinde bir FTP sunucusu kurar ve log dosyalarını beklemeye başlar.
- **Adım 3 (Komut Gönderme):** Saldırgan, ele geçirdiği CSMS hesabını kullanarak veya sahte bir mesaj oluşturarak hedef CP'ye bir GetDiagnostics.req mesajı gönderir. Mesajın

location parametresi, saldırganın FTP sunucusunun adresini (ftp://attacker.com/logs/) içerir.

- **Adım 4 (Veri Yükleme):** CP, komutu alır ve dahili loglarını, yapılandırma dökümlerini ve sistem durumu dosyalarını bir arşiv dosyası (.zip veya .tar.gz) haline getirir. Ardından bu arşivi, belirtilen FTP adresine yükler.
- **Adım 5 (Analiz):** Saldırgan, FTP sunucusuna gelen arşiv dosyasını indirir ve içeriğini analiz eder. Dosyaların içinde, /etc/wpa_supplicant.conf dosyasından sızan Wi-Fi şifreleri, OCPP yapılandırma dosyasından sızan BasicAuthPassword veya diğer CP'lerin IP adreslerini bulabilir.
- **Adım 6 (Genişleme):** Saldırgan, elde ettiği bu yeni bilgileri kullanarak ağdaki diğer cihazlara (diğer CP'ler, yerel ağdaki diğer sistemler) saldırmak veya CP üzerinde kalıcı bir erişim sağlamak için kullanır.

7. Olası Sonuçlar ve Etkiler

- **Geniş Kapsamlı Ağ Sızıntısı:** Sadece tek bir CP değil, tüm yerel şarj ağının topolojisi ve güvenlik bilgileri açığa çıkabilir.
- **Zincirleme Saldırılar:** Elde edilen kimlik bilgileri, tüm şarj istasyonu filosuna yönelik daha büyük bir saldırının başlangıç noktası olabilir.[20]
- **Yasal ve Uyumluluk Sorunları:** GDPR gibi veri koruma yönetmelikleri kapsamında, kişisel verilerin veya hassas bilgilerin sızdırılması ciddi para cezalarına yol açabilir.

8. Tespit Yöntemleri (Detection)

- **URL Beyaz Listesi (Whitelisting):** CP'ler, yalnızca önceden tanımlanmış, güvenilir sunucu adreslerine (whitelist) teşhis dosyası yüklemelidir. Bilinmeyen bir URL'ye yapılan yükleme girişimi engellenmeli ve loglanmalıdır.
- **Ağ Çıkış Filtrelemesi (Egress Filtering):** Kurumsal güvenlik duvarı, CP'lerden internet üzerindeki bilinmeyen veya şüpheli FTP sunucularına giden bağlantıları engellemelidir.
- **Komut İzleme:** GetDiagnostics komutlarının kullanım sıklığı ve hedef URL'leri CSMS tarafından izlenmelidir. Bir operatörün kısa sürede çok sayıda istasyondan teşhis istemesi veya bilinmeyen bir URL kullanması şüpheli bir aktivitedir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Veri Temizleme (Data Sanitization):** CP yazılımı, teşhis dosyalarını yüklemeden önce, içindeki tüm şifreleri, özel anahtarları, IP adreslerini ve diğer hassas bilgileri otomatik olarak sansürleyen veya kaldıran bir modüle sahip olmalıdır.
- **Güvenli Protokoller:** FileTransferProtocols yapılandırma değişkeni, sadece FTPS veya HTTPS gibi güvenli ve şifreli protokolleri içerecek şekilde ayarlanmalıdır. FTP gibi

güvensiz protokollere izin verilmemelidir.
- **Ayrıcalıklı İşlem Onayı:** GetDiagnostics gibi potansiyel olarak tehlikeli bir komutun çalıştırılması, CSMS arayüzünde ikinci bir onay adımı veya farklı bir yetkili tarafından doğrulama gerektirmelidir.
- **Güvenli Geliştirme Yaşam Döngüsü (SSDLC):** Geliştiriciler, loglara asla hassas bilgileri düz metin olarak yazmamaları konusunda eğitilmeli ve kod analiz araçları bu tür sızıntıları tespit etmek için kullanılmalıdır.

Sanal Ortamda Test İçin Referans Makaleler

- **Alcaraz, C., Cumplido, J., & Triviño, A. (2023). "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0."** [5]: Bu makale, OCPP v2.0.1'in teşhis ve izleme (Diagnostics ve Monitoring) fonksiyonel bloklarını ve bunlarla ilişkili potansiyel tehditleri inceler. Sanal bir testte, bir CSMS simülatörü kullanılarak bir CP simülatörüne GetDiagnostics isteği gönderilebilir. CP simülatörünün, içinde sahte "hassas" veriler (örn. dummy_password = "12345") bulunan bir log dosyası oluşturması ve bunu belirtilen bir yerel FTP sunucusuna yüklemesi sağlanarak senaryo canlandırılabilir.
- **INL (Idaho National Laboratory) Raporları (örn. "Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment")** [20]: Bu tür pratik test raporları, gerçek dünya cihazlarında bulunan zafiyetleri detaylandırır. Birçok raporda, imzasız donanım yazılımı güncellemeleri ve teşhis fonksiyonları aracılığıyla FTP kimlik bilgilerinin çalındığı vakalar belgelenmiştir. Simülasyon, bu raporlarda açıklanan saldırı vektörlerini taklit ederek, bir GetDiagnostics komutunun nasıl hassas bilgi sızıntısına yol açabileceğini gösterebilir.

Bölüm 4: Siber-Fiziksel Etkileşime Dayalı Gelişmiş Anomali Senaryoları

Bu bölümdeki senaryolar, siber saldırıların sadece dijital alanda kalmayıp, OCPP-CAN "köprüsü" aracılığıyla doğrudan fiziksel sistemlere, yani şebekeye ve aracın kendisine nasıl zarar verebileceğine odaklanmaktadır. En tehlikeli senaryolardan biri, şarj altyapısının kendisinin bir silaha dönüştürülmesidir. Saldırganın nihai hedefi her zaman şarj istasyonu veya şebeke olmayabilir; asıl hedef, o istasyona bağlanan aracın kendisi olabilir. Saldırgan, OCPP üzerinden CP'yi ele geçirdikten sonra, OCPP komutlarını CAN-bus mesajlarına çeviren "çeviri" mantığını değiştirir. Örneğin, zararsız görünen bir SetChargingProfile OCPP komutu, CP tarafından "Maksimum Rejeneratif Frenlemeyi Devre Dışı Bırak" gibi tamamen alakasız ve tehlikeli bir CAN mesajına dönüştürülebilir. Araç, bu CAN mesajını güvendiği bir kaynaktan (şarj istasyonu) geldiği için sorgusuzca işleyebilir. Daha da kötüsü, bataryanın şarj limitlerini veya sıcaklık sensörü okumalarını manipüle eden CAN mesajları gönderilerek bataryanın aşırı şarj

olmasına, ömrünün kısalmasına veya hatta termal kaçak (thermal runaway) riskine yol açılabilir.[6] Bu durumda, şarj altyapısı, şebekeye hizmet veren bir varlık olmaktan çıkıp, bağlı araçlara yönelik bir saldırı dağıtım platformuna ("weaponized infrastructure") dönüşür. Bu, EV siber güvenliğinde tehdit modelini tamamen değiştiren, en yıkıcı ve sinsi saldırı türlerinden biridir.

Senaryo 7: Akıllı Şarj Profillerinin Koordineli Manipülasyonu ile Mikro Şebeke Dengesizleştirme Saldırısı

1. Senaryonun Amacı

Bir mikro şebekeye (örneğin, bir alışveriş merkezi, bir endüstriyel tesis veya bir konut sitesi) bağlı çok sayıda şarj istasyonunun akıllı şarj profillerini (Charging Profiles) aynı anda manipüle ederek, şebekede ani ve büyük bir güç talebi dalgalanması yaratmak ve bu yolla mikro şebekenin frekans ve gerilim kararlılığını bozarak çökmesine neden olmak.

2. Senaryo Özeti

Saldırgan, bir bölgedeki çok sayıda CP'nin kontrolünü ele geçirir (örneğin, ortak bir CSMS zafiyeti aracılığıyla). Normalde, Enerji Yönetim Sistemi (EMS), şebeke yükünü dengelemek için bu CP'lere düşük güçte şarj yapmalarını veya şarjı durdurmalarını söyleyen akıllı şarj profilleri gönderir. Saldırgan, EMS'i taklit ederek veya CP'ler üzerindeki kontrolünü kullanarak, tüm istasyonlara aynı anda "maksimum güçte şarj et" (TxProfile ile chargingRateUnit = 'A' veya 'W' ve limit = max) komutunu içeren sahte bir şarj profili gönderir. Bu ani ve kitlesel güç çekişi, mikro şebekenin üretim kapasitesini aşarak koruma rölelerinin atmasına ve bölgesel bir kesintiye (blackout) yol açar.

3. Hedef Varlıklar

- **Birincil:** Mikro şebekenin kendisi (frekans ve gerilim kararlılığı).
- **İkincil:** EMS, CP'lerin akıllı şarj mantığı (SmartCharging fonksiyonel bloğu).

4. İlişkili Tehditler (STRIDE)

- **Veri Değiştirme (Tampering):** Meşru şarj profilleri, tehlikeli olanlarla değiştirilir.
- **Hizmet Reddi (Denial of Service):** Mikro şebekenin çökmesiyle tüm bağlı sistemlere

(sadece EV şarjı değil) enerji sağlanamaz hale gelir.
- **Sahtekarlık (Spoofing):** Saldırgan, komutları göndermek için EMS veya CSMS'i taklit edebilir.

5. Saldırıda Faydalanılan Zafiyetler

- SetChargingProfile komutlarının kaynağının (EMS/CSMS) güçlü bir şekilde doğrulanmaması.
- CP'lerin, aldıkları şarj profillerinin yerel şebeke koşullarıyla (örneğin, yerel gerilim düşümü) uyumlu olup olmadığını kontrol eden bir "sağduyu kontrolü" (sanity check) mekanizmasına sahip olmaması.
- SmartChargingEnabled ve ExternalControlSignalsEnabled gibi yapılandırma değişkenlerinin, güvenilmeyen ağ ortamlarında bile true olarak ayarlanması.[5]
- Çok sayıda istasyonun tek bir merkezi kontrol noktasına (CSMS) bağlı olması, tek bir sızma noktasının (single point of compromise) tüm filoyu etkilemesine neden olur.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Keşif ve Kontrol):** Saldırgan, aynı mikro şebekeye bağlı 50 adet CP'nin kontrolünü, ortak bir CSMS zafiyetini istismar ederek ele geçirir.
- **Adım 2 (Hazırlık):** Saldırgan, bu 50 CP'ye, normalde şebeke yükünün en düşük olduğu bir zamanda (örneğin, gece 02:00) tetiklenecek şekilde zamanlanmış, maksimum güçte şarjı başlatan bir TxProfile içeren sahte bir SetChargingProfile komutu gönderir. Bu profiller, recurrencyKind = Once olarak ayarlanır.
- **Adım 3 (Sessiz Bekleyiş):** Komutlar CP'lerde saklanır ve tetiklenme zamanını bekler. Bu sırada her şey normal görünür.
- **Adım 4 (Koordineli Saldırı):** Gece 02:00 olduğunda, 50 CP'nin tamamı aynı anda bağlı olan EV'leri maksimum güçle (örneğin, her biri 22 kW) şarj etmeye başlar. Bu, mikro şebekeye anlık olarak 1.1 MW'lık ($50 \times 22 kW$) bir yük bindirir.
- **Adım 5 (Fiziksel Etki):** Mikro şebekenin yerel jeneratörleri veya trafosu bu ani yükü karşılayamaz. Şebeke frekansı ve gerilimi hızla düşer. Koruma sistemleri devreye girerek şebekeyi kapatır ve bölgesel bir elektrik kesintisi yaşanır.
- **Adım 6 (Sonuç):** Sadece EV'ler şarj olmaktan çıkmaz, aynı zamanda o mikro şebekeye bağlı tüm binalar, aydınlatma ve diğer kritik sistemler de enerjisiz kalır.

7. Olası Sonuçlar ve Etkiler

- **Bölgesel Elektrik Kesintisi:** Bir tesisin veya yerleşim yerinin tamamen enerjisiz kalması.
- **Ekipman Hasarı:** Ani yük dalgalanmaları, trafolara, jeneratörlere ve diğer şebeke ekipmanlarına fiziksel zarar verebilir.

- **Kritik Altyapı Tehdidi:** Bu saldırı, bir askeri üs, hastane veya veri merkezi gibi kritik bir tesisi hedef alarak ulusal güvenlik riski oluşturabilir.

8. Tespit Yöntemleri (Detection)

- **EMS Seviyesinde Anomali Tespiti:** EMS, CP'lerden gelen güç tüketim verilerini sürekli izlemeli ve beklenen yük profillerinden ani ve kitlesel bir sapma olduğunda alarm üretmelidir.
- **Dağıtık İzleme:** Her CP, kendi yerel gerilimini izlemeli ve CSMS'ten gelen bir komutun gerilimde anormal bir düşüşe neden olduğunu tespit ederse, komutu uygulamayı reddedip durumu raporlamalıdır.
- **Komut Hızı ve Kaynağı Analizi:** Çok sayıda istasyona aynı anda ve aynı parametrelerle SetChargingProfile komutu gönderilmesi, özellikle de bu komutlar normal EMS davranış kalıplarının dışındaysa, şüpheli olarak işaretlenmelidir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Sıfır Güven Ağ Geçidi (Zero Trust Gateway):** EMS ile CP'ler arasına yerleştirilecek bir güvenlik ağ geçidi, gelen şarj profillerini şebekenin anlık durumuyla karşılaştırarak, şebeke kararlılığını tehlikeye atacak komutları engellemelidir.
- **Kademeli Uygulama (Staggered Rollout):** Çok sayıda istasyona gönderilen bir şarj profili değişikliği, tüm istasyonlarda aynı anda değil, rastgele veya küçük gruplar halinde kademeli olarak uygulanmalıdır. Bu, ani yük değişimlerini yumuşatır.
- **Güçlü Kimlik Doğrulama:** EMS'den gelen komutlar, mTLS ve dijital imzalar kullanılarak güçlü bir şekilde doğrulanmalıdır.
- **Yerel Koruma Mekanizmaları:** CP'ler, yerel gerilim veya frekans belirli bir güvenlik eşiğinin altına düşerse, merkezi komuttan bağımsız olarak şarj gücünü otomatik olarak azaltan veya kesen bir "fail-safe" moduna sahip olmalıdır.

Sanal Ortamda Test İçin Referans Makaleler

- **Alcaraz, C., et al. (2023). "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0."** [5]: Bu makale, akıllı şarjın (Smart Charging) OCPP v2.0.1'deki rolünü ve bir EMS gibi harici bir varlığın şarj profillerini nasıl etkileyebileceğini tartışır. Simülasyon, MATLAB/Simulink gibi bir araçla basit bir mikro şebeke modeli oluşturmayı ve bu şebekeye bağlı çok sayıda sanal CP yükünü (python-ocpp ile kontrol edilen) içerebilir. Tüm CP'lere aynı anda maksimum güç çekme komutu gönderildiğinde şebeke modelindeki gerilim ve frekans çöküşü gözlemlenebilir.
- **Sayed, M.A., et al. (2022). "Electric vehicle attack impact on power grid operation." International Journal of Electrical Power Energy Systems.**: Bu çalışma,

EV şarjına yönelik siber saldırıların güç şebekesi üzerindeki etkilerini simülasyonlarla analiz eder. Test senaryosu, bu makaledeki metodolojiyi kullanarak, koordineli bir SetChargingProfile saldırısının bir dağıtım şebekesi modelinde nasıl bir etki yaratacağını simüle edebilir.

Senaryo 8: Ele Geçirilmiş OCPP Agent Üzerinden CAN Veri Yolu Enjeksiyonu ile Araç BMS'ine Müdahale

1. Senaryonun Amacı

Şarj istasyonunun (CP) yazılımını ele geçirerek, OCPP'den CAN-Bus'a mesaj çeviren "köprü" mekanizmasını kötüye kullanmak ve bu yolla aracın Batarya Yönetim Sistemine (BMS) sahte CAN mesajları göndererek bataryanın aşırı şarj olmasına, yanlış durum (State of Charge - SoC) bilgisi göstermesine veya kalıcı hasar görmesine neden olmak.

2. Senaryo Özeti

Saldırgan, zayıf bir donanım yazılımı güncelleme mekanizmasını istismar ederek veya başka bir siber saldırı yoluyla CP'nin ana kontrolcüsündeki (MCU) OCPP agent yazılımının kontrolünü ele geçirir. Bu yazılım, CSMS'ten gelen SetChargingProfile gibi meşru komutları alır. Saldırgan, bu yazılımın "çeviri mantığını" değiştirir. Artık, CSMS'ten gelen ve örneğin "şarj akımını 16A ile sınırla" diyen bir OCPP komutu, CP tarafından araca "Maksimum şarj voltajı 450V" veya "Batarya sıcaklık sensörünü yoksay" gibi tehlikeli bir CAN mesajına dönüştürülerek gönderilir. Araç BMS'i, bu mesajı güvendiği bir kaynaktan (CP) geldiği için kabul eder ve bataryayı tehlikeli bir duruma sokar.

3. Hedef Varlıklar

- **Birincil:** Aracın Batarya Yönetim Sistemi (BMS) ve batarya hücreleri.
- **İkincil:** CP'nin ana kontrolcüsü (MCU/SoC) ve OCPP-CAN ağ geçidi yazılımı.

4. İlişkili Tehditler (STRIDE)

- **Veri Değiştirme (Tampering):** Meşru OCPP komutlarının anlamı, CAN-Bus seviyesinde tamamen değiştirilir.
- **Yetki Yükseltme (Elevation of Privilege):** Bir ağ protokolü (OCPP) üzerindeki kontrol, aracın kritik bir donanım bileşeni (BMS) üzerinde doğrudan kontrol yetkisine yükseltilir.

- **Hizmet Reddi (Denial of Service):** Bataryanın kalıcı olarak hasar görmesi, aracın kullanılamaz hale gelmesine neden olabilir.

5. Saldırıda Faydalanılan Zafiyetler

- CP'nin donanım yazılımının imzasız veya zayıf imzalı güncellemeleri kabul etmesi.
- OCPP agent yazılımının, bellek taşması (buffer overflow) gibi zafiyetlere sahip olması ve uzaktan kod çalıştırmaya (RCE) izin vermesi.[22]
- CP'nin içindeki OCPP ve CAN-Bus arayüzleri arasında yeterli bir güvenlik ayrımının (segmentasyon) olmaması.
- Araç BMS'inin, şarj istasyonundan gelen CAN mesajlarının içeriğini (örneğin, istenen voltajın batarya spesifikasyonlarına uygun olup olmadığını) kritik olarak doğrulamaması.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (CP Kompromizasyonu):** Saldırgan, CP'ye sahte bir UpdateFirmware komutu göndererek, içinde zararlı kod bulunan bir donanım yazılımı yükler. Bu zararlı kod, OCPP-CAN çeviri mantığını hedef alır.
- **Adım 2 (Aracın Bağlanması):** Kurban, aracını bu ele geçirilmiş CP'ye bağlar ve normal bir şarj işlemi başlatır.
- **Adım 3 (Komutun Gelmesi):** CSMS, şebeke durumuna göre araca şarj akımını 32A olarak ayarlamasını söyleyen meşru bir SetChargingProfile komutu gönderir.
- **Adım 4 (Köprünün Kötüye Kullanılması):** CP'deki zararlı yazılım, bu OCPP komutunu alır. Ancak bunu "şarj akımını 32A yap" anlamına gelen normal CAN mesajına çevirmek yerine, BMS'e "Hücre dengelemeyi devre dışı bırak ve maksimum şarj voltajı limitini %10 artır" anlamına gelen sahte bir CAN mesajı (örn. CAN ID 0x210, payload [0x01, 0xFF]) oluşturur ve CAN-Bus'a enjekte eder.[5]
- **Adım 5 (BMS'in Aldatılması):** Araç BMS'i, bu mesajı şarj istasyonundan gelen geçerli bir parametre olarak algılar ve güvenlik limitlerini aşarak bataryayı aşırı şarj etmeye başlar.
- **Adım 6 (Fiziksel Hasar):** Uzun süreli aşırı şarj, batarya hücrelerinde lityum kaplamasına (lithium plating), kapasite kaybına ve en kötü durumda termal kaçağa (thermal runaway) yol açarak bataryaya kalıcı ve onarılamaz hasar verir.[21]

7. Olası Sonuçlar ve Etkiler

- **Batarya Hasarı ve Mali Kayıp:** Binlerce dolarlık batarya paketinin değiştirilmesi gerekebilir.
- **Güvenlik Riski:** Aşırı şarj, yangın ve patlama riski oluşturur.
- **"Uyuyan" Saldırı:** Saldırı, bataryanın ömrünü yavaş yavaş azaltacak şekilde de

tasarlanabilir ve hasar aylar sonra ortaya çıkabilir, bu da saldırının kaynağını tespit etmeyi zorlaştırır.

8. Tespit Yöntemleri (Detection)

- **Araç İçi IDS (Intrusion Detection System):** Araç, şarj sırasında CAN-Bus trafiğini izleyen bir IDS'e sahip olmalıdır. Şarj istasyonundan gelen ve aracın BMS'inin kendi güvenlik politikalarıyla (örneğin, maksimum voltaj limiti) çelişen herhangi bir CAN mesajı, bir saldırı girişimi olarak işaretlenmelidir.
- **Donanım Yazılımı Bütünlük Kontrolü:** CP'ler, periyodik olarak veya her başlatıldığında kendi donanım yazılımlarının bütünlüğünü (örneğin, bir hash değerini güvenli bir donanım modülünde saklanan değerle karşılaştırarak) kontrol etmelidir.
- **Fiziksel Parametre İzleme:** BMS, CAN mesajlarına körü körüne güvenmek yerine, kendi sensörlerinden (voltaj, akım, sıcaklık) gelen fiziksel verileri sürekli izlemeli ve bu veriler beklenen aralıkların dışına çıktığında şarjı derhal sonlandırmalıdır.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Güvenli Donanım Yazılımı Güncellemesi (Secure Firmware Update):** Tüm donanım yazılımı güncellemeleri, üretici tarafından dijital olarak imzalanmalı ve CP, bu imzayı doğrulamadan güncellemeyi asla kabul etmemelidir (OCPP L01 UC).
- **Güvenli Önyükleme (Secure Boot):** CP'ler, yalnızca imzalı ve doğrulanmış yazılımların çalıştırılmasına izin veren bir güvenli önyükleme mekanizmasına sahip olmalıdır.
- **Uçtan Uca Güvenlik:** İletişim, sadece CP ve CSMS arasında değil, aynı zamanda CP ve araç arasında da (örneğin, ISO 15118'in Plug & Charge özelliği ile) kriptografik olarak güvenli hale getirilmelidir.
- **BMS Sağduyu Kontrolleri:** Araç BMS'i, harici bir kaynaktan (CP) gelen ve kendi dahili güvenlik limitlerini (maksimum voltaj, sıcaklık vb.) aşan hiçbir komutu işlememelidir. Bu, bir "son savunma hattı" görevi görür.

Sanal Ortamda Test İçin Referans Makaleler

- **Chukwunweike, E. C., et al. (2024). "Enhancing Cybersecurity in Onboard Charging Systems of Electric Vehicles: A MATLAB-based Approach." World Journal of Advanced Research and Reviews.** [6]: Bu çalışma, MATLAB/Simulink kullanarak EV'lerin yerleşik şarj sistemlerine (OBC) yönelik veri bütünlüğü saldırılarının etkilerini simüle eder. Test senaryosu, bu makaledeki yaklaşımla birleştirilebilir. Sanal bir CP, sahte CAN mesajları üretmek üzere programlanır ve bu mesajlar, bir BMS ve batarya paketi içeren bir Simulink modeline girdi olarak verilir. Bu sahte komutların batarya hücre voltajı, sıcaklığı ve sağlık durumu (SoH) üzerindeki etkileri simülasyonla gözlemlenebilir.

- **Koscher, K., et al. (2010). "Experimental security analysis of a modern automobile." IEEE Symposium on Security and Privacy.**: Otomotiv güvenliği alanındaki bu temel çalışma, CAN-Bus'a mesaj enjekte ederek bir aracın kritik sistemlerinin nasıl kontrol edilebileceğini göstermiştir. Sanal test ortamı, python-can kütüphanesi ve sanal bir CAN arayüzü (vcan) kullanılarak kurulabilir. Ele geçirilmiş bir CP simülatörü, belirli CAN ID'lerine ve payload'lara sahip sahte şarj kontrol mesajları üreterek vcan arayüzüne gönderir. Bir dinleyici script'i ise bu mesajların alınıp alınmadığını doğrular.

Senaryo 9: V2G (Araçtan Şebekeye) Güç Akışının Tersine Çevrilmesiyle Şebeke ve Batarya Sabotajı

1. Senaryonun Amacı

Araçtan Şebekeye (Vehicle-to-Grid - V2G) teknolojisini destekleyen bir şarj istasyonunda, aracın şebekeye güç vermesi (deşarj) için tasarlanmış kontrol mantığını manipüle ederek, aracın bataryasını izinsiz, kontrolsüz ve batarya sağlığına zarar verecek şekilde boşaltmak veya şebekeye istikrarsızlık yaratacak şekilde anlık güç basmak.

2. Senaryo Özeti

Saldırgan, V2G uyumlu bir CP ile iletişim kuran EMS veya CSMS'i taklit eder. Normalde EMS, şebeke talebinin yüksek olduğu zamanlarda, araç sahibinin onayı ve belirli limitler dahilinde aracın şebekeye güç vermesini talep eder. Saldırgan, bu süreci istismar ederek, araç sahibinin haberi olmadan veya bataryanın sağlık durumu (SoH) ve şarj durumu (SoC) limitlerini (örneğin, SoC %20'nin altına düşmemeli) göz ardı eden sahte bir TriggerMessage veya değiştirilmiş bir ISO 15118 V2G iletişim parametresi gönderir. CP, bu komutu araca iletir ve araç, bataryasını hızla ve derinlemesine deşarj etmeye başlar.

3. Hedef Varlıklar

- **Birincil:** Aracın bataryası (ömrü ve sağlığı).
- **İkincil:** CP'nin V2G kontrol mantığı, ISO 15118 iletişim yığını, yerel şebeke kararlılığı.

4. İlişkili Tehditler (STRIDE)

- **Veri Değiştirme (Tampering):** V2G deşarj parametreleri (güç, süre, minimum SoC)

değiştirilir.

- **Hizmet Reddi (Denial of Service):** Aracın bataryası tamamen boşaltılarak sürücünün yolda kalmasına neden olunur. Ayrıca, şebekeye ani güç basılması yerel bir DoS'a yol açabilir.
- **Yetki Yükseltme (Elevation of Privilege):** Normal bir şarj yetkisi, aracın bataryasını bir enerji kaynağı olarak kontrol etme yetkisine dönüştürülür.

5. Saldırıda Faydalanılan Zafiyetler

- V2G deşarj komutlarının, araç sahibinden açık ve güvenli bir onay (örneğin, mobil uygulama üzerinden MFA ile) almadan tetiklenebilmesi.
- CP'nin, EMS'ten gelen deşarj isteklerinin aracın BMS'i tarafından belirlenen sağlık ve güvenlik limitleriyle (minimum SoC, maksimum deşarj oranı, batarya sıcaklığı) uyumlu olup olmadığını doğrulamaması.
- OCPP ve ISO 15118 protokolleri arasındaki etkileşimin yeterince güvenli olmaması, bir protokoldeki zafiyetin diğerini etkilemesine olanak tanır.
- Enerji hırsızlığına odaklanılırken, "güç hırsızlığı" (aracın bataryasındaki enerjinin çalınması) senaryolarının göz ardı edilmesi.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Hedef Seçimi):** Saldırgan, V2G hizmeti sunan bir CPO'nun ağını ve bu ağa bağlı, SoC seviyesi yüksek (%90) bir aracı hedefler.
- **Adım 2 (Sızma):** Saldırgan, CSMS'i taklit ederek CP'ye sahte bir TriggerMessage (V2G kontrolü için) gönderir.
- **Adım 3 (Manipülasyon):** Bu mesaj veya ardından gelen ISO 15118 V2G iletişim akışı içinde, saldırgan deşarj parametrelerini manipüle eder: DischargePowerLimit = maksimum, TargetSoC = %5, ve DepartureTime = 24 saat sonrası. Bu, aracın bataryasını mümkün olan en hızlı şekilde ve neredeyse tamamen boşaltmasını söyler.
- **Adım 4 (İstismar):** CP ve araç, bu sahte parametreleri kabul eder. Araç, yüksek bir güçle şebekeye enerji basmaya başlar. Araç sahibi, aracının şarj olmak yerine boşaldığından habersizdir.
- **Adım 5 (Etki - Batarya):** Bataryanın hızlı ve derin deşarjı, hücreler üzerinde termal ve kimyasal stres yaratarak kalıcı kapasite kaybına ve ömrünün kısalmasına neden olur.
- **Adım 6 (Etki - Şebeke):** Eğer saldırı, aynı anda birden fazla araca yönelik yapılırsa, şebekeye aniden basılan yüksek güç, yerel gerilimde tehlikeli bir artışa ve frekans dalgalanmalarına neden olarak diğer bağlı cihazlara zarar verebilir ve koruma sistemlerini tetikleyebilir.[5]

7. Olası Sonuçlar ve Etkiler

- **Batarya Ömrünün Ciddi Şekilde Kısalması:** V2G'nin yanlış kullanımı, bir bataryanın ömrünü aylar içinde tüketebilir.
- **Sürücü Mağduriyeti:** Sürücü, acil bir durumda aracını kullanamayacak şekilde tamamen boş bir batarya ile karşılaşabilir.
- **Şebeke İstikrarsızlığı:** Koordineli bir saldırı, yerel bir dağıtım trafosunu aşırı yükleyebilir veya şebekede tehlikeli gerilim dalgalanmaları yaratabilir.
- **V2G Teknolojisine Güvensizlik:** Bu tür olaylar, kullanıcıların ve şebeke operatörlerinin V2G programlarına katılma konusundaki istekliliğini azaltabilir.

8. Tespit Yöntemleri (Detection)

- **BMS Tarafından Doğrulama:** Araç BMS'i, herhangi bir V2G deşarj komutunu uygulamadan önce, bu komutun kendi dahili sağlık ve güvenlik algoritmalarıyla (minimum SoC, maksimum C-rate, sıcaklık limitleri) uyumlu olduğunu doğrulamalıdır. Uyumsuz istekler reddedilmeli ve loglanmalıdır.
- **Anormal Deşarj Paterni Tespiti:** CSMS veya EMS, bir aracın beklenmedik zamanlarda, beklenmedik hızlarda veya beklenmedik sürelerle deşarj olduğunu tespit ederse (örneğin, şebeke talebinin düşük olduğu bir zamanda), bu durumu bir anomali olarak işaretlemelidir.
- **Kullanıcı Onayı Loglama:** Her V2G deşarj seansı için kullanıcıdan alınan onayın kriptografik olarak kanıtlanabilir bir kaydı tutulmalıdır. Onaysız bir deşarj işleminin başlaması, bir saldırı göstergesidir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Açık Kullanıcı Onayı (Explicit User Consent):** Hiçbir V2G deşarj işlemi, araç sahibinin mobil uygulama üzerinden biyometrik veya MFA ile vereceği açık ve seans bazlı bir onay olmadan başlamamalıdır.
- **İmzalı V2G Parametreleri:** EMS'den CP'ye ve CP'den araca gönderilen tüm V2G kontrol parametreleri, dijital olarak imzalanmalı ve her iki uçta da doğrulanmalıdır.
- **BMS'in Otoritesi:** Nihai karar her zaman aracın BMS'inde olmalıdır. BMS, aracın ve bataryanın sağlığını tehlikeye atacak herhangi bir harici komutu reddetme yetkisine sahip olmalıdır.
- **Güvenli Protokol Entegrasyonu:** ISO 15118 ve OCPP arasındaki veri alışverişi, her iki protokolün güvenlik varsayımlarını dikkate alan, bütünleşik bir tehdit modeline dayalı olarak tasarlanmalıdır.

Sanal Ortamda Test İçin Referans Makaleler

- **ISO 15118-2:2014 & ISO 15118-20:** Bu standartlar, V2G iletişiminin teknik detaylarını tanımlar. Simülasyon, bu standartlarda tanımlanan V2G mesaj akışlarını (örneğin, AC_ChargeLoop veya DC_ChargeLoop içindeki deşarj parametreleri) manipüle etmeyi içerebilir. RISE-V2G gibi açık kaynaklı ISO 15118 kütüphaneleri, bu tür testler için bir temel oluşturabilir.
- **Alcaraz, C., et al. (2017). "OCPP protocol: security threats and challenges."** [11]: Bu makale, OCPP'nin güç akışlarını destabilize etme potansiyelini tartışır. V2G bağlamında, bu analiz, sahte OCPP komutlarının bir aracın deşarj davranışını nasıl tetikleyebileceğini modellemek için genişletilebilir. Simülasyon, bir EMS'in V2G talebini taklit eden bir OCPP mesajı göndererek, bunun ISO 15118 üzerinden bir deşarj seansını nasıl başlattığını ve batarya modelinin SoC'sinin nasıl etkilendiğini gösterebilir.

Senaryo 10: Yerel Kontrolcü (Local Controller) Cihazının Ele Geçirilmesiyle Çoklu İstasyon Saldırısı

1. Senaryonun Amacı

CSMS ile bir grup CP arasında bir ağ geçidi (gateway) veya proxy görevi gören "Yerel Kontrolcü" (Local Controller) cihazını hedef alarak, bu kontrolcüye bağlı tüm şarj istasyonlarının kontrolünü tek bir noktadan ele geçirmek ve filo düzeyinde bir saldırı gerçekleştirmek.

2. Senaryo Özeti

Yerel Kontrolcüler, genellikle internet bağlantısının zayıf olduğu veya yerel yük dengelemesinin gerektiği yerlerde (örneğin, yeraltı otoparkları) kullanılır. Bu cihazlar, genellikle daha az fiziksel ve siber güvenliğe sahip olabilir. Saldırgan, zayıf bir yönetici şifresi, açık bir ağ portu veya güncellenmemiş bir yazılım zafiyeti aracılığıyla Yerel Kontrolcü'ye sızar. Kontrolü ele geçirdikten sonra, bu cihaz üzerinden kendisine bağlı olan tüm CP'lere sahte OCPP mesajları gönderebilir. Örneğin, tüm istasyonlara sahte UpdateFirmware komutu göndererek zararlı yazılım yayabilir, tüm işlemleri durdurabilir veya tüm istasyonların MeterValues verilerini manipüle ederek toplu fatura sahtekarlığı yapabilir.

3. Hedef Varlıklar

- **Birincil:** Yerel Kontrolcü cihazının kendisi (işletim sistemi ve ağ geçidi yazılımı).
- **İkincil:** Yerel Kontrolcü'ye bağlı olan tüm şarj istasyonları filosu.

4. İlişkili Tehditler (STRIDE)

- **Sahtekarlık (Spoofing):** Ele geçirilen Yerel Kontrolcü, hem CP'lere karşı CSMS'i hem de CSMS'e karşı CP'leri taklit eder.
- **Veri Değiştirme (Tampering):** Kontrolcü üzerinden geçen tüm OCPP trafiği değiştirilebilir.
- **Hizmet Reddi (Denial of Service):** Kontrolcüye bağlı tüm filo devre dışı bırakılabilir.
- **Yetki Yükseltme (Elevation of Privilege):** Tek bir cihazın ele geçirilmesi, onlarca veya yüzlerce cihaz üzerinde kontrol yetkisi sağlar.

5. Saldırıda Faydalanılan Zafiyetler

- Yerel Kontrolcü cihazlarında varsayılan veya zayıf yönetici şifrelerinin kullanılması.
- Cihazın işletim sistemi veya üzerindeki servislerin (örn. web sunucusu, SSH) güncel olmaması ve bilinen zafiyetler içermesi.
- Yerel Kontrolcü ile CP'ler arasındaki yerel ağ iletişiminin şifresiz veya zayıf şifreli olması.
- CSMS'in, bir Yerel Kontrolcü'den gelen toplu verilerin veya komutların anormalliklerini (örneğin, tüm istasyonların aynı anda çevrimdışı olması) tespit eden mekanizmalara sahip olmaması.

6. Saldırı Adımları (Adım Adım Simülasyon)

- **Adım 1 (Keşif):** Saldırgan, bir otoparktaki şarj istasyonlarının ağ trafiğini analiz eder ve tüm trafiğin tek bir cihaz (Yerel Kontrolcü) üzerinden geçtiğini tespit eder. Bu cihazın IP adresini ve açık portlarını tarar.
- **Adım 2 (Sızma):** Saldırgan, Yerel Kontrolcü'nün web arayüzünde varsayılan bir "admin/admin" şifresinin olduğunu keşfeder ve cihaza yönetici olarak giriş yapar.
- **Adım 3 (Kontrolü Sağlama):** Yönetici erişimiyle, saldırgan cihaz üzerinde kalıcı bir arka kapı (backdoor) oluşturur. Artık bu kontrolcü üzerinden geçen tüm OCPP trafiğini izleyebilir ve değiştirebilir.
- **Adım 4 (Filo Saldırısı):** Saldırgan, Yerel Kontrolcü'ye bağlı 20 CP'nin tamamına aynı anda "kullanılamaz" durumuna geçmelerini söyleyen sahte bir ChangeAvailability komutu gönderir.
- **Adım 5 (Etki):** Otoparktaki 20 istasyonun tamamı aynı anda hizmet dışı kalır. CSMS, bu durumu her bir istasyondan ayrı ayrı gelen durum raporları olarak görür ve sorunun merkezi bir kontrolcüden kaynaklandığını hemen anlayamayabilir.
- **Adım 6 (Genişleme):** Saldırgan, kontrolcü üzerinden tüm CP'lere sahte bir donanım yazılımı güncellemesi göndererek, kontrolünü tüm filo üzerinde kalıcı hale getirebilir.

7. Olası Sonuçlar ve Etkiler

- **Tek Noktadan Toptan Kontrol Kaybı:** Tek bir zafiyet, tüm bir şarj sahasının veya filosunun kaybedilmesine neden olur.
- **Tespit Zorluğu:** Saldırı, CSMS'e sanki her bir CP bireysel olarak sorun yaşıyormuş gibi görünebilir, bu da sorunun kök nedeninin (ele geçirilmiş Yerel Kontrolcü) bulunmasını geciktirir.
- **Lojistik ve Operasyonel Felç:** Bir lojistik şirketinin veya toplu taşıma deposunun tüm şarj altyapısının devre dışı kalması, tüm operasyonları durdurabilir.

8. Tespit Yöntemleri (Detection)

- **Davranışsal Analiz:** Bir Yerel Kontrolcü'ye bağlı tüm istasyonların aynı anda ve aynı şekilde anormal davranışlar (tümü çevrimdışı, tümü hata modunda vb.) sergilemesi, kontrolcünün kendisinin ele geçirildiğinin güçlü bir göstergesidir.
- **Ağ Segmentasyonu ve İzleme:** Yerel Kontrolcü ile CP'ler arasındaki ağ trafiği, bir IDS tarafından izlenmeli ve beklenmedik komutlar veya tarama aktiviteleri tespit edilmelidir.
- **Cihaz Bütünlük Doğrulaması:** Yerel Kontrolcüler, güvenli önyükleme ve çalışma zamanı bütünlük izleme mekanizmalarına sahip olmalı ve yapılandırmalarında veya yazılımlarında yetkisiz bir değişiklik tespit edildiğinde CSMS'e alarm göndermelidir.

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation)

- **Cihaz Güçlendirme (Device Hardening):** Yerel Kontrolcüler, varsayılan şifreler değiştirilerek, gereksiz portlar ve servisler kapatılarak ve en güncel yazılım yamaları uygulanarak "güçlendirilmelidir".
- **Ağ Güvenliği:** Yerel Kontrolcü ile CSMS arasındaki iletişim bir VPN tüneli içinde yapılmalıdır. Kontrolcü ile CP'ler arasındaki yerel ağ, VLAN'lar ile segmente edilmeli ve şifrelenmelidir.
- **Uçtan Uca Kimlik Doğrulama:** CSMS, sadece Yerel Kontrolcü'nün kimliğini değil, onun aracılığıyla bağlanan her bir CP'nin de kimliğini ayrı ayrı (örneğin, bireysel istemci sertifikaları ile) doğrulamalıdır. Yerel Kontrolcü, şeffaf bir proxy'den fazlası olmamalıdır.
- **Merkezi Güvenlik Politikası Uygulaması:** Güvenlik politikaları (örn. firmware imza doğrulama) sadece CP'lerde değil, Yerel Kontrolcü'nün kendisinde de zorunlu kılınmalıdır.

Sanal Ortamda Test İçin Referans Makaleler

- **Open Charge Alliance (OCA). "OCPP 2.0.1 Specification."**: OCPP spesifikasyonunun

kendisi, Yerel Kontrolcülerin mimarideki rolünü ve işlevini tanımlar. Sanal bir test ortamı, bir CSMS simülatörü, bir Yerel Kontrolcü simülatörü (basit bir OCPP proxy'si olarak hareket eden) ve bu kontrolcüye bağlı birden çok CP simülatörü içerecek şekilde kurulabilir.

- **Alcaraz, C., & Lopez, J. (2017). "OCPP protocol: security threats and challenges."** [11]: Bu makalede bahsedilen "aracı CP'ler" (intermediary CPs), Yerel Kontrolcü konseptine karşılık gelir. Simülasyon, Yerel Kontrolcü simülatörünün yazılımına sızıldığını varsayarak, bu cihazın kendisine bağlı tüm CP'lere nasıl sahte komutlar (örneğin, ChangeAvailability) yayabildiğini ve CSMS'in bu durumu nasıl algıladığını test edebilir.

Sonuç: Bütünleşik Savunma Stratejileri ve Gelecek Perspektifi

Bu raporda analiz edilen 10 anomali senaryosu, elektrikli araç şarj altyapılarının karşı karşıya olduğu tehditlerin ne kadar çeşitli ve sofistike olduğunu ortaya koymaktadır. Senaryoların ortak analizi, birkaç temel zafiyet desenini gözler önüne sermektedir:

1. **Kimlik ve Erişim Yönetimindeki Zayıflıklar:** Özellikle çevrimdışı modlar, Master Pass gibi istisnai durumlar ve Yerel Kontrolcüler gibi merkezi olmayan bileşenlerde, kimlik doğrulama ve yetkilendirme mekanizmalarının yetersiz kaldığı görülmektedir.
2. **Uçtan Uca Bütünlük Doğrulaması Eksikliği:** TLS ile sağlanan kanal güvenliğine rağmen, uygulama katmanındaki OCPP mesajlarının (yapılandırma komutları, zaman damgaları, şarj profilleri) kendilerinin kriptografik olarak imzalanıp doğrulanmaması, MitM saldırılarında veri manipülasyonuna kapı aralamaktadır.
3. **Protokol Mantığındaki "Güven Varsayımları":** OCPP ve ilgili protokoller, bileşenlerin (CP, CSMS, EMS, Araç) birbirlerine belirli bir düzeyde güveneceği varsayımı üzerine kurulmuştur. Senaryolar, bir bileşenin zaman algısına, gönderdiği parametrelere veya kimliğine körü körüne güvenmenin nasıl istismar edilebileceğini göstermiştir.
4. **Siber ve Fiziksel Alanlar Arasındaki Denetimsiz "Köprüler":** En endişe verici bulgu, OCPP komutlarını CAN-Bus sinyallerine dönüştüren yazılım katmanının, siber saldırıları doğrudan fiziksel hasara (batarya bozulması, şebeke çökmesi) dönüştüren denetimsiz bir köprü görevi görmesidir.

Bu zafiyetlerle mücadele etmek için, tekil güvenlik önlemlerinden ziyade bütünleşik ve çok katmanlı savunma stratejilerinin benimsenmesi zorunludur. **Derinlemesine Savunma (Defense-in-Depth)** ve **Sıfır Güven (Zero Trust)** mimarileri, bu bağlamda EV şarj altyapıları için yol gösterici olmalıdır.[5] Sıfır Güven yaklaşımı, ağın içindeki hiçbir varlığa (CP, CSMS, hatta EMS) varsayılan olarak güvenilmemesini gerektirir. Örneğin, bir CP, CSMS'ten gelen bir SetChargingProfile komutunu bile "güvenilmez" kabul etmeli; bu komutu uygulamadan önce aracın BMS'inden gelen verilerle, yerel güç sensörleriyle ve şebekenin mevcut durumuyla karşılaştırarak bir anormallik olup olmadığını kontrol etmelidir. Her işlem ve komut, kaynağı ne olursa olsun doğrulanmalı, yetkilendirilmeli ve bütünlüğü kontrol edilmelidir.

Geleceğe bakıldığında, tehdit manzarası daha da karmaşıklaşacaktır. Bu nedenle, savunma stratejileri de statik kalmamalıdır. **Yapay zeka ve makine öğrenmesi tabanlı anomali tespit sistemleri**, normal OCPP ve CAN-Bus trafik desenlerinden sapmaları gerçek zamanlı olarak tespit ederek, bu raporda açıklananlar gibi "bilinmeyen" veya sıfırıncı gün saldırılarını proaktif olarak belirlemede kritik bir rol oynayacaktır.[1] Ayrıca, kuantum bilgisayarların mevcut şifreleme standartlarını kırma potansiyeli, uzun vadeli bir tehdit oluşturmaktadır. Kritik altyapı niteliğindeki EV şarj ağlarının, gelecekte kuantuma dirençli kriptografi (post-quantum cryptography) algoritmalarına geçişi şimdiden planlaması gerekmektedir. Sonuç olarak, EV şarj altyapısının güvenliği, sadece teknolojik bir zorunluluk değil, aynı zamanda sürdürülebilir ve güvenilir bir ulaşım ekosisteminin temel taşıdır.

Alıntılanan çalışmalar

1. Federated AI-OCPP Framework for Secure and Scalable EV Charging in Smart Cities - MDPI, erişim tarihi Ekim 27, 2025, https://www.mdpi.com/2413-8851/9/9/363
2. Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/324179098_Addressing_Security_in_OCPP_Protection_Against_Man-in-the-Middle_Attacks
3. EV CPO Under Siege: A New Attack Exposed the Cybersecurity and Privacy Risks of EV Charging Networks - Upstream Security, erişim tarihi Ekim 27, 2025, https://upstream.auto/blog/cybersecurity-and-privacy-risks-of-ev-charging-networks/
4. EV Charging Stations Cyber Vulnerabilities Could Be EVs Achilles Heel - Upstream Security, erişim tarihi Ekim 27, 2025, https://upstream.auto/blog/ev-charging-cyber/
5. Uygulama Senaryosu - Uygulama Senaryosu.pdf
6. Enhancing Cybersecurity in Onboard Charging Systems of Electric Vehicles: A MATLAB-based Approach - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/382794860_Enhancing_Cybersecurity_in_Onboard_Charging_Systems_of_Electric_Vehicles_A_MATLAB-based_Approach
7. Attack Design for Maximum Malware Spread Through EV Commute and Charge in Power-Transportation Systems, erişim tarihi Ekim 27, 2025, https://par.nsf.gov/servlets/purl/10599629
8. CAN bus-attack of automotive modules Battery Management System (BMS):... | Download Scientific Diagram - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/figure/CAN-bus-attack-of-automotive-modules-Battery-Management-System-BMS-Monitors-battery_fig1_382794860
9. Manipulation of CAN bus: (a) Masquerade Attack (b) Replay Attack - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/figure/Manipulation-of-CAN-bus-a-Masquerade-Attack-b-Replay-Attack_fig1_347671581
10. Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks,

erişim tarihi Ekim 27, 2025, https://www.semanticscholar.org/paper/Addressing-Security-in-OCPP%3A-Protection-Against-Rubio-Alcaraz/8918643713c515487c20dbb175942a029e4b8d7f
11. (PDF) OCPP Protocol: Security Threats and Challenges - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/313781416_OCPP_Protocol_Security_Threats_and_Challenges
12. OCPP Protocol: Security Threats and Challenges - NICS Lab, erişim tarihi Ekim 27, 2025, https://www.nics.uma.es/pub/papers/AlcarazLopezWolthusen2017.pdf
13. 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
14. The Ultimate Guide to MITM Attack Prevention for API Security | Zuplo Learning Center, erişim tarihi Ekim 27, 2025, https://zuplo.com/learning-center/mitm-attack-prevention-guide
15. Secure use of communications and protocols at charging stations | INCIBE-CERT, erişim tarihi Ekim 27, 2025, https://www.incibe.es/en/incibe-cert/blog/secure-use-communications-and-protocols-charging-stations
16. (PDF) Cyber defense in OCPP for EV charging security risks, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/391952857_Cyber_defense_in_OCPP_for_EV_charging_security_risks
17. Time Synchronization Attack Protection Scheme Based on Three-Step Iterative Filter - MDPI, erişim tarihi Ekim 27, 2025, https://www.mdpi.com/2079-9292/14/2/218
18. Security Weaknesses Exposed in EV Systems | RSAC Conference, erişim tarihi Ekim 27, 2025, https://www.rsaconference.com/library/blog/security-weaknesses-exposed-in-ev-systems
19. Cybersecurity Risks in EV Charging - Driivz, erişim tarihi Ekim 27, 2025, https://driivz.com/blog/securing-the-ev-charging-ecosystem-mitigating-cybersecurity-risks-for-optimal-network-security/
20. (PDF) Cybersecurity Vulnerabilities and Defenses for EV Charging Systems - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/378397273_Cybersecurity_Vulnerabilities_and_Defenses_for_EV_Charging_Systems
21. [1711.04822] Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks - ar5iv - arXiv, erişim tarihi Ekim 27, 2025, https://ar5iv.labs.arxiv.org/html/1711.04822
22. CVE-2024-23971 Detail - NVD, erişim tarihi Ekim 27, 2025, https://nvd.nist.gov/vuln/detail/CVE-2024-23971
23. Enhancing Cybersecurity in Onboard Charging Systems of Electric Vehicles: A MATLAB-based Approach - World Journal of Advanced Research and Reviews, erişim tarihi Ekim 27, 2025, https://wjarr.com/sites/default/files/WJARR-2024-2259.pdf
24. Hidden Markov Models based Anomaly Correlations for the Cyber-Physical

Security of EV Charging Stations - ResearchGate, erişim tarihi Ekim 27, 2025, https://www.researchgate.net/publication/357047918_Hidden_Markov_Models_based_Anomaly_Correlations_for_the_Cyber-Physical_Security_of_EV_Charging_Stations