

BİLGİ SİSTEMLERİ VE GÜVENLİĞİ

GRUP-2

Elektrikli Araç Şarj Altyapısı:
Güvenlik Anomalileri ve Risk Analizi

Tarih
04/11/2025

 github.com/BSG-Project





EKİBİMİZ

 02 AHMET POLAT

 12 MERT KÖROĞLU

 22 MEHMET BULUT

 32 MUHAMMED KARTAL

 42 MUHAMMED ERYILMAZ

 52 MUHAMMET YUSUF BAŞÇI

 62 MUHAMMED AZEM GÖKÇER

 72 İLAYDA NUR UÇAR

 82 İSHAK KARATAŞ

 92 YUNUS EMRE ŞİMŞEK

 102 DOĞUKAN ALPEREN

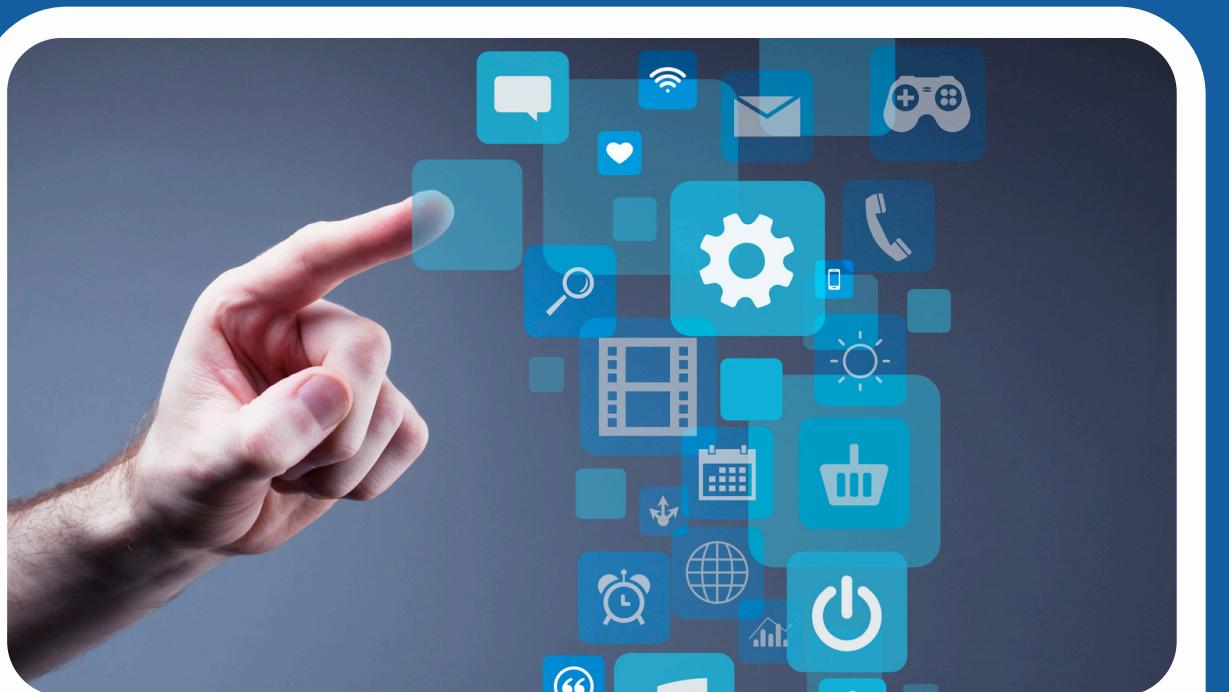
 112 AHMET EMİR ÇETİN

 122 MEHMET ONUR BOYRAZ

Süreç Yönetimi



Toplantı Takvimi



Kullanılan Araçlar



**Değerlendirme
Tablosu**

Toplantı Takvimi

Yapılan Toplantılar

Toplantı
1

20.10.2025
Pazartesi 15.15-16.30

Toplantı
2

27.10.2025
Pazartesi 15.15-16.30

Toplantı
3

03.11.2025
Pazartesi 15.15-16.30



Toplantı Takvimi

Yapılan Toplantılar

Toplantı
1

20.10.2025
Pazartesi 15.15-16.30

Toplantı
2

27.10.2025
Pazartesi 15.15-16.30

Toplantı
3

03.11.2025
Pazartesi 15.15-16.30



Toplantı Takvimi

Katılım Durumları

02 205541032 AHMET POLAT
12 215541025 MERT KÖROĞLU
22 225541043 MEHMET BULUT
32 225541604 MUHAMMED KARTAL
42 235541011 MUHAMMED ERYILMAZ
52 235541023 MUHAMMET YUSUF BAŞÇI

62 235541038 MUHAMMED AZEM GÖKÇER
72 235541054 İLAYDA NUR UÇAR
82 235541073 İSHAK KARATAŞ
92 235541095 YUNUS EMRE ŞİMŞEK
102 235541129 DOĞUKAN ALPEREN
112 235542012 AHMET EMİR ÇETİN
122 245541023 MEHMET ONUR BOYRAZ

20.10.2025 Pazartesi 15.15 Toplantı katılımı

27.10.2025 pazartesi 15.15 Toplantı katılım yoklaması

- 02 205541032 AHMET POLAT
- 12 215541025 MERT KÖROĞLU
- 22 225541043 MEHMET BULUT
- 32 225541604 MUHAMMED KARTAL
- 42 235541011 MUHAMMED ERYILMAZ
- 52 235541023 M. YUSUF BAŞÇI
- 62 235541038 M. AZEM GÖKÇER
- 72 235541054 İLAYDA NUR UÇAR
- 82 235541073 İSHAK KARATAŞ
- 92 235541095 YUNUS EMRE ŞİMŞEK
- 102 235541129 DOĞUKAN ALPEREN (il dışında)
- 112 235542012 AHMET EMİR ÇETİN
- 122 245541023 M. ONUR BOYRAZ

03.11.2025 pazartesi 15.15 Toplantı katılım yoklaması

- 02 205541032 AHMET POLAT
- 12 215541025 MERT KÖROĞLU
- 22 225541043 MEHMET BULUT
- 32 225541604 MUHAMMED KARTAL
- 42 235541011 MUHAMMED ERYILMAZ
- 52 235541023 M. YUSUF BAŞÇI
- 62 235541038 M. AZEM GÖKÇER
- 72 235541054 İLAYDA NUR UÇAR
- 82 235541073 İSHAK KARATAŞ
- 92 235541095 YUNUS EMRE ŞİMŞEK Rahatsızlanmış
- 102 235541129 DOĞUKAN ALPEREN (il dışında)
- 112 235542012 AHMET EMİR ÇETİN
- 122 245541023 M. ONUR BOYRAZ

Kullanılan Araçlar

Trello

The screenshot shows the Trello application interface with three boards:

- Yapılacaklar** (Yellow):
 - MEHMET BULUT-1
 - MUHAMMED KARTAL -1
 - M. AZEM GÖKÇER-1
 - İLAYDA NUR UÇAR-1
 - DOĞUKAN ALPEREN-1
 - AHMET EMİR ÇETİN-1
- Yapılıyor** (Green):
 - MEHMET ONUR BOYRAZ-1
 - İSHAK KARATAŞ-1
 - MERT KÖROĞLU-1
 - YUNUS EMRE ŞİMŞEK-1
 - MUHAMMED ERYILMAZ-1
 - M. YUSUF BAŞÇI-1
- Tamamlandı** (Dark Green):
 - + Kart ekle

At the bottom of the Trello board, there are buttons for "Gelen Kutusu", "Planlayıcı", "Pano" (highlighted in blue), and "Panoları değiştir".



Kullanılan Araçlar

Github

Organization permissions (1)

- Members (11)
- Outside collaborators
- Pending collaborators
- Invitations
- Failed invitations
- Security Managers

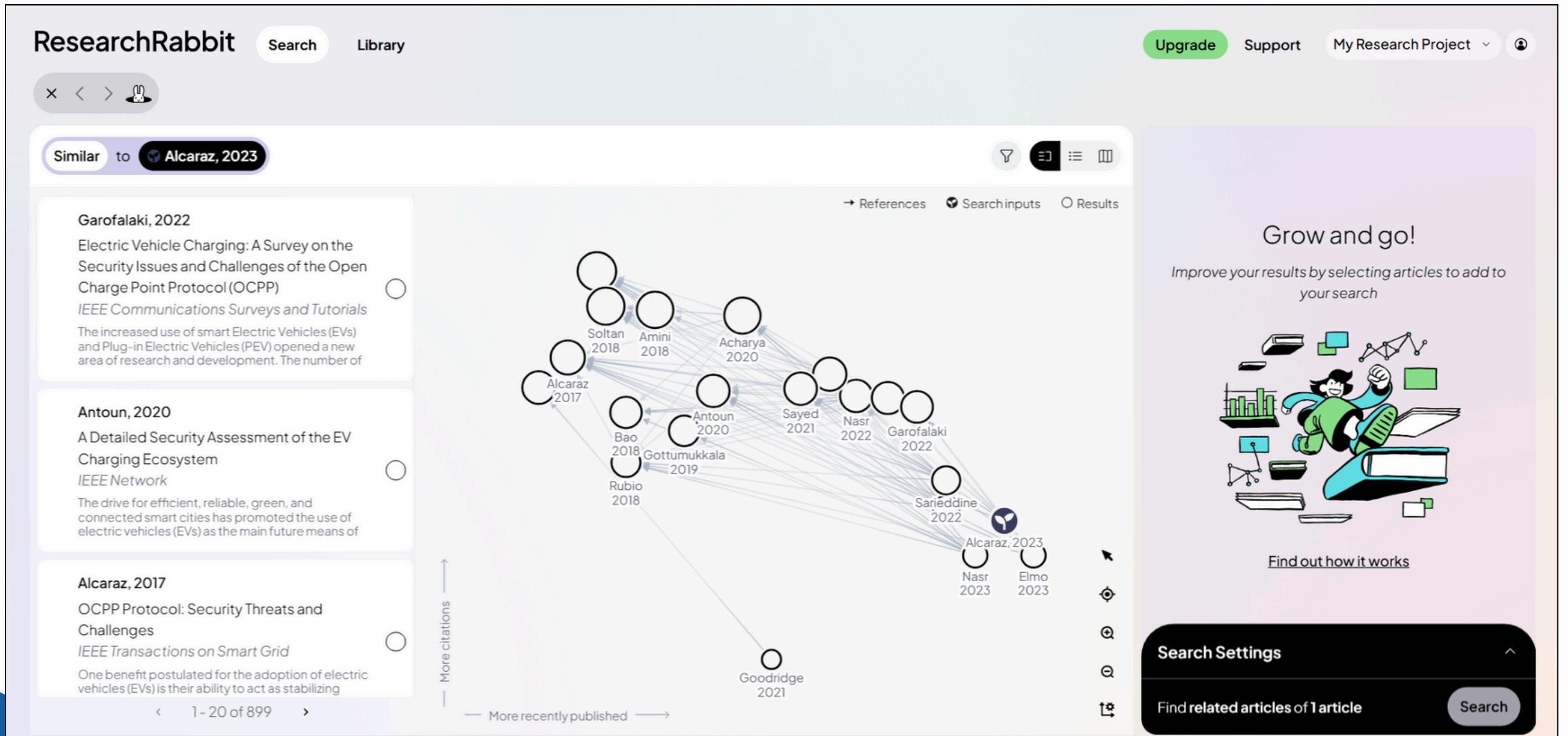
Member	2FA	Private	Role	Teams	...
AhmetEmirCetin	2FA	Private	Member	0 teams	1 role
DogukanAlperen	2FA	Private	Member	0 teams	0 roles
İlayda Nur	2FA	Private	Member	0 teams	0 roles
İshak KARATAŞ	2FA	Private	Owner	0 teams	1 role
JUZOSAN	2FA	Private	Member	0 teams	1 role
Mert Koroğlu	2FA	Private	Owner	0 teams	0 roles
MuhammedAzem	2FA	Private	Member	0 teams	0 roles

 github.com/BSG-Project



Kullanılan Araçlar

ResearchRabbit



Değerlendirme Tablosu: 20.10.2025-27.10.2025

Hafta-1

HAFTA 1	Sıra	Değerlendirme Maddesi	Odak Alanı	Kanıt Kaynağı	Öğrenci Sıra No:	2	12	22	32	42	52	62	72	82	92	102	112	122
	1	Proje için oluşturulan GitHub deposuna daveti kabul etti ve 27.10.2025 saat 23:59'a kadar başarıyla katılım sağladı.	Teknik Katılım (GitHub)	GitHub Üye Listesi/Kayıt Tarihi		Y	T	Y	T	T	T	T	T	T	T	T	T	T
	2	Proje için oluşturulan Trello panosuna katıldı ve panoda kart oluşturması gerçekleştirdi.	Proje Yönetimi (Trello)	Trello Üye Listesi ve Pano Tarihçesi (Listeyi Oluşturan Kişi)		Y	T	Y	T	T	T	Y	T	T	T	T	T	T
	3	ResearchRabbit aracı üzerinden atanın makaleyi bulduğunu ve en az 1 adet ek ilgili makaleyi araca kaydettiğini gösteren kanıtı (ekran görüntüsü veya dosya) Drive/E-posta yoluyla paylaştı.	Araştırma Süreci Başlangıcı	Paylaşılan Kanıtın Zaman Damgası		Y	T	Y	T	T	T	Y	T	T	T	T	T	T
	4	WhatsApp grubu üzerinden, hafta boyunca yapılan tüm duyuru ve tartışmalara (toplantı saati, görev tanımı vb.) aktif olarak yanıt verdi ve Hafta içinde yapılan son toplantıya (mazereti onaylananlar hariç) katıldı.	İletişim Disiplini	WhatsApp/İletişim Kanalı Mesaj Kayıtları		Y	T	Y	T	T	T	Y	T	T	T	T	T	T
	5	Hafta boyunca hazırladığı tüm bireysel çalışmaları (Makale başlığı, SWOT taslağı, vb.) 27.10.2025 saat 23:59'a kadar GitHub'daki ilgili klasöre ve Google Docs/Drive Yükleme Tarihi	Doküman Yönetimi ve Teslim	GitHub Commit Tarihi ve Google Docs/Drive Yükleme Tarihi		Y	T	Y	T	T	T	Y	T	T	T	T	T	T
		her madde 2 puan	Alınan toplam puan:	0	10	0	10	10	10	2	10	10	10	10	10	10	10	10

T: tamamladı Y: yapmadı

Değerlendirme Tablosu:

Hafta-3

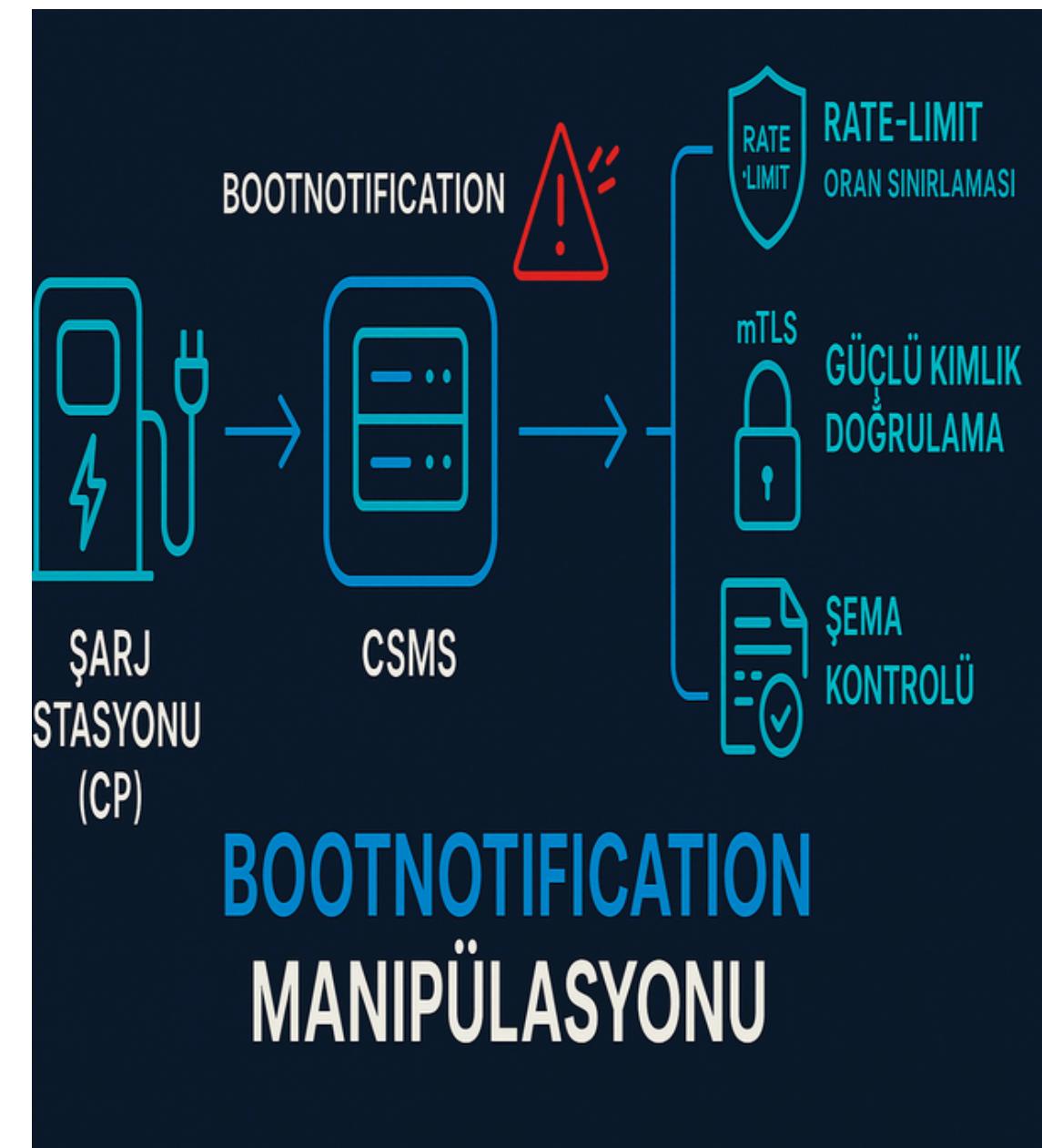




ANOMALİ SENARYOLARI

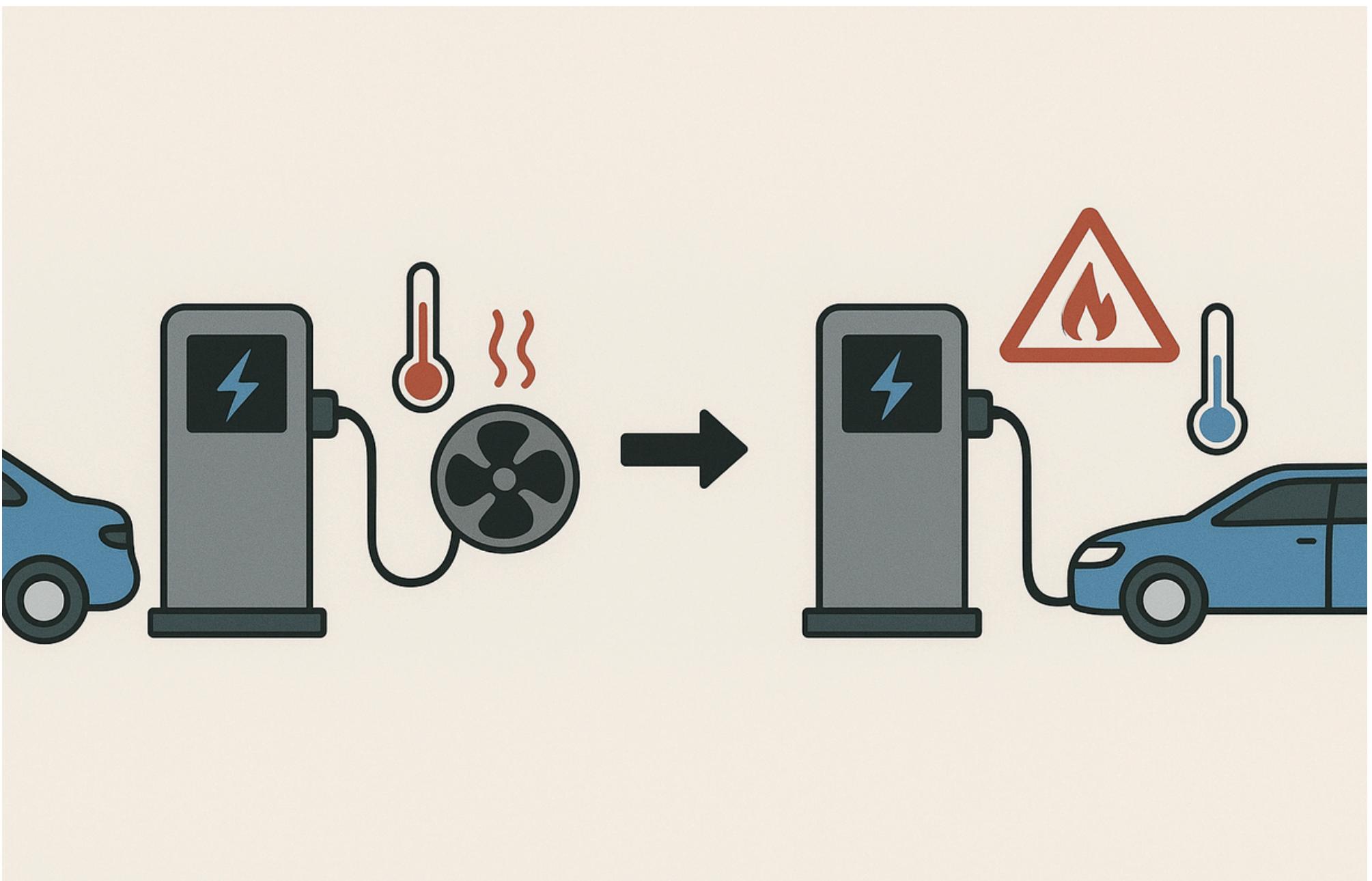
Bootnotification Anomali Senaryosu

BootNotification, istasyonun açılışta OCPP ile CSMS'e kendini tanıttığı kaydolma adımıdır; saldırgan bu adımı "BootNotification manipülasyonu" ile kötüye kullanarak model/üretici/seri numarası/firmware gibi alanları hatalı, aşırı uzun veya beklenmedik değerlerle, ya da çok sık/tekrarlı göndererek kayıt ve zamanlama mantığını bozabilir. Sonuçta istasyonlar yanlış kimlikle kaydedilebilir, heartbeat aralıkları sapar, komut/oturum başlatma hataları ve hatta hizmet reddi (DoS) oluşabilir. Tespit için açılış mesajlarındaki alanları katı şema ve tip/uzunluk kontrolleriyle doğrulamak, duplicate/idempotency kontrolleri uygulamak ve anormal sıklık/pattern'leri (rate-limit, throttling) izlemek gereklidir. Ek olarak mTLS ile güclü kimlik doğrulama, hatalı kayıt denemelerinde otomatik uyarı ve karantina, anomalı log korelasyonu (BootNotification ↔ bağlantı/heartbeat/komut başarısızlıkları) önerilir.



Ters Soğutma Döngüsü Anomalisi (RCLA)

Bu anomali, elektrikli araç şarj istasyonunun soğutma sisteminin sıcaklık verilerini yanlış yorumlamasıyla oluşur. Bazı durumlarda cihaz soğukken kendini sıcak zanneder ve fanlarını gereksiz yere çalıştırarak enerji israfına ve donanım yıpranmasına neden olur. Daha tehlikeli olan ters durumda ise cihaz ısınmış olmasına rağmen kendini soğuk algılar; fanlar devreye girmez, iç sıcaklık hızla yükselir ve güç modüllerinde kalıcı hasar veya yanın riski ortaya çıkar. Kısaca, cihaz çevresini doğru okuyamadığında – ya gereksiz soğutur, ya da hiç soğutmaz. Her iki durumda da sistem kararlılığı ve donanım ömrü ciddi biçimde etkilenir.

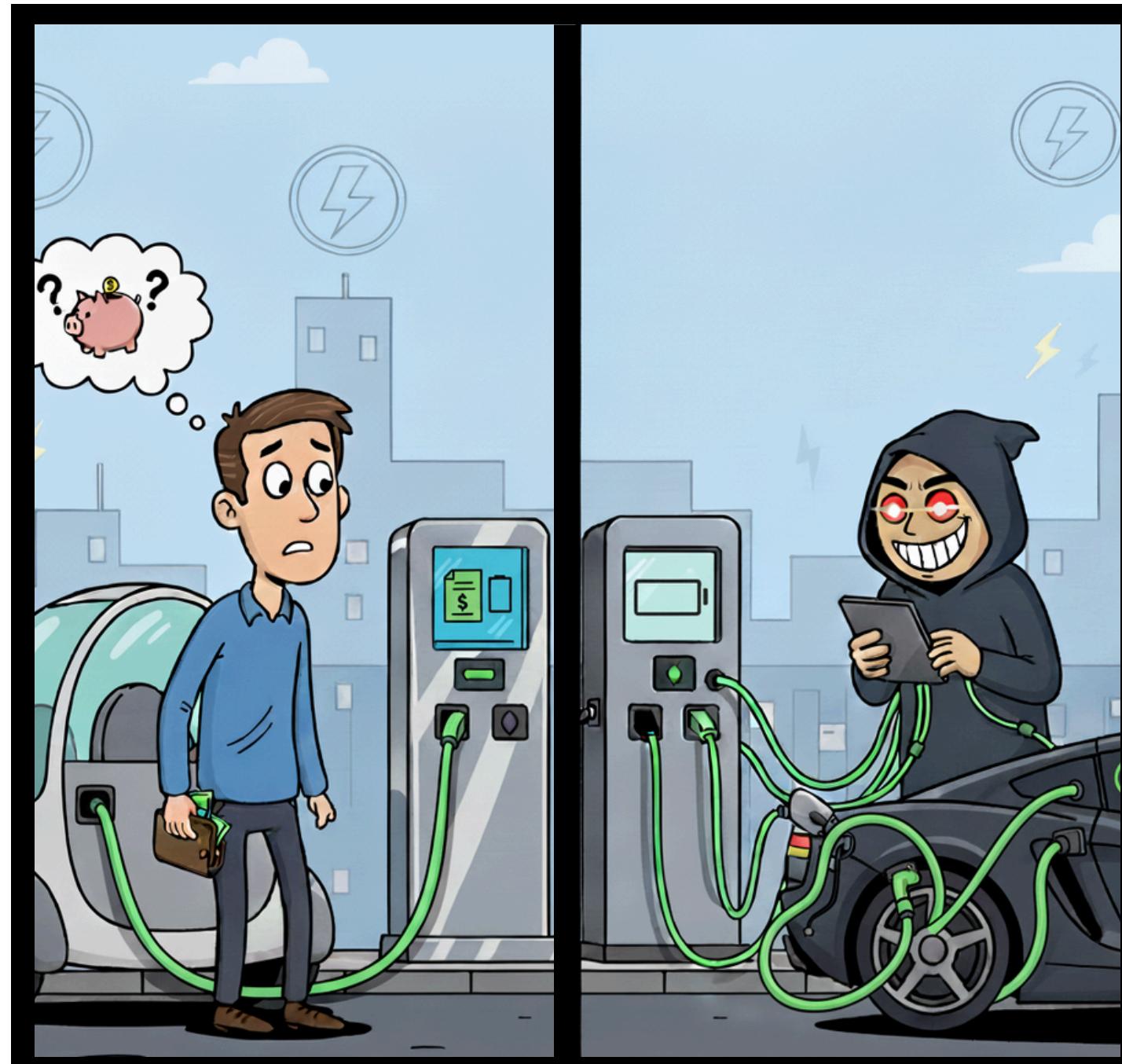


Fatura Yönlendirme Anomali Senaryosu

Bu senaryoda,

- OCPP tabanlı şarj altyapısında Man-in-the-Middle konumlanan saldırgan, kurban istasyonun (CP1) Authorize mesajından idTag bilgisini çalıyor ve aynı anda saldırganın eriştiği şarj istasyonu (CP2) CSMS'e CP1 gibi tanıtmak için BootNotification'ı manipüle ediyor (spoofing).
- Böylece CSMS, CP2'den gelen StartTransaction'ı kurbanın idTag'ıyla ve CP1'miş gibi kabul ediyor; şarj işlemi CP2'de gerçekleşirken fatura kurbana yansıyor.

Simülasyon, proxy ile mesaj yakalama/değiştirme, idTag hırsızlığı ve işlem yönlendirmeyi uçtan uca göstererek, zayıf TLS/kimlik doğrulama ve yetersiz korelasyon (idTag-IP) kontrollerinin finansal suistimale nasıl yol açabileceğini ortaya koyuyor.

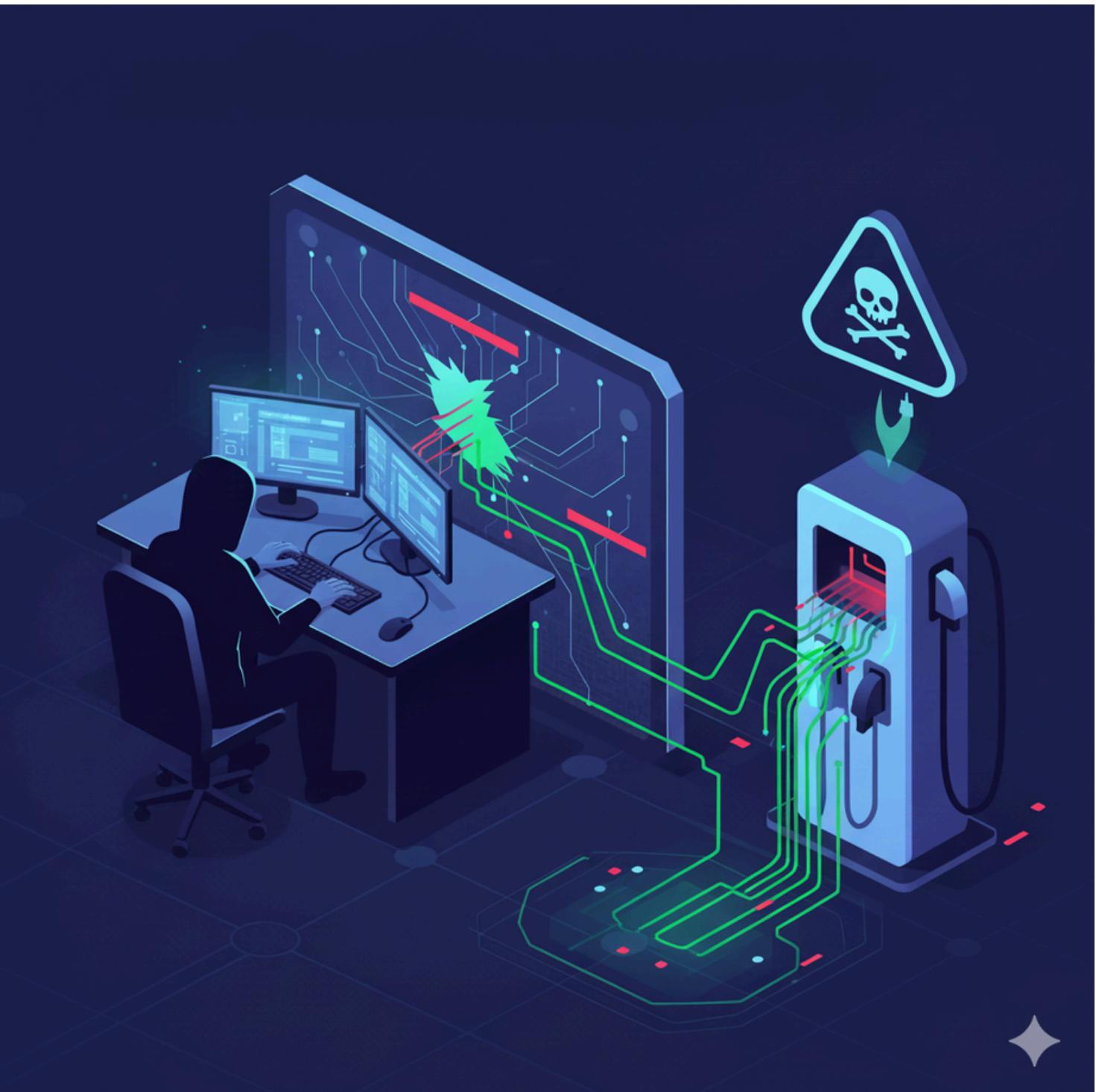


Diagnostic Fonksiyonlarının Kötüye Kullanılmasıyla Hassas Konfigürasyon Verilerinin Sızdırılması:

bu senaryo, bir saldırganın, elektrikli araç şarj istasyonlarının (CP) meşru bir bakım fonksiyonu olan OCPP GetDiagnostics komutunu nasıl istismar edebileceğini anlatıyor.

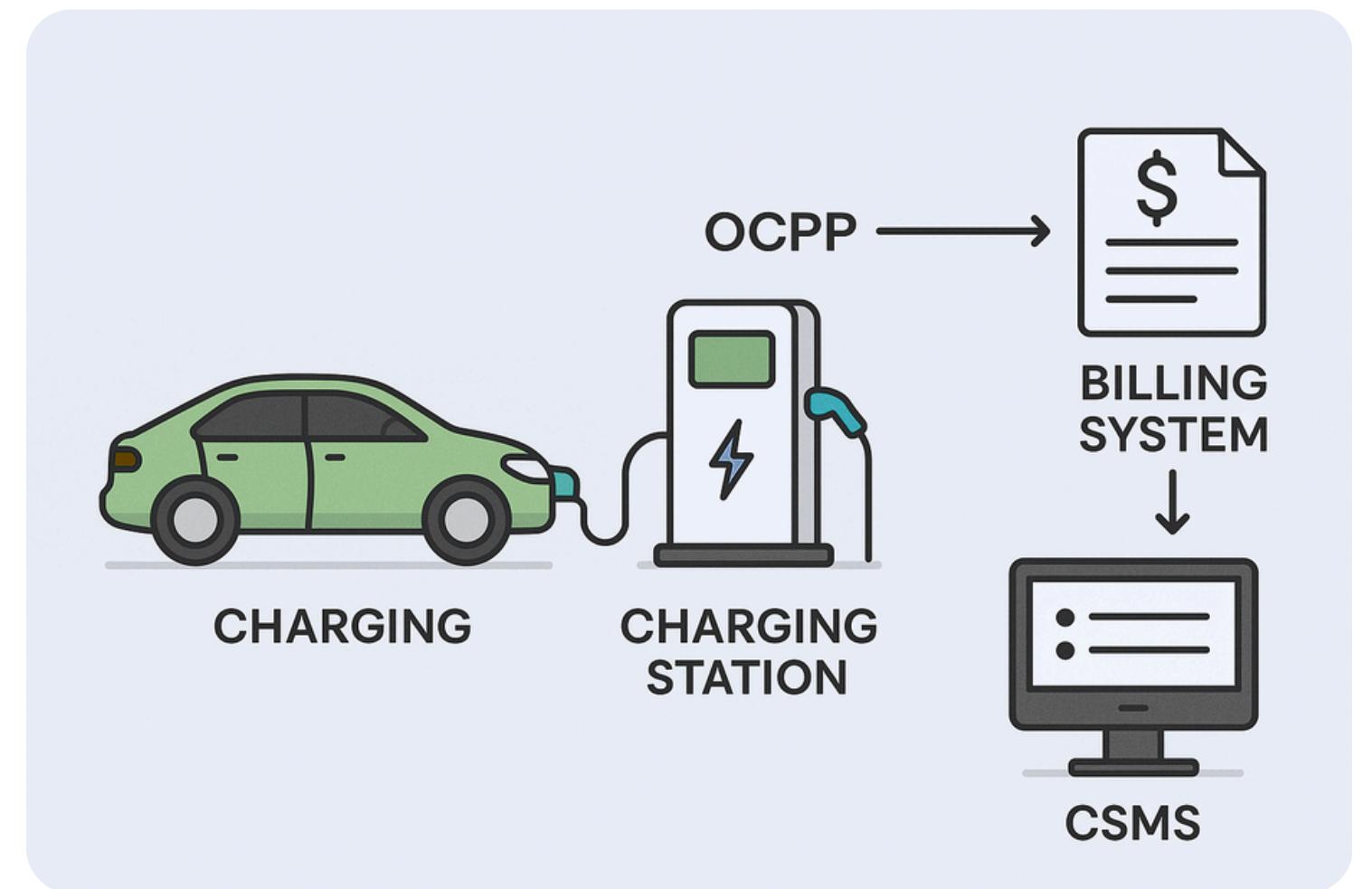
Saldırı şu adımlarla gerçekleşir:

1. İlk Erişim: Saldırgan, bir Merkezi Sistem (CSMS) operatörünün hesabını ele geçirir veya ağı dinleyerek (MitM) araya girer.
2. Komut Gönderme: Saldırgan, bu hesabı kullanarak hedef şarj istasyonuna bir GetDiagnostics isteği gönderir. Bu istek, istasyona "tüm teşhis loglarını topla ve benim kontrolümdeki şu sunucu adresine yükle" talimatını verir.
3. Zafiyet (Veri Temizleme Eksikliği): Eğer şarj istasyonunun yazılımı, bu log dosyalarını göndermeden önce içerdikleri Wi-Fi şifreleri, ağ ayarları, parolalar veya diğer hassas bilgileri "temizlemiyorsa" (sanitization/sansürleme), tüm bu veriler olduğu gibi paketlenir.
4. Veri Sızıntısı: Şarj istasyonu, bu hassas bilgileri içeren log dosyasını, saldırganın belirttiği sunucuya yükler.
5. Sonuç: Saldırgan, normalde asla erişememesi gereken kritik sistem bilgilerini ele geçirir.



Akıllı Sözleşme Tabanlı Ödeme Uyuşmazlığı

Bu senaryoda şarj işleminin tutarı, blokzincir üzerinde çalışan akıllı sözleşmeler (smart contract-based settlement) tarafından otomatik hesaplanmaktadır. Bu hesaplama kulanılan fiyat ve tüketim verileri, harici veri sağlayıcılar (oracle data feeds) üzerinden geldiği için bu veriler yanlış gönderilirse sistem hatalı ücret çıkarabilir. Böyle bir durumda kullanıcı gerçekten tükettiğinden fazla ödeme yapabilir ya da saldırgan düşük tüketim göstererek haksız kazanç sağlayabilir; yani ödeme mekanizması manipüle edilir. Bu anomalinin tespiti için OCPP üzerinden gelen sayaç bilgileri, zincir üzerindeki ödeme kayıtlarıyla karşılaştırılarak uyumsuzluk durumlarında sistem otomatik uyarı üretmelidir. Ayrıca işlem sıralaması manipülasyonları (transaction ordering / MEV attacks) gibi blok içi avantaj kazanma girişimlerine karşı da ek güvenlik kontrolleri uygulanmalıdır.



Anomali Senaryosu

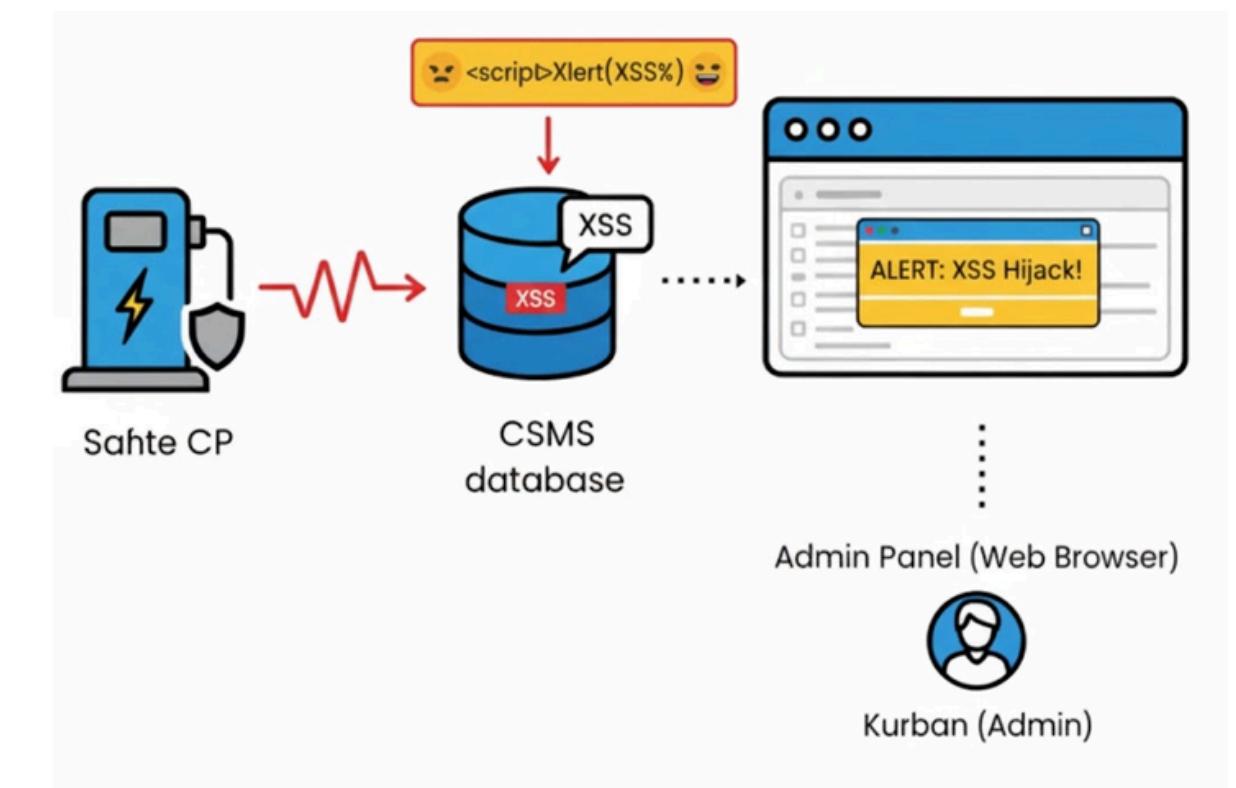
Bu senaryo, **IoT Protokol Verisine Kör Güven** duyulmasından kaynaklanan, protokol ve web uygulama katmanlarının kesişimindeki hibrit bir güvenlik açığını kanıtlar.

1. Enjeksiyon ve Kalıcılık (Truva Atı)

- Saldırgan, sahte bir **Şarj İstasyonu (CP)** rolü üstlenir.
- Standart **OCPP BootNotification** mesajının model veya seri no alanına **kötü amaçlı JavaScript (Kalıcı XSS Payload)** yerleştirir.
- CSMS (SteVe), bu zehirli veriyi veritabanına kalıcı olarak kaydeder.

2. Tetikleme ve İstismar

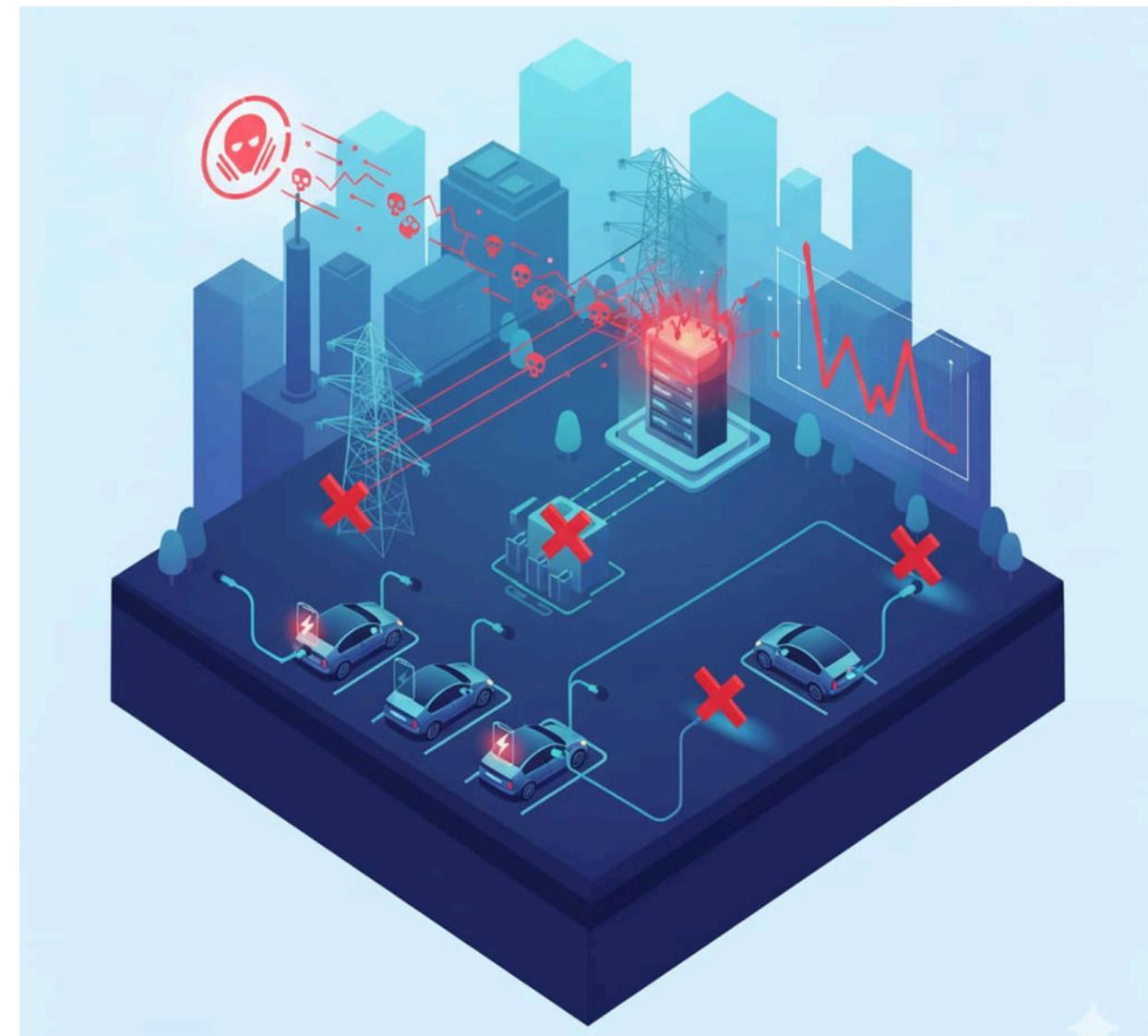
- Sistem Yöneticisi (Admin), **CSMS** Yönetici Paneline girer ve "Şarj İstasyonları" listesini açar.
- Yöneticinin web tarayıcısı, veritabanından gelen temizlenmemiş kodu çalıştırır.
- **Sonuç:** Yönetici oturumu ele geçirilir, sistemin gizliliği ve bütünlüğü bozulur.



Anı Yük Düşürme Saldırı Senaryosu

"Anı Yük Düşürme Saldırısı" , elektrikli araç (EV) şarj altyapılarına yönelik kritik bir siber güvenlik açığıdır. Saldırganlar, şarj istasyonlarının yönetim sistemlerine sizarak binlerce araca aynı anda "şarjı durdur" komutu gönderir. Bu eylem, enerji şebekesinde ani ve tehlikeli bir yük azalması (load drop) yaratarak enerji dengesini bozar.

Bu kitlesel komut, şebeke kararlılığını tehdit eder ve ani gerilim dalgalarlarına, kritik cihaz hasarlarına veya bölgesel elektrik kesintilerine yol açabilir. Bu anomali, Makine Öğrenmesi modelleriyle veya zaman serisi analiziyle tespit edilebilir. Önlenmesi için ise güçlü kimlik doğrulama ve iletişim kanallarının şifrelenmesi gibi tedbirler zorunludur.



MeterValue Kurcalaması Anomali Senaryosu

MeterValue Kurcalaması, elektrikli araç (EV) şarj altyapılarında yönelik kritik bir siber güvenlik açığıdır. Saldırganlar, şarj istasyonu (CP) ile yönetim sistemi (CSMS) arasındaki iletişime araya girerek, enerji tüketim verilerini manipüle ederler. Bu eylem, faturalama sistemini yanıltarak yetkisiz şarj başlatma, akım limiti manipülasyonu veya faturalama bozulması yaratır.

Bu senaryoda saldırgan, Man-in-the-Middle (MitM) yöntemiyle kurban bir şarj istasyonundaki (CP1) meşru kullanıcının enerji tüketim verilerini (MeterValues) yakalar. Saldırgan daha sonra bu veriyi manipüle ederek (örneğin 15 kWh'yi 0.5 kWh olarak değiştirir) CSMS'ye gönderir. Sonuç olarak, enerji CP1'den çalınırken, tüm fatura işlemi başlatan kurban kullanıcıya yansıtılır.

Temel Zafiyet: OCPP 1.6'da MeterValues mesajlarının uygulama katmanında dijital olarak imzalanmaması ve bütünlük kontrolünün bulunmaması.

Saldırı Adımları: (1) Keşif - Hedef CSMS'nin IP ve portunun belirlenmesi, (2) Hazırlık - ARP Spoofing ile MitM konumunun sağlanması, (3) Enjeksiyon - MeterValues mesajlarının yakalanması, (4) Manipülasyon - Enerji tüketim verilerinin değiştirilmesi, (5) İletme - Manipüle edilmiş mesajın CSMS'ye gönderilmesi.

⚠ Tehdit Kategorisi

STRIDE: Tampering (Değiştirilme), Repudiation (İnkar), Denial of Service

📊 Potansiyel Etki

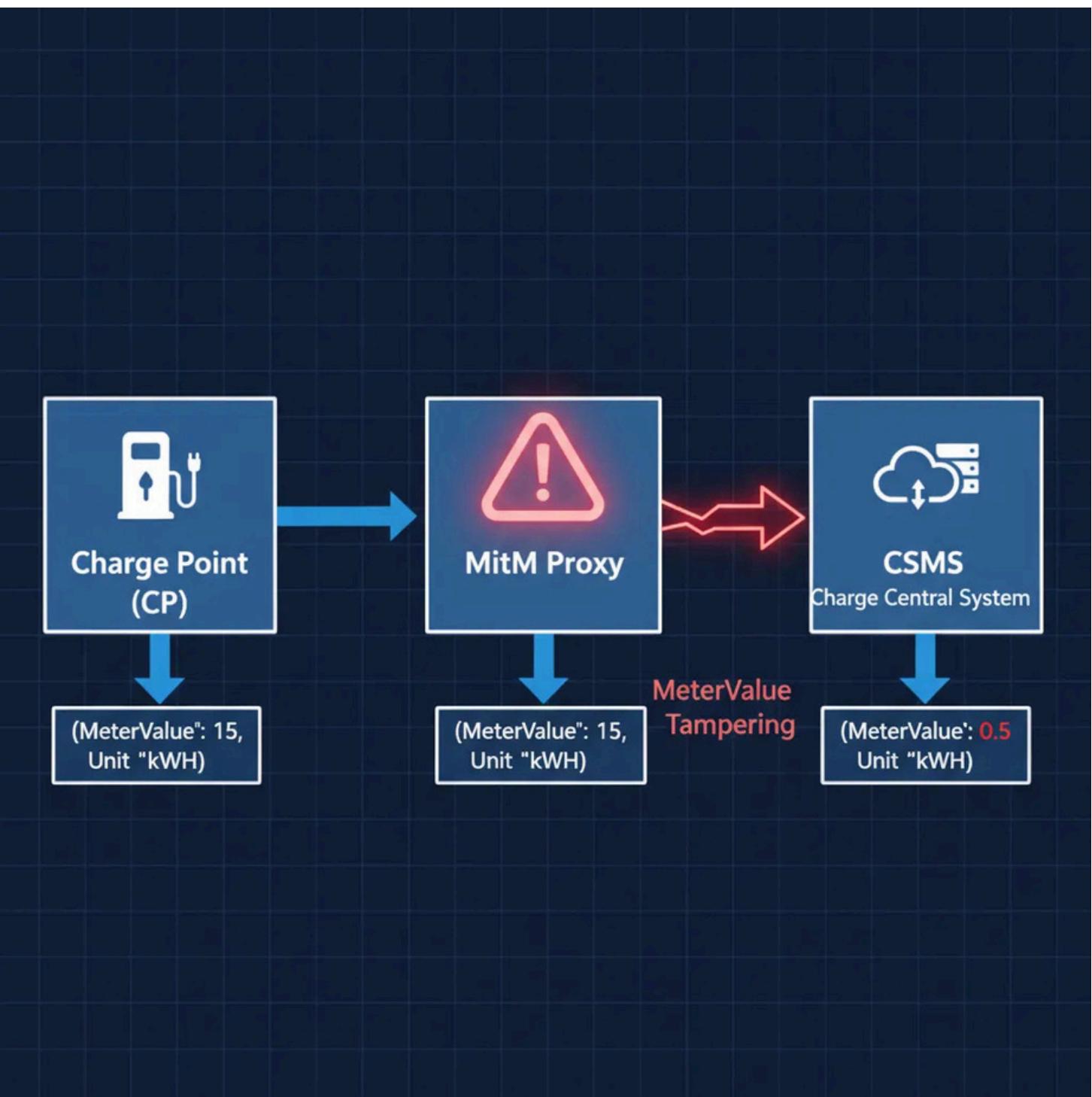
Finansal: Doğrudan gelir kaybı

İtibar: Müşteri güven kaybı, yasal yaptırımlar

Operasyonel: Sistem güvenilirliğinin sorgulanması

✓ Karşı Önlemler

- Dijital İmza (OCPP 2.0.1)
- Mutual TLS (mTLS)
- Mantıksal Doğrulama



Anomali Senaryosu: eMSP Alt-CA'sının Ele Geçirilmesi

Bu senaryo, tüm "Tak ve Şarj Et" (Plug & Charge) ekosisteminin güvendiği zincirdeki kritik bir halkayı kırmayı amaçlar. Hedef, bir e-Mobilite Hizmet Sağlayıcısının (eMSP) alt Sertifika Otoritesi (sub-CA) özel anahtarını (private key) çalmaktır.

1. Sızma ve Anahtar Hırsızlığı

***Hedef Tespiti:** Saldırganlar, ekosistemdeki en zayıf güvenlikli eMSP'yi hedefler.

***İlk Sızma:** Oltalama (phishing) veya zafiyet kullanarak eMSP'nin kurumsal ağına ilk erişim sağlanır.

***Keşif:** Ağ içinde yanal hareket edilerek sertifika otoritesi (CA) altyapısını barındıran sunucular tespit edilir.

***Anahtar Hırsızlığı:** Sunucuya yönetici erişimi elde edilir ve alt-CA'nın özel anahtar dosyası ağ dışına sızdırılır (exfiltrate).

2. İstismar ve Ticarileştirme

***Sahte Üretim:** Saldırganlar, çaldıkları özel anahtarı kullanarak binlerce sahte araç kontrat sertifikası (eMAID) üretir.

***İstismar:** Bu sahte kimlikler, herhangi bir Plug & Charge uyumlu istasyonda (farklı operatörlere ait olsalar bile) enerji hırsızlığı için kullanılır.

***Ticarileştirme:** Üretilen sahte kimlikler, "ömür boyu ücretsiz şarj" vaadiyle karanlık ağa (dark web) satılır.

***Sonuç:** Şarj operatörleri (CPO) için katastrofik finansal kayıplar ve tüm ekosistemin güveninin çökmesi.

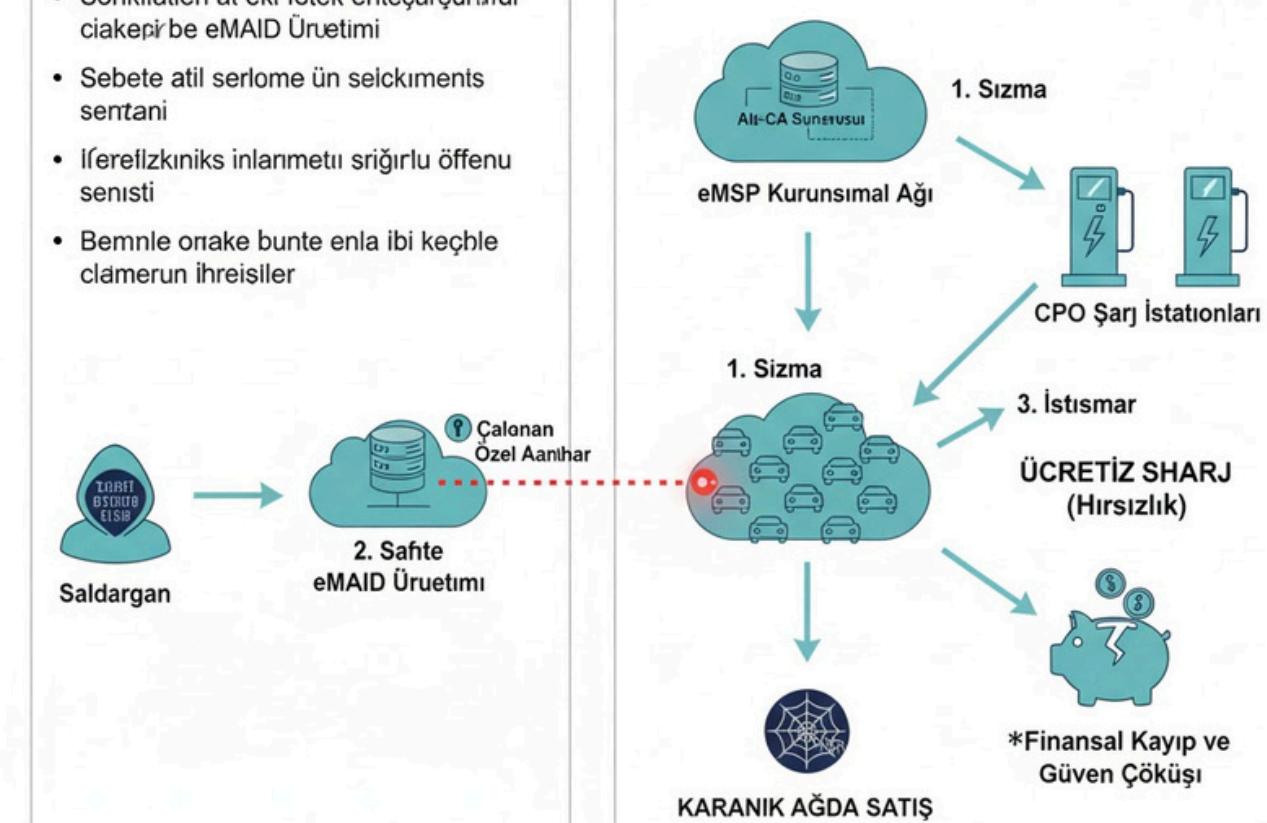
Anomali Senaryous: eMSP Alt-CA'sının Ele Geçirilmesi

Bu senaryo, tüm "Tak a Star Et" (Plug & Charge) ekosisteminin güvendiği zincirdeki kritik halkayı kırmayı amaçlar. Hedef, bir e-Mobilite Hizet Sağlayıcı (eMSP) Sertifika Otoritesi (sub-CA) özel anahtarını (private key) çalır.

1. Sızma ve Anakar Hırsızlığı

- Sönkiaitien at ekt fetek enteçürürürür ciakeri be eMAID Üretimi
- Sebete atıl serlome ün selckiments sentani
- İşerelzkiniks inlanmetü srıgırı öffeni senisti
- Bemnle orake bunte enla ibi keçble clamerun iħreisiller

2. İstismar ve Ticarileşterme

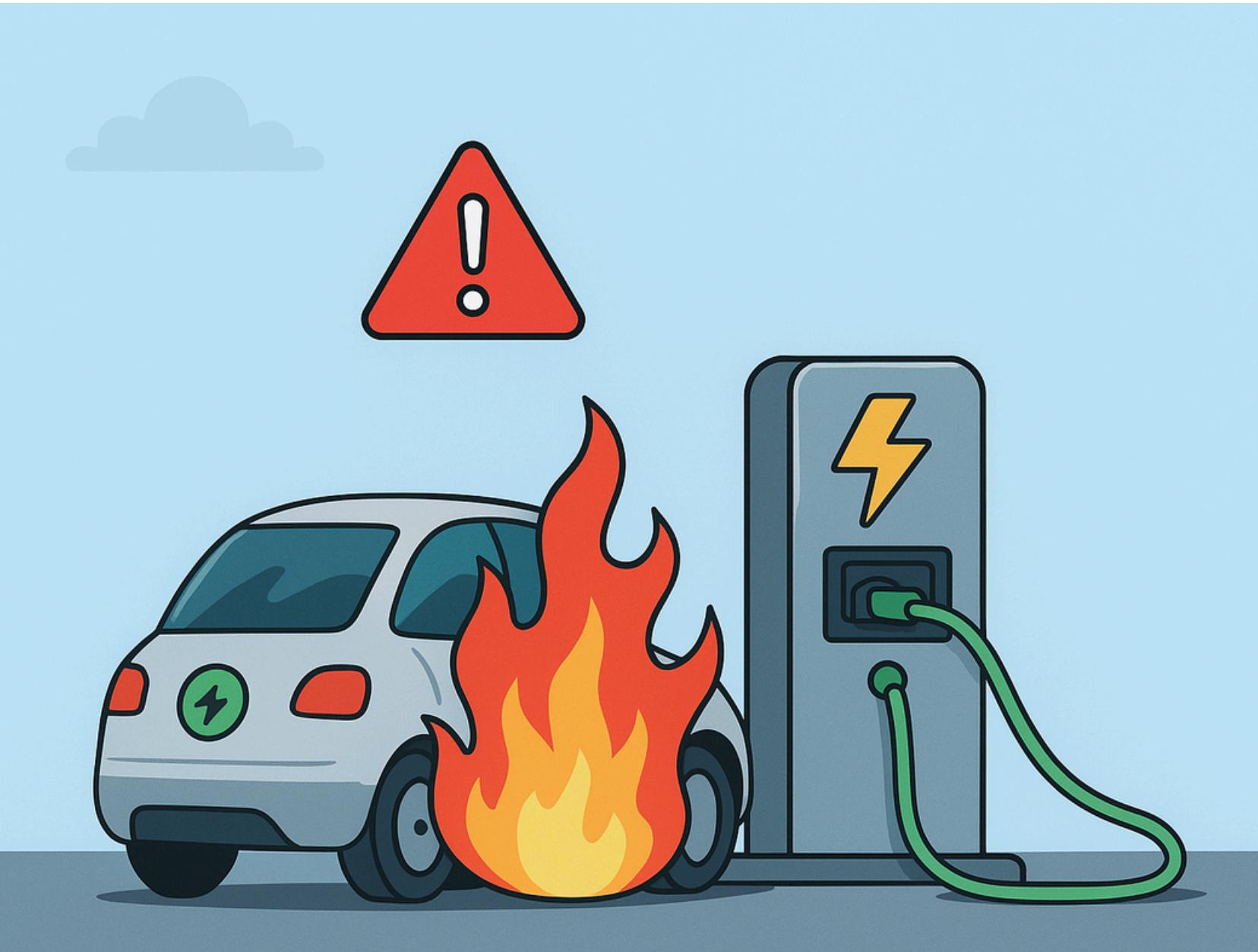


Anomali Senaryosu–Aşırı Talep Enjeksiyonu

Bu senaryo, siber-fiziksel kontrol protokolü verisine (PWM) gereğinden fazla güvenilmesinin yol açtığı kritik bir güvenlik açığını kanıtlamayı amaçlamaktadır. Saldırı, dijital kontrol katmanı ile fiziksel güç dağıtım katmanının kesişim noktasında gerçekleşen hibrit bir istismardır.

1. Enjeksiyon ve Taşıyıcı: Saldırgan, aracın şarj denetleyicisini ele geçirir veya Kontrol Pilotu (CP) teli üzerinde sahte bir Elektrikli Araç (EV) rolü üstlenir. Araç ile şarj cihazı arasındaki standart Darbe Genişlik Modülasyonu (PWM) sinyali, bir Truva Atı görevi üstlenir.
2. Güven İstismarı (Payload Enjeksiyonu): Bu sahte veya ele geçirilmiş EV, şarj cihazına "yalan söyler". PWM sinyalini kullanarak, şarj cihazının nominal güvenlik sınırlarının (örn. 40 Amper) çok ötesinde, aşırı yüksek bir akım talebini (örn. 80 Amper) meşru bir istek gibi göstererek şarj cihazına kalıcı olarak ileter.
3. Tetikleme ve Fiziksel İstismar: Kurban rolündeki Şarj Cihazı (EVSE), araçtan gelen bu sinyale zımnem güvenir. Bağımsız bir donanım tabanlı aşırı akım korumasına sahip olmayan cihaz, bu "zehirli" isteği yerine getirmeye çalıştığı an, fiziksel istismar tetiklenir. Cihaz, kaldırılamayacağı düzeyde yüksek bir akımı kablolara ve bileşenlere zorlar.

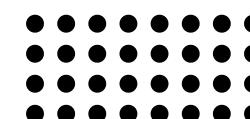
Fiziksel donanımın hızla aşırı ısınması, kablo yalıtılmının erimesi ve potansiyel olarak yanım (termal kaçak) ile sonuçlanır. Bu, Dijital Kontrol Sinyali Güvenliği (PWM) ile Fiziksel Güç Güvenliğini (Donanımsal Koruma) birleştiren özgün bir yaklaşımındır.





BİLGİ
SİSTEMLERİ
VE GÜVENLİĞİ

TEŞEKKÜRLER



GRUP-2