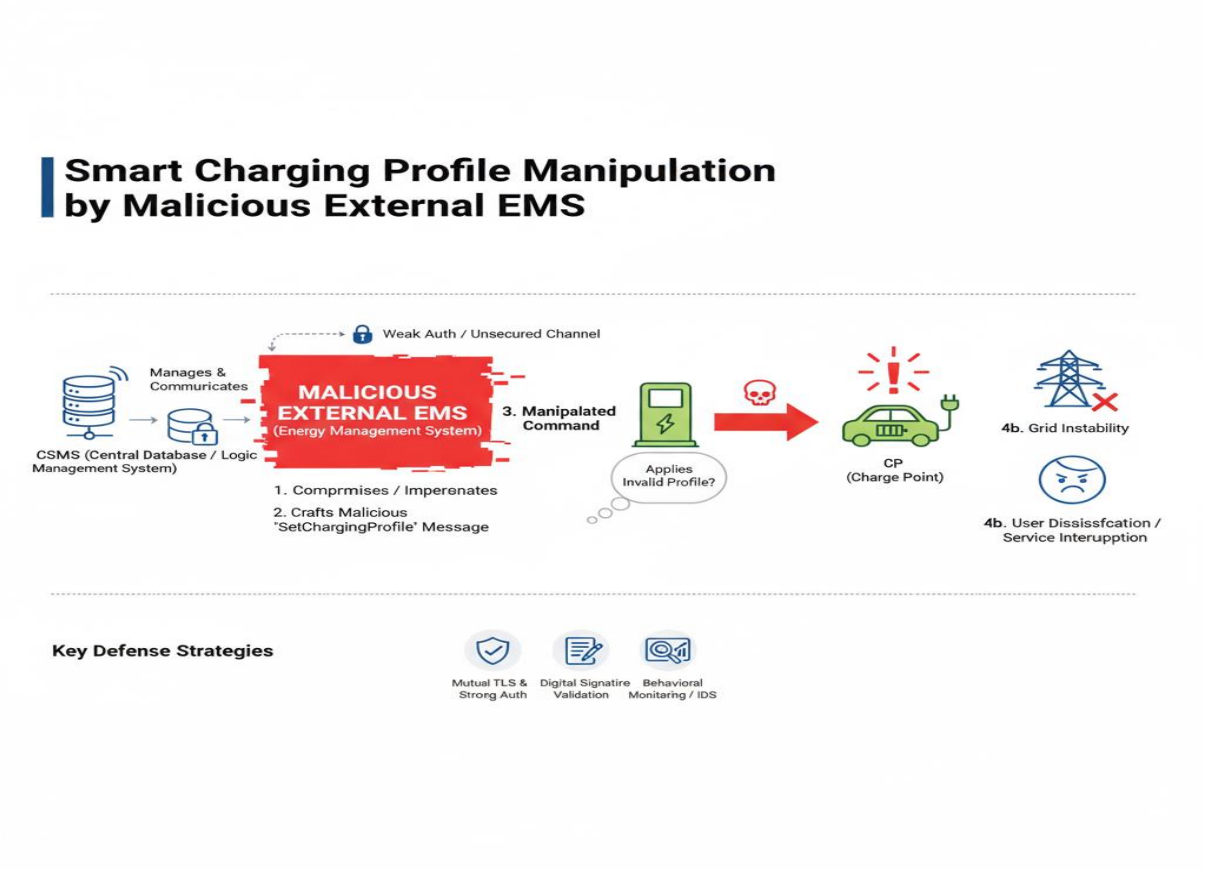
KÖTÜ AMAÇLI DIŞ EMS İLE AKILLI ŞARJ PROFİLİ MANİPÜLASYONU



1. Özet

Bu senaryo, akıllı şebekeye bağlı elektrikli araç şarj altyapılarında kullanılan OCPP protokolü üzerinden **harici bir Enerji Yönetim Sistemi (EMS)** tarafından yapılan kötü niyetli veya yetkisiz şarj profili değişikliklerini ele almaktadır.
Normalde EMS, ağ yükünü dengelemek için şarj akımını ve zamanlamayı optimize eder. Ancak sistem ele geçirildiğinde veya kimlik doğrulama zayıf olduğunda, EMS tarafından **"SetChargingProfile"** mesajı kötüye kullanılarak, şarj akışı kasıtlı biçimde kısıtlanabilir, geciktirilebilir veya aniden artırılarak enerji dengesizliği yaratılabilir.
Bu durum hem **şebeke stabilitesi hem de batarya güvenliği** açısından ciddi bir anomali olarak değerlendirilir.

---

2. Amaç

Amaç, OCPP tabanlı akıllı şarj altyapısında **EMS kaynaklı profil manipülasyonlarının etkilerini anlamak**, olası anomali göstergelerini belirlemek ve bu tür saldırılara karşı alınabilecek **erken tespit ve azaltma önlemlerini** tanımlamaktır.

---

3. Kapsam

Bu çalışma, merkezi şarj yönetim sistemi (CSMS), şarj cihazı (CP) ve harici EMS arasındaki veri akışını incelemektedir.
Senaryo, yalnızca **OCPP 1.6J ve üstü** sürümlerde bulunan **SmartCharging** özelliğine sahip istasyonları kapsamaktadır.
Fiziksel cihaz saldırıları, firmware manipülasyonu veya enerji hırsızlığı gibi konular bu kapsamda **yer almamaktadır**.

---

4. Tehdit Sınıflandırması

Kategori	Açıklama
Saldırı Tipi	Uygulama Katmanı – Mesaj Manipülasyonu (Integrity / Availability)
Kaynak	Kompromize veya kötü niyetli harici EMS
Vektör	`SetChargingProfile`, `ClearChargingProfile`, `ChangeAvailability` mesajları
Etkilenen Varlıklar	CP (şarj istasyonu), CSMS, bağlı EV, enerji yönetim altyapısı
Amaçlanan Etki	Yük dengesizliği, hizmet reddi (DoS), batarya aşırı yüklenmesi veya yetersiz şarj

---

5. Gerekli Koşullar

- CSMS veya CP tarafında EMS ile iletişim yetkisi açık olmalı.
- EMS kimliği doğrulanmadan `SetChargingProfile` mesajı gönderebilmeli (zayıf TLS / yanlış sertifika).
- CSMS, gelen profili imza doğrulaması olmadan CP'ye yönlendirmeli.
- SmartCharging özelliği aktif durumda olmalı.

6. Saldırı Yöntemi ve Akış

1. **Hazırlık:** Saldırgan, dış EMS sunucusunu taklit eder veya meşru EMS hesabını ele geçirir.
2. **Bağlantı:** EMS, OCPP kanalına bağlanarak sahte `SetChargingProfile` mesajı gönderir.
3. **Manipülasyon:**
    - Akım limiti düşürülür (örneğin 32 A → 2 A).
    - Zamanlama kaydırılır (ör. `startSchedule` ileri alınır).
    - Profil tipi değiştirilir (`TxProfile` → `DefaultProfile`).
4. **Etkileme:** CP, gelen profili geçerli sanıp uygular; şarj işlemi yavaşlar veya durur.
5. **Sonuç:**
    - Şebekede dengesizlik oluşur.
    - Kullanıcı gecikme veya kesinti yaşar.
    - Enerji ölçüm kayıtları anormal görünür.

---

7. Tespit Yöntemleri ve Anomali Göstergeleri

Göstergeler	Açıklama
Zaman Uyumsuzluğu	EMS profil zaman damgaları CSMS senkronizasyonundan sapıyor.
Anormal Akım Profili	Saniyelik ölçümlerde beklenmeyen akım düşüşü (ör. ani 32 A → 0 A).
Beklenmeyen Profil Güncelleme Sıklığı	Normalde birkaç saatte bir olan profil değişiklikleri dakikalar içinde tekrar ediyor.
İmza / Sertifika Uyuşmazlığı	EMS'den gelen mesajda geçersiz sertifika veya eksik dijital imza.
Profil Çakışması	Aynı `connectorId` için birden fazla aktif profil tespit ediliyor.

Bu göstergeler, CSMS veya CP tarafında **anomali tespiti (IDS)** modülüne girdi olarak kullanılabilir.

---

8. Olası Etkiler

- **Hizmet Kesintisi:** Şarj işlemi durur veya plan dışı kesilir.
- **Enerji Verimsizliği:** Şebeke yük dengesizleşir, talep dalgalanır.
- **Kullanıcı Güveni Kaybı:** Şarj istasyonunun güvenilirliği sorgulanır.
- **Veri Tutarsızlığı:** Faturalama ve raporlama sistemlerinde hatalı enerji değerleri oluşur.
- **Zincirleme Etki:** Çoklu istasyonlarda aynı anda uygulandığında, yerel dağıtım ağında frekans kararsızlığı görülebilir.

---

9. Önlemler ve Azaltma Stratejileri

Alan	Önlem
Kimlik Doğrulama	EMS-CSMS arasında mutual TLS ve güçlü sertifika doğrulaması kullanılmalı.
Yetkilendirme	EMS yalnızca belirli `connectorId` ve profil tiplerinde işlem yapabilmeli.
İmza Doğrulama	`SetChargingProfile` mesajı dijital imza (XML DSig / JWS) ile doğrulanmalı.
Davranışsal İzleme	CSMS, profil değişiklik sıklığını ve akım eğrilerini izlemeli; eşik dışı durumlarda alarm üretmeli.
Yedekleme	Profil değişiklikleri için sürüm kontrolü tutulmalı, geri alma (rollback) mekanizması sağlanmalı.

---

10. Sonuç

Bu senaryo, akıllı şarj sistemlerinde **EMS tabanlı anomali riskinin** önemini göstermektedir. OCPP mesajlarının güvenliğini sadece şifreleme ile değil, **kaynak doğrulama ve davranış analizi** ile desteklemek gerekmektedir.
Uygulama düzeyinde geliştirilecek IDS/IPS çözümleri, bu tür profil manipülasyonlarını erken fark edip hem **kullanıcı hem de şebeke güvenliğini** koruyabilir.