**CAN Bus mesaj Taklidi ID Spoofing**

## 1. Anomali Tanımı

Elektrikli araç (EV) içerisindeki **CAN Bus**, batarya yönetimi (BMS), şarj kontrol birimi ve diğer ECU'lar arasında iletişimi sağlar.
Bu protokolde gönderilen mesajlarda **kaynak doğrulaması veya şifreleme** bulunmaz.

Bir saldırgan, şarj portuna fiziksel erişim (örneğin OBD-II üzerinden) sağlayarak **şarj kontrol birimi gibi davranabilir** ve sahte mesajlar göndererek sistemin davranışını değiştirebilir.
Bu tür mesaj manipülasyonuna "**ID Spoofing**" (mesaj taklidi) denir.

### 2. Olası Nedenler

| Kategori | Olası Sebep | Açıklama |
|---|---|---|
| **Protokol** | Kimlik doğrulama eksikliği | CAN Bus mesajlarında kaynağı doğrulayan güvenlik katmanı yoktur. |
| **Donanım** | Korumasız fiziksel portlar | Şarj sırasında açık kalan bağlantı noktalarına (ör. servis portu) erişim mümkündür. |
| **Yazılım** | Mesaj filtreleme yokluğu | ECU'lar gelen verinin güvenilirliğini analiz etmez, doğrudan işler. |

## 3. Olası Riskler ve Etkiler (Şarj Esnasında)

- **Fazla akım talimatı gönderme** → Batarya hücreleri zarar görebilir veya ısınma/yangın riski oluşabilir.
- **Şarjın erken sonlandırılması** → Araç eksik şarjla bırakılır, kullanıcı mağdur olur.
- **Soğutma sisteminin devre dışı bırakılması** → Batarya sıcaklığı kontrolsüz şekilde yükselir.
- **Yanıltıcı SOC (State of Charge) verisi gönderme** → Gösterge panelinde %100 dolu görünmesine rağmen batarya gerçekte boş olabilir.
- **BMS'nin yanıt veremez hale gelmesi** → Şarj işlemi kilitlenir, araç servis gerektirir.

## 4. İlgili Standart Referansı

- **ISO 11898** – Road Vehicles – Controller Area Network
- **IEC 61851-24** – Digital Communication between EV and DC Charging Station
- **ISO 26262** – Functional Safety for Automotive Systems
- **ISO 15118** – Vehicle-to-Grid Communication Interface

## 55. Çözüm Önerileri

*Donanım Düzeyinde:*

- Servis portları ve şarj soketleri fiziksel olarak korunmalı.
- Şarj sırasında dış erişim noktaları devre dışı bırakılmalı.

*Yazılım Düzeyinde:*

- Şarj esnasında alınan CAN mesajlarının kimliği yazılımsal olarak doğrulanmalı.
- BMS ve şarj kontrolcüsü, olağan dışı veri desenlerini (ör. hızlı akım artışı) reddetmeli.

*Protokol Geliştirme:*

- CAN Bus seviyesine **dijital imza veya mesaj doğrulama kodu (MAC)** entegre edilmeli.
- Yeni nesil CAN protokolleri (örneğin **CAN-FD + CANsec**) göz önüne alınmalı.

## 6. Sonuç ve Değerlendirme

Şarj sırasında mesaj taklidi yapılabilmesi, yalnızca araç güvenliğini değil, **kullanıcı hayatını ve altyapının bütünlüğünü** tehdit eden ciddi bir açıklıktır.
Fiziksel bağlantı noktalarının korunmaması ve mesaj doğrulama mekanizmalarının eksikliği, saldırganlara şarj sürecini doğrudan manipüle etme fırsatı verir.

Bu nedenle açıklık, **"kritik öncelikli protokol güvenlik açığı"** olarak değerlendirilmelidir ve hem araç hem de şarj istasyonu üreticileri tarafından sistematik olarak test edilmelidir

## 7. Kaynakça


- ISO 11898 – Controller Area Network (CAN)
- IEC 61851-24 – Digital communication between a d.c. EV supply equipment and an EV
- O.A.M. Al Isawi (2023). *CAN Bus Cyber-Attacks Detection*, Khalifa University
- SAE J3061 – *Cybersecurity Guidebook for Cyber-Physical Systems*
- Miller & Valasek (2014). *A Survey of Remote Automotive Attack Surfaces*