

Anomali Senaryosu: Zaman Senkronizasyonu Manipölasyonu (Time Desync Attack)

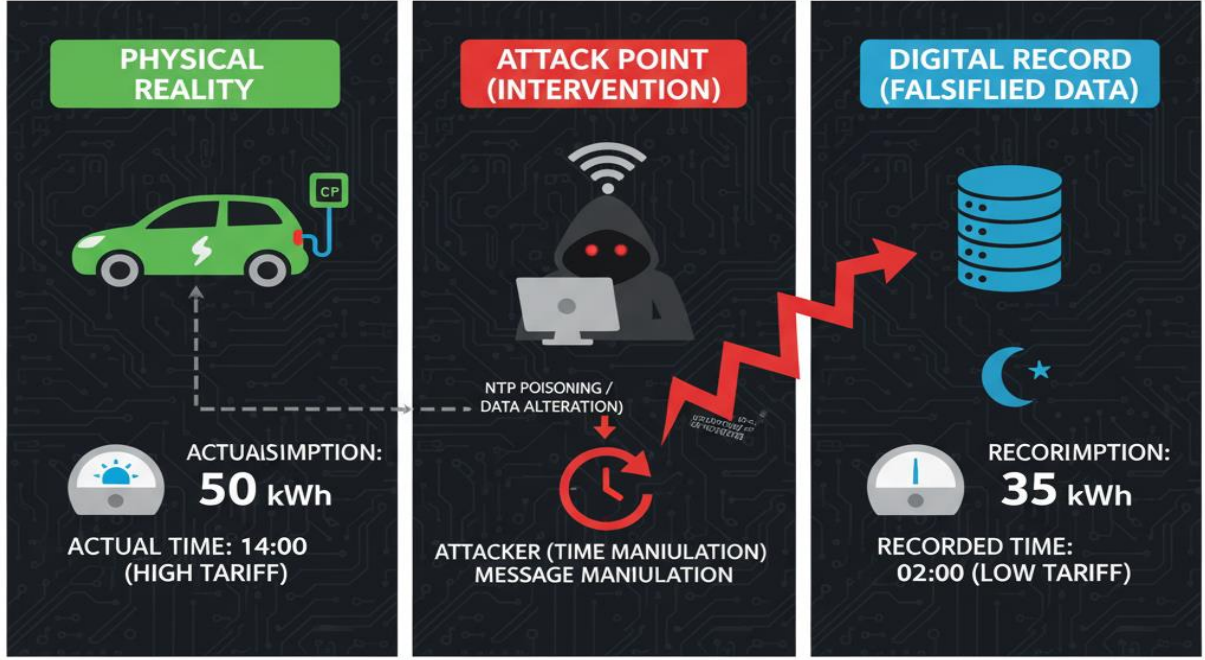
Başlık: Zaman Kaydırma ile Enerji Maskelenmesi

Hazırlayan: Berat EROL / 235541010 – Takım 1

Tarih: 27.10.2025

Referans Makale: *Cloud-Edge Model Predictive Control of Cyber-Physical Systems Under Cyber Attacks* (IEEE Transactions on Circuits and Systems I, 2025)

TIME SHIFTING ENERGY MASKING: DIGITAL VS. PHYSICAL CONFLICT



RESULT: REVENUE LOSS / FINANCIAL DAMAGE

1. Amaç

Bu senaryonun amacı, elektrikli araç şarj istasyonlarında (EVCS) OCPP tabanlı haberleşme kanalında zaman bilgisinin veya enerji verilerinin manipüle edilmesi yoluyla yanlış faturalandırma, hatalı yük dengeleme ve veri tutarsızlığı gibi sonuçların ortaya çıkabileceğini göstermektir.

Saldırı, özellikle Cloud-Edge tabanlı kontrol sistemlerinde (örneğin enerji optimizasyonu yapan sistemlerde) gizli bir anomali olarak etkili olabilir.

2. Hedef Sistem Bileşenleri

- **Bulut Katmanı (Cloud):** Merkezi Yönetim Sistemi (CSMS). OCPP trafiğini toplar, faturalandırma ve yük yönetimi kararlarını verir.
- **Kenar Katman (Edge):** Şarj İstasyonu (Charge Point - CP). OCPP istemcisi olarak çalışır, CAN-Bus üzerinden donanım modüllerini kontrol eder.
- **Cihaz Katmanı (Device):** Şarj kontrol birimi, enerji ölçüm modülü (Meter) ve röle sürücüsü. Gerçek enerji akışını ve ölçüm işlemlerini yürütür.

Bu yapıda CP, bulut sistemiyle OCPP protokolü üzerinden haberleşir ve aynı zamanda yerel donanım bileşenleriyle CAN-Bus üzerinden iletişim kurar. Böylece, OCPP ile başlayan bir siber saldırı fiziksel donanım davranışlarını etkileyebilir.

3. Saldırı Özeti

Saldırgan, OCPP trafiğine Man-in-the-Middle (MitM) yöntemiyle müdahale eder. Bu müdahale sırasında:

- `MeterValues` veya `TransactionEvent` mesajlarının zaman damgasını değiştirir.
- Şarj istasyonunun NTP sunucusunu zehirleyerek (NTP spoofing) sistem saatini birkaç saat kaydırır.

Sonuç olarak:

- Yüksek tarifeli saatlerdeki enerji tüketimi, düşük tarifeli zaman dilimine aitmiş gibi görünür.
 - Merkezi sistemde (CSMS) yanlış enerji raporları oluşur.
 - Cloud-Edge mimarisi kullanan kontrol sistemlerinde enerji tahmin ve planlama algoritmaları yanlış veriye dayanarak karar alır.
-

4. Saldırı Akışı

1. Saldırgan, şarj istasyonunun bulunduğu yerel ağa veya istasyonun internet trafiğine erişim sağlar.
2. Sahte bir NTP sunucusu çalıştırarak istasyonun saatini iki saat geri alır veya ileri kaydırır.
3. OCPP mesajlarındaki zaman damgalarını (`MeterValues.timestamp`) değiştirir.
4. Enerji tüketim değerlerini (`sampledValue`) düşürerek (örneğin 50 kWh yerine 35 kWh) raporlar.
5. Merkezi yönetim sistemi (CSMS), bu manipüle edilmiş veriye dayanarak hatalı faturalandırma ve planlama yapar.

5. Saldırının Başarılı Olma Sebepleri

- Güvenli zaman protokolü (NTPsec/NTS) kullanılmıyor.
- `MeterValues` mesajları dijital olarak imzalanmadığı için değiştirilebilir.
- OCPP bağlantısı Mutual TLS yerine zayıf kimlik doğrulama (örneğin self-signed sertifika) ile sağlanıyor.
- Replay koruması bulunmadığından aynı veri paketleri tekrar gönderilebiliyor.
- Saat farkı veya zaman tolerans kontrolü yapılmıyor.

6. Saldırının Sonuçları ve Etkileri

- **Finansal Etki:** Faturalandırma hatası ve gelir kaybı oluşur.
- **Operasyonel Etki:** Şebeke yönetim sisteminde hatalı enerji verisi nedeniyle yük dengeleme algoritmaları yanlış çalışır.
- **Güven Etkisi:** Kullanıcı ve operatör güveni azalır.
- **Yasal Etki:** MID ve ISO 15118 standartlarına göre kayıt bütünlüğü bozulur, yasal geçerlilik kaybedilir.

7. Tespit ve Savunma Önlemleri

Protokol Seviyesinde:

- OCPP 2.0.1 sürümünde yer alan `SignedMeterValues` özelliği etkinleştirilmelidir.
- Tüm OCPP bağlantılarında Mutual TLS (karşılıklı sertifika doğrulaması) kullanılmalıdır.

Zaman Senkronizasyonunda:

- Güvenli zaman protokolleri (NTPsec veya NTS) tercih edilmelidir.
- Alternatif olarak GPS tabanlı yedek zaman kaynakları kullanılabilir.

Veri Doğrulama:

- CSMS tarafında enerji ve zaman verileri için tutarlılık kontrolü uygulanmalıdır (örneğin $\pm\%10$ sapma tespiti).
- CP içinde fiziksel sayaç ile raporlanan değerler periyodik olarak karşılaştırılmalıdır.

Yerel Savunma (Edge):

- CP üzerinde basit bir CAN-IDS (anormallik tespiti) sistemi çalıştırılabilir.
 - OCPP komutlarından CAN mesajlarına dönüşümde yalnızca izinli mesajların geçmesine izin veren “whitelisting” mekanizması uygulanmalıdır.
-

8. Uygulama Planı (Simülasyon)

1. Normal durumda, CSMS \rightarrow CP \rightarrow CAN akışı düzgün çalışır.
 - o RemoteStartTransaction mesajı \rightarrow CAN ID 0x200
 - o MeterValues mesajı \rightarrow CAN ID 0x300
 2. Saldırı senaryosunda, MitM proxy üzerinden MeterValues mesajlarının zaman damgası değiştirilir.
 - o CP, CAN üzerinden hatalı enerji değerlerini gönderir.
 3. Savunma senaryosunda, CP'ye güvenli zaman protokolü (NTPsec/GPS) eklenir.
 - o Zaman farkı algılandığında CSMS tarafında alarm oluşturulur.
-

9. Kaynaklar

1. X. Zhang et al., "Cloud-Edge Model Predictive Control of Cyber-Physical Systems Under Cyber Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2025.
 2. Open Charge Alliance, "OCPP 2.0.1 Specification," 2020.
 3. ISO/IEC 15118:2019, "Road Vehicles — Vehicle to Grid Communication Interface."
-