OCPP Yetkilendirme Token Replay / Nonce Yeniden Kullanımı Anomalisi

Kapsam: Elektrikli Araç Şarj İstasyonları — OCPP tabanlı CSMS/Charge Point iletişimi

Hazırlayan: Yiğit Erdoğan 230542029

---

1. Özet (Executive summary)

Bu rapor, OCPP (Open Charge Point Protocol) veya benzeri EV şarj yönetim protokollerindeki **yetkilendirme token/nonce yeniden kullanımı** zafiyetine odaklanır. Zayıf nonce üretimi veya sunucu tarafı tekrar kullanım kontrolünün eksik olması, yakalanan token/nonce çiftlerinin yeniden oynatılmasıyla yetkisiz oturum başlatma, faturalama hileleri ve operasyonel bozulmaya yol açabilir. Rapor, saldırı senaryosu, test adımları, tespit/izleme önerileri, makale/referans listesi, SWOT analizi ve neden simülasyon yapılamayabileceğine dair mantıklı analiz içerir.

---

2. Tehdit modeli & Varsayımlar

- Sistem bileşenleri: Charge Point (CP/istasyon), CSMS/Cloud (CPO backend), yetkilendirme mekanizması (token, nonce, timestamp), TLS (mevcut veya eksik olabilir).

- Varsayım: Saldırgan, istasyon ile CSMS arasındaki iletişimi pasif olarak dinleyebilir (network sniffing) veya ağ içinde MitM yapabilir; ayrıca saldırgan, önceden geçerli bir yetkilendirme token/nonce çiftini ele geçirmiştir.

- Hedefler: yetkisiz StartTransaction/StopTransaction başlatmak, faturalama karışıklığı yaratmak, hizmet reddi/nadir durum operasyonel bozukluk.

---

3. Anomali açıklaması (teknik)

Ad: Token/Nonce Replay (Yeniden Oynatma)

- OCPP yetkilendirme akışında (ör. Authorize, StartTransaction) kullanılan kısa ömürlü token/nonce/timestamp çiftleri zayıf, tahmin edilebilir veya sunucu tarafında *used-once* kontrolü yoktur.

- Saldırgan bu token'ları yakalar ve **aynı token/nonce** ile farklı CP'lerde veya aynı CP'de farklı zamanlarda StartTransaction, MeterValues veya StopTransaction gibi mesajları yeniden oynatır.

- Sonuç: CSMS, isteği doğrulanmış gibi kabul ederek oturumu başlatabilir veya ölçümleri işleyebilir; faturalama yanlış atanabilir veya oturumlar çakışabilir.

---

4. Adım adım saldırı senaryosu

Ön koşullar: Saldırgan ağa erişim veya trafik yakalama yeteneğine sahip; bir geçerli token/nonce çiftini elde etti.

1. Pasif dinleme veya MitM ile "Authorize" / "StartTransaction" mesajlarından token/nonce/timestamp yakalanır.

2. Saldırgan, aynı token/nonce ile yeni bir StartTransaction isteği oluşturur veya StopTransaction/MeterValues gibi mali/operasyonel mesajları yeniden oynatır.

3. CSMS, token doğrulaması yetersizse isteği kabul eder ve oturum açar; sayaç değerleri veya oturum meta verisi CSMS'de hatalı işlenir.

4. Operatör raporları, faturalama kayıtları ve kullanıcı deneyimi etkilenir; kötü niyetli zincirleme etkiler (çoklu istasyonlarda tekrar) mümkündür.

---

5. Test planı (manüel + otomatik)

Hedef

Token/nonce tekrar kullanımını tespit etmek ve protokol implementasyonlarının koruma eksikliklerini ortaya çıkarmak.

Test ortamı (öneri)

- İzole test ağı (VM veya VLAN) içinde bir CSMS emülatörü (EmuOCPP veya gerçek CSMS test inst.), 2–3 sanal Charge Point (Open-source CP emulators) ve bir trafik yakalayıcı (Wireshark) veya özel OCPP dissector. cite turn0search2 turn0search16

Test vakaları

1. **Replay Basit:** Geçerli Authorize -> StartTransaction token'ı yakala, aynı token ile farklı CP ID ile StartTransaction gönder. Beklenen: CSMS reddetmeli; eğer kabul ederse zaafiyet var.

2. **Timestamp Esnekliği:** Token içeriğinde timestamp varsa eski bir token ile isteği gönder; CSMS zaman sınırını ihlal edip etmiyor?

3. **Token Tek Kullanım Kontrolü:** Aynı token ile iki kez StartTransaction gönder (aynı CP). CSMS ikinciyi reddediyor mu?

4. **Faturalama Karışıklığı:** Replay edilen MeterValues ile sayaç/enerji kaydı değişimi yarat; raporlama tablosunda anomaliler oluşuyor mu?

5. **Scalability Replay:** Otomatik script ile çok sayıda farklı CP_ID ile token tekrar oynatma (flood) — CSMS davranışı ve alarm yükünü gözle.

6. **MitM-tamper varyantı:** Token içeriğinde imza varsa, imzanın da replay koruması var mı (nonce, ECDSA nonce reuse analiz). cite turn0search22 turn0search4

Test araçları (öneri)

- EmuOCPP (veya CheckOCPP) ve Wireshark OCPP dissector. cite turn0search2 turn0search16

- Özel replay script (Python, websocket client) — StartTransaction JSON mesajlarını kaydet/yeniden oynat.

- Log korelasyon (CSMS event logs, timestamp karşılaştırması).

---

6. Ölçütler / Başarı kriterleri

- CSMS'nin aynı token/nonce için *used-once* veya token revocation mekanizması göstermesi.

- StartTransaction/Authorize için kısa zaman aralığı (timeout) ve timestamp doğrulaması.

- İmzalı mesajlarda (örn. OCPP 2.0.1 security) nonce/timestamp kontrollerinin varlığı ve geçerliliği. cite turn0search20

---

7. Tespit ve izleme önerileri

- Sunucu tarafında token kullanım tablosu (token_id -> kullanıldı mı, ilk kullanım zamanı, CP_ID).

- Hedeflenmiş IDS kuralları: aynı token ile farklı CP_ID görünümü, kısa süre içinde aynı token tekrar kullanımı, aynı CP için ardışık çakışan start/stop.

- Log zenginleştirme: mesaj hash'i + kaynağın TLS sertifika bilgisi + client/CP kimliği.

- Anomali-detection ML: normal oturum modelleri oluşturup anormallik tespiti (çoklu oturum başlatma, beklenmedik enerji değerleri). cite turn0search14

---

8. Mitigasyon (kısa & uygulanabilir)

1. **Used-once token enforcement**: CSMS, token'ı kullandıktan sonra işaretlemeli ve tekrar kabul etmemeli.

2. **Kriptografik imza + nonce**: Mesajlara ECDSA/HMAC imzası ekleyin; imza içinde tek kullanımlık nonce ve timestamp olsun. (ECDSA nonce yönetimine dikkat). cite turn0search22

3. **TLS + mutual authentication**: CP ve CSMS arasında mutual TLS (mTLS) ile kanal güvenliği. Eğer mTLS mümkün değilse, mesaj uygulama-katmanı imzası kritik. cite turn0search12

4. **Rate-limiting & anomaly detection**: Aynı token ile kısa sürede tekrar istekleri engelle.

5. **Firmware/Protocol upgrade**: OCPP 2.0.1 güvenlik özelliklerini mümkünse uygulamaya koy. cite turn0search20

---

9. SWOT Analizi

Güçlü Yanlar (Strengths)

- Protokol düzeyinde uygulanırsa replay riskini kalıcı azaltır (used-once token, imzalama).

- Log ve deteksiyon ile yanlış faturalama erkenden saptanır.

Zayıf Yanlar (Weaknesses)

- Legacy istasyonlar ve CSMS'lerde yazılım/firmware güncellemesi zor olabilir.

- Kriptografik çözümler işlem yükü/artırılmış cihaz maliyeti gerektirebilir.

Fırsatlar (Opportunities)

- Standart güncellemeleri ve uyumluluk iyileştirmeleri (OCPP 2.0.1 adoption). cite turn0search20

- Operatörler için güvenlik sertifikasyon süreçleri, güven oluşturma.

Tehditler (Threats)

- Saldırganların daha sofistike MitM ve replay araçları geliştirmesi.

- Regülasyon ve uyumluluk gereksinimleri karşılanmazsa ağır cezalar ve müşteri güven kaybı.

---

10. Literatür ve kaynak önerileri (seçme)

- Alcaraz, C., & Wolthusen, S. (2017). *OCPP Protocol: Security Threats and Challenges.* cite turn0search4

- Boussaha et al., *Effective and Scalable OCPP Security and Privacy Testing* (USENIX, 2025) — EmuOCPP araç seti. cite turn0search2

- Hamdare et al., *Cyber defense in OCPP for EV charging security risks* (Springer, 2025). cite turn0search18

- Jahangir et al., *Charge-manipulation-attacks-against-smart-electric-vehicle* (WRAP, 2024). cite turn0search15

- NREL report, *Cybersecurity for Electric Vehicle Fast-Charging* (2021). cite turn0search26

- CheckOCPP / OCPP dissector tooling (paper + repo). cite turn0search16 turn0search2

---

11. Simülasyon imkânı ve neden tam simülasyon yapılamayabilir

Simülasyon yapılabilecekler: İzole test ağı içinde replay attack'ı emüle edip CSMS tepkisini gözlemleyebilirsin (EmuOCPP + CP emülatörleri). Bu, işlevsel açıdan replay etkilerini gösterir. cite turn0search2

Neden tam gerçek dünyada simülasyon zor olabilir:

- Gerçek CSMS üretim ortamlarına erişim genellikle sınırlıdır (gizlilik, SLA, maliyet).

- Gerçek CP firmware'leri kapalı kaynak veya donanım sınırlamaları içerir; gerçek zamanlı enerji sayaçları ve fiziksel güç akışı davranışı tam replicasyon gerektirir.

- Yasal / etik kısıtlar: canlı operasyonlarda faturalama/servis kesintisi yaratmak izin verilmez.

Bu nedenle raporda **mantıklı nedenlerle** (teknik sınırlar, etik ve yasal sebepler) laboratuvar emülasyonu ve log-analiz ile değerlendirme önerilmiştir.

---

12. Rapor / Sonuç ve aksiyon önerileri

1. Acil: CSMS üzerinde token/nonce used-once ve timestamp kontrolü uygulansın.

2. Kısa vadeli: OCPP trafiği için log korelasyon kuralları ve IDS imzaları uygulanıp test edilsin.

3. Orta vadeli: mTLS ve/veya uygulama katmanı imzalama (HMAC/ECDSA) kullanılsın; ECDSA nonce yönetimi denetlensin.

4. Uzun vadeli: Tüm CP'lerin firmware güncelleme yol haritası çıkarılsın ve OCPP 2.0.1'e geçiş planlansın.

---

13. Ek: Örnek OCPP JSON (Replay için yakalanabilecek alanlar)

```json
{
 "messageTypeId":2,
 "uniqueId":"12345",
 "action":"StartTransaction",
 "payload":{
  "connectorId":1,
  "idTag":"TOKEN-ABC-123",
  "timestamp":"2025-11-10T18:00:00Z",
  "meterStart":0
 }
}
```

Yukarıda `uniqueId`, `idTag` (token), `timestamp` alanları replay için kritik hedeftir.

---

14. Kısa eğitim/hint ladder (sunuma uygun)

- Gentle: Replay saldırısı, ağ trafiğinin yakalanıp tekrar gönderilmesidir; nonce/use-once mantığı bunu engeller.

- Guided: OCPP'de hangi mesajlar oturum başlatır? (Authorize, StartTransaction). Bu mesajlardaki token/idTag yeniden oynatılabilir.

- Explicit: Test için EmuOCPP + Wireshark kullanıp StartTransaction örneklerini kaydet/yeniden oynat.
