OCPP 1.6 Protokolü SWOT Analizi (Alcaraz et al., 2017 Makalesi Temelinde)

Giriş: Bu analiz, Cristina Alcaraz, Javier Lopez ve Stephen Wolthusen tarafından 2017'de yayınlanan "OCPP Protocol: Security Threats and Challenges" başlıklı makalede incelenen OCPP 1.6 protokolünün Güçlü Yönlerini, Zayıf Yönlerini, Fırsatlarını ve Tehditlerini (SWOT) değerlendirmektedir.

Strengths (Güçlü Yönler - İç Faktörler)

- **De-facto Standart:** OCPP, şarj noktaları (CP) ve merkezi sistemler (CS) arasında evrensel bir açık iletişim standardı sağlamayı amaçlayan, fiili bir standarttır.
- **Gelişmiş Fonksiyonellik (v1.2/1.5'e göre):** v1.6, Yerel Yetkilendirme Listesi (LAL) ve önbellek gibi yeni fonksiyonlar sunarak çevrimdışı (offline) çalışma ve daha hızlı kullanıcı yanıt süreleri sağlar.
- **Akıllı Şarj Yetenekleri:** Protokol, şarj işlemleri sırasında iletilen güç miktarını sınırlamak için akıllı şarj (smart charging) ile ilgili işlevler içerir.
- **Esnek İletişim Altyapısı:** SOAP/XML veya JSON üzerinden WebSockets (WS) gibi farklı iletişim altyapılarını destekler.
- **Yapılandırılmış İşlemler:** Protokol, Başlatma/Yapılandırma, İşlemler/Kontrol ve Bildirim/Bakım olmak üzere üç ana aşamada gruplanmış komut setleri sunar .

Weaknesses (Zayıf Yönler - İç Faktörler)

- **Yüzeysel Güvenlik Yaklaşımı:** Güvenliği büyük ölçüde alt katmanlara (TLS/WS-Security) bırakır ve bu katmanların kullanımını zorunlu kılmaz; yalnızca kritik veriler için TLS/SSL *önerir* .
- **Güvenilir Bileşen Varsayımı:** Protokol, iletişimdeki bileşenlerin (CP, CS) kendilerinin güvenilir olduğunu ve manipüle edilemeyeceğini varsayar.
- **Zayıf Kimlik Doğrulama:** En yaygın yöntem olan statik ID tabanlı RFID etiketlerinin (idTag) klonlanması kolaydır.
- **Web Teknolojisi Zafiyetleri:** SOAP/XML, JSON, WS ve HTTP kullanımı, bu teknolojilere özgü web tabanlı saldırılara (DoS, XML enjeksiyonu, SOAPAction sahteciliği vb.) açık kapı bırakır .
- **Çevrimdışı Mod Güvenlik Açığı:** CS'nin, CP çevrimdışıyken kuyruğa alınan işlemleri, doğrulama durumuna bakılmaksızın "kabul etmek" zorunda olması.
- **Sorumluluk (Non-repudiation) Eksikliği:** İşlemlerin kim tarafından yapıldığını inkâr edilemez şekilde kanıtlayan mekanizmalar yetersizdir.

- **İsteğe Bağlı Güvenlik Özellikleri:** v1.6'da bazı güvenlik artırıcı özelliklerin (örn. LAL listesinin hash ile transferi) kaldırıldığı veya isteğe bağlı olduğu belirtilmiştir [12].
- **Genel Tanımlayıcılar:** Bileşenleri (örn. konnektörleri) tanımlamak için kullanılan ID_{EVSE} gibi genel tanımlayıcılar, ayrıntılı (fine-grained) takip ve hesap verebilirliği zorlaştırır .
- **Zorunlu Olmayan Kritik Veriler:** Bazı önemli veriler (örn. `StatusNotification.req` içindeki zaman damgası) isteğe bağlıdır.
- **Firmware Güncelleme Kontrol Eksikliği:** Firmware güncelleme sürecinde kurulumu durdurma veya durum kontrolü gibi mekanizmalar eksiktir.

Opportunities (Fırsatlar - Dış Faktörler)

- **Gelecek Sürümler (OCPP 2.0):** Makalenin yazıldığı sırada geliştirilmekte olan OCPP 2.0'ın, talep-yanıt yönetimi, fiyatlandırma, gelişmiş izleme/kontrol gibi alanlarda iyileştirmeler ve potansiyel güvenlik artışları sunma potansiyeli[16].
- **Güvenli Protokollerin Zorunlu Kılınması:** Gelecekteki standartlarda veya uygulamalarda HTTPS, FTPS gibi güvenli protokollerin uçtan uca tünelleme için zorunlu hale getirilmesi.
- **Hafif Tespit Mekanizmaları:** Kısıtlı Saldırı Tespit Sistemleri (IDS) ve güven tabanlı sistemler gibi hafif çözümlerin entegrasyonu.
- **Güçlü Kimlik Doğrulama Standartları:** IEC-62351 gibi standartlarda belirtilen rol tabanlı, izin tabanlı ve bağlamsal kimlik doğrulama/yetkilendirme mekanizmalarının benimsenmesi.
- **Gelişmiş Kayıt Tutma:** Hesap verebilirlik ve inkâr edilemezlik (non-repudiation) için daha ayrıntılı loglama mekanizmalarının geliştirilmesi.
- **Fiziksel Güvenlik Gelişmeleri:** Kontrolörlerin ve sayaçların fiziksel olarak kurcalamaya dayanıklı (tamper-resistant) hale getirilmesi.
- **Standardizasyon Kuruluşlarıyla İşbirliği:** OASIS ve IEC gibi kuruluşlarla yapılacak işbirlikleriyle protokolün daha güvenli ve standart hale getirilmesi.

Threats (Tehditler - Dış Faktörler)

- **Man-in-the-Middle (MitM) Saldırıları:** Protokolün temel zafiyetlerinden biri olup, diğer birçok saldırının (veri sızdırma, manipülasyon, DoS) önünü açar. Özellikle TLS zafiyetleri istismar edilebilir .
- **Denial of Service (DoS / DoES):**
    - Heartbeat interval manipülasyonu .
    - Rezervasyonların süresiz yapılması.

    - LAL/Önbellek temizlenip çevrimdışı moda zorlama .
    - Aşırı büyük veri paketleri gönderme (coercive parsing).
    - TCP SYN flooding / RST enjeksiyonu.
    - CP'nin durumunu `Inoperative` olarak değiştirme[30].
- **Veri Manipülasyonu (Tampering):**
    - Şarj profillerinin değiştirilmesi (şebeke istikrarsızlığı riski) .
    - Firmware veya teşhis dosyası indirme/yükleme URL'lerinin değiştirilmesi .
    - Sayaç değerlerinin (`meterStart`/`meterStop`) değiştirilmesi (enerji hırsızlığı) .
    - LAL listesine sahte ID'ler eklenmesi.
    - Zaman bilgisinin (`currentTime`) değiştirilmesi.
- **Kimlik Sahteciliği (Spoofing):**
    - RFID etiketlerinin klonlanması.
    - Bir CP'nin başka bir CP'nin kimliğine bürünmesi (örn. Algorithm 3).
    - Sahte SOAPAction veya WS-Addressing kullanımı .
- **Enerji Hırsızlığı / Dolandırıcılık:**
    - Sayaç değeri manipülasyonu .
    - İşlemin başka bir istasyona yönlendirilip faturanın kurbana kesilmesi (Algorithm 3) .
    - İçeriden müdahale ile enerjinin başka EVSE'ye yönlendirilmesi.
- **Gizli Saldırılar (Stealth Attacks):**
    - Yan kanal (side-channel) ve gizli kanal (covert-channel) saldırıları.
    - Pasif trafik analizi ile kullanıcı alışkanlıklarının öğrenilmesi.
    - Mahalle izleme (Neighborhood monitoring).
- **Fiziksel Saldırılar:** CP bileşenlerine fiziksel müdahale.

Sonuç: Alcaraz vd. (2017) makalesine göre OCPP 1.6, EV şarj altyapısı için önemli bir standart olmasına rağmen, temel güvenlik varsayımları, zorunlu olmayan güvenlik mekanizmaları ve web teknolojilerine bağımlılığı nedeniyle ciddi siber-fiziksel tehditlere açıktır. Protokolün gelecekteki sürümleri ve tamamlayıcı güvenlik önlemleri (güçlü kimlik doğrulama, zorunlu şifreleme, IDS, fiziksel güvenlik) bu riskleri azaltmak için kritik öneme sahiptir.