BİLGİ SİSTEMLERİ GÜVENLİĞİ DERSİ RAPORU

MAKALE: MitM Cyber Risk Analysis in OCPP enabled EV Charging Stations (OCPP Etkin EV Şarj İstasyonlarında MitM Siber Risk Analizi) **Yazarlar:** Safa Hamdare, David J. Brown, Omprakash Kaiwartya, Yue Cao, Manish Jugran

SWOT ANALİZİ RAPORU

Bu analiz, elektrikli araç (EV) şarj altyapısında yaygın olarak kullanılan Açık Şarj Noktası Protokolü'nün (OCPP) v1.6 sürümündeki güvenlik zafiyetlerini, özellikle Ortadaki Adam (Man-in-the-Middle) saldırılarını inceleyen makalenin güçlü ve zayıf yönlerini, sektörel fırsatlarını ve mevcut tehditlerini değerlendirmektedir.

1. (S) Strengths (Güçlü Yönler)

Madde	Açıklama
Pratik Saldırı Kanıtı	Makale, teorik bir tartışmanın ötesine geçerek, Ubuntu ve Kali Linux sanal makineleri kullanarak OCPP 1.6 üzerinde **başarılı bir MitM saldırısı** (ARP sahteciliği yoluyla) gerçekleştirmiştir [cite: 7, 48, 211-217].
Spesifik Zafiyet Tespiti	En güçlü bulgusu, protokolün TLS 1.2 kullanmasına rağmen güvensiz olduğunu kanıtlamasıdır[cite: 7]. Zafiyeti, TLS el sıkışma (handshake) sürecinde **şifreleme paketleri (cipher suites), oturum kimliği (session ID) ve uygulama protokolü** gibi kritik bilgilerin *düz metin (plaintext)* olarak ifşa edilmesi olarak net bir şekilde tanımlamıştır[cite: 8, 227, 248, 254, 301].
Detaylı Mesaj Analizi	OCPP 1.6'nın Boot Notification, Authorize Request, Start/Stop Transaction ve Meter Value Request gibi her bir mesajını tek tek analiz etmiş; bu mesajlarda hangi verilerin (örn. firmware sürümü, kullanıcı kimliği, sayaç değeri) savunmasız olduğunu ve "Kötü Amaçlı Kullanım" senaryolarını (örn. sahte faturalandırma, hizmet reddi) detaylandırmıştır [cite: 119-197].

Risk Genişliğini Vurgulama	Saldırıların sonuçlarını sadece veri hırsızlığı ile sınırlamamış, aynı zamanda **sahte şarj oturumları, hizmet reddi (DoS) ve hatta elektrik şebekesinin istikrarını bozma** gibi kritik altyapı risklerine bağlamıştır[cite: 41, 73].

2. (W) Weaknesses (Zayıf Yönler)

Madde	Açıklama
OCPP Versiyon Kısıtlılığı	Tüm analiz ve pratik saldırı, **yalnızca OCPP 1.6** sürümüne odaklanmıştır[cite: 5, 7, 43, 86]. Makale, 2.0.1 gibi daha yeni sürümlerin varlığından bahsetse de[cite: 18, 32], bu sürümlerdeki güvenlik durumunu veya keşfedilen zafiyetin oralarda geçerli olup olmadığını analiz etmemiştir.
Genel Çözüm Önerileri	Önerilen karşı önlemler (daha yeni bir TLS sürümüne geçmek, VPN kullanmak, Uç Nokta Tespiti ve Yanıtı (EDR) araçları kullanmak) doğru olmakla birlikte, oldukça genel siber güvenlik tavsiyeleridir[cite: 293, 295]. Protokole özgü (OCPP özelinde) yenilikçi bir savunma mekanizması sunmamıştır.
Saldırı Kapsamı	Çalışma, TLS el sıkışma verilerinin *okunduğunu* başarılı bir şekilde göstermiştir[cite: 8]. Ancak, şifrelenmiş uygulama verilerinin (JSON yükünün) *şifresinin çözüldüğünü (decrypted)* iddia etmemekte, sadece "sofistike saldırıların potansiyel olarak şifreyi çözebileceğini" belirtmektedir[cite: 91, 252].

3. (O) Opportunities (Fırsatlar)

Madde	Açıklama
Protokol Standardı Gelişimi	Makalenin bulguları, standartları belirleyen kurumları ve üreticileri, OCPP 1.6'dan uzaklaşmaya ve TLS 1.3 gibi el sıkışma bilgilerini de şifreleyen daha modern güvenlik protokollerini zorunlu kılmaya teşvik etmektedir [cite: 10, 266, 293-294].
Güvenlik Çözümleri Pazarı	Tespit edilen riskler, özellikle "Eski Sistemler" (Legacy) için, makalede de belirtildiği gibi VPN veya EDR gibi ağ güvenliği çözümleri sağlayan şirketler için net bir pazar fırsatı yaratmaktadır[cite: 295].
Gelecek Araştırma Alanları	Makale, OCPP 1.6'daki güvenlik açıklarının daha fazla değerlendirilmesi [cite: 267] ve aynı MitM metodolojisinin daha yeni OCPP sürümleri (örn. 2.0.1) üzerinde test edilmesi için bir temel oluşturmaktadır.

4. (T) Threats (Tehditler)

Madde	Açıklama
Eski Sistem Riskleri (Legacy Threat)	En büyük tehdit, makalenin analiz ettiği **OCPP 1.6'nın hala yaygın olarak kullanılıyor olmasıdır**[cite: 19]. Bu durum, makaledeki saldırıların sadece teorik değil, sahadaki binlerce istasyon için hala geçerli ve tehlikeli olduğunu göstermektedir.
Hatalı Güvenlik Algısı	Kritik bir tehdit, istasyon operatörlerinin "TLS 1.2 kullandıkları için" güvende olduklarını varsaymalarıdır[cite: 7, 21, 87]. Bu makale, bu varsayımın yanlış olduğunu ve temel TLS 1.2 uygulamasının bile MitM saldırılarına karşı yetersiz kaldığını kanıtlamaktadır[cite: 301].

Düşük Saldırı Eşiği	Saldırının, nmap ve arpspoof gibi yaygın ve erişilebilir penetrasyon testi araçlarıyla gerçekleştirilmiş olması, düşük teknik beceriye sahip saldırganların bile bu zafiyeti istismar edebileceği tehdidini ortaya koymaktadır [cite: 213-217].
Finansal ve Operasyonel Risk	Saldırganların Meter Value (Sayaç Değeri) mesajlarını [cite: 165-166]veya Stop Transaction (İşlemi Durdur) mesajlarını [cite: 179] manipüle etme potansiyeli, operatörler için doğrudan finansal kayıp (sahte faturalandırma) ve hizmet kesintisi (DoS) tehditleri oluşturmaktadır.