BİLGİ SİSTEMLERİ GÜVENLİĞİ DERSİ RAPORU

MAKALE: EmuOCPP: Effective and Scalable OCPP Security and Privacy Testing (EmuOCPP: Etkili ve Ölçeklenebilir OCPP Güvenlik ve Gizlilik Testi) Yazarlar: Soumaya Boussaha, Victor Fresno Gómez, Thomas Barber, Daniele Antonioli

SWOT ANALİZİ RAPORU

Bu analiz, elektrikli araç (EV) şarj altyapısında kullanılan Açık Şarj Noktası Protokolü (OCPP) güvenliğini test etmek için tasarlanmış 'EmuOCPP' adlı gelişmiş bir test aracını tanıtan makalenin, güçlü ve zayıf yönlerini, sektörel fırsatlarını ve mevcut tehditlerini değerlendirmektedir.

1. (S) Strengths (Güçlü Yönler)

Madde	Açıklama
Pratik ve Kapsamlı Test Aracı	Makale, 'EmuOCPP' adında, OCPP v1.6, v2.0, v2.0.1 ve üç güvenlik profilini de (SP1-SP3) destekleyen, ölçeklenebilir ve pratik bir test çerçevesi (framework) sunmaktadır[cite: 343, 374].
Beş Yeni Zafiyet Keşfi	Bu test aracı kullanılarak, protokolün güvenlik profili yükseltme/düşürme (downgrade) mantığını ve CS kimlik doğrulama süreçlerini istismar eden beş yeni ve kritik saldırı (M2, M3, M4, I1, I2) keşfedilmiş ve kanıtlanmıştır [cite: 346, 623-624].
Geniş Kapsamlı Doğrulama	Saldırılar teoride kalmamış; aralarında açık/kapalı kaynaklı sistemler, gerçek bir şarj istasyonu (OpenEVSE) ve büyük bir şirketin operasyonel (production) ağı da bulunan dokuz farklı hedef üzerinde başarılı bir şekilde test edilmiştir [cite: 349, 810-812].

Yüksek Ölçeklenebilirlik	VM (Sanal Makine) tabanlı çözümlerin aksine, konteyner emülasyonu (IPMininet) kullanarak, düşük maliyetli donanımlarla ve tek bir bilgisayarda yüzlerce şarj istasyonunu taklit edebilme kapasitesi kanıtlanmıştır [cite: 344, 375, 382-383, 900].

2. (W) Weaknesses (Zayıf Yönler)

Madde	Açıklama
Tehdit Modeli Kısıtlaması	Tanımlanan tüm saldırılar, saldırganın (fiziksel veya Wi-Fi ile) "şarj ağına erişebildiği" bir yerel ağ (LAN) senaryosunu varsayar[cite: 481, 622]. İnternet üzerinden uzaktan (remote) gerçekleştirilebilecek saldırıları kapsamamaktadır.
Açık Kaynak Test Sınırlılığı	Keşfedilen yeni ve kritik SP2/SP3 saldırıları (M2, M3, M4), test edilen popüler açık kaynaklı sistemler (SteVe, Open E-Mob) bu profilleri desteklemediği için bu sistemler üzerinde doğrulanamamıştır [cite: 824, 826, 829-830, 840].
Harici Bağımlılık	EmuOCPP aracı, 'Mobility House' kütüphanesinin eski bir sürümüne bağımlıdır, çünkü kütüphanenin yeni sürümleri OCPP 2.0 desteğini kaldırmıştır[cite: 577]. Bu durum, aracın gelecekteki bakımını ve güncelliğini zorlaştırabilir.

3. (O) Opportunities (Fırsatlar)

Madde	Açıklama
Protokol Standardı Gelişimi	Bulgular (özellikle I1 - CS Sahteciliği), standarttaki "tanımsız davranışları" ortaya çıkarmıştır. Bu bulguların Open Charge Alliance (OCA) ile paylaşılması [cite: 352, 391, 771], standardın ve uyumluluk testlerinin güçlendirilmesi için bir fırsat yaratmıştır[cite: 734].
Açık Kaynak Güvenlik Ekosistemi	EmuOCPP'nin açık kaynak olarak yayınlanması[cite: 352, 409], üreticilerin, operatörlerin ve diğer araştırmacıların kendi sistemlerini test etmelerine, aracı geliştirmelerine ve tüm ekosistemin güvenliğini artırmalarına olanak tanır.
Disiplinler Arası Entegrasyon	Makale, EmuOCPP'nin Araçtan Şebekeye (V2G) emülatörleri (MiniV2G) veya otomatik fuzzing araçları (OCPPStorm) ile entegre edilerek daha karmaşık siber-fiziksel saldırı senaryolarının incelenmesi için bir kapı aralamaktadır [cite: 926, 942-943].

4. (T) Threats (Tehditler)

Madde	Açıklama
Yaygın Güvensiz Altyapı Tehdidi	Makalenin test ettiği popüler açık kaynaklı CSMS'lerin (SteVe, Open E-Mob) güvenlik profillerini (SP) hiç desteklememesi[cite: 824, 829, 1052, 1060], sahadaki altyapının büyük bir kısmının en temel saldırılara karşı savunmasız olduğu tehdidini doğrulamaktadır.
Fiziksel Güvenlik İhlali Riski	CS Kimlik Sahteciliği (I1) saldırısının, istasyonun üzerine basılmış ve herkesin görebileceği "seri numarası" gibi statik ve kamuya açık bilgilerle yapılabilmesi[cite: 489, 757, 1146], fiziksel güvenliğin siber güvenliği nasıl doğrudan tehlikeye attığına dair büyük bir tehdittir.
Tutarsız Uygulama Tehdidi	Aynı kimlik sahteciliği (I1) saldırısına karşı farklı CSMS'lerin farklı tepkiler vermesi (bazılarının kabul etmesi, bazılarının reddetmesi, bazılarının eski bağlantıyı koparması) [cite: 759, 770, 818-821], sektör genelinde standart bir savunma hattı oluşturmayı imkansız kılan ciddi bir tutarsızlık tehdididir.
SP Düşürme (Downgrade) Tehdidi	M4 saldırısı, sistemlerin bir üst güvenlik profiline (örn. SP3) geçtikten sonra eski ve güvensiz profilleri (örn. SP1) silmemesi gibi basit uygulama hatalarından kaynaklanmaktadır [cite: 732-733].