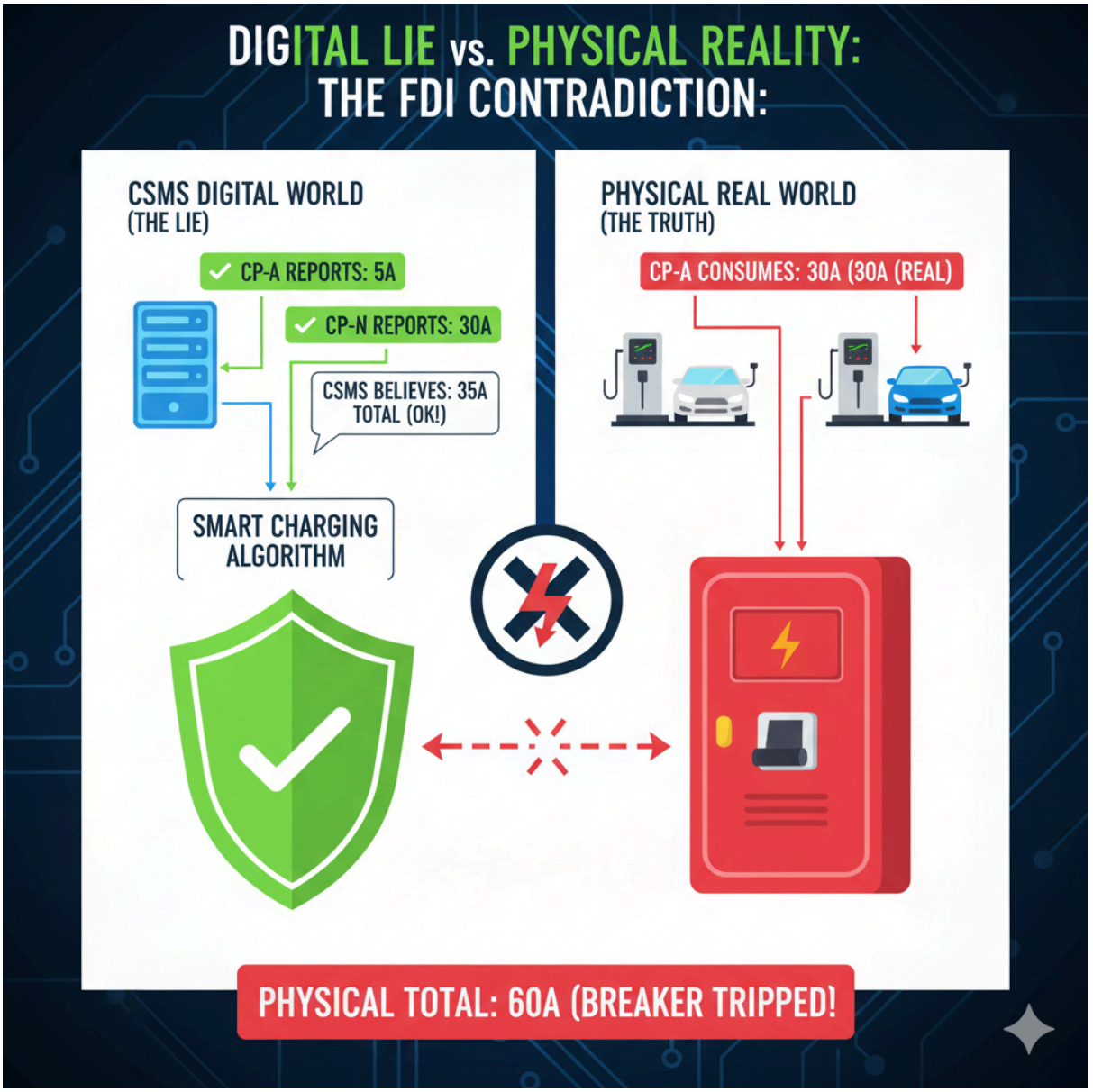
Anomali Senaryosu SWOT Analizi (FDI Saldırısı) SWOT Analizi

Bu analiz, "Akıllı Şarj Hatalı Veri Enjeksiyonu (FDI)" senaryosunun, bir saldırı vektörü olarak güçlü/zayıf yönlerini ve "SecVolt" projesi için yarattığı fırsat/tehditleri değerlendirmektedir.



Resim 1: Saldırı akış yapısı

Güçlü Yönler (Strengths)

(Saldırının, tespit edilmesini zorlaştıran üstünlükleri)

- **Şifrelemeyi Bypass Etme:** Saldırı, wss:// (Güvenli WebSocket) gibi güçlü şifreleme mekanizmalarına dayanmaz. Veri, *kaynakta* (istasyonun içinde) manipüle edildiği için, şifreli kanaldan "meşru" bir veri gibi görünerek geçer.
- **Gizlilik (Stealth):** Geleneksel güvenlik duvarları (Firewall) veya saldırı tespit sistemleri (IDS) için neredeyse görünmezdir. Giden paket (sahte MeterValues) protokol standartlarına (OCPP) %100 uygundur; anormal bir format veya imza taşımaz.
- **Kolektif Hasar (DoS):** Tek bir istasyonu değil, aynı fiziksel devreye (sigortaya) bağlı *tüm* istasyonları etkileyerek bölgesel bir hizmet reddine (DoS) yol açar. Etkisi bireysel değil, kolektifdir.
- **Algoritmik Manipülasyon:** Güvenlik açığı bir kodda değil, CSMS'in "Akıllı Şarj" *algoritmasının mantığındadır*. CSMS'in "güven varsayımı" üzerine kuruludur.

Zayıf Yönler (Weaknesses)

(Saldırının, uygulanmasını zorlaştıran kısıtları)

- **Yüksek Giriş Eşiği:** Saldırının en zor kısmı, "ilk sızma" eylemidir. Saldırganın, istasyonun (CP) işletim sistemine (firmware) JTAG, 0-day açığı veya fiziksel erişim gibi yöntemlerle sızmış olmasını gerektirir.
- **Bağımlılık:** Saldırının yıkıcı etkisi, tamamen CSMS'in "Akıllı Şarj" (Yük Dengeleme) özelliğini *aktif olarak kullanmasına* bağlıdır. Bu özellik kapalıysa, saldırı anlamsız kalır.
- **Dolaylı Etki:** Saldırı, saldırgana doğrudan finansal kazanç (ücretsiz şarj) sağlamaz; amacı sabotaj ve hizmet kesintisidir.

Fırsatlar (Opportunities)

(Bu senaryonun "SenVolt" projesi için yarattığı değer ve imkanlar)

- **Gelişmiş Anomali Tespiti:** Bu senaryo, "SenVolt" için en büyük satış vaadini oluşturur. "SenVolt", sadece OCPP loglarına bakmak yerine, bu logları **bölgesel akıllı sayaç verileri (fiziksel gerçeklik)** ile çapraz doğrulayarak (cross-validation) bu saldırıyı tespit edebilen *tek* platform olma fırsatına sahiptir.
- **Üretici Denetimi (Danışmanlık):** "SenVolt", istasyon (CP) üreticilerine "Firmware Denetimi" hizmeti sunabilir. Firmware'in, MeterValues (tüketim) ile donanımın kendi çektiği akım arasında bir "sağduyu kontrolü" (sanity check) yapıp yapmadığını test edebilir.
- **Sektörel Farkındalık:** Projenin, "Güvenlik sadece şifreleme değildir, aynı zamanda mantıksal doğrulamadır" temasını işlemek için bu niş senaryoyu kullanma fırsatı vardır.

Tehditler (Threats)

(Bu senaryonun, "SenVolt" projesi veya tüm pazar için oluşturduğu riskler)

- **Sektörel Atalet (Yavaş Tepki):** İstasyon üreticilerinin, bu tür "mantıksal" zafiyetleri düzeltmek için gerekli firmware güncellemelerini yayınlamakta yavaş kalması en büyük tehdittir.
- **Yanlış Güvenlik Algısı:** Pazardaki CSMS operatörlerinin "Biz wss:// kullanıyoruz, güvendeyiz" şeklindeki yanlış güvenlik algısı, "SenVolt"un bu gelişmiş tehdit modelini pazarlamasının önünde bir engel teşkil edebilir.
- **Artan Saldırı Yüzeyi:** İstasyonlar akıllandıkça (daha fazla yazılım içerdikçe), saldırganların "ilk sızma" (Grup 1'in Zayıf Yönü) için kullanabileceği yazılım açıkları ve sızma yöntemleri de artmaktadır.