**Makale Başlığı: Hibrit Tehdit Modeli: Elektrikli Araç Şarj İstasyonlarında (CP) Çevrimdışı Yetkilendirme Zafiyetinin İstismarı Üzerine Bir Anomali Senaryosu (E-01)**

**Yazar:** [Adınız/Grup Adınız] **Kurum:** [Üniversiteniz/Bölümünüz] **Ders:** BSG - Bilgi ve Sistem Güvenliği

**1. Özet (Abstract)**

Elektrikli araç (EA) şarj altyapısı, modern siber-fiziksel sistemlerin kritik bir bileşeni haline gelmektedir. Bu sistemler, Şarj Noktaları (CP) ve Merkezi Şarj İstasyonu Yönetim Sistemleri (CSMS) arasında sürekli bir iletişim gerektirir. Ancak, bu iletişimin kesintiye uğradığı "çevrimdışı" durumlar için tasarlanan mekanizmalar, ciddi güvenlik zafiyetlerine yol açabilir. Bu makale, bir Hizmet Reddi (DoS) saldırısı ile zayıf bir yapılandırma ayarının birleştirildiği hibrit bir saldırı senaryosunu (E-01) analiz etmektedir. Senaryo, STRIDE metodolojisi kapsamında "Ayrıcalık Yükseltme" (Elevation of Privilege) olarak sınıflandırılmıştır. Çalışma, bir siber saldırının nasıl doğrudan fiziksel bir kaynak (enerji) hırsızlığına dönüştüğünü ve bu tür anomalilerin tespit edilme zorluklarını ortaya koymaktadır.

**2. Giriş**

Elektrikli araçların yaygınlaşması, geniş ve dağıtık bir şarj istasyonu ağını zorunlu kılmıştır. Bu ağlar, temel olarak OCPP (Open Charge Point Protocol) gibi protokoller aracılığıyla bir merkezi yönetim sistemi (CSMS) ile iletişim kuran şarj noktalarından (CP) oluşur. CSMS, kullanıcı yetkilendirme, faturalandırma ve istasyon yönetimi gibi kritik işlevleri yerine getirir. Ancak, ağ bağlantısındaki kesintiler (örneğin, zayıf sinyal veya kasıtlı saldırılar) nedeniyle CP'ler periyodik olarak çevrimdışı çalışmak zorunda kalabilir. Bu çalışma, bu çevrimdışı modun hatalı yapılandırılmasının yarattığı güvenlik riskine odaklanmaktadır.

**3. Senaryo Analizi: E-01 Zafiyeti**

Analiz edilen senaryo, iki aşamalı bir saldırı vektörüne dayanmaktadır. Saldırının temel amacı, yetkisiz bir kimlik kullanarak şarj istasyonundan ücretsiz enerji temin etmektir.

**3.1. Aşama 1: Ağ İzolasyonu (DoS Saldırısı)**

Saldırının ilk adımı, hedeflenen CP'nin CSMS ile olan iletişimini kesmektir. Saldırgan, CP'nin ağ arayüzüne (Wi-Fi, 4G/LTE veya Ethernet) yönelik bir Hizmet Reddi (DoS) saldırısı (örneğin, bir sinyal bozucu (jammer) kullanarak veya TCP/IP sel saldırısı ile) gerçekleştirir.

* **Anomali Tespiti (Ağ Seviyesi):** Bu aşamada, CSMS tarafında ilgili CP'den periyodik "Heartbeat" (Kalp Atışı) mesajlarının gelmemesi veya CP'nin "Offline" statüsüne geçmesi bir anomali olarak gözlemlenir. Ancak bu durum, genellikle basit bir ağ kesintisi olarak yorumlanabilir ve kötü niyetli bir eylem olarak hemen ayırt edilemeyebilir.

**3.2. Aşama 2: Çevrimdışı Modun İstismarı**

CSMS'e ulaşamayan CP, yapılandırmasına göre "çevrimdışı mod"a geçer. Saldırının kilit noktası bu aşamada devreye girer. Birçok şarj istasyonu, çevrimdışı durumlarda bile hizmet sürekliliğini sağlamak için esnek yapılandırma parametrelerine sahiptir.

* **Zayıf Yapılandırma:** OfflineTxForUnknownIdEnabled = true
* **Açıklama:** Bu boolean parametre, CP'nin çevrimdışıyken, CSMS tarafından bilinmeyen veya yerel beyaz listede (LocalAuthList) bulunmayan RFID kartları (IdTag) bile kabul etmesine izin verir.

**3.3. Saldırı Akışı ve Ayrıcalık Yükseltme**

1. **Bağlantı Kesme:** Saldırgan, DoS saldırısı ile CP'yi çevrimdışı moda zorlar.
2. **Kimlik Doğrulama Girişimi:** Saldırgan, aracını istasyona bağlar ve herhangi bir geçersiz, sahte veya klonlanmış bir RFID kartı okutur.
3. **Yerel Yetkilendirme (İstismar):** CP, okutulan IdTag'i doğrulamak için CSMS'e danışamaz. OfflineTxForUnknownIdEnabled ayarı true olduğundan, CP bu bilinmeyen kimliği "geçici olarak geçerli" kabul eder.
4. **Ayrıcalık Yükseltme (STRIDE: E):** Saldırgan, "kimliği doğrulanmamış kullanıcı" statüsünden, "şarj işlemi yapmaya yetkili kullanıcı" statüsüne yükselir.
5. **İşlem Başlatma:** CP, şarj işlemini başlatır ve enerji akışına izin verir.

**4. Etki ve Anomali Tespiti (Sistem Seviyesi)**

Bu saldırının nihai etkisi, doğrudan finansal kayba yol açan yetkisiz erişim ve enerji hırsızlığıdır.

* **Anomali Tespiti (İşlem Seviyesi):** Saldırının tespiti genellikle *post-facto* (olay sonrası) gerçekleşir. CP tekrar çevrimiçi olduğunda, çevrimdışı modda gerçekleştirdiği işlemleri (Transaction.req) CSMS'e gönderir. CSMS, bu işlem kayıtlarını analiz ettiğinde, sistemde kayıtlı olmayan veya bakiyesi bulunmayan bir IdTag ile başarılı bir şarj işlemi yapıldığını fark eder. Bu durum, belirgin bir yetkilendirme anomalisidir.
* **Siber-Fiziksel Etki:** Bu senaryo, bir siber güvenlik zafiyetinin (zayıf yapılandırma) ve bir ağ saldırısının (DoS), nasıl doğrudan bir fiziksel varlığın (elektrik enerjisi) çalınmasına yol açtığını net bir şekilde göstermektedir.

**5. Önerilen Karşı Tedbirler ve Sonuç**

Bu tür bir anomali senaryosunun ve istismarın önlenmesi için "derinlemesine savunma" (defense-in-depth) prensibi uygulanmalıdır:

1. **Güvenli Yapılandırma (Altın Kural):** OfflineTxForUnknownIdEnabled parametresi, istisnai durumlar dışında daima false olarak ayarlanmalıdır.
2. **Yerel Beyaz Liste (LocalAuthList) Kullanımı:** Çevrimdışı yetkilendirme gerekiyorsa, bu işlem yalnızca CSMS'ten periyodik olarak senkronize edilen, bilinen ve onaylanmış kullanıcıların IdTag'lerini içeren bir yerel beyaz liste (LocalAuthList) üzerinden yapılmalıdır.
3. **Ağ İzleme ve Dayanıklılık:** CP'lerin ağ bağlantıları, anormal trafik paternlerini (DoS tespiti) izleyen sistemler (IDS/IPS) ile korunmalı ve mümkünse yedekli iletişim kanalları (örn. 4G ve Ethernet birlikte) kullanılmalıdır.
4. **İşlem Hacmi Sınırlaması:** Çevrimdışı modda gerçekleştirilebilecek toplam işlem sayısına veya enerji miktarına (kWh) bir sınır getirilebilir.

**Sonuç olarak,** E-01 senaryosu, dağıtık siber-fiziksel sistemlerde hizmet sürekliliği (availability) sağlamak amacıyla eklenen özelliklerin, güvenli yapılandırılmadığı takdirde nasıl ters etki yaratarak Ayrıcalık Yükseltme (Elevation of Privilege) saldırılarına kapı açtığını göstermektedir. Bilgi ve sistem güvenliği uzmanları, sadece çevrimiçi tehditlere değil, aynı zamanda sistemlerin çevrimdışı çalışma modlarının mantıksal zafiyetlerine de odaklanmalıdır.