Elektrikli Araç Şarj Yüklerinin Doğrusal Olmayan Yapısından Kaynaklanan Yüksek Reaktif Güç Talebi Saldırısı

◇ 1. Giriş

Elektrikli araçlar (EV), enerji sistemlerinin vazgeçilmez bir parçası haline gelirken , akıllı şebekeye olan bağlantıları, siber saldırılar için yeni ve kritik yüzeyler yaratmaktadır. EV şarj yüklerinin doğasından kaynaklanan kendine has özellikler, geleneksel siber saldırılardan daha yıkıcı sonuçlar doğurabilecek yeni siber-fiziksel saldırı vektörlerine zemin hazırlamaktadır. Bu raporda, EV şarj yüklerinin **doğrusal olmayan (non-linear)** yapısının kötüye kullanılmasıyla gerçekleştirilen **"Yüksek Reaktif Güç Talebi Saldırısı (High Reactive Power Demand Attack)"** incelenmiştir.

◇ 2. Temel Kavramlar

- **Reaktif Güç (Reactive Power / VAR):** Şebekedeki gerilim seviyelerini etkileyen ve alternatif akım (AC) devrelerinde manyetik alanlar için alınıp verilen güçtür.

- **Doğrusal Olmayan Yük (Non-linear Load):** Sinüzoidal gerilimden sinüzoidal olmayan akım çeken yüklerdir. EV şarjı, redresör devrelerine dayandığı için tipik bir doğrusal olmayan yüktür ve bu durum yüksek harmonik bozulmaya yol açar.

- **Düşük Güç Faktörü (Low Power Factor - pf):** EV şarj yükleri, yüksek reaktif güç talebi nedeniyle genellikle düşük bir güç faktörüne (örneğin pf=0.6 lagging) sahiptir. Bu, aynı aktif güç için şebekeye çok daha fazla yük bindirir.

◇ 3. Saldırının Tanımı

Yüksek Reaktif Güç Talebi Saldırısı, bir saldırganın şarj iletişim protokollerindeki güvenlik zafiyetlerini kullanarak ele geçirdiği çok sayıda şarj istasyonundan (botnet)

oluşan EV'lere, **şebekeyi destabilize edecek şekilde senkronize edilmiş yüksek reaktif güç çekme** komutunu göndermesidir.

Bu saldırı, aktif güç (MW) değişimi yerine, özellikle voltaj kararlılığı ile yakından ilişkili olan reaktif güce (MVAR) odaklanır. Saldırının kritik etkisi şudur.

Geleneksel konut yükleriyle yapılan daha büyük bir saldırı (48 MW), şebekede yalnızca bir frekans düşüşüne neden olurken, **daha küçük bir EV yük saldırısı** (30 MW), şebekeyi tamamen senkronizasyon dışına çıkarıp tam bir çöküşe yol açabilir.

◇ 4. Saldırının Gerçekleşme Aşamaları

1. **Keşif ve Zafiyet Analizi:** Saldırgan, OCPP (v1.6/v2.0.1) protokolündeki isteğe bağlı (optional) şifreleme ve kimlik doğrulama mekanizmalarındaki boşlukları veya EVCS'nin firmware'indeki bilinen zafiyetleri (örneğin SQL Enjeksiyonu veya Hard-Coded şifreler) tespit eder. Şebeke kararlılık analiz yöntemleri (PV/QV eğrileri) kullanılarak saldırı için en zayıf baralar (buses) belirlenir.

2. **Yetki Yükseltme ve Botnet Oluşturma:** Tespit edilen zafiyetler (XML/External Entity Injection, XSS) kullanılarak EVCS'lere sızılır ve Yönetici (Admin) yetkileri ele geçirilir. Bu yetkilerle EVCS'ler, uzaktan kontrol edilebilir bir botnet'e dönüştürülür. Kontrol edilebilir güç dönüştürücülerine sahip EVCS'ler, reaktif güç (VAR) çekimi için manipüle edilmeye hazır hale getirilir.

3. **Saldırı Komutu ve Uygulama:** Saldırgan, ele geçirdiği EVCS'lere, hedef şebeke barası üzerinde **yüksek reaktif güç (düşük güç faktörü)** çekecek şekilde senkronize edilmiş şarj komutlarını gönderir.

4. **Şebeke Çöküşü:** Şebekeye aniden eklenen yüksek reaktif yük, voltaj seviyelerinde hızlı düşüşlere, jeneratörlerin aktif ve reaktif güç çıkışlarında kaotik (salınımlı) dalgalanmalara yol açar. Bu durum, sistemin senkronizasyonunu kaybetmesine ve koruma rölelerinin tetiklenerek geniş çaplı elektrik kesintisine (blackout) yol açar.

◇ 5. Olası Etkiler

- **Voltaj Kararsızlığı ve Gerilim Çökmesi:** Elektrikli araç (EV) yüklerinin doğalından gelen yüksek reaktif güç talebi, şebekedeki kritik gerilim seviyelerinin hızla düşmesine yol açar ve sistemi gerilim çökmesi (voltage collapse) noktasına yaklaştırır.
- **Fiziksel Ekipman Hasarı:** Saldırı sonucu, jeneratörlerin aktif ve reaktif güç çıkışlarında meydana gelen hızlı ve şiddetli salınımlar (osilasyonlar), türbinlerde aşırı titreşimlere neden olur. Bu durum, milyonlarca dolarlık geri dönüşü olmayan ekipman hasarına yol açar.
- **Geniş Çaplı Sistem Çöküşü:** Şebekenin tamamen destabilize olması, jeneratörlerin senkronizasyonu kaybetmesine ve koruma rölelerinin tetiklenmesine neden olarak geniş çaplı bölgesel elektrik kesintilerine (blackout) yol açar.
- **Artan Operasyonel ve Finansal Maliyetler:** Anormal yük artışları ve frekans/voltaj dalgalanmaları, şebekeyi optimal dağıtım noktasından saptırarak iletim kayıplarını yükseltir. Ayrıca, tepe yük jeneratörlerinin düzensiz çalıştırılması, bakım ve işletme maliyetlerinin ciddi oranda artmasına neden olur.
-

◇ 6. Anomali Tespiti (Detection)

Bu tür siber-fiziksel saldırılar, hem iletişim ağında hem de fiziksel şebeke üzerindeki anormal yük değişimleriyle tespit edilebilir.

- **Şebeke Tabanlı Tespit (Grid-Based Detection):**
  - **Reaktif Güç İzleme:** İletim ve dağıtım seviyelerinde, normal yük profillerinden sapan **ani ve yüksek reaktif güç talebi artışı** ve **harmonik seviyelerdeki yükseliş** sürekli olarak izlenmelidir.
  - **Kompanzasyon Durumu:** VAR kompanzasyon mekanizmalarının çıkışları ve durumları, anormal reaktif güç ihtiyacının ek bir göstergesi olarak algoritmaya dahil edilebilir.
- **Makine Öğrenmesi Modelleri (EVCS-Based Detection):**
  - **Toplu İzleme (Top View):** Makine öğrenimi algoritmaları (örneğin Isolation Forest, Autoencoder), normal şarj davranışından (tarihsel veriler) sapma gösteren, **doğal olmayan toplu şarj/deşarj seanslarını** tespit etmek için kullanılmalıdır.

- **Bireysel İzleme (Station View):** Her bir şarj istasyonuna gömülü küçük ajanlar, kendi rutininden sapan (örneğin aniden düşük güç faktöründe çalışmaya başlamak gibi) bireysel anormallikleri tespit ederek merkezi kontrol sistemine alarm göndermelidir.

◇ 7. Önleme ve Güvenlik Önerileri

- **Protokol Güvenliğinin Zorunluluğu:** OCPP (v2.0.1) ve ISO 15118 gibi protokollerdeki **şifreleme (TLS) ve sertifika tabanlı karşılıklı kimlik doğrulama** ayarları, maliyet düşürmek adına **esnek bırakılmayıp zorunlu hale getirilmelidir**.
- **Yazılım Güvenliği Pratikleri:** SQL/XML/XSS enjeksiyonları gibi yazılım zafiyetlerini önlemek için **parametreleştirilmiş sorgular** kullanılmalı, HTTP parametreleri filtrelenmeli ve EVCS'ler için **güvenli-tasarım (secure-by-design)** ilkeleri benimsenmelidir.
- **Komuta Doğrulama ve Ağ Segmentasyonu:** Kritik işlemler (şarj başlatma/durdurma, konfigürasyon değiştirme) için çok faktörlü doğrulama veya onay mekanizması eklenmelidir. Şarj istasyonları, saldırganın yanal hareketini engellemek için genel internet erişiminden **ağ segmentasyonu** ile izole edilmelidir.
- **Donanım Koruması:** Fiziksel erişim yoluyla sertifika çalınmasını veya firmware kurcalanmasını önlemek için **şok dirençli kasalar** ve yazılım tabanlı kurcalama önleyici çözümler uygulanmalıdır.

◇ 8. Sonuç

Yüksek Reaktif Güç Talebi Saldırısı, elektrikli araç şarj altyapılarının ve dolaylı olarak ulusal enerji sistemlerinin kararlılığı için yüksek riskli bir tehdidi temsil eder. Saldırının yıkıcı potansiyeli (ekipman hasarı ve bölgesel kesintiler) göz önüne alındığında, **bütünlük (Integrity)** ve **erişilebilirlik (Availability)** gereksinimlerini karşılamak için protokol güvenliğinden (TLSv1.3), anomalileri tespit eden makine öğrenimi tabanlı izleme sistemlerine kadar bütüncül güvenlik çözümleri zorunludur.

◇ 9. Kaynaklar

Sayed, 2021 Electric Vehicle Attack Impact on Power Grid Operation *International Journal of Electrical Power & Energy Systems*

Alcaraz, 2023 OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0 *International Journal of Information Security*