Anomali Senaryosu

Senaryo Adı: Şarj İstasyonu Kimlik Sahteciliği Anomalisi (Charging Station Identity Spoofing)

Hazırlayan: Betül ALTUNYUVA

Tarih: 2.11.2025

Senaryo Özeti:

Bu senaryoda saldırgan, bir şarj istasyonunun kimliğini taklit ederek (spoofing) aracı yanlış bir enerji kaynağına yönlendirir veya araca zararlı konfigürasyon/komutlar gönderir. Sonuç olarak araç, güvenli olmayan bir kaynaktan enerji alabilir, kimlik doğrulama sürecini atlatarak yetkisiz erişime maruz kalabilir veya şarj sürecinde veri bütünlüğü bozulabilir.

Senaryonun Amacı:

- Araç-şarj istasyonu oturumu sırasında kimlik doğrulamayı atlatmak veya değiştirmek.
- Aracın şarj profili, fatura bilgisi ya da güvenlik parametrelerini manipüle ederek ek mali zarar veya güvenlik riski oluşturmak.
- İleri aşamada araca zararlı komutlar (ör. firmware update tetiklemesi) göndererek sistem bütünlüğünü bozmak.

Senaryonun Kapsamı:

- **Hedef sistem:** EV ile şarj istasyonu arasındaki iletişim protokolleri (OCPP, ISO 15118, PLC üzerinden şarj haberleşmesi), şarj istasyonu kimlik doğrulama mekanizmaları, araç şarj kontrol modülü.
- **Ortam:** Halka açık şarj ağları, ev/iş yerindeki şarj istasyonları, hızlı şarj (DC) terminalleri.
- **Saldırı vektörleri:** Rogue (sahte) şarj istasyonu kurulumu, man-in-the-middle (MITM) saldırısı, DNS/PKI sahtekarlığı, sahte sertifika kullanımı.

Hedefler ve Tehdit Modeli:

- **Hedef:** Aracın bağlantı kurduğu şarj istasyonunun kimliğini değiştirmek veya taklit etmek; yetkisiz enerji sağlama/cihaz komutları gönderme.
- **Tehdit aktörü:** Bireysel siber saldırganlar, organize gruplar veya kötü niyetli bakım personeli.

- **Yetki düzeyi:** Orta (ağ seviyesinde erişim) → Yüksek (fiziksel istasyon kurulumuna sahip).
- **Başarının ölçütü:** Araç ile istasyon arasında güvenli, doğrulanmış bir oturum kurulamayacak veya araç yanlış/zararlı komutlar uygulayacak.

Adım Adım Saldırı Akışı:

1. **Keşif:** Saldırgan, hedef bölgede kullanılan şarj protokollerini (ISO 15118, OCPP) ve sertifika yapılarını analiz eder.
2. **Hazırlık:** Geçersiz fakat araç tarafından kabul edilebilecek sahte sertifikalar, veya MITM için uygun ağ cihazları hazırlanır.
3. **Konumlandırma:** Saldırgan fiziksel olarak sahte bir şarj istasyonu kurar veya gerçek bir istasyonun arayüzüne MITM cihazı yerleştirir.
4. **Başlatma:** Araç şarj portuna bağlandığında, sahte istasyon kimliğini sunar; eğer araç/istasyon arasında PKI doğrulaması zayıf ise kimlik kabul edilir.
5. **Manipülasyon:** Sahte istasyon, şarj akımı, gerilim profili, fatura bilgileri veya OTA güncelleme isteği gibi paketleri manipüle eder.
6. **Sürdürme / Kaçış:** Saldırgan oturumu sürdürerek veri çalma, ücretlendirme hilesi veya kötü amaçlı güncelleme tetikleme yapar; eylem sonra izler silinir.

Beklenen Etkiler:

- Araç güvenlik parametrelerinin veya enerji profillerinin bozulması (aşırı/yanlış şarj).
- Kullanıcının mali zarara uğraması (faturalandırma manipülasyonu).
- Araç yazılımının yetkisiz güncellenmesi veya konfigürasyonunun değiştirilmesi → fonksiyon kayıpları / arıza.
- Şarj altyapısına olan güvenin azalması ve düzenleyici sorunlar.

Tespit Metodları:

- Karşılıklı PKI doğrulaması başarısızlık/log incelemeleri (sertifika zinciri hataları).
- OCPP/ISO 15118 oturum loglarında beklenmeyen komutlar veya sıra dışı istekler.
- Fiziksel istasyon envanterinin ve ağ topolojisinin tutarsızlığı (kayıtlı istasyon listesi ile eşleşmeme).
- Anormal faturalandırma/paket hacmi tespiti (ör. aynı anda birçok oturum açma).
- Araç tarafında şarj profili anormalliklerinin tespiti (beklenen SoC artış eğrisinden sapma).

- IDS/IPS ya da ağ tabanlı anomaly detection sistemleri ile MITM belirtilerinin yakalanması.

Önleme Yöntemleri:

- **Güçlü PKI & Sertifika Yönetimi:** Araç ve şarj istasyonu arasında çift yönlü, güçlü sertifika doğrulaması; sertifika iptal listesi (CRL) ve OCSP kullanımının zorunlu tutulması.
- **Mutual TLS / Güvenli Kanallar:** Şarj haberleşmesini TLS/DTLS gibi güvenli kanallar üzerinden yürütmek ve MITM riskini azaltmak.
- **Donanım Tabanlı Güvenlik:** Araçta ve istasyonda TPM/HSM gibi güvenli elementler kullanarak kritik anahtarları korumak.
- **Oturum ve Mesaj İmzalama:** Tüm kontrol mesajlarının dijital imzalanması ve nonce/timestamp ile replay koruması.
- **Ağ İzleme ve Anomali Tespiti:** Şarj ağlarında gerçek zamanlı trafik analizi ve anormal oturumların otomatik engellenmesi.
- **Yetkilendirme Politikaları:** Sahte istasyonların hızlı tespiti için merkezi envanter ve lokasyon tabanlı doğrulama (istasyon ID + GPS koordinat kontrolü).
- **Güncelleme Politikaları:** OTA güncellemeler için ek doğrulama (imza, sürüm eşleştirme, kullanıcı onayı) ve rollback koruması.
- **Kullanıcı Farkındalığı:** Kullanıcıya, bilinmeyen veya kayıtlı değil istasyonlara bağlanmama uyarısı ve manuel onay talebi.