T - Tampering (Tahrifat / Kurcalama)

Hedef: Verilerin veya sistem bileşenlerinin (yazılım/donanım) bütünlüğünü bozarak yetkisiz değişiklikler yapmak.

1. Saldırı Ağacı - Enerji Ölçüm Verisi Tahrifatı (MitM)

Hedef: Şarj Faturasını Düşürmek/Sıfırlamak

Adım 1: CS ve CSMS Arasındaki İletişime Araya Girmek (MitM)
Alt Adım 1a: İstasyonun kullandığı 3G/4G/Wi-Fi ağına (örn. sahte baz istasyonu, Rogue AP) veya fiziksel Ethernet hattına erişim sağla.
Alt Adım 1b: ARP Spoofing veya DNS Spoofing ile trafiği kendi cihazın üzerinden geçir.

Adım 2: Şifresiz OCPP Trafiğini Dinlemek
Alt Adım 2a: İletişimin ws:// (şifresiz WebSocket) olduğunu doğrula.

Adım 3: İlgili Mesajı Yakalamak
Alt Adım 3a: Şarj bittiğinde gönderilen StopTransaction.req OCPP mesajını yakala.

Adım 4: Mesajı Manipüle Etmek

Alt Adım 4a: Mesaj içindeki meterStop: 50000 (Wh) değerini meterStop: 1000 (Wh) olarak değiştir.

Adım 5: Değiştirilmiş Mesajı CSMS'e İletmek
Alt Adım 5a: CSMS, tahrif edilmiş veriyi alır ve kullanıcıyı sadece 1 kWh için faturalandırır.

2. Sömürü Senaryoları

Firmware Manipülasyonu: İstasyonun firmware güncellemesini güvensiz bir HTTP bağlantısı üzerinden veya imzasız olarak alması. Saldırgan, MitM ile bu güncellemeyi yakalar ve içine zararlı kod (örn. veri çalan bir servis veya bir botnet ajanı) enjekte edilmiş sahte bir firmware yükler.

Şarj Fiyatlandırması Değiştirme: CSMS'in admin paneline veya API'sine (örn. SQL Injection, BFLA) sızan saldırgan, fiyat tarifesini (örn. kWh başına 0 TL veya 1000 TL) değiştirerek finansal kaos yaratır.

3. Azaltma Stratejileri (Mitigation)

OCPP Güvenlik Profili 2 veya 3 (wss://): Tüm OCPP iletişimini zorunlu olarak Güvenli WebSocket (TLS üzerinden) ile yapmak. Bu, MitM saldırganının trafiği okumasını ve değiştirmesini engeller.

İmzalı Firmware ve Güvenli Önyükleme (Secure Boot): Tüm firmware güncellemelerinin üretici tarafından kriptografik olarak imzalanmasını ve istasyonun donanımının (örn. TPM/Secure Boot) sadece bu imzalı kodu çalıştırmasını zorunlu kılmak.

Sıkı Erişim Kontrolü (CSMS): Fiyatlandırma gibi kritik veritabanı tablalarına/API'lerine erişimi en aza indirmek, MFA (Çok Faktörlü Kimlik Doğrulama) ve "En Az Yetki Prensibi" uygulamak.

4. Tespit Mekanizmaları (Detection)

İletişim Uyumsuzluğu: wss:// (şifreli) bekleyen bir CSMS'in, ws:// (şifresiz) bir bağlantı denemesi alması durumunda kritik alarm üretmesi.

Mantıksız Veri Analizi: CSMS'in, "Şarj 3 saat sürdü ancak meterStop değeri 0 geldi" gibi mantıksız işlem kayıtlarını tespit etmesi.

Dosya Bütünlük İzleme (FIM): İstasyonun, periyodik olarak kendi firmware dosyasının hash (bütünlük) değerini CSMS'e raporlaması. CSMS, bu hash'in beklenen değerle uyuşmadığını tespit ederse

T - Tampering (Tahrifat / Kurcalama)

Tehdit Senaryosu: "Enerji Ölçüm Verisi Tahrifatı (MitM ile)"
(Saldırganın, StopTransaction mesajındaki enerji miktarını (meterStop) değiştirerek faturayı sıfırlaması.)

D - Damage Potential (Zarar Potansiyeli): 8
Gerekçe: Doğrudan ve tekrarlanabilir finansal kayba (ücretsiz şarj) yol açar. Güvenilirliği sarsar ve yaygınlaşırsa operatörün gelir modelini çökertir.

R - Reproducibility (Tekrarlanabilirlik): 7
Gerekçe: TLS (wss://) kullanılmıyorsa ve saldırgan ağa (örn. sahte Wi-Fi) girebilirse, bu saldırı yüksek bir başarı oranıyla tekrarlanabilir.

E - Exploitability (İstismar Edilebilirlik): 6
Gerekçe: MitM pozisyonuna (ağa) girmek ve OCPP protokolünü anlayıp anlık olarak manipüle edecek (örn. Scapy, Burp) araçları kullanmak için orta seviye üzerinde teknik bilgi gerektirir.

A - Affected Users (Etkilenen Kullanıcılar): 9
Gerekçe: Saldırganın bulunduğu ağdaki (örn. bir AVM otoparkı) tüm istasyonlar ve o istasyonları o an kullanan tüm kullanıcılar etkilenir (sadece saldırgan değil, herkesin işlemi manipüle edilebilir).

D - Discoverability (Keşfedilebilirlik): 5
Gerekçe: Ağ trafiğini (Wireshark) dinleyerek ws:// (şifresiz) bağlantı aramak gerekir. Herkese açık bir bilgi değildir, ancak ağa erişimi olan biri için tespiti kolaydır.

Risk Skoru: 35/50 (Yüksek Risk)

Sacide Aişenur Direk