S - Spoofing (Kimlik Sahtekarlığı)

Hedef: Başka bir varlığın (kullanıcı, istasyon, CSMS) kimliğine bürünerek yetkisiz eylemler gerçekleştirmek.

1. Saldırı Ağacı - RFID Kart Kopyalama

Hedef: Ücretsiz Şarj Almak

Adım 1: Meşru Bir Kullanıcının RFID Kartına Erişim
Alt Adım 1a: Yakın mesafe okuyucu (skimmer) ile kartı gizlice okumak.
Alt Adım 1b: Sosyal mühendislik ile kartı anlık olarak ödünç almak.

Adım 2: Kart ID'sini Kopyalamak
Alt Adım 2a: Zayıf kart protokolü (örn. Mifare Classic) kullanılıyorsa, ID'yi ve veriyi kopyala.

Adım 3: ID'yi Boş Bir Karta veya Cihaza Yazmak
Alt Adım 3a: Kopyalanan ID'yi boş bir klon karta yaz.
Alt Adım 3b: ID'yi bir akıllı telefona (NFC) veya Proxmark gibi bir araca kaydet.

Adım 4: Klon Kart/Cihaz ile Şarjı Başlatmak
Alt Adım 4a: Şarj istasyonuna git ve klon kartı okut.
Alt Adım 4b: CSMS, klonlanan ID'yi meşru kullanıcı olarak doğrular ve şarj başlar.

2. Sömürü Senaryoları

EV Kimlik Doğrulama Bypass (Plug & Charge - ISO 15118): "Plug & Charge" teknolojisi, aracın dijital bir sertifika (EVCCID) ile kimliğini doğrulamasını kullanır. Eğer bu sertifika yönetimi (PKI) zayıfsa veya özel anahtar (private key) araçtan çalınabilirse, bir saldırgan bu aracı taklit ederek şarj alabilir.

Sahte Şarj İstasyonu Saldırısı (CS Spoofing): Bir saldırgan, dizüstü bilgisayarında sahte bir istasyon (OCPP istemcisi) çalıştırır. Eğer CSMS, istasyonları sadece ChargeBoxID (basit bir metin) ile doğruluyorsa ve mTLS (karşılıklı sertifika) kullanmıyorsa, saldırgan kendini meşru bir istasyon gibi CSMS'e bağlayabilir.

Buradan merkeze sahte şarj kayıtları gönderebilir veya ağ hakkında bilgi toplayabilir.

3. Azaltma Stratejileri (Mitigation)

Güçlü RFID Teknolojisi: Klonlanması çok zor olan (Mifare Classic yerine) Mifare DESFire EV2/EV3 gibi kriptografik imzalama yeteneğine sahip kartlar kullanmak.

OCPP Güvenlik Profili 3 (mTLS): CSMS ve şarj istasyonu arasındaki iletişimde karşılıklı TLS (mTLS) kimlik doğrulamasını zorunlu kılmak. Bu, istasyonun da CSMS'e geçerli bir istemci sertifikası sunmasını gerektirir ve "Sahte İstasyon" saldırılarını engeller.

ISO 15118 PKI: "Plug & Charge" için güvenli donanım (HSM) tabanlı, sağlam bir Açık Anahtar Altyapısı (PKI) kurmak ve araçtaki özel anahtarların Güvenli Eleman (SE) içinde saklanmasını sağlamak.

İkincil Doğrulama: RFID'ye ek olarak mobil uygulama üzerinden "Şarjı Onayla" bildirimi göndermek (İki Faktörlü Doğrulama).

4. Tespit Mekanizmaları (Detection)

Korelasyon Analizi (SIEM): Aynı RFID ID'sinin, coğrafi olarak imkansız iki lokasyonda (örn. 5 dakika arayla İstanbul ve Ankara'da) aynı anda kullanılmaya çalışılması durumunda alarm üretmek.

Anormal Bağlantı: CSMS'in, daha önce hiç bağlanmadığı bir IP adresinden veya beklenmedik bir coğrafi konumdan bilinen bir ChargeBoxID ile bağlantı denemesi alması.

Sertifika Hataları: mTLS kullanımında, başarısız olan veya geçersiz sertifika sunan bağlantı denemelerini loglamak ve alarm üretmek.

S - Spoofing DREAD Değerlendirmesi

Tehdit Senaryosu: "Sahte Şarj İstasyonu Saldırısı (CS Spoofing)"

(Saldırganın, kendi cihazını CSMS'e meşru bir istasyon gibi bağlaması.)

D - Damage Potential (Zarar Potansiyeli): 6
Gerekçe: CSMS'e sahte şarj kayıtları (sahte gelir) gönderebilir, ağ topolojisi hakkında bilgi toplayabilir veya merkeze yönelik diğer saldırılar için (örn. Fuzzing) bir başlangıç noktası olabilir. Doğrudan yıkıcı değildir ancak kritik bir sızma noktasıdır.

R - Reproducibility (Tekrarlanabilirlik): 9
Gerekçe: Eğer sistem mTLS (Güvenlik Profili 3) yerine sadece Temel Kimlik Doğrulama (Basic Auth) veya daha kötüsü sadece ChargeBoxID kullanıyorsa, bu kimlik bilgileri çalındığında saldırı %100 başarıyla tekrarlanabilir.

E - Exploitability (İstismar Edilebilirlik): 7

Gerekçe: OCPP protokolünü taklit edecek (örn. Python scripti) bir yazılım bilgisi ve (eğer kullanılıyorsa) istasyonun Basic Auth şifresini/sertifikasını çalmak için fiziksel erişim veya başka bir zafiyet gerekir.

A - Affected Users (Etkilenen Kullanıcılar): 3
Gerekçe: Doğrudan son kullanıcıları etkilemez. Esas olarak operatör (CSMS) etkilenir (yanlış veriler, ağ güvenliği ihlali).

D - Discoverability (Keşfedilebilirlik): 4
Gerekçe: Sistemin mTLS kullanıp kullanmadığını dışarıdan bilmek zordur. Genellikle bir istasyonun donanımını veya firmware'ini analiz ederek (tersine mühendislik) keşfedilebilir.

Risk Skoru: 29/50 (Yüksek-Orta Risk)

Sacide Aişenur Direk