Anomali Senaryosunun Temel Bileşenleri ve Protokol Mimarisi

Bu senaryo, şarj istasyonlarında iki farklı iletişim katmanını birbirine bağlayan kritik bir güvenlik açığına odaklanmaktadır. Sistemde üç ana bileşen yer alır:

1. **OCPP (Şarj Protokolü):** Şarj istasyonu (CP) ile merkezi yönetim sistemi (CSMS) arasındaki geniş alan ağı (WAN) protokolüdür. Uzaktan komutların iletimi bu kanal üzerinden yapılır.
2. **CAN-bus (Lokal Protokol):** Şarj istasyonu içindeki röle kontrolü, güç elektroniği ve ölçüm birimleri gibi yerel kontrol birimleri arasındaki haberleşmeyi sağlayan protokoldür. Bu, fiziksel işlemleri yöneten yerel ağdır.
3. **CP Ana Kontrolcüsü (Köprü/Gateway):** Köprü görevi gören bu bileşen, OCPP ajanın çalıştığı yerdir ve CAN alıcı-vericisi (transceiver) ile arabirim kurar. Temel fonksiyonu, OCPP'den gelen komutları alıp, bunları uygulama mantığından geçirerek uygun CAN frame'lerine dönüştürmektir.

Saldırı Öncesi Normal İşleyiş (Clean Akış)

Sistem normal çalıştığında, CSMS'ten gelen uzaktan yönetim komutları, CP içindeki fiziksel donanıma şu şekilde ulaşır:

CSMS, bir şarj işlemini durdurmak istediğinde `Remote Stop Transaction` adlı OCPP mesajını gönderir. CP'deki Köprü bileşeni, bu mesajı alır ve belirlenen mantığa göre **CAN ID 0x201** olan bir CAN frame'ine dönüştürür. Bu frame, `[tx_id, stop_cmd]` gibi bir yük (payload) içerir ve lokal CAN-bus hattına enjekte edilerek röle kontrol modülüne şarjı kesme emrini iletir. Bu akış, uzaktan yönetimin sağlıklı çalışmasını sağlar.

Güvenlik Zafiyeti ve Anomali Noktası

Saldırıya olanak tanıyan anomali, Köprü bileşeninin OCPP kanalından gelen komutları yeterince doğrulamamasından kaynaklanır:

1. **Zafiyetin Başlangıcı:** Bir saldırgan, zayıf şifreleme veya **MitM** (Man-in-the-Middle) saldırısı gibi yöntemlerle OCPP kanalını ele geçirirse, CSMS'ten geliyormuş gibi sahte komutlar üretebilir.
2. **Saldırı Tipi:** Sizin simüle ettiğiniz saldırı, **Uzaktan Komut Taklidi** olarak adlandırılır ve saldırganın sahte bir `Remote Stop Transaction` göndermesiyle başlar.
3. **Fiziksel Sonuç:** Köprü, normalde güvenilir CSMS'ten gelmesi gereken bu sahte komutu da alır ve tıpkı normal akıştaki gibi CAN-bus formatına çevirir. Bunun sonucunda, bir ağ protokolü zafiyeti, CP'nin manipüle edilmiş yazılımı üzerinden **CAN aracılığıyla gerçek röle/şarj kontrol modülüne** iletilir. Bu durum, OCPP zafiyetlerinin **fiziksel işlem/cihaz kontrolü** (şarjı kesme) ile sonuç olabileceğini gösteren bir Hizmet Reddi (DoS) anomalisidir.