Siber-Fiziksel Sınırı İstismar Etmek: "Enerji Vampiri" Saldırısı

Bu bölüm, tamamen dijital bir zafiyetin doğrudan ve tehlikeli bir fiziksel sonuç olan yangını yaratmak için istismar edildiği yeni ve endişe verici bir saldırı vektörünü detaylandırmaktadır. EV ekosisteminde siber güvenliğin temel bir bileşeni olarak fiziksel güvenliğin dikkate alınmasının kritik ihtiyacını vurgulamaktadır.

5.1 Teknik Mekanizma: PWM Sinyalinin Ele Geçirilmesi ve Güvenin İstismarı

Bağlam: Bir EV ile Seviye 2 AC şarj cihazı arasındaki iletişim genellikle kontrol pilotu (CP) teli üzerinden bir Darbe Genişlik Modülasyonu (PWM) sinyali kullanır. Bu sinyal, araca şarj cihazının güvenli bir şekilde ne kadar akım sağlayabileceğini bildirir. Araç da durumunu şarj cihazına geri iletir.

Zafiyet Detayları: Araştırmalar, şarj cihazının genellikle araçtan gelen sinyallere zımnen güvendiğini göstermiştir.[12] Bir saldırgan bu güveni istismar edebilir. Aracın şarj denetleyicisini ele geçirerek veya PWM sinyalini ele geçirmek için kötü amaçlı bir cihaz kullanarak, saldırgan şarj cihazına "yalan söyleyebilir" ve nominal güvenlik sınırlarının çok ötesinde bir akım sağlamasını talep edebilir (örneğin, 40 amper için derecelendirilmiş bir şarj cihazından 80 amper talep etmek).[12]

Etki: Kendi bağımsız donanım tabanlı aşırı akım korumasına sahip olmayan şarj cihazı, kötü amaçlı isteği yerine getirmeye çalışır. Bu, bu kadar yüksek akımı kaldıramayacak şekilde tasarlanmış şarj kabloları ve bileşenleri üzerinden büyük miktarda akım geçmesine neden olur. Sonuç, hızlı aşırı ısınma, kablo yalıtımının erimesi ve potansiyel olarak kablonun alev almasıdır - termal kaçak olarak bilinen bir olgudur.[12]