Akıllı Şarj Mantığına Yönelik Hatalı Veri Enjeksiyonu (FDI) Saldırısı

Enes Kızılca: 235541116

1. Senaryo Özeti

Bu belge, "SecVolt" projesi kapsamında incelenen kritik bir siber-fiziksel anomali senaryosunu detaylandırmaktadır. Senaryo, elektrikli araç (EV) şarj altyapısının temel bir bileşeni olan "Akıllı Şarj" (Smart Charging) sistemlerinin mantıksal bir zafiyetini hedef almaktadır.

Saldırı, **güvenliği ihlal edilmiş tek bir şarj istasyonunun (CP)**, merkezi yönetim sistemine (CSMS) kasıtlı olarak **manipüle edilmiş telemetri verisi (sahte tüketim değeri)** göndermesi esasına dayanır. Merkezi sistemin (CSMS) yük dengeleme algoritması, bu sahte veriyi "gerçek" kabul ederek hatalı kararlar verir. Bu durum, birden fazla istasyonun bulunduğu bir lokasyonda (örn. bir ofis otoparkı veya apartman) **fiziksel altyapının aşırı yüklenmesine** yol açar.

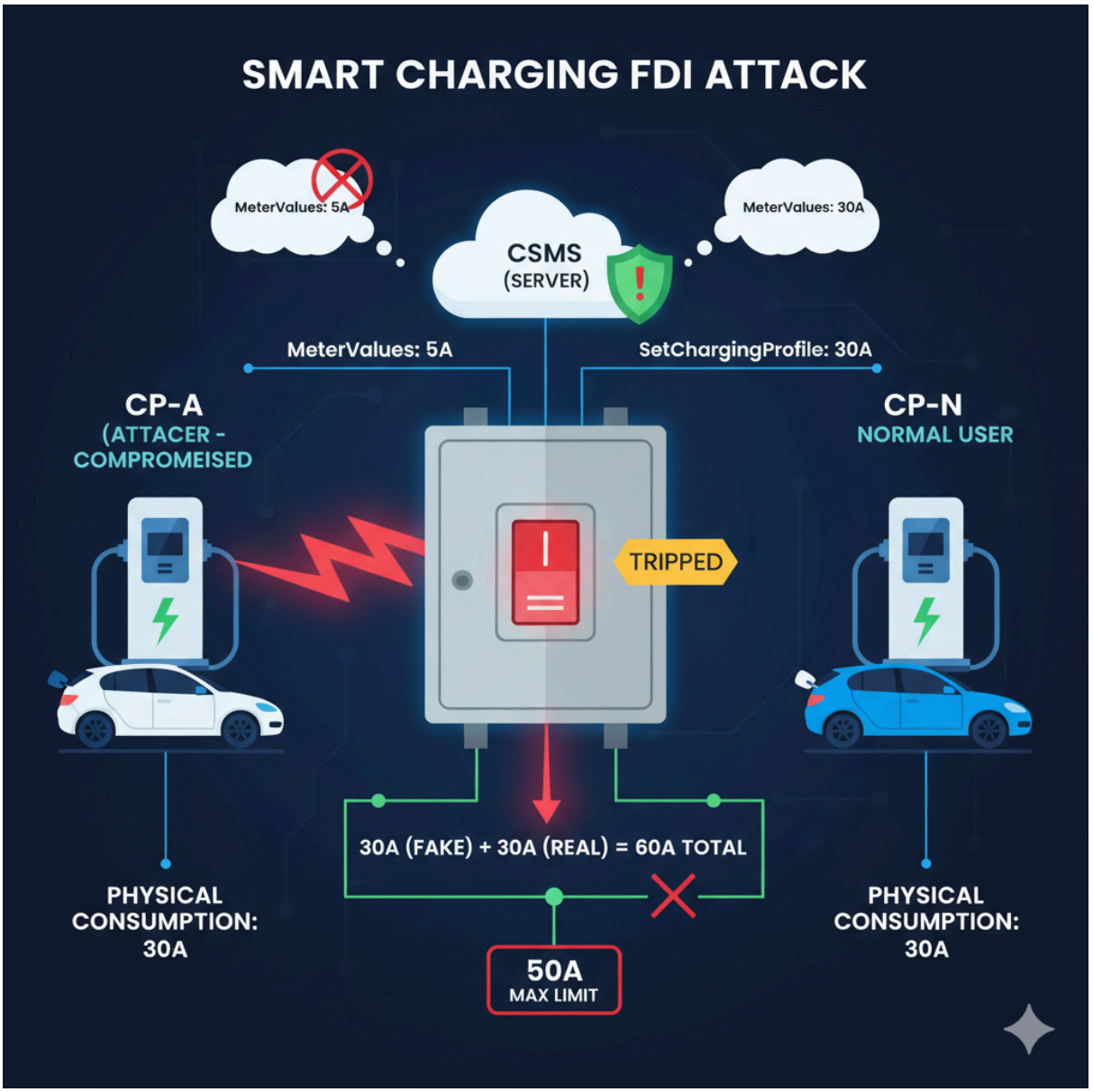
Nihai sonuç, bölgesel sigorta devrelerinin tetiklenmesi (sigorta atması) ve o bölgedeki **tüm şarj hizmetlerinin durmasına (Denial-of-Service - DoS)** neden olan siber-fiziksel bir çöküştür.

2. Senaryo Bağlamı ve Tehdit Modeli

Elektrikli araçların yaygınlaşması, yerel elektrik şebekeleri üzerinde benzeri görülmemiş bir talep baskısı oluşturmaktadır. Bu baskıyı yönetmek için, CSMS platformları "Akıllı Şarj" veya "Yük Dengeleme" algoritmaları kullanır. Bu algoritmalar, belirli bir lokasyondaki istasyon grubunun toplam tüketiminin, o lokasyonun fiziksel elektrik kapasitesini (örn. 50 Amper) aşmamasını garanti eder.

Bu sistemin temel taşı, **güvendir**. CSMS, her bir istasyonun MeterValues (Sayaç Değerleri) mesajıyla anlık olarak ne kadar güç tükettiğini "doğru" bildirdiğini varsayar.

Tehdit Modeli: Bu senaryo, "içeriden gelen tehdit" (insider threat) veya "ele geçirilmiş uç nokta" (compromised endpoint) modeline dayanır. Saldırganın, istasyonun firmware'ine (örn. JTAG, zayıf parola, 0-day yazılım açığı) sızarak root erişimi elde ettiğini varsayıyoruz. Bu noktadan sonra saldırgan, istasyonun CSMS'e gönderdiği mesajların içeriğini, şifreli kanal (wss://) bozulmadan önce, doğrudan kaynakta manipüle edebilir.



3. Saldırı Vektörünün Tanımı

Saldırı vektörü, CSMS'in karar verme mekanizmasına yönelik bir "algoritmik manipülasyon" olarak özetlenebilir.

CSMS'in yük dengeleme algoritması, basit bir matematiksel işleme dayanır:

$$Limit_{Fiziksel} - \sum Tüketim_{Raporlanan}$$

Saldırgan, ele geçirdiği istasyonun (CP-1) Tüketim_{Raporlanan} değerini, *gerçek tüketiminden* çok daha düşük bir seviyede (örn. gerçekte 30A çekerken 5A olarak) raporlar.

CSMS, bu hatalı veriye dayanarak KapasiteKalan değerini yanlış hesaplar. Sonuç olarak, gruba yeni katılan diğer (normal) istasyonlara (CP-2), gerçekte var olmayan bir kapasiteye dayanarak şarj izni verir.

Fiziksel gerçeklik (CP-1'in gerçek tüketimi + CP-2'nin gerçek tüketimi), dijital dünyada hesaplanan toplamı (CP-1'in *sahte* tüketimi + CP-2'nin gerçek tüketimi) aştığı anda, altyapının koruma mekanizmaları (devre kesiciler) devreye girer.

4. İş Etkisi ve Potansiyel Sonuçlar

Bu saldırının başarısı, "SenVolt" gibi bir şarj ağı operatörü için çok katmanlı ve ciddi sonuçlar doğurur:

- **Hizmet Kesintisi (DoS):** Saldırı, sadece saldırganın bulunduğu istasyonu değil, aynı sigorta devresine bağlı *tüm masum kullanıcıları* etkileyen bölgesel bir kesintiye yol açar.
- **Müşteri Memnuniyetsizliği ve Güven Kaybı:** Sürekli kesintiye uğrayan veya güvenilmez bir şarj hizmeti, kullanıcıların markaya olan güvenini (brand trust) hızla aşındırır.

- **Operasyonel Maliyet:** Kesintiye uğrayan her bölge, fiziksel bir müdahale (sigortanın manuel olarak kaldırılması) veya en azından sorunun tespiti için saha ekibi zamanı gerektirebilir.
- **Tespit Zorluğu (Gizlilik):** Bu saldırının tespiti geleneksel yöntemlerle zordur. CSMS loglarına bakıldığında, her şey normal görünür; toplam yük hiçbir zaman limiti aşmamış *gibi* görünür. Anomali, CSMS'in dijital kayıtları ile fiziksel dünyanın gerçekliği arasındaki "çelişki"de yatmaktadır.

5. Test Ortamı ve Metodoloji

Anomaliyi gözlemlemek ve simüle etmek için kontrollü bir sanal test ortamı (Ubuntu üzerinde) kurulmuştur. Bu ortam, gerçek dünyadaki bir şarj ağı altyapısının temel bileşenlerini temsil etmektedir:

- **vCSMS (Merkezi Sunucu):** Ağın beyni olarak "SteVe" veya benzeri bir OCPP yönetim yazılımı kullanılmıştır. Görevi, "Akıllı Şarj" profillerini (örn. 50A grup limiti) yapılandırmak ve istasyonları yönetmektir.
- **vCP-N (Normal İstemci):** `vCSMS`'e bağlı, standart, modifiye edilmemiş bir sanal şarj istasyonu (simülatör). Görevi, `vCSMS`'ten gelen anlık güç limitlerine harfiyen uymaktır.
- **vCP-A (Saldırgan İstemci):** `vCSMS`'e bağlı, ancak kaynak kodu *modifiye edilmiş* "yalancı" bir sanal şarj istasyonu. Bu istemci, gerçek tüketimini simüle ederken, `vCSMS`'e kasıtlı olarak sahte `MeterValues` (Sayaç Değeri) telemetrisi gönderecek şekilde programlanmıştır.

6. Anomalinin Uygulanışı (Saldırı Akışı)

Saldırı, dört temel adımda gerçekleştirilmiştir:

1. **Yapılandırma (Tuzak Kurma):** `vCSMS` üzerinde, `vCP-N` ve `vCP-A` istasyonlarını içeren bir gruba 50A'lik bir "Akıllı Şarj" (Yük Dengeleme) profili atanır.
2. **Yürütme (Yalanın Başlaması):** `vCP-A` (Saldırgan), şarj işlemini başlatır. Simülasyon içinde *gerçekte 30A* güç çekecek şekilde ayarlanır, ancak `vCSMS`'e gönderdiği `MeterValues` mesajında tüketimini **"5A"** olarak raporlar.
3. **Hatalı Karar (Yemleme):** `vCSMS`, sistem yükünü "5A" olarak algılar ve kalan kapasitenin "45A" olduğuna karar verir. Bu esnada `vCP-N` (Normal) 30A'lik bir şarj talebinde bulunur. `vCSMS`, kalan kapasite (45A) yeterli olduğu için bu talebi onaylar.
4. **Fiziksel Sonuç (Başarılı DoS):** Altyapı üzerindeki *gerçek yük* aniden (30A + 30A) = **60A**'e ulaşır. 50A'lik fiziksel limit aşıldığı için, simüle edilen devre kesici (sigorta) atar ve her iki istasyonun da enerjisi kesilir.

7. Gözlemlenen Anomali ve "SecVolt" Tespiti

Saldırı başarılı olduğunda, `vCSMS` (SteVe) loglarında tespit edilecek anomali, **beklenen dijital kayıtlar ile fiziksel sonuç arasındaki çelişkidir:**

- **CSMS Log Kaydı (Dijital Yalan):** SteVe'nin loglarına göre, toplam yük (5A + 30A = 35A) hiçbir zaman 50A'lik limiti aşmamıştır. Loglarda herhangi bir "aşırı yük" hatası *görünmez*.
- **Gözlemlenen Sonuç (Fiziksel Gerçek):** Logların "her şey normal" demesine rağmen, o gruba bağlı `vCP-A` ve `vCP-N` istasyonlarının *her ikisi de* eş zamanlı olarak bağlantı hatası (Connection Lost / Offline) verir.

"SecVolt" Güvenlik Platformu'nun tespiti: Anomali, "Yük limitleri aşılmamış görünürken, bir şarj grubundaki *tüm* istasyonların eş zamanlı olarak ve beklenmedik bir şekilde çevrimdışı olması" arasındaki **korelasyona** dayanır. Bu durum, geleneksel bir ağ hatasından ziyade, siber-fiziksel bir manipülasyona işaret eder.

Konunun ele alındığı bazı akademik makale örnekleri:

https://www.sciencedirect.com/science/article/pii/S2666792422000166?via%3Dihub

https://www.mdpi.com/1996-1073/14/16/5149