Yapan: Ebubekir Akın - 230541132

Anomali: Sahte Veri Enjeksiyonu (FDI) – SCADA Operatör Yanıltma Anomalisi

1. Anomali Tanımı

Sahte Veri Enjeksiyonu (FDI), bir güç şebekesi operatörünün SCADA (Denetleyici Kontrol ve Veri Toplama) sistemini hedef alan, operatörü yanıltmak ve fiziksel sisteme zarar vermek amacıyla gerçekleştirilen bir siber-fiziksel saldırıdır. Saldırı, operatörün izlediği kritik sistem verilerini sahte, normal gibi görünen verilerle değiştirir.

Nasıl Çalışıyor? Simülasyon, bir trafo merkezini (transformer_sunucusu.py) temsil eden bir Modbus sunucusu üzerinde çalışır. Bu sunucu iki kritik veri tutar:

1. **Güvensiz Veri (Register 100):** Operatörün SCADA panelinde gördüğü, saldırıya açık olan dijital veri.
2. **Güvenli Veri (Register 200):** Gerçek fiziksel yükü temsil eden, doğrulanmış "ground truth" verisi.

Saldırgan (fdi_saldirgan.py), sunucunun Modbus portuna (502) bağlanır ve "Güvensiz Veri" register'ına (Reg 100) sürekli olarak düşük, sahte bir değer (simülasyonda %10) yazar. Bu sırada "Güvenli Veri" (Reg 200) arka planda artmaya devam eder (gercek_fiziksel_yuk += 1.0).

Bu hile, operatörün yükü %10 gibi güvenli bir seviyede görmesine, ancak gerçek yükün %90'ın üzerine çıkarak (transformer_sunucusu.py içindeki felaket senaryosu) trafonun fiziksel olarak yanmasına neden olur.

2. SWOT Analizi: Şarj İstasyonu Güvenlik Açıklıkları

Kategori	Analiz
G (Güçlü Yönler)	**Standardizasyon ve İşlerlik:** OCPP gibi standart protokollerin kullanılması, farklı üreticilerin cihazlarının merkezi sistemlerle (CSMS) uyumlu çalışmasını sağlar. CAN-Bus, araç içi ve endüstriyel kontrolde kendini kanıtlamış, verimli bir yerel ağ protokolüdür.
Z (Zayıf Yönler)	1. Zayıf Şifreleme ve Kimlik Doğrulama: * **Problem:** Zayıf şifreleme, verilerin ağ üzerinde (örn. TLS/WSS olmadan, plain ws ile) şifresiz veya kolayca çözülebilir bir formatta iletilmesidir. * **Etkisi:** Bu zafiyet, MitM saldırganlarının OCPP trafiğini (komutlar, fatura verileri) okumasına ve değiştirmesine olanak tanır.

Z (Zayıf Yönler)	2. Güvensiz Yazılım/Firmware Güncelleme Süreçleri: * **Problem:** "Firmware imzalama" veya "secure boot" gibi mekanizmaların eksikliği. * **Etkisi:** Bu zafiyet, saldırganların CP'ye (şarj istasyonu) zararlı bir firmware enjekte etmesine olanak tanır. Ele geçirilen firmware, CP'nin davranışını CAN seviyesinde değiştirerek (örn. sahte CAN mesajları gönderme) fiziksel sabotaj veya dolandırıcılığa yol açabilir.
F (Fırsatlar)	**Gelişmiş Savunma Mekanizmaları:** * **CAN-IDS:** CAN trafiğini izleyerek anormallikleri (beklenmeyen ID'ler, anormal frekans) tespit eden "Saldırı Tespit Sistemleri" (IDS) kurma fırsatı. * **Güçlü Güvenlik:** İletişim kanalını "Mutual TLS" ile güçlendirme ve "firmware imzalama" süreçlerini zorunlu hale getirme.
T (Tehditler)	3. Ortadaki Adam (MitM) Saldırıları: * **Problem:** Zayıf şifreleme veya sahte sertifikalar kullanılarak CP ve CSMS arasına giren saldırgan. * **Amaç:** Saldırganın amacı, komutları manipüle etmektir (örn. şarjı durdurma/başlatma komutlarını değiştirme) veya bizim senaryomuzda olduğu gibi MeterValues verisini değiştirerek faturalama hilesi yapmak. 4. Yetkisiz Erişim ve Komut Enjeksiyonu: * **Problem:** Bir saldırganın, MitM veya ele geçirilmiş firmware yoluyla sisteme sızması. * **Amaç:** Bu tehdidin nihai amacı, OCPP'den CAN'e bir "köprü" oluşturarak fiziksel dünyaya etki etmektir. Saldırgan, CSMS'yi taklit ederek veya doğrudan CP yazılımını kullanarak CAN ağına komutlar (örn. şarj profilini değiştirme , röleleri açma/kapama) gönderebilir. Bu, sadece ekonomik kayba değil, aynı zamanda fiziksel hasara da yol açabilir.

3. Olası Riskler ve Etkiler

- **Fiziksel Hasar ve Yıkım:** Saldırının en büyük riskidir. transformer_sunucusu.py script'inde tanımlandığı gibi, operatör sahte veriye (%10) aldanırken gerçek yükün (%90'ın üzerine) çıkması, "TRAFO AŞIRI YÜKLENDİ VE YANDI!" senaryosuna, yani milyonlarca dolarlık ekipman hasarına yol açar.
- **Operasyonel Felaket (Karartma):** Operatör, sahte "düşük yük" verisine dayanarak şebiyeye daha fazla yük vermeye karar verebilir. Bu, mevcut aşırı yüklenmeyi hızlandırarak bölgesel veya ulusal ölçekte bir elektrik kesintisine (blackout) neden olabilir.
- **Ekonomik Kayıp:** Sadece fiziksel ekipman maliyeti değil, aynı zamanda hizmet kesintisinden kaynaklanan endüstriyel ve sivil ekonomik kayıplar muazzam boyutlara ulaşabilir.
- **Gizli Saldırı (Stealth Attack):** Bu saldırı, gürültülü bir "servis dışı bırakma" (DoS) saldırısı değildir. guvenlik_onlemi_scada.py (IDS) script'i devrede olmasaydı, operatör paneline yansıyan %10'luk veri normal bir operasyon gibi görünecek ve saldırı fark edilmeyecekti.

4. İlgili Standartlar ve Kurallar

- **Modbus TCP:** Simülasyonda kullanılan, Endüstriyel Kontrol Sistemleri'nde (ICS) en yaygın kullanılan, ancak doğası gereği güvensiz (kimlik doğrulama, şifreleme yok) olan iletişim protokolü.
- **IEC 62351:** Güç sistemi operasyonları için özel olarak tasarlanmış, Modbus gibi eski protokollere güvenlik (şifreleme, kimlik doğrulama, izinsiz giriş tespiti) eklemeyi amaçlayan uluslararası standart.
- **Purdue Modeli (ISA-95):** Endüstriyel ağları (OT) ve kurumsal ağları (IT) birbirinden ayırmak için kullanılan, ağ segmentasyonunu tanımlayan temel mimari model. Bu saldırı, OT ağının (Seviye 0, 1, 2) içindeki zafiyetleri istismar etmektedir.
- **Sıfır Güven (Zero Trust):** "Asla güvenme, her zaman doğrula" prensibidir. Simülasyonumuzdaki guvenlik_onlemi_scada.py script'i, Reg 100'den gelen veriye "güvenmeyip" onu Reg 200 ile "doğrulayarak" bu prensibin basit bir örneğini uygular.

5. Simülasyon Sonuçları

Kali Linux sanal ortamında gerçekleştirilen FDI saldırısı, guvenlik_onlemi_scada.py (IDS/Güvenlik Sistemi) tarafından başarıyla tespit edilmiştir. IDS, her 2 saniyede bir "Dijital Veri (Reg 100)" ile "Fiziksel Veri (Reg 200)" arasındaki farkı kontrol etmiştir.

Anomali Log Kayıtları: Aşağıdaki tablo, scada_guvenlik_logu.txt dosyasından alınan, saldırının ve tespitin kanıtı olan örnek log kayıtlarını göstermektedir:

Alınma Zamanı (IDS Log)	Raporlanan Dijital Veri (Reg 100)	Doğrulanan Fiziksel Veri (Reg 200)	Fark Yüzdesi (%)	IDS Durumu (Alarm)

2025-11-10 07:27:14	51%	116%	65%	**[FDI SALDIRISI TESPİT EDİLDİ!]**
2025-11-10 07:27:16	51%	116%	65%	**[FDI SALDIRISI TESPİT EDİLDİ!]**
...	...	...	...	...
2025-11-10 07:27:44	**10%**	122%	112%	**[FDI SALDIRISI TESPİT EDİLDİ!]**
2025-11-10 07:27:46	10%	122%	112%	**[FDI SALDIRISI TESPİT EDİLDİ!]**
...	...	...	...	...
2025-11-10 07:30:19	10%	153%	143%	**[FDI SALDIRISI TESPİT EDİLDİ!]**
2025-11-10 07:30:21	10%	153%	143%	**[FDI SALDIRISI TESPİT EDİLDİ!]**

- **1. Log Analizi Metriği (Çapraz Doğrulama - TDD):** guvenlik_onlemi_scada.py script'inin ana tespit yöntemidir. Script, fark = abs(dijital_veri - fiziksel_veri) formülü ile iki kaynak arasındaki mutlak farkı hesaplamıştır.
- **2. Log Analizi Metriği (Güvenlik Eşiği):** Script, if fark > 5: kuralı ile basit ama etkili bir alarm eşiği belirlemiştir. Simülasyon loglarında, farkın (%65, %112, %143) bu %5'lik toleransın çok üzerinde olduğu ve alarmın anında, istisnasız olarak tetiklendiği görülmüştür. IDS, "GÜVENLİK ÖNLEMİ: Sistem fiziksel veriye (Güvenli Mod) geçiriliyor" tepkisini vererek doğru savunma eylemini başlatmıştır.

Sistem Geliştirme Odaklı Öneriler:

- **Güçlü Kimlik Doğrulama:** transformer_sunucusu.py gibi kritik varlıklar, bağlanan hiçbir istemciye varsayılan olarak güvenmemeli, her bağlantı (IEC 62351'in önerdiği gibi) sertifika veya token ile doğrulanmalıdır.
- **Ağ Segmentasyonu:** Saldırganın sunucuya erişimini en baştan engellemek için Purdue Modeli'ne uygun sıkı ağ segmentasyonu ve güvenlik duvarı kuralları uygulanmalıdır.
- **Veri Bütünlüğü:** Reg 200 gibi "güvenli" verilerin bile, kaynaktan (sensörden) merkeze (SCADA) gelene kadar kriptografik olarak imzalanması, verinin bütünlüğünü garanti altına alır.

6. Sonuç ve Değerlendirme

Bu ders projesi kapsamında yürütülen simülasyon, FDI saldırılarının siber-fiziksel sistemler üzerindeki **çifte etkisini** (siber manipülasyon ve fiziksel yıkım) pratik olarak kanıtlamıştır.

Elde edilen log kayıtları (scada_guvenlik_logu.txt), iki şeyi net olarak göstermi "

1. **Zafiyetin Uygulanabilirliği:** fdi_saldirgan.py, kimlik doğrulaması olmayan Modbus TCP protokolünü istismar ederek kritik bir veriyi (%10'da sabitleyerek) başarıyla manipüle etmiştir.
2. **Savunmanın Etkinliği:** guvenlik_onlemi_scada.py (IDS) script'inin kullandığı "fiziksel-dijital çapraz doğrulama" yöntemi, bu gelişmiş ve gizli saldırıyı tespit etmede %100 başarılı olmuştur.

Bu çalışma, endüstriyel kontrol sistemlerinin (ICS) güvenliğinde, tek bir dijital veri noktasına asla güvenmemenin ve her zaman fiziksel bir doğrulama (ground truth) katmanına sahip olmanın hayati önem taşıdığını ortaya koymaktadır.

7. Kaynaklar

(Bu simülasyonu oluşturan Python script'leri ve çıktılar)

1. transformer_sunucusu.py (Modbus TCP Trafo Sunucusu Simülasyonu)
2. fdi_saldirgan.py (FDI Saldırgan Simülatör Scripti)
3. guvenlik_onlemi_scada.py (IDS/SCADA Savunma ve İzleme Scripti)
4. scada_guvenlik_logu.txt (Simülasyon Sırasında Toplanan Anomali Log Kaydı)