Anomali Senaryosu Raporu

Senaryo Adı: Enerji Hırsızlığı ve Dolandırıcılık (İşlem Yönlendirme)

Referans Makale: Alcaraz, C., Lopez, J., & Wolthusen, S. (2017). *OCPP Protocol: Security Threats and Challenges*.

1. Senaryonun Amacı:

Saldırının temel amacı, meşru bir elektrikli araç kullanıcısının kimliğini (idTag) kurban bir şarj istasyonundan (CP1) ele geçirmek, bu kimliği kullanarak farklı (ve genellikle saldırganın kontrolündeki) bir şarj istasyonundan (CP2) enerji çalmak ve yapılan şarj işleminin faturasını kurban kullanıcıya yansıtmaktır.

2. Senaryo Özeti:

Saldırgan, Man-in-the-Middle (MitM) pozisyonu alarak hem kurban istasyon (CP1) hem de suç ortağı istasyon (CP2) ile Merkezi Yönetim Sistemi (CSMS) arasındaki ağ trafiğini dinler ve değiştirir. CP1'deki meşru kullanıcı kartını okuttuğunda, saldırgan bu yetkilendirme isteğini (Authorize.req) yakalar ve idTag bilgisini kopyalar. Saldırgan, CP1'in iletişimini keserken, CP2 istasyonunu kullanarak (ancak CP1'in kimliğine bürünerek) ve çaldığı idTag ile CSMS'e yeni bir şarj işlemi başlatma talebi gönderir. CSMS, bu sahte talebi CP1 istasyonundaki meşru kullanıcıdan geliyormuş gibi algılar, işlemi onaylar ve CP2 üzerindeki konnektörü açar. Saldırgan CP2'den aracını şarj ederken, tüm fatura CP1'deki kurban kullanıcıya yansıtılır.

3. Hedef Varlıklar:

- **Şarj İstasyonu 1 (CP1):** Kurban kullanıcının bulunduğu ve kimlik bilgisinin çalındığı istasyon.
- **Şarj İstasyonu 2 (CP2):** Saldırganın fiziksel olarak erişiminin olduğu ve enerjiyi çaldığı istasyon.
- **Merkezi Yönetim Sistemi (CSMS):** Yetkilendirme ve faturalama mantığı manipüle edilen ana sunucu.
- **Ağ Altyapısı (CP-CSMS İletişimi):** Saldırganın MitM saldırısı için hedef aldığı iletişim kanalı (örn. WebSocket/TLS).

4. İlişkili Tehditler (STRIDE):

- **Spoofing (Kimlik Sahteciliği):** CP2 istasyonu, CSMS'e karşı CP1'in kimliğine bürünür. Saldırgan, CP1'deki kullanıcının idTag kimliğine bürünerek CSMS'i kandırır.

- **Tampering (Veri Manipülasyonu):** Ağ paketlerinin akışı kasıtlı olarak değiştirilir; CP1'in paketleri engellenir, CP2'nin paketleri ise CP1'den geliyormuş gibi değiştirilir.
- **Repudiation (İnkâr):** Saldırgan, işlemi CP1 adına yaptığı için suçun CP2 (veya kendisi) tarafından işlendiğini inkâr edebilir. Aynı zamanda, kurban kullanıcı (CP1) de bu işlemi kendisinin yapmadığını iddia edecektir (fatura itirazı).
- **Information Disclosure (Bilgi İfşası):** MitM saldırısı sırasında meşru kullanıcının idTag bilgisi çalınır.

5. Saldırıda Faydalanılan Zafiyetler:

- **Zayıf TLS ve Oturum Yönetimi:** Makale, saldırganın (Algorithm 1'de açıklandığı gibi) TLS el sıkışmasına müdahale ederek oturum anahtarını (Ksession) ele geçirebildiğini varsayar . Bu, iletişimin dinlenmesini ve değiştirilmesini mümkün kılar.
- **Yetersiz Cihaz Kimlik Doğrulaması:** CSMS'in, kendisine bağlanan bir CP'nin gerçekten iddia ettiği CP olduğunu (örn. IDCP1) doğrulamak için (sertifika tabanlı kimlik doğrulama gibi) güçlü mekanizmalara sahip olmaması.
- **Kimlik ve İşlem Bağımsızlığı:** Kullanıcı kimliğinin (idTag), fiziksel istasyondan ve işlemden bağımsız olarak yakalanıp başka bir istasyonun işlem talebinde (kopyala-yapıştır gibi) kullanılabilmesi.
- **Güvenilir Ağ Varsayımı:** OCPP 1.6 protokolünün, CP ve CSMS arasındaki ağın güvenli olduğunu varsayması ve MitM saldırılarına karşı kendi katmanında yerleşik bir koruma sunmaması.

6. Saldırı Adımları (Adım Adım Simülasyon):

Makalenin 3. Algoritmasına ve Şekil 3'teki pratik uygulamasına dayanarak:

1. **Aşama 1: Hazırlık (Konumlanma):**
    a. Saldırgan (A), hem CP1 hem de CP2 istasyonlarının CSMS ile olan ağına Man-in-the-Middle (MitM) olarak yerleşir. (Makalede bu işlem için `ettercap` kullanılmıştır).
2. **Aşama 2: Kimlik Sahteciliği (Spoofing):**
    a. Saldırgan, CP2'nin CSMS'e gönderdiği `BootNotification.req` paketini yakalar.
    b. Paket içeriğini, CP2'nin kimliğini CP1'in kimliği (IDCP1) ile değiştirecek şekilde manipüle eder ve CSMS'e gönderir. (Makalede bu işlem için `netsed` aracı kullanılmıştır).
    c. CSMS, artık CP2'den gelen bağlantıyı CP1'e ait zanneder ve bu sahte kimlikle bir oturum (KsessionCP1-2) açar.
3. **Aşama 3: Veri Yakalama:**

    a. CP1 istasyonundaki meşru kullanıcı, aracını şarja takar ve RFID kartını (idTagCP1) okutarak bir `Authorize.req` isteği gönderir.
4. **Aşama 4: Manipülasyon ve Engelleme:**
    a. Saldırgan, CP1'den gelen bu `Authorize.req` paketini yakalar.
    b. Paketten idTagCP1 bilgisini kopyalar ve kaydeder.
    c. Saldırgan bu paketin CSMS'e ulaşmasını engeller (paketi düşürür) ve CP1'den gelen diğer tüm iletişimi yok saymaya başlar.
5. **Aşama 5: Saldırıyı Başlatma (İşlem Yönlendirme):**
    a. Saldırgan, CP2 istasyonunu kullanarak (ve hala CP1 kimliğine bürünerek) CSMS'e bir `StartTransaction.req` komutu gönderir.
    b. Bu komutun içine, 3. Adımda çaldığı meşru kullanıcının kimliğini (idTagCP1) yerleştirir.
6. **Aşama 6: Yetkilendirme ve Enerji Hırsızlığı:**
    a. CSMS, CP1 kimliğinden ve meşru idTagCP1'den geldiğini düşündüğü bu sahte talebi onaylar (`StartTransaction.conf`).
    b. Onay CP2'ye iletilir, CP2 konnektörü açar ve saldırgan aracını şarj etmeye başlar.
7. **Aşama 7: Faturalama:**
    a. Saldırgan şarjı bitirdiğinde (CP2 üzerinden `StopTransaction.req` gönderilir), CSMS işlemi durdurur ve tüketilen tüm enerjinin faturasını CP1'den yakalanan meşru idTagCP1 kullanıcısının hesabına yansıtır.

7. Olası Sonuçlar ve Etkiler:

- **Finansal Etki:** Meşru kullanıcı (CP1), hiç almadığı bir hizmet (enerji) için faturalandırılır. Bu durum, kullanıcı ile şarj operatörü arasında finansal anlaşmazlıklara yol açar.
- **Güven Kaybı:** Kullanıcıların şarj ağı altyapısına olan güveni ciddi şekilde sarsılır.
- **Veri Bütünlüğünün Bozulması:** CSMS'in işlem kayıtları (logları) bozulur. Kayıtlarda, CP1 istasyonunda (aslında CP2 olmasına rağmen) idTagCP1 kullanıcısının şarj yaptığı görünür, bu da adli analizleri ve hata ayıklamayı imkansız hale getirir.
- **Operasyonel Etki:** CP1'in meşru kullanıcısı, isteği saldırgan tarafından engellendiği için hizmet alamaz.

8. Tespit Yöntemleri (Detection):

- **Korelasyon Analizi (Anomali Tespiti):** CSMS tarafında, aynı idTag'in, fiziksel olarak imkansız olan farklı lokasyonlardaki (örn. CP1 ve CP2 farklı şehirlerdeyse) istasyonlardan çok kısa zaman aralıklarıyla işlem başlatma girişimlerini izleyen bir anomali tespit sistemi (IDS) kurulmalıdır.

- **Ağ İzleme (Network Monitoring):** Ağ trafiğinde `ettercap` gibi araçların kullandığı ARP zehirlenmesi, sahte sertifikalar veya beklenmedik yönlendirmeler gibi MitM saldırı belirtileri aktif olarak izlenmelidir.
- **Oturum ve IP Analizi:** CSMS'in, bir CP'den (örn. IDCP1) gelen bağlantının kaynak IP adresini, o CP için kayıtlı/beklenen IP adresi havuzuyla karşılaştırması ve tutarsızlıkları işaretlemesi gerekir.
- **Kullanıcı Geri Bildirimi (Adli):** Kurban kullanıcının (CP1) faturasında veya işlem geçmişinde tanımadığı bir işlemi bildirmesi (saldırı sonrası tespit).

9. Önleme ve Azaltma Yöntemleri (Prevention/Mitigation):

- **Güçlü ve Zorunlu Şifreleme:** Makalenin ana önerisi, sadece TLS önermek yerine, karşılıklı kimlik doğrulamalı (mutual authentication - hem istemci/CP hem de sunucu/CSMS sertifika doğrular) güçlü TLS sürümlerini (örn. TLS 1.2/1.3) zorunlu kılmaktır. Bu, MitM saldırısını büyük ölçüde zorlaştırır.
- **Güçlü Cihaz Kimlik Doğrulaması:** CP'lerin CSMS'e bağlanırken sadece basit bir metin tabanlı ID yerine, değiştirilemez donanımsal kimlikler (örn. TPM - Güvenilir Platform Modülü) veya x.509 istemci sertifikaları kullanması sağlanmalıdır.
- **İşlem-Lokasyon Bağıntısı:** CSMS, bir idTag ile bir şarj işlemini ilişkilendirirken, bu idTag'in "kilitli" olup olmadığını (yani halihazıra başka bir istasyonda aktif bir oturumu olup olmadığını) kontrol etmelidir.
- **Ağ Güvenliği (IDS/IPS):** Şarj istasyonlarının bulunduğu ağı, izinsiz girişleri ve anormal trafik modellerini (MitM gibi) tespit edebilen ve engelleyebilen Saldırı Tespit/Önleme Sistemleri (IDS/IPS) ile korumak.
- **Kayıt ve Denetim (Logging):** Makalenin önerdiği gibi, tüm işlemlerin ayrıntılı (fine-grained) olarak, kim (who), ne (what), nerede (where) ve ne zaman (when) sorularını yanıtlayacak şekilde ve inkârı önleyecek (non-repudiation) şekilde kaydedilmesi.