**MAKALE**

**Bao, K., Valev, H., Wagner, M. *ve diğerleri.* Araçtan şebekeye şarj protokolü ISO 15118'in tehdit analizi . *Comput Sci Res Dev* 33 , 3–12 (2018).** [**https://doi.org/10.1007/s00450-017-0342-y**](https://doi.org/10.1007/s00450-017-0342-y)

**ÖZET**

**Bu çalışma, araçtan şebekeye şarj protokolü ISO 15118'in güvenlik analizini gerçekleştirmekte ve şarj hizmetinin kullanılabilirliğini veya iletişimin bütünlüğünü, gerçekliğini veya gizliliğini protokol düzeyinde nasıl tehlikeye atabileceğinize dair çeşitli senaryolar sunmaktadır. Ayrıca, kimlik doğrulama, bilgi aktarımı ve sertifika hiyerarşisiyle ilgili süreçleri, bir saldırganın şarj süreci üzerinde haksız avantaj elde etmek ve bunu kendi çıkarları için kullanmak, çoğunlukla meşru kullanıcılara veya diğer katılımcılara zarar vermek için kullanabileceği güvenlik açıkları açısından analiz etmektedir.**

**ANOMALİ SENARYOSU 12: ISO 15118 (PLC) Sinyal Müdahalesi (Plug & Charge Sahteciliği)**

**Amacı ve Kapsamı**

**Amaç: Bu senaryonun temel amacı, Elektrikli Araç Şarj Altyapılarının (EVCI) yeni nesil standardı olan ISO 15118 (Plug & Charge - Tak ve Şarj Et) protokolünün, özellikle fiziksel katman (Power Line Communication - PLC) üzerindeki zafiyetlerini göstermektir. Saldırı, aracın şarj istasyonuyla kimlik doğrulaması ve ödeme yapması için şarj kablosu üzerinden gönderdiği PLC sinyalini hedef alarak, iki kritik sonuca ulaşmayı amaçlar: Finansal (Sertifika Klonlama) ve Fiziksel (Batarya Manipülasyonu).**

**Kapsam: Aracın şarj protokolü iletişimindeki (ISO 15118/HPGP) sinyallerin dinlenmesi, manipüle edilmesi, ödeme sertifikalarının çalınması ve istasyona sahte şarj parametreleri enjekte edilerek bataryanın fiziksel olarak tehlikeye atılması.**

**Özet**

**Saldırgan, halka açık bir şarj istasyonunun konektörüne veya şarj kablosuna, Man-in-the-Middle (MitM) işlevi gören minyatür, özel bir donanım implantı yerleştirir. Bir araç "Plug & Charge" yapmak için bağlandığında, araç ödeme sertifikasını ve şarj talebini PLC üzerinden istasyona gönderir. İmplant, bu iletişimi keser ve iki yönlü, eş zamanlı bir saldırı başlatır: (1) Aracın benzersiz dijital kimlik sertifikasını klonlar (daha sonra başka bir istasyonda ücretsiz şarj için kullanmak üzere) ve (2) Aracın güvenli akım talebini (örn. 100A), tehlikeli bir aşırı akım talebiyle (örn. 300A) değiştirerek istasyona iletir. Bu, hem finansal hırsızlığa hem de batarya üzerinde yıkıcı fiziksel hasara yol açar.**

**Hedef Varlıklar**

* **Araç Kimlik Sertifikası (Vehicle Identity Certificate): "Plug & Charge" ödemeleri için kullanılan, araca özel dijital anahtar (Finansal hedef).**
* **PLC Veri Katmanı (HomePlug Green PHY): ISO 15118 tarafından kullanılan ve şarj komutlarını taşıyan fiziksel iletişim sinyali (Saldırı vektörü).**
* **Batarya Yönetim Sistemi (BMS) Güvenlik Limitleri: Bataryanın fiziksel sağlığını koruyan ve kritik kararlar alan birim (Saldırının dolaylı fiziksel hedefi).**
* **Faturalandırma ve Kimlik Doğrulama Süreçleri: Saldırının finansal ve güvenlik politikası hedefi.**

**İlgili Zafiyetler**

* **Fiziksel Güvenlik Eksikliği: Halka açık şarj kablolarının denetimsiz olması ve donanımsal müdahaleye (tampering) karşı savunmasız kalması, MitM implantının yerleştirilmesini kolaylaştırır.**
* **HPGP Sinyal Dinleme Zafiyetleri: PLC standardının (HomePlug Green PHY), güvenli olmayan ortamlarda sinyal dinlemeye (eavesdropping) ve sinyal enjeksiyonuna karşı zayıflıklar barındırması.**
* **Çapraz Kontrol Eksikliği: İletişim protokolü (PLC) katmanından gelen verinin, araç içi kontrol ağı (CAN-Bus) sensör verileriyle (örneğin Batarya Sıcaklığı) gerçek zamanlı olarak tutarlılık kontrolünden geçirilmemesi.**
* **Protokol Güven Zafiyeti: ISO 15118 uygulama katmanında TLS şifrelemesi kullansa bile, fiziksel katmanda sinyallerin MitM donanımı ile yakalanıp bozulmasını veya geciktirilmesini engellemenin zor olması.**

**Tehdit Kategorisi (STRIDE)**

* **Kurcalama (Tampering): Aracın istediği güvenli şarj parametrelerinin (Akım/Voltaj), MitM implantı tarafından tehlikeli olanlarla değiştirilerek fiziksel bir tehlike oluşturması.**
* **Bilgi İfşası (Information Disclosure): Aracın benzersiz kimliğinin (MAC adresi) ve "Plug & Charge" ödeme sertifikasının pasif veya aktif dinleme yoluyla çalınması.**
* **Sahtecilik (Spoofing): Çalınan sertifikanın daha sonra saldırgan tarafından, kurbanın aracını taklit etmek (impersonate) ve ücretsiz şarj almak için kullanılması (Finansal Sahtecilik).**

**Saldırı Vektörü ve Adımları**

**Vektör: Şarj konektörüne veya şarj kablosuna gizlenmiş, PLC sinyallerini okuyup yazabilen, pille çalışan özel bir MitM donanım implantı.**

1. **Adım 1 (Erişim/Yerleştirme): Saldırgan, donanım implantını halka açık istasyona fiziksel olarak takar ve kablo/konektör arasına yerleştirir.**
2. **Adım 2 (Dinleme/Kopyalama): Kurban araç bağlandığında, implant ISO 15118 "el sıkışma" ve "ödeme yetkilendirme" paketlerini yakalar ve aracın dijital sertifikasını hafızasına kopyalar.**
3. **Adım 3 (Manipülasyon): İmplant, aracın güvenli şarj profilini (örn. "Maksimum 100A") yakalar, ancak istasyona iletmez. Bunun yerine, istasyona sahte ve tehlikeli bir aşırı akım profili (örn. "Maksimum 300A talep ediyorum") gönderir (Tampering).**
4. **Adım 4 (Sonuç): İstasyon, güvenilir bir kaynakmış gibi görünen bu talebi işler ve araca aşırı akım basarak bataryaya fiziksel zarar verilmesini tetikler.**

**Tespit Yöntemleri (BlockSentinel'in Rolü)**

**Bu saldırı doğrudan PLC seviyesinde gerçekleştiği için, CAN verisini izleyen BlockSentinel tarafından doğrudan görülemez. Ancak saldırının fiziksel etkileri ve mantıksal tutarsızlıkları sistem seviyesinde tespit edilebilir:**

* **Çapraz Protokol Analizi (Korelasyon Motoru): BlockSentinel’ın ana odak noktasıdır. PLC üzerinden istenen (300A) akım değeri ile aracın CAN-Bus’ında bildirilen güvenli akım limitleri (100A) veya Batarya Yönetim Sistemi (BMS) durumu arasında ölümcül bir çelişkinin (tutarsızlığın) tespit edilmesi.**
* **Trend Analizi (YZ/DL): Batarya sıcaklık sensörlerinde, normal şarj eğrisinin çok ötesinde, anormal hızlı bir artış trendinin (eğim analizi) tespiti. YZ modeli, *Thermal Runaway* öncesi belirtileri yakalar.**
* **Fiziksel Kısıtlama İhlali Tespiti: BMS'in talep ettiği (istenen) akım ile bataryaya fiziksel olarak giren (ölçülen) akım arasındaki tutarsızlığın loglanması ve beklenmeyen bir akım değeri verildiğinde otomatik kesme komutunun tetiklenmesi.**

**Etki ve Sonuçlar**

* **Finansal (Yüksek Risk): "Plug & Charge" sertifikalarının klonlanması sonucu yaygın ödeme sahtekarlığı ve kimlik hırsızlığı. CPO için önemli gelir kaybı.**
* **Fiziksel ve Can Güvenliği (Yıkıcı): Aracın BMS'inin istediğinden çok daha yüksek akım verilmesi sonucu Bataryada Geri Dönülemez Hasar ve potansiyel Termal Kaçak (yangın/patlama) riski.**
* **Sektörel Güven Kaybı: ISO 15118 standardının en önemli özelliği olan "Plug & Charge" özelliğine olan güvenin tamamen sarsılması ve bu teknolojinin yaygınlaşmasının sekteye uğraması.**

**SWOT Analizi (Detaylı)**

**Güçlü Yönler (Strengths) – (İçsel ve Olumlu)**

**Bu tehdide karşı BlockSentinel'in mevcut mimarisinin sağladığı avantajlardır:**

* **Çok Katmanlı Güvenlik (Multi-Layer Correlation): Projenin temelindeki Yapay Zekâ (YZ) ve Korelasyon Motoru, saldırıyı doğrudan PLC seviyesinde göremese bile, saldırının ikincil etkilerini yakalar. PLC üzerinden sahte bir akım talebi gönderildiğinde, bu durumun araç içindeki CAN-Bus üzerindeki BMS (Batarya Yönetim Sistemi) verileriyle (örn. anormal sıcaklık artışı, beklenmedik voltaj değişimleri) çelişmesi, YZ motoru tarafından hızla tespit edilir.**
* **Kanıt Kaydı için Blockchain: Klonlanan sertifikalarla ücretsiz şarj yapılması veya anormal akım enjeksiyonu gibi olaylar tespit edildiği anda, bu anomalilerin zaman damgaları ve detayları blok zinciri tabanlı kayıt defterine işlenir. Bu, operatörler için saldırının inkâr edilemez (non-repudiation) kanıtını sağlar.**
* **Erken Uyarı Mekanizması: Batarya sıcaklık sensörlerinde normal şarj eğrisinden sapma gösteren anormal hızlı artış trendinin (eğim analizi) tespiti, Termal Kaçak riski oluşmadan önce otomatik kesme komutlarının tetiklenmesine izin verir.**

**2. Zayıf Yönler (Weaknesses) – (İçsel ve Olumsuz)**

**Bu tehdide karşı projenin mevcut haliyle yaşadığı kısıtlamalar ve eksikliklerdir:**

* **Fiziksel Katman Körlüğü (Doğrudan Tespit Eksikliği): Saldırı, donanım ve fiziksel katmanda (PLC) gerçekleşir. BlockSentinel, esasen yazılım ve protokol (OCPP/CAN) katmanlarını izlemek üzere tasarlandığından, saldırgan implantı yerleştirirken veya sinyali yakalarken bunu doğrudan sinyal seviyesinde göremez.**
* **Mitigasyonda Gecikme: Tespit, ancak saldırı başladıktan sonra, batarya sıcaklığı artmaya başladığında veya CAN verisi ile PLC verisi çeliştiğinde (dolaylı olarak) yapılabilir. Bu, saldırının en azından kısa bir süre etkili olduğu ve zararın tamamen önlenemediği anlamına gelir.**
* **Ek Donanım Gereksinimi: PLC sinyallerini gerçek zamanlı olarak okumak ve analiz etmek, standart CAN-Bus donanımından farklı ve daha pahalı, özel HomePlug Green PHY izleme donanımı (ve uzmanlığı) gerektirir.**

**3. Fırsatlar (Opportunities) – (Dışsal ve Olumlu)**

**Bu tehdidin, BlockSentinel projesine piyasada sağlayabileceği avantajlar ve büyüme alanlarıdır:**

* **Bütüncül Güvenlik Çözümüne Geçiş: Bu anomali, BlockSentinel'in kendisini sadece bir CAN/OCPP analiz aracı olmaktan çıkarıp, PLC izlemeyi de kapsayan bütüncül bir EVSE Güvenlik Çözümü haline getirmesi için bir fırsattır. Bu, pazarda büyük bir rekabet avantajı sağlar.**
* **"Plug & Charge" Güven Sertifikasyonu: ISO 15118'e olan güvenin bu tip saldırılarla sarsılma potansiyeli, CPO'ların ve üreticilerin "Sertifikalı Güvenli Plug & Charge" çözümlerine olan talebini artıracaktır. BlockSentinel, bu alanda lider bir sertifikasyon rolü üstlenebilir.**
* **Klonlanmış Sertifika Kara Listeleme (Blockchain): Blok zinciri altyapısı, çalınan ve klonlanmış ödeme sertifikalarının (Plug & Charge sertifikaları) değiştirilemez ve anında güncellenebilir bir kara listesini (Revocation List) sunmak için mükemmel bir zemin oluşturur.**

**4. Tehditler (Threats) – (Dışsal ve Olumsuz)**

**Bu tehdit senaryosunun, projenin başarısını ve yaygınlaşmasını zorlaştırabilecek dış faktörlerdir:**

* **Geliştirme Karmaşıklığı ve Maliyet: PLC sinyallerini gerçek zamanlı olarak analiz etme yeteneği kazanmak, CAN-Bus'tan farklı ve özel donanım (HW) uzmanlığı, yazılım entegrasyonu ve API'ler gerektirecektir. Bu durum, projenin zaman çizelgesini ve bütçesini önemli ölçüde artırabilir.**
* **Saldırganın Adaptasyonu: Saldırganların tespiti zorlaştırmak için daha "akıllı" MitM implantları geliştirmesi (örneğin sıcaklık artışını simüle eden veya sinyal manipülasyonunu CAN'a yansıtmadan yapan implantlar).**
* **Üretici Entegrasyon Engelleri: Özellikle BMS verilerine ve kritik akım sensörlerine erişim, araç ve şarj istasyonu üreticilerinin güvenlik politikalarına bağlıdır. Üreticiler bu kritik verilere üçüncü taraf yazılımların erişimini kısıtlayabilir.**