Suat İSKENDER
Netcom Bilgisayar A.Ş
Teknik Genel Müdür Yardımcısı

Elektrikli Araçlarda Siber Güvenlik: Tehditler ve Çözümler

“Elektrikli araçlarda siber güvenlik neden önemlidir? Bunun ana sebebi güvenlik kaygısıdır. Elektrikli araçların üzerinde yapılan araştırmalar, bu araçların geleneksel araçlara kıyasla daha fazla uzak bağlantıya ihtiyaç duyduğu ve çok amaçlı hizmetlere cevap verebilecek karmaşık yazılım kodlarına sahip olduğunu göstermektedir. Bu özelliklerinden dolayı siber saldırılara daha çok maruz kalabileceğini öngörülmektedir”

Akıllı arabaların hayatımıza girmesi ve her geçen gün sayılarının artması ile bu araçların güvenlik durumları sorgulanmaya başlandı. Bu araçlar bizi ve ailemizi taşımak için yeterli güvenlik önlemine sahipler mi? Gerekli standartları taşıyorlar mı? Bu sorular artık herkes tarafından sorulmakta ve araştırılmaktadır. Son zamanlarda üretilen araçların birçoğu yazılım tabanlı elektronik kontrol sistemi ile yönetilmekte ve araç ister benzinle ister elektrikle çalışsın bu sistemlerdeki güvenlik açıkları bütün araçları tehdit etmektedir. Şu bir gerçek ki, bu sistemler arabalarımızı daha akıllı hâle getirirken diğer yandan bilgisayar korsanlarının yararlanabileceği potansiyel güvenlik açıklarını birlikte getirmektedir.

Elektrikli araçlarda siber güvenlik neden önemlidir? Bunun ana sebebi güvenlik kaygısıdır. Elektrikli araçların üzerinde yapılan araştırmalar, bu araçların geleneksel araçlara kıyasla daha fazla uzak bağlantıya ihtiyaç duyduğu ve çok amaçlı hizmetlere cevap verebilecek karmaşık yazılım kodlarına sahip olduğunu göstermektedir. Bu özelliklerinden dolayı siber saldırılara daha çok maruz kalabileceğini öngörülmektedir. Siber güvenlik açıklarının sömürülmesi durumunda, aracın kontrolden çıkmasına ya da istek dışı hızlanma veya frenleme gibi güvenlik risklerine yol açmasına sebep olabilir.

Siber güvenlik zayıflıkları ve riskleri nelerdir? Saldırı yüzeyi, bir ortamdaki yetkisiz kullanıcılar tarafından kullanılabilecek ve veri ihlalinde sebep olabilecek tüm güvenlik açıklarını ve giriş noktalarını ifade eder. Bunlar bilgisayar korsanlarının yetkisiz erişim elde etmek için hedeflediği tüm alanlardır. Elektrikli araçlarda potansiyel saldırı vektörleri arasında bulunan Bluetooth, Wi-Fi, GPS gibi kablosuz haberleşme teknolojilerinin haricinde önemli olan bazı kritik haberleşme protokolleri aşağıda açıklanmıştır.

- **CAN (Bus-Controller Area Network):** Kontrolör Alanı Ağı (CAN), motor, şanzıman, frenler gibi otomobilin sistemleri arasında arasındaki iletişimi sağlayan bir ağ protokolüdür.
- **LIN (Local Interconnect Network):** Pencereler ve koltuklar gibi daha az kritik sistemler arasındaki iletişimi sağlayan bir ağ protokolüdür.
- **FlexRay:** Daha yüksek veri hızı ve güvenilirlik gerektiren kritik sistemler için kullanılan bir ağ protokolüdür.

- **OBD (On-Board Diagnostics):** Aracın motor sistemleri hakkında veri almak için kullanılan bir standarttır.
- **ISO 15118:** Elektrikli araçların şarj istasyonlarıyla iletişim kurmasını sağlayan standarttır.

Haberleşme protokolleri ve standartlar araç içi sistemlerin birbirleri ile haberleşmesinde kullanıldığı gibi araç dışı haberleşmede kullanılarak verilerin uzak noktalar gönderilmesinde (Telemetri) rol alırlar. Bu durum ise doğal olarak zayıflık ve risk faktörlerini oluşturur. Diğer önemli husus, elektrikli araçlarda kullanılan Elektronik Kontrol Ünitesi (ECU)‘dir. ECU, “Motorun Beyni” olarak adlandırılır ve motor kontrol modülü, transmisyon kontrol ünitesi, şarj dinamosu modülü vb. sistemlerin kontrol edilmesi sağlar. Bu modüllerin ECU ile güvenilir haberleşmesi, CAN protokol ile sağlanmaktadır. CAN protokolünün hacklenerek ECU'ların istenmeyen aktörler tarafından kontrol alınabileceği ise kanıtlanmıştır.

Elektrikli araçlarda kullanılan kablosuz ağ teknolojilerinin güvenlik tehdidi oluşturduğu zaten bilinmekte (Bluetooth, Wi-Fi, GSM-4G/5G mobil broadband vb.) ve bunları kullanmak ise siber güvenlikte daha farklı açıdan güvenlik sorunlarını beraberinde getirmektedir.

Saldırı yüzeyleri hakkında son değineceğimiz konu ise elektrikli araçların şarj istasyonlarının güvenliği olacak. Birçok kişi elektrikli araç şarj istasyonlarının siber saldırıya uğrama olasılığını hiç düşünmemiş olabilir fakat şarj istasyonları sayısının son zamanlarda artmasıyla bilgisayar korsanlarının hedefi haline geldiği bir gerçektir. Genel yapılandırmada elektrikli araç şarj istasyonları, içlerinde araç kullanıcılarının ücretlendirme ve faturalandırma sisteminin bulunduğu şebeke operatörlerine bağlanır (kredi kartı, mobil ödeme, RFID kart okutma) ve internet tabanlı olarak kullanılan sistemlerde yetkilendirme yapmak esastır. Gerekli önlemler alınmadığı müddetçe ağa bağlı elektrikli araç şarj istasyonları, yetkisiz erişim, kişisel bilgilerin ele geçirilmesi ve veri hırsızlığından tutunda istasyon bağlantılarının kesintiye uğramasına kadar çeşitli bilgisayar korsanlığı saldırılarına karşı savunmasız hale gelebilmektedir. Yukarıda belirtilen tehditler karşısında elektrikli araç üretici ve kullanıcıları aşağıdaki önlemleri alarak araçlarını siber saldırılara karşı koruyabilirler.

Elektrikli araçlarda ilerleyen zamanda daha da karmaşık hale gelecek olan yazılım kontrol sistemleri, elektronik bileşenler vb. sistemler berberinde daha farklı siber güvenlik açıklarını oluşturacakları bir gerçektir.

Standartlar ve Regülasyonlar

Elektrikli araç üretici firmalar uluslararası siber güvenlik standartlarına sahip olmalıdır.

- ISO 27001 Bilgi Güvenli sertifikası
- ISO/SAE 21434 Otomotiv Endüstrisi için Siber Güvenlik yönetim sistemi standardı

Yazılım kaynaklarının kodlarının kontrol edilmesi ve güvenli yazılım geliştirme süreçleri

- Araç yazılımları güvenli kaynaklar tarafından geliştirilmeli ve yazılımın tasarımı, geliştirme süreçleri mümkünse aracı üreten firma tarafından yapılmalıdır.
- Yazılım siber saldırılara karşı güvenilir olacak şekilde tasarlanmalı ve geliştirilmelidir. Yazılım tamamlandıktan sonra kapsamlı siber güvenlik testine tabi tutulmalıdır.
- Yazılımın geliştirme süreci tamamlandıktan sonra, sonradan ortaya çıkabilecek siber tehditlere karşı güvenli iletişim kanallarından ve güvenli protokoller aracılığı ile güncellemeye imkân sağlamalıdır.