Elektrikli Araç Ağları için CAN Bus Protokolü Güvenlik Analizi ve Çözüm Önerileri

Giriş

Controller Area Network (CAN) protokolü, modern araçların elektronik kontrol üniteleri (ECU'lar) arasındaki iletişimin temelini oluşturmaktadır. CAN Bus, hafif, sağlam ve hızlı olacak şekilde tasarlanmış olup, gerçek zamanlı sistem gereksinimlerini karşılamaktadır. Ancak, 1983 yılında tanıtıldığında, izole bir ortam varsayımıyla geliştirilmesi nedeniyle doğasında güvenlik eksiklikleri barındırmaktadır.

Bu rapor, kaynaklar ışığında CAN Bus protokolünün temel özelliklerini, barındırdığı kritik güvenlik zafiyetlerini, bu zafiyetleri hedef alan saldırı vektörlerini ve bu tehditlere karşı geliştirilmiş ileri düzey çözüm ve hafifletme (mitigasyon) mekanizmalarını detaylı olarak analiz etmektedir. Siber güvenlik düzenlemeleri (örneğin **UN Regulation No. 155 - UNR 155**) artık otomobil üreticilerinden araç içi ağlarda siber saldırıları tespit etme ve önleme tedbirleri almasını zorunlu kılmaktadır.

Bölüm 1: CAN Bus Protokolüne Genel Bakış

CAN Bus, modern bir araçta bulunan yaklaşık 70 ECU arasında **1 Mbps'ye kadar** veri iletişim hızları sağlayabilen bir protokoldür.

Temel Özellikler ve İletişim Mekanizması

1. **Mimarisi:** CAN, iki telli (CAN High ve CAN Low) diferansiyel bir çoklu ana (multi-master) protokoldür. Diferansiyel sinyalleme, CAN Bus'ı elektriksel ve manyetik parazitlere karşı oldukça dirençli hale getirir.
2. **Yayın Ortamı (Broadcast):** CAN mesajları, pakette gönderen ve hedef adres içermez. Bunun yerine, ağdaki her düğüm mesaj yayınlayabilir ve alabilir. ECU'lar, mesajın içeriğini belirten tanımlayıcıya (ID) bakarak ilgili olup olmadığını kontrol eder.
3. **Arbitrasyon (Önceliklendirme):** CAN, **CSMA/CD+AMP** (Taşıyıcı Algılamalı Çoklu Erişim/Çarpışma Algılama ve Tahkim Mesaj Önceliği) ilkesini kullanır.
    - Mesajlar, önceliklerini tanımlamak için bir **tanımlayıcı çerçevesine (identifier frame)** sahiptir.
    - Mesaj gönderiminde çakışma olduğunda, **daha düşük ID değerine sahip mesajlar daha yüksek önceliğe sahiptir** ve tahkim sürecini (arbitration) kazanır. Bu özellik, meşru ECU'ların mesajlarının iletimini garanti eder, ancak aynı zamanda saldırganlar için bir zafiyet vektörü oluşturur.

Bölüm 2: CAN Bus Güvenlik Zafiyetleri ve Saldırı Vektörleri

CAN protokolü, izole bir ortam varsayımıyla tasarlandığından, modern araçların dış dünyaya (OBD-II portu, Wi-Fi, Bluetooth gibi) bağlantısı arttıkça ciddi güvenlik zafiyetleri ortaya çıkmıştır.

Temel Tasarım Zafiyetleri

1. **Kimlik Doğrulama Eksikliği:** CAN protokolünün tasarımındaki en temel zafiyet, gönderilen mesajların menşeini doğrulayan **bir mekanizmanın olmamasıdır**. Herhangi bir ECU, herhangi bir kimlikle mesaj yayınlayabilir.
2. **Şifreleme Eksikliği:** İletişim trafiği **şifrelenmez** (unencrypted traffic). Şifreleme, protokolün hafif ve hızlı olma doğasına ters düşeceği düşünülerek uygulanmamıştır. Şifrelemenin olmaması, saldırganların düşük maliyetli donanımlarla trafiği kolayca **dinlemesine (sniff)** olanak tanır.
3. **Veri Bütünlüğü ve İnkar Edilemezlik Eksikliği:** CAN mesajları, veri bütünlüğünü sağlamak için CRC (Döngüsel Artıklık Kontrolü) kullanır, ancak bu alan yalnızca iletim hatalarını tespit eder, **saldırgan manipülasyonunu (data integrity)** veya **mesajın kaynağını (non-repudiation)** doğrulamaz.

Başlıca Saldırı Türleri

Bu tasarım zafiyetleri, saldırganların araç işlevlerini tehlikeye atmasına olanak tanır:

1. **Denial of Service (DoS) Saldırısı:**
    - Saldırgan, **en yüksek önceliğe sahip CAN ID'lerini (örneğin 0x000)** sürekli yüksek frekansta enjekte ederek arbitrasyonu kazanır.
    - Bu, diğer meşru ECU'ların kritik mesajlarını (örneğin motor veya fren sistemi) iletmesini engeller. Bu saldırı, sistemin çalışamaz hale gelmesine neden olabilir.
2. **Spoofing (Taklit) ve Injection (Enjeksiyon) Saldırıları:**
    - Saldırganlar, OBD-II portu gibi erişim noktaları aracılığıyla CAN Bus'a bağlanır.
    - **Spoofing** sırasında, saldırgan meşru bir ECU'dan geliyormuş gibi **sahte (forged) bir ID** ile zararlı mesajlar gönderir. Bu, aracın işlevlerinin (örneğin hız, vites seçimi) manipülasyonuna yol açabilir.
    - **Injection** saldırıları, mesaj sıklığını veya yükünü anormal bir hızda değiştirerek simüle edilmiş olaylar oluşturur.
3. **Masquerade (Kimlik Sahtekarlığı) Saldırısı:**
    - Bu saldırı, bir ECU'nun yerine geçerek (impersonate) kötü niyetli mesajlar enjekte edilmesidir. Saldırganlar, CAN Bus'ın yayın ortamı yapısını ve kimlik doğrulama eksikliğini sömürür.
4. **Replay (Tekrar Oynatma) Saldırısı:**
    - Saldırganlar, daha önce kaydedilmiş geçerli CAN mesajlarını kaydeder ve bunları daha sonra tekrar oynatarak yetkisiz eylemlere neden olabilir. Güvenlik protokolleri, bu tür saldırıların önüne geçmek için nonce (tek kullanımlık sayı) veya sayaç kullanmalıdır.

5. **Fuzzy Attack:**
    - Rastgele oluşturulan ID'ler ve rastgele yükler, iletişim kanalına yüksek frekansta enjekte edilir. Amaç, sistemde rastgele manipülasyon veya arızaya neden olmaktır.

Bölüm 3: CAN Bus Güvenlik Çözümleri ve Karşı Tedbirler

CAN Bus güvenliğini sağlamak için iki temel strateji bulunmaktadır: (1) Mesajın orijinalliğini garanti eden **Kriptografik Kimlik Doğrulama Protokolleri** ve (2) Anormal davranışları tespit eden **Saldırı Tespit Sistemleri (IDS)**.

3.1. Kriptografik Kimlik Doğrulama (Authentication) Çözümleri

CAN'ın sınırlı veri yükü boyutu (8 byte) nedeniyle kriptografik yöntemlerin (özellikle MAC'lerin) uygulanması zorludur. Bu zorluk, genellikle MAC boyutunun kısaltılması (tag truncation) veya iki mesaj halinde bölünerek gönderilmesiyle aşılmaya çalışılır.

Güvenli Protokol Yaklaşımları

Yapılan güvenlik analizlerine göre, **iç saldırganlara** karşı direnç sağlamada en etkili protokol yaklaşımları şunlardır:

1. **Hash Zincirleri (Hash Chains): LCAP (Lightweight CAN Authentication Protocol)**, önceden paylaşılan gizli anahtarlar ve hash zincirleri kullanarak kaynak kimlik doğrulamasını sağlar.
2. **Asimetrik Şifreleme: AuthentiCAN** gibi protokoller, asimetrik kriptografik ilkeler üzerine inşa edilmiştir ve tek bir paylaşılan anahtarın tehlikeye atılmasını önlemeyi hedefler.
3. **M-MAC'ler (Mixed Message Authentication Codes): LiBrA-CAN** protokolü, anahtar bölme (key splitting) ve MAC karıştırma (MAC mixing) paradigmalarına dayanır ve CAN-FD veya CAN+ üzerinde çalışarak daha iyi performans hedefler.

İletişim Geliştirmeleri ve Protokol Yenilikleri

- **CAN Multiplexed MAC (CAN-MM):** Bu teknik, MAC digest verisini, standart CAN iletişimiyle paralel olarak, **frekans modülasyonu (OOK)** kullanarak çoğaltır.
    - CAN-MM, orijinal çerçeve formatını değiştirmediği için tüm standart CAN protokol versiyonlarıyla **geri uyumluluğu (backward compatibility)** korur.
    - MAC iletiminde neden olduğu **Ekstra Zamanın (MET)** ihmal edilebilir olması, planlama (schedulability) sorunlarını çözmeye yardımcı olur.
- **TACAN (Transmitter Authentication through Covert Channels):** Bu şema, CAN protokolünde değişiklik yapmadan veya ek trafik yükü oluşturmadan ECU kimlik doğrulamasını sağlamak için **gizli kanalları (covert channels)** kullanır.
    - TACAN, mesajların **Varışlar Arası Sürelerini (IAT)**, **saat sapmalarını (offset)** ve **veri yükünün En Önemsiz Bitlerini (LSB)** manipüle ederek kimlik doğrulama mesajlarını gizler.

Diğer Kriptografik Protokoller ve Teknikler

- **SecOC (Secure Onboard Communication):** AUTOSAR tarafından tanımlanan bu çerçeve, veri bütünlüğünü ve orijinalliğini sağlamak için her veri çerçevesine bir MAC özeti (digest) dahil edilmesini gerektirir.
- **Donanım Güvenlik Modülleri (HSM):** Kriptografik anahtarların ve güvenlik parametrelerinin güvenli bir şekilde saklanması için ECU'lara **"root of trust"** modülleri olarak entegre edilmelidir.

3.2. Saldırı Tespit Sistemleri (IDS)

Saldırı Tespit Sistemleri, CAN trafiğini analiz ederek anormal veya kötü niyetli desenleri belirlemek için hayati öneme sahiptir.

Sinyal Farkındalığına Sahip IDS (X-CANIDS)

X-CANIDS, geleneksel IDS'lerin aksine, CAN mesajı yüklerini (payload) doğrudan ham bit temsilleri yerine, **CAN veritabanı (DBC)** kullanarak **insan tarafından anlaşılabilir sinyallere** (örneğin motor devri, tekerlek hızı) dönüştürür.

- **Performans Avantajı:** Sinyallerin kullanılması, IDS'in tespit performansını artırır, çünkü bunlar aracın bağlamını yansıtır.
- **Açıklanabilirlik (Explainability):** X-CANIDS'in en büyük katkısı, saldırı tespit edildiğinde, saldırıdan **hangi sinyalin veya ECU'nun etkilendiğini açıklayabilen** ek bilgi sunmasıdır. Bu, olay müdahale ekipleri için önemlidir.
- **Yöntem:** X-CANIDS, **BiLSTM tabanlı bir otomatik kodlayıcı (autoencoder)** kullanır. Bu model, saldırı anında sinyal bazlı yeniden yapılandırma hatasını (reconstruction error) analiz ederek anomalileri belirler ve sıfır gün saldırılarını (zero-day attacks) dahi tespit edebilir.

Derin Öğrenme ve Fiziksel Özellik Tabanlı IDSs

1. **Derin Öğrenme (DL) Yöntemleri:** Derin öğrenme modelleri, CAN trafiğindeki karmaşık zamansal ve mekansal desenleri analiz ederek tehditleri tespit etmede etkilidir.
    - **Zamansal Analiz: LSTM** ve **GRU** gibi Tekrarlayan Sinir Ağları (RNN) varyantları, sıralı verilerdeki uzun vadeli bağımlılıkları yakalar. **Bi-directional LSTM (Bi-LSTM)**, hem geçmiş hem de gelecekteki bağlamdan öğrenerek anomali tespitini daha da güçlendirir.
    - **Mekansal Analiz: VGG-16** gibi Evrişimli Sinir Ağları (CNN) varyantları, CAN verisini görüntü temsillerine dönüştürerek saldırı imzalarını görsel olarak tanır ve derin özellik çıkarımı sağlar.
2. **Fiziksel Özellik Tabanlı Tespit:**
    - **Saat Sapması (Clock Skew):** CIDS (Clock-based IDS), ECU'ların benzersiz saat sapmalarını ölçerek Masquerade saldırılarını tespit eder.
    - **Voltaj Sinyal Karakteristikleri:** Viden ve VoltageIDS gibi sistemler, CAN sinyallerinin benzersiz elektriksel özelliklerini (voltaj) kullanarak saldırgan ECU'yu tanımlar.

Sonuç

CAN Bus protokolünün güvenliği, temel tasarımında kimlik doğrulama ve şifreleme mekanizmalarının bulunmaması nedeniyle ciddi risk altındadır. Bu zafiyetler, DoS, Spoofing, Injection ve Masquerade gibi hayati tehlike taşıyan saldırılara yol açmaktadır.

Güvenlik çözümleri, ya **MAC tabanlı kriptografik protokoller** (LiBrA-CAN, AuthentiCAN, LCAP) ya da **gelişmiş IDS sistemleri** (X-CANIDS, Derin Öğrenme tabanlı IDS'ler) aracılığıyla bu açıkları kapatmayı amaçlamaktadır. Özellikle **CAN-MM** gibi geri uyumlu donanım çözümleri, güvenlik sertifikalarını (MAC) mevcut CAN 2.0 sistemlerine entegre etme zorluğunu aşarken, **X-CANIDS** gibi sinyal farkındalığına sahip IDS'ler ise saldırıları tespit etme ve saldırının kökenini analiz etme (açıklanabilirlik) konusunda kritik adımlar atmaktadır.

En yüksek güvenlik standardına ulaşmak için, **hash zincirleri** ve **asimetrik şifreleme** gibi yöntemleri kullanan protokollerin (özellikle CAN-FD gibi daha geniş bant genişliği sunan protokollerle birlikte) **HSM** gibi donanım güvenlik modülleri ve **yapay zeka tabanlı IDS** çözümleriyle entegre edilmesi gerekmektedir.