**1. CAN Protokolünün Güvenlik Zafiyetleri**

CAN (Controller Area Network) protokolü, araç içi ECUs (Elektronik Kontrol Üniteleri) arasında veri iletişimini sağlar. Ancak, protokol tasarımında **güvenlik önlemleri (şifreleme, kimlik doğrulama, mesaj bütünlüğü kontrolü) bulunmadığı için** saldırılara açıktır.

**Başlıca Zafiyetler**

1️⃣ **Şifreleme Eksikliği**

* CAN mesajları **düz metin (plaintext) olarak iletilir**, yani saldırganlar ağ trafiğini dinleyerek verilere doğrudan erişebilir.
* **Örnek:** Bir saldırgan, aracın fren sistemine ait verileri okuyabilir ve analiz edebilir.

2️⃣ **Kimlik Doğrulama Yok**

* CAN protokolü, mesajları gönderen ECU’ların kimliğini doğrulamaz.
* **Örnek:** Saldırgan, ECU’ların birinden mesaj gönderiyormuş gibi davranabilir (spoofing).

3️⃣ **Yayın (Broadcast) Yapısı**

* CAN üzerindeki tüm mesajlar **tüm ECU’lar tarafından alınır**, yani bir saldırganın sisteme dahil olup sahte mesaj göndermesi kolaydır.
* **Örnek:** ECU’ların tümüne frenleme mesajı göndererek aracı aniden durdurmak.

4️⃣ **Öncelik Tabanlı Çakışma Çözümü**

* CAN çerçevelerinde öncelikli mesajlar, daha düşük öncelikli mesajları geçersiz kılar.
* **Örnek:** Bir saldırgan, sürekli yüksek öncelikli mesajlar göndererek ağın tamamını devre dışı bırakabilir (Denial of Service - DoS saldırısı).

**2. CAN Protokolüne Yönelik Saldırılar ve Gerçekleşme Yöntemleri**

**2.1. Mesaj Enjeksiyon Saldırıları**

* Saldırgan, **geçerli bir ECU gibi davranarak** sahte mesajlar enjekte eder.
* **Gerçekleşme Yöntemi:**
  1. OBD-II bağlantı noktasından (fiziksel erişim) veya kablosuz (Wi-Fi/Bluetooth) erişim ile ağa bağlanır.
  2. ECU’ları taklit ederek **fren, hızlanma veya direksiyon komutları gönderir**.
* **Örnek:** Fren sistemi ECU’suna sürekli “Freni bırak” mesajı göndererek aracın durmasını engellemek.

**2.2. Hizmet Reddi (DoS) Saldırıları**

* Ağa sürekli **yüksek öncelikli mesajlar göndererek** ECU’ların normal işlemlerini engellemek.
* **Gerçekleşme Yöntemi:**
  1. CAN veri yolu üzerinde en yüksek öncelikli mesajlar sürekli tekrar edilir.
  2. Diğer ECU’lar mesajlarını iletemez hale gelir.
* **Örnek:** **Acil fren ECU’sunun devre dışı bırakılması**, böylece kaza anında sistem yanıt veremez.

**2.3. ECU Kimlik Sahtekarlığı (ECU Masquerading)**

* Saldırgan, var olan ECU’ları taklit ederek **sahte veriler gönderir**.
* **Gerçekleşme Yöntemi:**
  1. ECU’ların kimlik doğrulaması olmadığı için saldırgan, bir ECU’nun kimliğini kopyalar.
  2. Mevcut birim yerine sahte komutlar göndererek araç sistemlerini manipüle eder.
* **Örnek:** Araç içi sensörlerden hız bilgilerini yanlış göstererek aracın hız limitini aşmasına neden olmak.

**2.4. Fuzzing (Bozulmuş Veri Saldırısı)**

* Rasgele veya bozulmuş mesajlar göndererek **ECU’ların beklenmeyen davranışlar sergilemesine neden olmak**.
* **Gerçekleşme Yöntemi:**
  1. CAN protokolü üzerinde bilinmeyen veya geçersiz veri paketleri gönderilir.
  2. ECU’lar bu verileri işleyemez ve **kilitlenebilir veya arızalanabilir**.
* **Örnek:** Farklı hızlarda sahte motor sıcaklığı mesajları göndererek **motor kontrol ünitesinin yanlış çalışmasına neden olmak**.

**2.5. GPS Sahtekarlığı ve Sensör Manipülasyonu**

* Araç içi **GPS, radar veya kamera verilerinin değiştirilmesi**.
* **Gerçekleşme Yöntemi:**
  1. GPS alıcısına **yanıltıcı sinyaller göndererek** yanlış konum bilgisi oluşturulur.
  2. Otonom sistemler yanlış tepki verebilir.
* **Örnek:** Otonom bir aracın yanlış yöne yönlendirilmesi veya hız limiti sahtekarlığı.

**3. CAN Güvenliği İçin Alınabilecek Önlemler**

| **Saldırı Türü** | **Önleme Yöntemi** |
| --- | --- |
| Mesaj Enjeksiyonu | **Şifreleme ve kimlik doğrulama** kullanımı |
| DoS Saldırıları | **Hız sınırlama (Rate Limiting) ve zaman damgası (Timestamping)** |
| ECU Sahtekarlığı | **İleri seviye kimlik doğrulama mekanizmaları** |
| Fuzzing | **Özel mesaj filtreleme ve anormallik tespiti** |
| GPS Sahtekarlığı | **Gelişmiş sinyal işleme teknikleri ve çoklu veri kaynağı doğrulaması** |

**3.1. Kimlik Doğrulama ve Şifreleme**

* **AES veya RSA tabanlı şifreleme** kullanarak ECU’ların güvenli veri alışverişi yapması sağlanabilir.
* **Örnek:** ECU’lar arasındaki veri alışverişinde şifrelenmiş anahtarlar kullanmak.

**3.2. Gelişmiş Saldırı Tespit Sistemleri (IDS)**

* **Makine öğrenmesi tabanlı** IDS sistemleri kullanarak saldırılar tespit edilebilir.
* **Örnek:** DNN (Derin Sinir Ağları) veya Random Forest kullanarak anormal CAN mesajlarını belirleme.

**3.3. Hibrit Güvenlik Yaklaşımları**

* **Ağ segmentasyonu** ve **bütünlük kontrolleri** ile saldırı alanını kısıtlama.
* **Örnek:** Fren sistemini diğer ECU’lardan izole etmek.

**3.4. Fiziksel Güvenlik Önlemleri**

* OBD-II portuna **yetkisiz erişimi önlemek için fiziksel güvenlik mekanizmaları eklemek**.
* **Örnek:** Yetkisiz fiziksel erişimi önleyen kilitli bağlantı noktaları.

**4. Sonuç ve Öneriler**

* CAN protokolü **şifreleme, kimlik doğrulama ve mesaj bütünlüğü gibi güvenlik özelliklerinden yoksun** olduğu için saldırılara açıktır.
* **Makine öğrenmesi tabanlı IDS, şifreleme yöntemleri ve ağ segmentasyonu** kullanılarak güvenlik artırılabilir.
* Özellikle **otonom araçlarda güvenlik açıklarının giderilmesi kritik öneme sahiptir**.

📌 **Öneri:** Gelecekte **CAN protokolü yerine güvenlik önlemleri içeren Ethernet tabanlı sistemlerin** kullanılması önerilmektedir.

Bunlar üzerine çalışarak yüksek lisans tezinizde detaylı incelemeler yapabilirsiniz. Spesifik konular üzerine yoğunlaşmak isterseniz, hangi alanı detaylandırmak istediğinizi söyleyebilirsiniz. 😊