LINKEDIN GÖNDERİ TASLAĞI

Başlık: Hız Tuzağı: Yapay Zeka Düşünürken Faturayı Kim Ödüyor? ⚡ 🚗

Gönderi Metni: Dijital güvenlik dünyasında hepimiz genellikle şifreleme veya yetkisiz erişim konularına odaklanırız. Peki ya sisteminizi koruyan Yapay Zeka (AI), hırsızı görüp "dur" diyene kadar hırsız çoktan işini bitirip kaçmışsa?

Bu hafta Bilgi Sistemleri Güvenliği projemiz kapsamında ekibimizle kritik bir güvenlik simülasyonu gerçekleştirdik. Odak noktamız **"Latency Exploit" (Gecikme İstismarı)** idi.

🔍 **Senaryomuz Neydi?** Elektrikli araç şarj sistemlerini (CSMS) izleyen anomali tespit modellerinin veriyi işleyip karar vermesi milisaniyeler sürer. Saldırganlar, bu küçücük "düşünme süresini" (latency window) bildikleri için, AI henüz uyarı vermeden milisaniyeler içinde "Başlat/Durdur" (Start/Stop Transaction) mesajlarını göndererek faturalandırma sürecini atlatabilirler.

💡 **Ne Öğrendik?** Simülasyonumuz gösterdi ki;

1. Güvenlik sadece veri doğrulama değil, aynı zamanda hassas bir "zamanlama" meselesidir.
2. Yapay zeka ne kadar gelişmiş olursa olsun, operasyonel süreçlerle tam senkronize çalışmazsa "post-facto" (olay sonrası) uyarılardan öteye gidemeyebilir.

Bu çalışma ile sistem mimarilerinde "Atomic Transaction" ve senkronizasyonun önemini uygulamalı olarak test etmiş olduk. Modern güvenlik açıklarına karşı, modern mimariler geliştirmeye devam ediyoruz! 🛡️ 💻

#CyberSecurity #AI #LatencyExploit #ElectricVehicles #OCPP #AnomalyDetection #InfoSecProject

GÖRSEL İÇERİK ÖNERİSİ

Konsept: "Zamanla Yarış: Saldırgan vs. AI"

Görsel Açıklaması (Tasarımcı veya AI Aracı İçin Prompt): Görsel, dijital bir yarış pistini andıran ikiye bölünmüş bir ekran olmalı.

- **Sol Tarafta (Saldırgan):** Çok hızlı hareket eden, arkasında neon yeşil bir iz bırakan "Elektrikli Araç Fişi" veya "Şimşek" ikonu. Altında "İşlem Süresi: 200ms" yazıyor.
- **Sağ Tarafta (Yapay Zeka):** Verileri analiz etmeye çalışan, etrafında dönen yükleme (loading) halkaları olan fütüristik bir "Yapay Beyin" veya "Kalkan". Altında "Tespit Süresi: 1500ms" yazıyor ve rengi hafifçe kırmızıya dönüyor (uyarı veriyor ama geç kalmış).
- **Ortada:** Büyük ve dikkat çekici bir yazı ile **"GAP DETECTED: LATENCY"** (Boşluk Tespit Edildi: Gecikme) yazısı yer almalı.