

Geleceğin Otomobillerinde Güvenlik Mümkün mü?

Artık otomobiller birbirine ve çeşitli iletişim cihazlarına bağlı olacak. Ancak bu, ne kadar güvenli?

19 Ocak 2017 12:15



Elektronik tasarım otomasyonu konusunda dünyanın önde gelen şirketlerinden **Mentor Graphics**'in Türkiye Distribütörü olan CDT Bilgi Teknolojileri Genel Müdürü Alpaz Göğüş, hizmet verdikleri otomotiv sektöründeki bu gelişmelerle ilgili bilgileri aktardı.

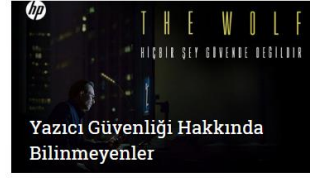
Birçok otomobil üreticisinin geleceğin araçlarında güvenliğin sağlanması konusunda yoğun araştırma ve çalışma içerisinde olduğunu dile getiren **CDT Bilgi Teknolojileri Genel Müdürü Alpaz Göğüş**, otomobil satın alan bir kullanıcının aracını uzun yıllar kullanmayı amaçladığını, bu nedenle güvenlik çözümleri dâhil getirilen her çözümün uzun vadeli olması gerektiğini belirterek sözlerine aşağıdaki gibi devam etti;

"Eskiden araçlar tümüyle mekanikti ve başkalarının arabanıza verebileceği en büyük zarar, arabanızı çalmak olurdu. Ancak şimdi öyle değil. Önümüzdeki on yıllık dönemde tüm araçlarda en az beş veya altı kablosuz erişim noktası bulunacak ve güvenliklerinin sağlanması gerekecek. Bu erişim noktaları arasında Wi-Fi, arabaların birbirleriyle ve altyapı sistemleriyle haberleşmesine olanak tanıyan Özel Kısa Mesafe İletişimi ve çarpışma uyarıları için LiDAR, telsiz, uydü, lastik basınç monitörlerinin Bluetooth bağlantıları ve Bluetooth ile ses iletişimi gibi diğer kablosuz teknolojileri sayabiliriz. Bunların tümü olası erişim noktaları. Otomobil üreticileri de, bilgisayar korsanları bu kablolu veya kablosuz erişim noktalarını kullanarak uzaktan bağlantı sağlasa bile arabaya zarar gelmeyeceğinden emin olmak istiyor. Bu durum sadece teknik özellikler için geçerli değil elbette. Güvenlik kayıtlarına erişimi olan ve ayrıldıkları firmayla sorun yaşayan çalışanlar, sonradan bu bilgilere ulaşmak isteyebilir. Bu da araç güvenliğinin tehlikeye atılmasına neden olabilir."

Mentor Graphics'in yakın zamanda işin yazılım ve yazılım mühendisliği tarafına dâhil olduğunu belirten Göğüş, geliştirecekleri ürünler sayesinde arabalardaki elektronik kumanda kutularının (ECU) koruma altında olup olmadığına dair şüphelerin ortadan kalkacağını belirterek şunları söyledi:

"Her elektronik kumanda kutusunun bir şifrelenmiş anahtarının olması sebebiyle yazılımın bir kutuya erişebilmesi için şifrelemenin öncelikle otomobil üreticisinde bulunan özel bir anahtarla eşleşmesi gerekecek. Böylece, herhangi bir yazılım değişimi gerçekleşmeden önce araçtaki elektronik kumanda kutularıyla asıl otomobil üreticisi arasında etkin şekilde güvenli bir elektronik bağlantı kurulmuş olacak. Bu yöntem, otomobil üreticisinin indirilen yazılım üzerinde denetim sahibi olmasını ve güvenliği sağlayacak."

Güvenlik sistemleri geliştirilir ve kullanıma sokulurken çok fazla enerji, zaman ve para harcadığını belirten Göğüş, uygulamadan seri üretime geçiş sırasında kullanılan yöntemlere yenilerinin eklenebileceğini ve kuşkusuz önümüzdeki kısa sürede tüm otomobil üreticilerinin güvenliği sağlanmış veritabanlarına sahip araçları kablosuz teknoloji veya mevcut tanımlama portları ile güncelleyebileceklerini belirtti. Göğüş, "Tüm bunlar yakın gelecekte hayatımıza girecek sürücüsüz araçların güvenliğinin sağlanmasının yolunu açacaktır." diyerek sözlerini tamamladı.



Yazıcı Güvenliği Hakkında Bilinmeyenler



İnternette nasıl ev sahibi olunur test ettik

Günün Fırsatları

CHIP'i Takip edin



E-Posta listemize katılın

E-posta adresiniz



Günün En çok Okunanları



TV Satın Alırken Bunları Kontrol Edin!



Blizzard, ilk StarCraft'ı yeniliyor!



Akbank'tan Açıklama Geldi!



İstanbul'un Surları Xaxe ile Yeniden Canlandı!

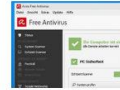


Toplanan Galaxy Note 7'lere Ne Olacak?

En Çok İndirilenler



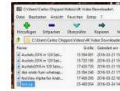
CCleaner
★★★★★



Avira Free
★★★★★



VLC media player (64 Bit)
★★★★★



7-Zip (64 Bit)
★★★★★



avast Free Antivirus
★★★★★

İlginizi Çekebilir



Windows'u Hızlandıran 6 Hızlı Önerim!