Los Tesla, en el punto de mira de los hackers

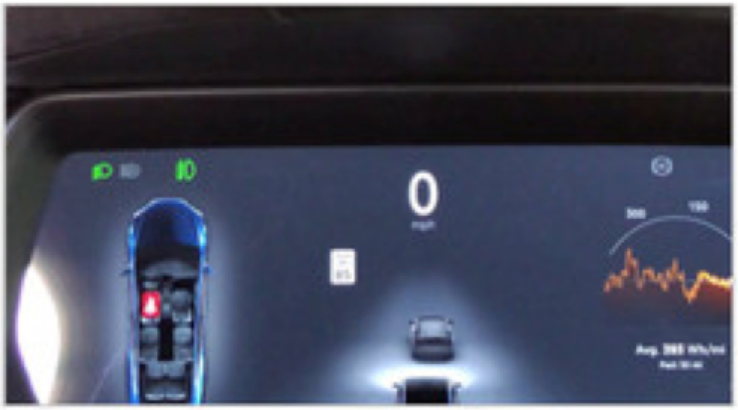
Recientemente, los investigadores de la empresa de ciberseguridad McAfee descubrieron que es posible engañar al sistema de cámaras **Mobileye Eye Q3** que tienen algunos vehículos Tesla.

Mobileye Eye Q3 utiliza las señales de límite de velocidad para adaptar la velocidad del crucero automático de Tesla (Tesla Automatic Cruise Control), aumentando o reduciendo la velocidad según las interpretaciones que haga el algoritmo de las señales de tráfico y GPS.

Aprendizaje automático adversario

Como veremos en el vídeo a continuación, con una simple cinta de 5 centímetros en una señal de límite de velocidad, **el algoritmo es engañado** y detecta 85 mph en lugar de lo que marca la señal (35 mph):

Este tipo de ataques se denominan "**aprendizaje automático adversario**": consiste en explotar las vulnerabilidades presentes en algoritmos de aprendizaje automático para conseguir resultados adversos.



El algoritmo entendió que el 35, realmente, era un 85, provocando que el vehículo

acelerada de inmediato.

McAfee advirtió de la vulnerabilidad a Tesla y MobilEye 90 días antes de publicar esta investigación, y afirmó que:

Ambos proveedores mostraron interés y agradecieron la investigación, pero no han expresado ningún plan actual para abordar el problema en la plataforma existente. MobilEye indicó que las versiones más recientes del sistema de cámaras abordan estos casos de uso

McAfee

Recientemente, hemos tenido el placer de conocer a EvanConnect: el hacker que fabrica dispositivos inhibidores de frecuencia para abrir, arrancar y hacer lo que quiera con tu coche.