FocalPoint/YouGov research reveals 82% of UK consumers say they are concerned about the risk of GPS spoofing affecting safety of driver-assisted and autonomous vehicles

Submitted by: Intelligent PR
Thursday, 3 August 2023

CAMBRIDGE, UK – A survey of 2000 UK consumers (78% motorists) conducted by YouGov and commissioned by FocalPoint, the provider of high-performance positioning technologies for vehicles, smartphones and wearables has revealed significant concerns among UK consumers regarding the impact of illegal ‘GNSS spoofing’ on driver assistance and autonomous driving systems.

Eighty-two percent of those surveyed believe that spoofing will have a detrimental effect on road safety as assisted driving applications and autonomous vehicles become increasingly available.

Concerns over cybersecurity and spoofing could impact the rates of adoption for autonomous vehicles (AVs) and vehicles with autonomous driver assistance systems (ADAS)

A further 45% of respondents stated the risk of cyberattacks as an influencing factor on the decision to purchase a car with partially or fully automated autonomous capabilities.

85% of respondents cited the risks of harm to either passengers or other road users and pedestrians as their top concern associated with spoofing.

Global Navigation Satellite System (GNSS) Spoofing is a form of cyber attack that targets satellite positioning systems such as GPS. Spoofers attack vehicles by broadcasting fake satellite signals to override legitimate satellite signals, confusing the GNSS receiver and causing potentially harmful disruption to the vehicle’s positioning systems.

Spoofing attacks are becoming worryingly frequent, leading the European Union Aviation Safety Agency to issue an alert warning about satellite navigation systems being jammed or spoofed around Ukraine and in nearby regions in 2022.

Modern vehicles rely on GNSS for route guidance and to determine absolute location for driving assistance systems. Spoofed signals can interfere with the vehicle navigation, ADAS or autonomous driving systems, putting passengers and other vehicles at risk.

The dangers of spoofing were reported back in 2019 when a Tesla Model 3 was experimentally spoofed successfully. Using off-the-shelf hardware and software, fake satellite signals were illegally broadcast by a spoofer, disrupting the behaviour of the vehicle.

This proved the vulnerability of a modern vehicle to an attack, where the spoofer can disrupt the computed location, speed and heading of a victim’s receiver, causing vehicles to believe they are in a different location and even potentially provide false information about road conditions, traffic, or obstacles. Spoofing can also be used as a method for theft and to hide the true location of a stolen vehicle as reported by its onboard security tracking systems.

With autonomous vehicles reliant on accurate navigation, time synchronisation and coordination with other vehicles, spoofing also has the potential to disrupt multiple autonomous vehicles simultaneously and eighty-two percent of those surveyed believe that spoofing will have a detrimental effect on road safety as assisted driving applications and autonomous vehicles become increasingly available.

As the tools required for spoofing become cheaper and easily available online, eradicating the threat becomes very difficult. A traditional method to protect against spoofing is to encrypt the radio signal, but this is expensive, complicated and relies on the management of the encryption key. An alternative technique is to use expensive and bulky arrays of antennas that can measure the arrival angle of the satellite signals and only use the ones coming from trusted directions. Such an approach, however, is not practical for typical consumer use cases including the automotive sector.

Commenting on the research Scott Pomerantz, CEO of FocalPoint, said: “Our automotive OEM customers want to solve the critical issue of safely extending the availability of advanced driver assistance systems (ADAS) into more locations, especially cities. To achieve this, you need to have a lot of confidence in your positioning system. At FocalPoint, we have developed groundbreaking SupercorrelationTM technology that enables a new class of performance and trust in a satellite positioning receiver. By measuring the direction of the incoming signals it allows the receiver to ignore reflected signals as well as fake ‘spoofed’ signals. This makes them incredibly accurate and reliable in cities, and more resilient against spoofing attacks. FocalPoint’s unique technology can instantly detect fake signals as spoofers, ignore those signals, and pinpoint where in the physical environment the signal is coming from. It is the only consumer-grade product in the market capable of these unique features.”

About FocalPoint
FocalPoint develops groundbreaking technologies that boost the accuracy, reliability and security of radio receivers. FocalPoint partners with Chipset manufacturers and OEMs to enhance the capability of their devices, helping to improve the lives of billions of people who rely on location technologies including smartphones, wearables and autonomous vehicles.

Founded in 2015 by Dr. Ramsey Faragher, the company is headquartered in Cambridge, with offices in Bristol and the US. FocalPoint’s technologies are multi-award winning, including Security Innovation of the Year at the 2023 National Technology Awards and the Royal Institute of Navigtation’s Technical Innovation Award. The company was named Europe’s Hottest Spacetech Startup in 2020. Their research and technical teams are recognised by the UK Royal Institute of Navigation and the US Institute of Navigation.

Its Supercorrelation™ technology is currently licensed by u-blox (SWX:UBXN) and is in advanced trials with several major device manufacturers.

Investors include Molten Ventures, Gresham House, Passion Capital, IQ Capital, Cambridge Angels, Cambridge Enterprise and GM Ventures.

Media Contact:

James Lambert
Intelligent PR
james@intelligentpr.co.uk