Study confirms that road users are jamming GPS signals

February 21 2012

The first direct evidence of GPS jammers in use on British roads will be presented today alongside predictions of a major incident involving ships in the English Channel over the next decade caused by disruption to navigation signals.

GNSS Vulnerability *2012: Present Danger, Future Threats* is organised by the ICT Knowledge Transfer Network and brings together the world's experts on location and timing systems to understand their susceptibility to attack.

Bob Cockshott, Director of Position, Navigation and Timing at the ICT Knowledge Transfer Network and organiser of the conference says: "Today's evidence from roadside monitoring shows that we have moved on from a potentially threatening situation to a real danger that we must address now. With the reliance on GPS systems in the maritime environment, highlighted by the General Lighthouse Authority, our vulnerability on land and at sea should not be underestimated. As well as immediate concerns, this conference has laid out the next generation of threats, in the form of spoofing and time sabotage – deliberately misleading users for criminal purposes rather than simply denying service. We must ensure that alongside dealing with the threat posed by jamming, we also stay ahead of advances in the criminal world."

The evidence of illegal jamming in the UK comes from roadside monitoring carried out by the SENTINEL project which looks at whether satellite navigation systems including GPS can be trusted by

their users.

Jamming monitors have so far been placed at around 20 locations in the UK. At one particular location that has been monitored continuously for the past 6 months over 60 individual jamming incidents were recorded and the results at another have already led to the recovery of a device. The next step is to update the monitoring equipment to be able to differentiate between different jammers, giving researchers a better idea of how many individuals at a particular location are jamming GPS signals.

The projects consortium is led by Chronos Technology, the Forest of Dean based supplier of timing and GPS solutions, whose founder Charles Curry presented its findings. He says: "SENTINEL was set up to tackle the threat of GPS Jamming in three stages - identification, detection and mitigation. Whilst the identification of the threat is well established, and through roadside monitoring we are making great strides in the detection and location of these devices, the final stage, mitigation, is still some way off depending on the application and industry sector. The question for the authorities is what we are going to do once the owners of these jammers are identified and how can we prevent others using them."

The results from SENTINEL will be accompanied by a presentation from the General Lighthouse Authorities highlighting how overly reliant ships are on GPS. In 2010 researchers produced low level jamming from the coast and reviewed its effect on various systems onboard ships in the English Channel. The impacts included:

- Ships veering off course without crew knowledge
- Ships give out false information to other ships about their position – significantly increasing the likelihood of a collision

- Communications channels failing, preventing crew talking to the coastguard
- The failure of the emergency service system which sends out alarms and guide rescuers
- Alarms from ship's radar and compass

Consultant and Location and Timing system expert, Prof David Last says: "Whilst we expected some disturbance to the ship's chart display, this research revealed four or five other systems, all reliant on GPS which failed. The spread of the jamming technology used in these trials, with devices available online for only £50, makes a major incident at sea, whether accidental or intentional, a real danger. In the English Channel, the world's busiest seaway, I personally believe we will see such an incident in the next decade."

Alongside GPS Jamming, speakers will look at the next major threat to navigation systems. Spoofing generates false GPS signals to alter user's perceptions of time and location. With the right technology it can be done without the victim ever knowing and is virtually untraceable.

Todd Humpheys from the University of Texas owns the world's most powerful civil GPS spoofer. At GNSS 2012 he reports on tests carried out by his team on GPS-based timing devices used in mobile phone transmitters in the US. Such attacks are capable of breaking up the network, preventing towers from handing over calls.

"So far no credible high profile attack has been recorded but we are seeing evidence of basic spoofing, likely carried out by rogue individuals or small groups. Whilst the leap to more advanced, untraceable spoofing is large, so are the rewards. It's therefore guaranteed that criminals are looking at this. All it takes is one person to put one together and publish it online and we have a major problem".

One sector at risk is high-frequency financial trading. At GNSS vulnerability 2012 Todd will warn that criminals could throw off the GPS timing systems that time-stamp financial trades, a process known as 'Time Sabotage". Even a few milliseconds discrepancy could create confusion and enable unscrupulous traders to leverage their knowledge of the timing discrepancy for financial gain via inter-market arbitrage.

Provided by National Physical Laboratory