# GETTING OUT OF A JAM

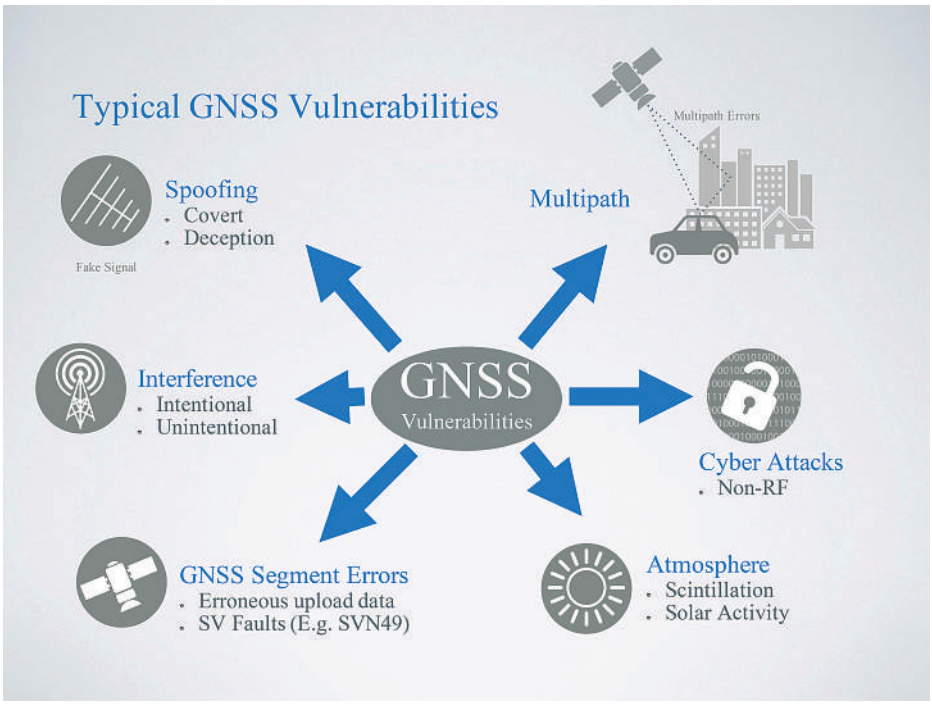
## DEVICES TO JAM GPS SIGNALS ALREADY EXIST AND GPS 'SPOOFING' HAS BEEN SHOWN TO WORK IN PRACTICE. BUT HOW BIG ARE THE THREATS AND WHAT CAN YOU DO TO MITIGATE PROBLEMS? GUY BUESNEL LOOKS AT HOW YOU CAN ASSESS THE RISKS

A lot has been written about the vulnerabilities of GNSS to signal disruption through jamming, spoofing or the effects of solar weather. Reading much of the material on this, one can be left with the feeling that GNSS is too vulnerable, that the low strength of its signals means that it is inherently unsuitable as the world's primary source of precision position, navigation and timing.

We know a great deal about the mechanisms that have the potential to disrupt GNSS signals but an often neglected point is how likely is it that a system will encounter disruption in normal use and what is the impact on the system if it does? This really deserves a good answer. If typical users will rarely encounter GNSS disruption and if they do, that disruption in terms of degraded availability or performance is minimal, then very little or no mitigation is likely to be required. On the other hand, if typical users can expect to regularly encounter GNSS disruptions that significantly affect availability and performance, then there is a good case for improving system resilience.

It's becoming progressively easier to get hold of jammers that can produce disruptive interference. Many websites sell unobtrusive 'personal privacy devices' (PPDs) that plug into a vehicle's cigarette lighter. These devices emit radio waves on common satellite frequencies, preventing equipment – such as SatNav or telematics systems – from receiving and processing satellite signals. The system is unable to calculate or report its own position or provide precise timing information while the jammer is on.

Jamming could be a threat to all businesses and industries that rely on GNSS for their operations. This includes the construction industry, where GNSS is used for surveying and where precise position and timing information from GNSS is used to track heavy vehicles and machinery. For instance, in the US, many concrete trucks are equipped with GNSS for tracking as it is important to deliver a correct mix to the customer in a very timely manner. Jamming has the potential for causing significant disruption to these kind of operations.




A commercially available GPS jammer or 'personal privacy device'

## The arrival of spoofing

GPS jamming is already widespread, but a new threat is emerging on the horizon. GPS spoofing involves a person or group broadcasting fake satellite signals to a GPS receiver to fool it into generating a false position and potentially following a false route. While GPS spoofing is in its infancy, the wider use of time and location spoofing for malicious or misguided purposes is already common.

Most spoofing today happens at the application layer: modifying or tricking location management software into misinterpreting location data. This is a widespread phenomenon in the entertainment industry, with users altering DNS (Dynamic Name Service) codes or using proxy and VPN (Virtual Private Network) services to trick online stores and streaming services into giving them content and prices not normally available in their country of residence.


The Spirent GSS 100-D interference detector

This type of spoofing indicates that people are prepared to falsify location data for personal gain and are prepared to learn how to do so. Spoofing at the GPS signal level requires a different type of technical expertise and a certain amount of specialist equipment, but is not beyond the abilities or budget of a determined hacker.

The rewards to be gained from GPS spoofing are potentially far greater than for jamming, making it an attractive proposition for those engaged in criminal activity.

At DEFCON 23 in the US in August last year, non-GPS specialists demonstrated how easy GPS spoofing was to carry out. At one of the hacker convention's less-reported sessions, Chinese security researchers Huang Lin and Yan Qing showed it's relatively straightforward to create a low-cost GPS signal emulator using cheap, off-the-shelf components and open source code. Using their home-made kit, they showed an audience of more than 600 how they were able to take control of the GPS receivers of a variety of devices, including smartphones, a drone, and a car satellite navigation system. The effects ranged from tricking the smartphones into displaying a time and date in the future, to causing a drone to drop to the ground in the belief that it had entered a 'no-fly zone', to fooling the car into thinking it was located in the middle of Namco Lake, rather than its actual position in an underground car park. In none of the attacks did the GPS receiver in the device recognise it was being attacked or emit a warning to this effect.

## Protect yourself

So what can users and manufacturers do to protect themselves and their customers? The most important single thing is to carry out a comprehensive risk assessment. This needs to determine the probability that systems or equipment will encounter one of the identified GNSS threat vectors in day-to-day operations, and understand system behaviour when exposed to a selection of threat vectors and what the impacts could be on business activities. This allows an informed decision to be taken on mitigating the risks and protecting operations.

Carrying out a thorough risk assessment requires a top level security audit as well as laboratory bench testing. The security audit consists of assessing how the system is used and identifying the threat vectors that are applicable to the system – for example, how likely is it that a well motivated hacker will target your system with fake RF signals? Is there any way that a hacker could manipulate positioning or timing data at the application layer? Are there GNSS receivers used for tracking that might be exposed to PPD jammers?

Once the threat vectors have been identified, tests of the system response to these threat vectors are conducted under

laboratory conditions. Today, it is possible to simulate a variety of GNSS jamming scenarios with real-world PPD-like interference waveforms or to simulate crude or more sophisticated varieties of spoofing attack, with key system parameters being continuously monitored. In this way any unexpected or unwanted system behaviour can be identified and characterised and the potential impact to operations assessed. This is really a vulnerability audit of the system.

Once all this information has been collected, collated and analysed, it becomes much easier for an informed decision to be made on the most cost-effective mitigation techniques, which depending on the scale of the identified problems, can range from the introduction of simple operational guidelines to the inclusion of a complementary (or back-up) system, such as eLORAN, which is a ground based 2-D fixing system. eLORAN signals are far less susceptible to interference than GNSS, given the much higher power level of the signals.

## Father says

Bradford Parkinson is widely recognised as being the father of GPS. In 1973 he became manager of the Navstar GPS development programme, and he is a key member of the US National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, which provides independent advice to the US government on GPS-related policy, planning, programme management, and funding profiles in relation to the current state of satellite navigation services. He says we must learn to 'protect, toughen and augment' GNSS to ensure that it meets users' needs. Protection is about taking pre-actions such as legislation, and re-acting when interference or spoofing occurs. Toughening is about making' equipment more resilient to GPS/GNSS threats. Augmenting is about using substitute PNT sources such as eLORAN or inertial sensors as a complement to existing GNSS.

Effective risk assessment fits in with this framework. Knowing the impact of GNSS threats on the operation of your business may give you tools that will help you lobby politicians and industry bodies for improved legislation or standards, whilst practically, this knowledge will also likely provide 'quick win' methods for improving the overall resilience of your system. It is also clear that a deep understanding of GNSS threat evolution in the real world is required to keep up to date with the development of technologies that are being used to attack PNT systems..

WE MUST LEARN TO 'PROTECT, TOUGHEN AND AUGMENT' GNSS TO ENSURE THAT IT MEETS USERS' NEEDS

***Guy Buesnel is product manager GNSS vulnerabilities at Spirent (www.spirent.com)***

A broadcast tower that uses GPS for precise timing

Container ship using GPS for navigation