

## GPS Vulnerability – Information for CIOs

### Executive Summary

The pervasiveness of business applications built on the US Global Positioning System (GPS) infrastructure means that many businesses are either explicitly or implicitly reliant on GPS for position or timing information. A disruption to GPS services could have a critical impact on your business.

It is important for you to understand the possible vulnerabilities that a dependency on GPS introduces to your infrastructure and to develop appropriate mitigation strategies.

This paper, which complements the CEO advisory paper released in March 2006, discusses potential threats to the performance of GPS:

- Solar disturbances in the earth's atmosphere
- Restricted lines of sight between GPS satellites and receivers
- Unintentional interference caused by electronic equipment
- Intentional jamming of GPS signals using radio interference
- Spoofing (imitating a GPS signal, potentially providing inaccurate data)

The paper also identifies possible countermeasures to these threats.

### Introduction

The open access provided by US authorities to precision positioning, navigation and timing signals from the Global Positioning System (GPS) satellites has fed a growing number of business applications built on this infrastructure. Many businesses now have a reliance on GPS but under-appreciate the degree to which their business operations depend, often critically, on continuity of access to the signals.

If your business requires position, navigation or timing information it is highly likely that it is critically dependent on GPS. Denial of or interference with GPS signals may be a critical point of vulnerability for your business. GPS-reliant business sectors include, but are not limited to, all modes of transportation and movement of goods, emergency services, communications, time-critical financial services (including ATM transactions), and commercial and evidential location-based services.

The pervasiveness of GPS as an information utility means that even if, at first sight, your business does not fall into this indicative list above it may nevertheless be exposed to risk should GPS services be disrupted. Your business operations may rely

**DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. The document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.**

in less apparent ways by Government systems, support, supply or customer chains that are themselves reliant on GPS.

The potential for your business to have a reliance on GPS warrants your attention and development of risk mitigation strategies.

### **Benefits of GPS-derived services**

It is not surprising that business around the world has moved to embrace GPS services as a key element of infrastructure. The reasons are manifold, and include:

- GPS signals are free, and will continue to be free, of any user charges and mass-produced consumer receivers are cheap.
- Reliability, continuity and integrity of GPS has proven extremely high.
- The accuracy of the free service is adequate for many applications.
- Where the basic positioning and navigation accuracy is inadequate, correction services exist (some are free, most are fee-for-service) or businesses may install their own differential reference stations to service a limited geographical area. Ultimate positional accuracy of a few cm is achievable.
- GPS-based timing signals are highly accurate – better than to within 1 microsecond of Universal Coordinated Time (UTC). Many businesses can make substantial economies by substituting multiple cheap GPS receivers for expensive precision clocks or timing signal distribution networks.

In the future there will be multiple systems which will be complementary to GPS. The European Union is in the process of building its Galileo service. The Russian Federation's GLONASS service will be revitalised over the next few years. Receivers offering reception of all three services will add robustness to the GPS service currently available. The multi-constellation developments (GPS combined with Galileo and GLONASS) are critical risk-mitigators for business reliance on GPS – but they are not yet a reality and may not be for about another decade.

### **Threats**

There are several issues that limit the performance of GPS.

Because the signals come from space they must travel through the upper reaches of earth's atmosphere, which can be affected by solar disturbances. Australia's latitude makes it unlikely for this to be a significant problem. Nevertheless, frequency errors sustained over periods of several hours attributable to solar disturbances have been observed in Australia at a level that may be significant for some timing-dependent businesses.

GPS normally has at least 24 active satellites in orbit and in open country enough are almost always visible. At least four are needed to obtain a position in three

dimensions; it's preferable that these are well distributed across the sky. In urban areas, open-cut mines, near or under foliage there will be restricted lines of sight to satellites. Four may not be visible and, even if they are, they may be in a restricted range of angles. Service will be compromised and you may suffer short- or long-term interruptions to operations. When Galileo comes on-line, and combined GPS/Galileo/GLONASS receivers are common, the problem of seeing at least four satellites will be eased but restricted sightlines will still limit positioning accuracy.

Indoors, GPS operation can be marginal or impossible, although more advanced systems in the future may improve the situation. It is important to have realistic expectations of GPS availability under conditions where there is not a clear view of the sky.

GPS signals can be denied or compromised by unfavourable siting; mobile reception in signal-shadowed areas may be unreliable. If access to GPS reception for your business has been carefully-designed, siting issues should have been addressed. It may be wise to review the basis for design to ensure that any assumptions as to sightlines remain valid.

The GPS signal is exceptionally weak. Each satellite transmits a signal equivalent to the power of a 25W light bulb from an distance of about 20,000 km.. Such a weak signal can be readily interfered with or denied by unintentional or deliberate radio interference.

Unintentional interference is caused by electronic equipment radiating in the GPS frequency band. Examples of such interference are television broadcast transmitters and mobile phones. Such equipment does not normally interfere with GPS but can do so if it is faulty or badly designed. It may radiate at the same frequency as the GPS signals and if this is powerful enough the GPS receiver will no longer be able to "hear" the satellite signal.

What is now emerging as a more serious threat to GPS access is the relative ease with which signals can be deliberately jammed by radio interference. The levels of interference needed to jam a typical consumer GPS receiver are quite low and jamming equipment can be small. A hand-held jammer effective over a 1 km radius can run for hours on a 9V battery so an effective attack on GPS could be mounted at low cost.

GPS jammers are readily available for purchase. Manufacture by a moderately skilled 'hacker' is straightforward and cheap, drawing on designs published on the Internet. GPS interference or jamming is not always obvious or continuous in its effect – it could have only a subtle impact on your business or it may completely shut you down. Finding and dealing with such interference could take weeks or longer.

Although illegal, to date GPS jammers have proven difficult to locate and there is no national authority in Australia charged to deal with such a threat. The Australian Communications and Media Authority (ACMA) will investigate any reported incident of GPS jamming but has no charter to ensure the continuity of your GPS-dependent business and could take some time to resolve any reported interference. Your business could be impacted for an indefinite time.

Timing applications are at particular risk because of the vulnerability of GPS to interference or jamming. The integrity and credibility of records, transactions or events “stamped” using time parameters derived from GPS is thereby decreased. This is highly relevant in a legal context unless appropriate mitigation measures and record keeping protocols are in place. These must be aimed at providing a reasonable guarantee that any periods of GPS performance degradation have been identified and the consequential timing errors bounded.

The effect of unintentional interference and intentional jamming is the same. The GPS receiver will fail to operate correctly. A more insidious form of intentional interference is ‘spoofing’. Spoofers are particularly sophisticated jammers which mimic the GPS satellite signal. The GPS receiver can be fooled into thinking that it is tracking the GPS satellites where instead it is tracking the spoofer. The spoofer can then introduce subtle errors in the position, velocity and time information within the GPS receiver. To a user, it will seem that the GPS receiver is operating normally, however it is providing inaccurate information with no warning or indication of the errors.

### **Countermeasures**

There are a number of methods to protect GPS receivers from radiofrequency attacks. These all raise the power levels required by the jammers to disrupt the receivers. However, no matter how much interference mitigation capability a GPS receiver has a powerful enough jammer can still cause it to fail. By introducing sufficient mitigation capability, you can protect the receiver to some degree from interference. If the receiver is sufficiently protected the effort required to disrupt the GPS receiver becomes either: (a) too expensive; (b) unsustainable in terms of the power required to run; or (c) easily detectable and therefore readily intercepted.

Perhaps the single most effective method is to introduce a “Controlled Reception Pattern Antenna” or CRPA. Such antennas are becoming commonplace in the military and are starting to become available to the civilian community. A CRPA has the capability of determining the direction of a jamming source and modifying its antenna reception pattern to ignore signals from that direction.

The second technique employed is called narrowband interference processing. Electronics behind the GPS antenna attempt to measure the frequency of the jamming signal and then ignore it. This technique only works well when the frequency band of

the jamming signal is much narrower than that of the GPS satellite signal. This is usually the case for unintentional interference and unsophisticated jamming. The technique does not work against jammers transmitting over a wide frequency band.

The third technique is to employ a jamming signal to thermal noise (J/N) ‘power-meter.’ By measuring the total amount of power received by the antenna, and knowing the amount of power expected from thermal noise, the receiver can measure the amount of received jamming power. In this way, the receiver can monitor the likelihood of becoming jammed and inform the user of its reliability. Although this does not eliminate the effect of the jammer, it does provide an integrity check on the reliability of the receiver.

Finally, inertial-aiding methods can be employed which aid the receiver in being able to keep track on the satellite signals under stressed conditions. With these methods the receiver is coupled with an inertial navigation system (INS) which provides extra information to allow it to maintain track on the satellites at higher jamming powers. An additional advantage of a coupled INS is that it provides an alternative navigation solution in the event of the GPS being jammed. The INS subsequently provides the receiver with continual estimates of its position which helps with the re-acquisition of the GPS signal.

Other mitigation strategies, such as physically shielding the GPS receiver’s antenna from interference sources, rely on a-priori knowledge of the location of the interference but may be useful under some circumstances. Most civilian installations of GPS antennas are probably only going to be affected by interference coming from low-elevation terrestrial sources. The installation of a “choke-ring” style of GPS antenna may provide significant mitigation against such interference sources at costs much lower than CRPA antennas.

Intentional spoofing is much harder to mitigate. Because a very high level of technical expertise is required to successfully deploy a spoofing attack and the equipment to successfully conduct an attack is relatively expensive, the risk associated with encountering such a threat is very low. Having said that, spoofing systems are easier to employ against stationary GPS receivers that access the GPS signal principally for the time component.

The largest threat to the integrity of GPS is through jamming rather than spoofing. If GPS receiver-based strategies to mitigate such interference are impractical, the only other option is to have back-up systems which come into effect in the case of a GPS failure. In the case where GPS is used for timing applications, a solution might be to employ a local oscillator. System design must ensure that it could determine when GPS was not working and then switch to the local oscillator for timing information until GPS is restored. Questions to consider here include:

- Has your system been designed to recognise when GPS is not working properly, *especially when the receiver may not be working due to electromagnetic interference* rather than because of a power failure or hardware fault?
- Does your system *switch over* to the backup system seamlessly?
- What loss of accuracy or precision is your overall system suffering from when using the backup system?
- Does your system *switch back* to GPS seamlessly when the GPS service has been restored?

### Strategies you may wish to implement

It is important that:

- you consider the type and level of dependence of your business processes on GPS;
- you complete a risk assessment that considers the impact of denial of or interference with GPS services, and the impact of such denial/interference on third parties critical to your business;
- you assess the tradeoffs in terms of the assessed risk, cost to the business of GPS interruption/denial, and costs of mitigation strategies;
- you consider having systems in place to monitor GPS signal reception and integrity, and to report on such events. It is quite possible that your system may not ‘recognise’ loss or compromise of GPS and you may find your business is relying on fall-back systems of unknown reliability without this fact being reported;
- you consider having in place strategies to mitigate the effects of failure to receive GPS, or jamming of GPS signals;
- you include plans for operation, possibly with an acceptable level of degradation, in the event of loss or degradation of GPS services;
- if your business has a critical dependence on GPS consider installing alternative or backup systems; and
- acknowledging that authorities currently have limited capacity to locate and shut down GPS jamming sources, you consider options for securing such services commercially if the assessed impact on your operations warrants it.

### Conclusion

Because of the pervasiveness of GPS it is timely to examine the reliance your company may have on this technology. The threat climate is perceived to be increasing. Until a more robust GPS infrastructure based on multiple satellite systems is a reality, it may be prudent to assess your own vulnerability in terms of the disruption to service (and associated costs) caused by loss of GPS. Mitigation procedures, such as those discussed above, may be a cost-effective strategy for your company in the light of the potential threats.

### For Further Information

This advisory has been prepared by the Australian Global Navigation Satellite Systems Coordination Committee (AGCC) in conjunction with the IT Security Expert Advisory Group<sup>1</sup>. The first port of call for additional information is Director Space, Missile Defence, and ISR, Department of Defence. Enquiries should be sent to [strategy.space@defence.gov.au](mailto:strategy.space@defence.gov.au).

### Other useful references

“Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System”, Final Report, Prepared by *John A. Volpe National Transportation Systems Centre* for *Office of the Assistant Secretary for Transportation Policy, US Department of Transportation*. August 29, 2001. Can be downloaded from <http://www.navcen.uscg.gov/gps/geninfo>

“GPS Receiver RF Interference Monitoring, Mitigation, and Analysis Techniques”, Philip W. Ward, **Navigation: Journal of The Institute of Navigation**, Vol.41, No.4, 1994-1995, pp.367-391.

“Understanding GPS, Principles and Applications”, Elliott D. Kaplan and Christopher J. Hegarty (Editors), Artech House, 2006 (2<sup>nd</sup> Edition).

---

<sup>1</sup> The IT Security Expert Advisory group (ITSEAG) is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN) which enables the owners and operators of critical infrastructure to share information on important issues. The ITSEAG provides advice on IT issues as they relate to critical infrastructure protection. It is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. More information on TISN can be sought from <http://www.tisn.gov.au>. The ITSEAG Secretariat can be contacted on (02) 6271 1656.