Trends in Information Security

Topic Description:
Infrastructure Vulnerabilities & Global Navigation Satellite Systems

Prof. Chris Johnson,
School of Computing, University of Glasgow.
Johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk

Introduction

Global Navigation Satellite Systems (GNSS) play an increasingly important role within national critical infrastructures. Implementations such as the US Global Positioning System or the Russian GLONASS constellation not only provide positioning data, they also enable the précising timing that is essential across many industries – for example in the synchronisation of electricity and gas distribution networks. Unfortunately, these first generation systems are too inaccurate to be used for many safety-critical applications. Multipath effects introduce delays when satellite signals bounce off buildings and other fixed obstacles before they reach a receiver. Similarly, ionospheric effects of solar radiation can influence the signals. In consequence, Europe has developed the EGNOS system and the US have developed WAAS – these are augmentation systems that correct many of the errors inherent in GPS signals and have for the first time been approved for safety rated applications including some forms of aircraft approach. However, these augmentation systems still rely on GPS signals that can be spoofed or jammed with relative ease.

Different Perspectives

Most government agencies recognise our growing dependency on GNSS. They also acknowledge the vulnerability of these infrastructures. However, there is little agreement about the appropriate course of action to take to increase the security of these systems:

- Reliability of the infrastructures? Some have argued that we can increase the security of these systems by introducing more rigorous forms of encryption and error checking into the underlying infrastructures, eg through the introduction of Galileo rather than GPS> Others have argued that these changes only address some of the integrity and availability concerns that arise from GNSS;
- Marketplace or government? Many companies are focused on the cost savings and additional functionality provided by GNSS – for instance in tracking the movement of goods between warehouse and supermarket. They often assume that the service is secure and reliable. There is also often an assumption that governments are responsible for insuring the integrity of these infrastructures. Equally government agencies, often assume that companies should take sufficient measures to ensure that they can continue to function following any interruption to GNSS.
- What is the nature of the threat? It is relatively cheap and easy to construct localised jamming devices. However, in most cases these transmitters can be detected and stopped

so any interruption will usually be short term. Some have argued that this is a complacent view, ignoring the threat from airborne jammers etc.

- Physical threats to satellites and other infrastructures? As mentioned previously, GNSS rely on satellite infrastructures that are vulnerable to physical damage for instance from orbital debris that could be created by the deliberate collision of two or more satellites. It is unclear how to assess the nature of this threat.
- Attacks on ground station controlled over networks and in some cases the public Internet? Other forms of attack focus less on physical threats but on the cybersecurity of communications infrastructures – for instance satellite uplinks and the ground stations used by augmentation systems. Some of these are accessible for configuration over the public Internet.

Open Research Questions

A number of research questions remain open in this area – a partial list includes the following:

- How can we accurately assess the reliability, integrity, continuity and availability of the existing infrastructures to know if they will be secure enough to support safety-critical systems?
- Assuming that we cannot provide 100% security, what technical measures should we adopt to protect end users? Hint: Work in this area considered techniques such as Receiver Autonomous Integrity Monitoring (RAIMS).
- What techniques can an individual company use to assess its vulnerability to any security threat against GNSS infrastructures?
- What is the best way for government to alert companies and coordinate action to mitigate the risks from GNSS attacks?

References

U.I. Bhatti and W.Y. Ochieng, Failure Modes And Models For Integrated GPS/INS Systems. The Journal of Navigation, 60(2):327–348, 2007.

A. Grant, P. Williams, N. Ward and S. Basker, GPS Jamming and the Impact on Maritime Navigation. The Journal of Navigation, 62(2): 173-187, 2009.

C.W. Johnson and A. Atencia Yepez, Safety Cases for Global Navigation Satellite Systems' Safety of Life (SoL) Applications. In H. Lacoste-Francis (ed.), Proceedings of the Fourth International Association for the Advancement of Space Safety, Huntsville Alabama, NASA/ESA, Available from ESA Communications, ESTEC, Noordwijk, The Netherlands, ISBN 978-92-9221-244-5, ESA Technical report SP-680, 2010.

RAE, Global Navigation Space Systems (GNSS): Reliance and Vulnerabilities, Royal Academy of Engineering, London, UK, 2011. Available as of 19/3/2011 on: http://www.raeng.org.uk/news/publications/list/reports/RAoE_Global_Navigation_Systems_Report.pdf