Montage: © Gangis Khan / Shutterstock. GPS satellite images: United States Government

Secure GNSS for all?

Nigel Davies argues that, as society becomes increasingly reliant on the security and continuity of GNSS, cloud computing can provide an additional way of bringing secure satellite navigation services to wider society

We know that the growth of a 'connected economy' has made our world more vulnerable to cyber-attack and transformed hacking into an attractive enterprise for criminals and state actors. Yet few realise that the same is also true of our growing reliance on remote navigational satellites as our real-time map and clock in the sky, continuously guiding vital decisions by humans and machines.

The signals they send have become essential to everything: from the pinpoint-accurate targeting of weapons systems to difficult precision-navigation manoeuvres; the smooth and seamless operation of transport networks, and the arrival of emergency services at the right time and place. And the growing reliance of millions of people and systems on increasingly ubiquitous GNSS (Global Navigation Satellite Systems) signals has transformed these constellations into major points of failure across much of the world.

A matter of national security

The Royal Academy of Engineering estimates that as much as 6-7% of global GDP is now dependent on satellite radio navigation. According to the Defence iQ Military Satellites: UK Space Capability Development report[1], 90% of military equipment platforms and systems also now depend on space signals, making the continuity, security and integrity of Position, Navigation and Timing (PNT) data "a matter of national security ".[2]

And the integrity of GNSS data also underpins the integrity of many of the key institutions of society. It guarantees the accuracy of the time-stamps[3] on billions of electronic trades that give us the causal sequence of events behind global market movements. Even the integrity of a court case, where GNSS data is used as evidence, can be called into question.[4]

This renders our economy and society highly vulnerable to the slightest interruption of GNSS signals or even worse, any attempt to manipulate them through false broadcasts masquerading as real GNSS data. And the threat of such disruption and manipulation is growing, with GNSS data facing increasingly multi-faceted threats from many directions.

The SENTINEL Project - a nationwide Government-backed UK investigation of GPS/GNSS signal jamming - has noted that even handheld electronic jammers, available to ordinary consumers, have dramatically increased in range and power in recent years.[5] It is claimed that for roughly ten minutes every day the London Stock Exchange experiences problems with the signals it receives from GPS satellites due to such inadvertent jamming.[6]

Cyber threat

As some satellite receivers are 'connected' to the Internet, the danger of ordinary hackers successfully compromising satellite receivers or using malware to send them false information is also increasing.[7] A recent paper warned that the openness of underlying GNSS standards, combined with the growth of software-defined radio technologies and the increasing availability of software tools, is making them increasingly vulnerable to cyber-attack.[8]

Because the specification for the commonly-used GNSS services is 'Open Source', it is also quite easy for an attacker to emulate or "spoof" the signals sent by GNSS satellites. Proof-of-concept

sentinel

chronos TECHNOLOGY

SENTINEL PROJECT

REPORT ON GNSS VULNERABILITIES

SENTINEL Project – GNSS Vulnerabilities

The SENTINEL Project investigated a number of interconnected activities involving mission-critical or safety-critical services which need to be able to "trust" GNSS signals at the point of use. The SENTINEL Project was concerned with GNSS interference and jamming, and techniques for mitigating such jamming. This Report also records some of the world-wide press and television coverage stimulated by presentations of the results of SENTINEL at numerous conferences and symposia.

The Government-backed SENTINEL Project addressed GNSS interference and jamming, and techniques for mitigating such jamming.

'spoofing devices' - which send out false position and location data camouflaged as genuine GNSS broadcasts - have begun to emerge, posing a threat to the integrity of the data on which society increasingly depends. As reprogrammable software-defined radio technologies drive down the cost of sophisticated spoofing systems, it will only become cheaper and easier to make electronic devices that 'spoof' genuine GNSS signals.

Meanwhile, a Chatham House research paper entitled "Space: The Final Frontier for Cyber Security" recently warned of the danger of cyber-attacks targeting the satellite constellations that provide GNSS, by tampering with control systems, mission packages or satellite control centres.[9]

Secure GNSS for all

Satellite navigation was first designed for military use so it is no surprise that the defence sector has been alive to these threats for some time. Military users in the US employ a separate encrypted GPS service, PPS, with heavily beefed-up security and jam resistance. Europe's Galileo satellite constellation similarly includes a Public Regulated Service (PRS), a robust and spoofing-resistant signal, heavily encrypted against cyber attacks and designed for government-authorised users.[10]

Last year's ground-breaking trial, involving Ordnance Survey, NSL and QinetiQ, successfully demonstrated three different "user scenarios" (that involving a UAV is pictured above) in which a GNSS receiver captured signals from both Galileo open access and PRS signals, as well as open GPS signals. These signals were sent, via cellular 3G links, into the 'cloud' to be processed. Position and time was calculated from the open-access signals by servers at the NSL site in Nottingham. The secure PRS signals were decrypted and authenticated by a QinetiQ site in Malvern that was hosting the cryptographic keys. This confirmed the position and timing reported by the open-access signals. Further trials are planned over the next 12 months that will bring end users into the project.

The problem is that these threats are no longer confined to the military as the ubiquity of GPS means that vital civilian services and the millions of employees providing them, from coastguards to fire brigades, now depend on highly secure, continuous satellite navigation. Yet the technology needed to access these robust signals can be too complex and expensive for many services that need it.

For example, PRS users need to be able to load, store, process, and destroy classified cryptographic keys, at a cost and complexity that is far beyond the reach of many ambulance services, humanitarian aid agencies and individual employees in the field.[11] This means that while secure satellite services such as PRS will in theory be available to government-authorised users, in practice the technology is prohibitively complex and expensive for all but major critical infrastructure operators and defence users.

Secure GNSS as a service?

The hunt is on for ways to open up military-grade satellite navigation to millions of ordinary government-authorised users, from aid workers to police officers with smartphones. And the answer may be coming from the cloud computing revolution.

We all know that cloud computing innovations such as 'infrastructure-as-a-service', which enables IT infrastructure to be stored in secure datacentres and accessed remotely, have enabled millions of SMEs and entrepreneurs to dramatically reduce the cost of storing their hardware on-site. What if the same could be done for secure satellite navigation?

May 2016 marked the first ever real-life demonstration that cloud computing could be used to give access to the Galileo PRS signal. In a ground-breaking trial involving the Ordnance Survey, Nottingham Scientific Ltd (NSL) and QinetiQ, a drone and a smartphone user were both independently able to get PRS-assured verification through the cloud of their locations in real-time by using internet access to remotely decrypt and authenticate the PRS signal in the cloud.[12]

Again in 2016, NSL and QinetiQ received a European space innovation award for pioneering work developing a 'sleeve' which could allow standard mobile phones to access PRS via the cloud, potentially bringing military-grade navigation to millions of workers 'in the field'.[13] The technology enables PRS to be accessed 'as a service' through GRIPPA - a small module that attaches to a mobile phone as a sleeve to give users PRS-assured location data.[14]

Enormous implications

The implications of these advances are enormous. They could bring the security, robustness and resilience of military-grade satellite navigation to emergency services, humanitarian aid agencies, coastguards and security forces across Europe, protecting critical functions from attack.

It would mean that secure satellite navigation would become available in the form of a pay-as-you-go or subscription-based on-demand service, just like cloud-based data and software.

Crucially, this will give people confidence in the integrity of data used to authenticate everything from financial trading to criminal trials, giving a stamp of 'quality assurance' to secure GNSS location data which will, in the future, be easily decrypted over the internet.

If we are to protect the vast web of interconnected services that now depend on GNSS, we must harness the cloud computing revolution to make quality-assured satellite navigation available 'as a service' across society.

References

1. http://www.raf.mod.uk/rafcms/mediafiles/CB2D1425_5056_A318_A805263A046FC8ED.pdf
2. http://www.raeng.org.uk/publications/reports/global-navigation-space-systems
3. http://www.insidegnss.com/node/4355
4. http://www.professordavidlast.co.uk/CISO.pdf
5. http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf
6. http://www.economist.com/news/international/21582288-satellite-positioning-data-are-vitalbut-signal-surprisingly-easy-disrupt-out
7. https://www.virusbulletin.com/blog/2016/september/turns-out-gps-technology-more-vulnerable-cyberattack-ever-security-expert-demonstrates/
8. https://www.virusbulletin.com/conference/vb2016/abstracts/gps-attacks-shoe-string-methods-analysis-and-countermeasures/
9. https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis-embargoed.pdf
10. https://www.gsa.europa.eu/security/prs
11.. http://www.esnc.info/index.php?anzeige=prs16.html
12. https://www.ordnancesurvey.co.uk/about/news/2016/galileo-prs-signal-accessed-via-cloud.html
13. https://www.gov.uk/government/news/uk-wins-european-space-innovation-competitions
14. http://www.esnc.info/index.php?anzeige=prs16.html

Nigel Davies is head of the Secured Navigation Group of QinetiQ, one of the UK's largest research and technology organisations (https://www.qinetiq.com)