Test Scenario Pack for GNSS Vulnerabilities and Threats

Problem

Threats to GPS and multi-GNSS systems are increasing and becoming more sophisticated. At the same time, GPS and other GNSS systems are being relied upon more for safety-related and commercially sensitive applications, such as autonomy and time synchronization.

This scenario pack will be of interest to you in the following cases:

- You have your own Spirent simulation systems and you want to perform your own testing against the latest baseline
- You understand the threat and vulnerability landscape is evolving but you do not wish to commit your own resources to staying abreast of the latest developments
- You recognise the complexity in assessing and re-creating some of the more complex threats and vulnerabilities, for example atmospheric, spoofing and some system errors

Spirent maintains a suite of test scenarios with the latest commercial GPS/ GNSS vulnerabilities and threats – including interference, spoofing, multipath, system events and atmospheric scintillation and solar weather.

The test scenarios are available in a test scenario pack. A purchase of this test pack provides access to new test scenarios for 12 months. After this period a subscription to enable ongoing access to new threats should be purchased.

It is important the test scenarios are kept up to date with new threats and vulnerabilities, in line with the continuing evolution that is being seen in the real-world. Spirent has developed a network of detection probes for GNSS interference and also has dedicated resources to scan for and evaluate new threats and vulnerabilities. These are then recreated using Spirent's test expertise and systems to enable laboratory testing of resynthesised threats and vulnerabilities. In addition to its own expertise, Spirent has developed partnerships with leaders in the field of GNSS interference, spoofing and atmospheric effects.

Service Description

This service offers access to the latest set of test scenarios from Spirent's library of system vulnerabilities and threats.

The threat and vulnerability types available with the scenario pack include:

- Interference
- Spoofing
- Atmospheric scintillation and space weather
- GNSS system outages and events
- Multipath environments
- Challenging situations for receivers, such as transitions around the equator, meridian and poles.

In order to regenerate the full range of threats and vulnerabilities, appropriate simulation hardware and software is required. Please refer to the table 1 in document MS 3096, Datasheet Specification for Test Scenario Pack for GNSS Vulnerabilities and Threats, for full details.

In addition to the test scenario pack, a custom scenario generation service is available for specific threats of vulnerabilities. This service is available separately and quoted on a case-by-case basis.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

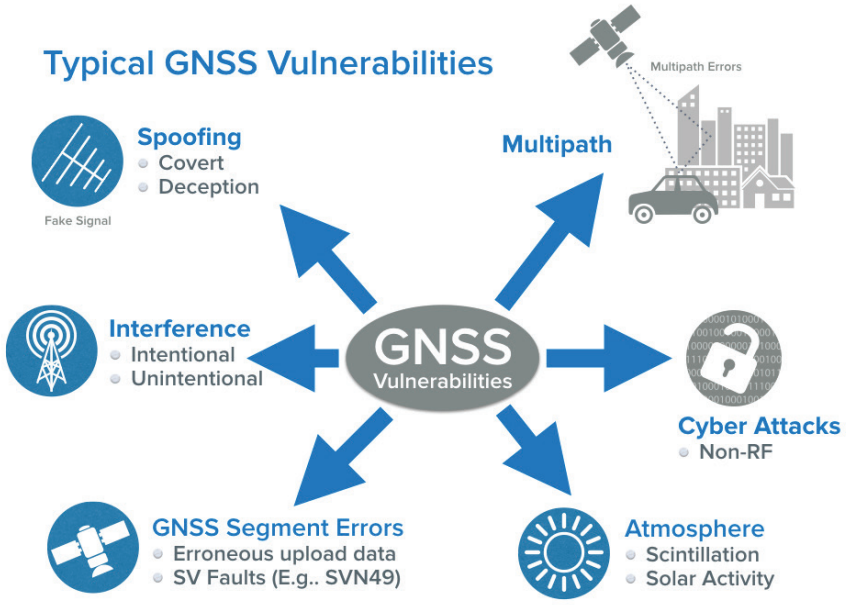

Figure 4 Range of vulnerabilities represented in the subscription-based cyber threat and intelligence library

Benefits and Value

- The test scenario pack provides access to the latest threats and vulnerabilities
- Always test using the latest baseline
- Regular updates as new threats and vulnerabilities are identified by Spirent
- No need to maintain your own independent assessment of the evolving threat and vulnerability landscape

AMERICAS 1-800-SPIRENT
+1-800-774-7368
sales@spirent.com

US Government & Defense
info@spirentfederal.com
spirentfederal.com

EUROPE AND THE MIDDLE EAST
+44 (0) 1293 767979
emeainfo@spirent.com

ASIA AND THE PACIFIC
+86-10-8518-2539
salesasia@spirent.com

spirent™ Promise. Assured.

MCD00230 | Issue 1-00 | Rev B | 12/18