Location Assurance and Privacy in GNSS Navigation

by Xihui Chen, Carlo Harpes, Gabriele Lenzini, Sjouke Mauw and Jun Pang

The growing popularity of location-based services such as GNSS (Global Navigation Satellite System) navigation requires confidence in the reliability of the calculated locations. The exploration of a user's location also gives rise to severe privacy concerns. Within an ESA (European Space Agency) funded project, we have developed a service that not only verifies the correctness of users' locations but also enables users to control the accuracy of their revealed locations.

Driving across unknown routes used to be stressful owing to the almost inevitable problem of getting lost. Thanks to Global Navigation Satellite Systems (GNSS) navigation devices, such problems are now in the past. These devices have revolutionized how we move: they guide us not only in unknown places but also within our own neighbourhoods. Our growing dependence on them to find our way is risky though: since the airwaves that carry GNSS signals are broadcast in the open air with a relatively weak strength, they are vulnerable to spoofing and meaconing attacks.

Spoofing interferes with GNSS signals and misleads a driver into calculating a different location. Instead of interfering, a meaconing attack intercepts, alters or delays GNSS signals.

Launching these attacks is illegal, but devices required for their implementation are easy for anyone to access. Although this may not bother many of us, for those who run businesses that depend on correct routing (transport of valuable goods), spoofing and meaconing represent serious threats.

To address these threats, researchers from the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg and engineers from 'itrust consulting' Luxembourg teamed up to execute a project funded by the European Space Agency (from 12/2010 to 11/2012). They designed and implemented a service that assesses the trustworthiness of a GNSS device's claim of being at a certain location [1]. The service, Localization Assurance Service Provider (LASP), runs on a trusted third party between location-based service providers and their users. The architecture where LASP runs is shown in Figure 1: all communications, except for those between GNSS and User Devices, rely on the Internet or the data mobile network infrastructure and they are supposed to be secure.

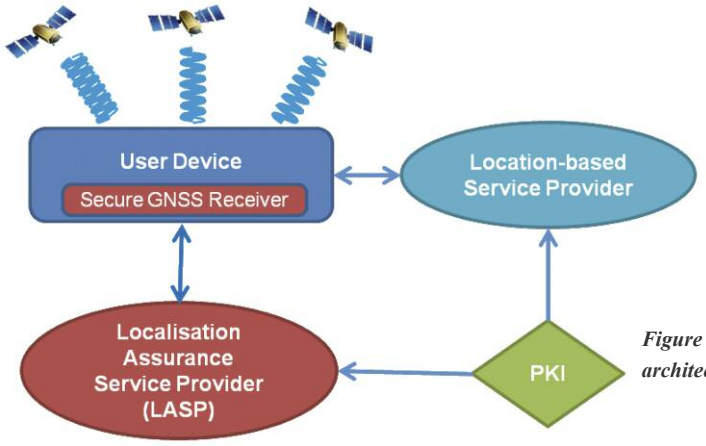

Figure 1: LASP service architecture

The LASP enacts a system of security checks, each check monitoring signal properties – such as signal strength, Doppler ratio, and clock bias [2] – that a GNSS navigation device has measured during localization. The outcomes of different security checks are intelligently processed based on a trust framework implemented with probabilistic conditional reasoning and subjective logic [3]. The results are then combined to obtain a value expressing to what extent a given localization can be trusted. This value, called localization assurance level, is embedded in a certificate issued by the LASP together with the putative user location. High assurance levels are given to localizations derived from untampered GNSS signals while low assurance levels to localizations that have been found to have inconsistencies likely due to spoofing.

In addition to the localization assurance, SnT researchers have studied solutions to protect location privacy. Thanks to a technique called selective blinding, users can control the accuracy of the location that is contained in a LASP certificate without invalidating the certificate. Location-based service providers can thus receive certified localizations that adhere to the need-to-know principle [4].

References:

[1] C. Harpes et al: "Implementation and validation of a localisation assurance service provider", in proc. IEEE NAVITEC'12, Noordwijk, The Netherlands, 2012

[2] D. Marnach et al: "Detecting Meaconing Attacks by analysing the Clock Bias of GNSS Receivers", Artificial Satellites, Journal of Planetary Geodesy 48(2), pp. 63-84, 2013

[3] X. Chen et al: "A trust framework for evaluating GNSS signal integrity", in proc. IEEE CSF'13, New Orleans, USA, 2013

[4] G. Lenzini, S. Mauw, J. Pang: "Selective location blinding using hash chains", in proc. SPW'11, Cambridge, UK, 2011

Please contact:

Carlo Harpes
itrust consulting, Luxembourg
E-mail: Carlo.Harpes@itrust.lu

Xihui Chen, Gabriele Lenzini, Sjouke Mauw, and Jun Pang
University of Luxembourg
E-mail: {Xihui.Chen, Gabriele.Lenzini, Sjouke.Mauw, Jun.Pang}@uni.lu