Galileo OSNMA for smartphones

Fourth annual GNSS Raw Measurements Taskforce Workshop

Carlo Sarto
On-line, Prague, 27 May 2020

Qascom

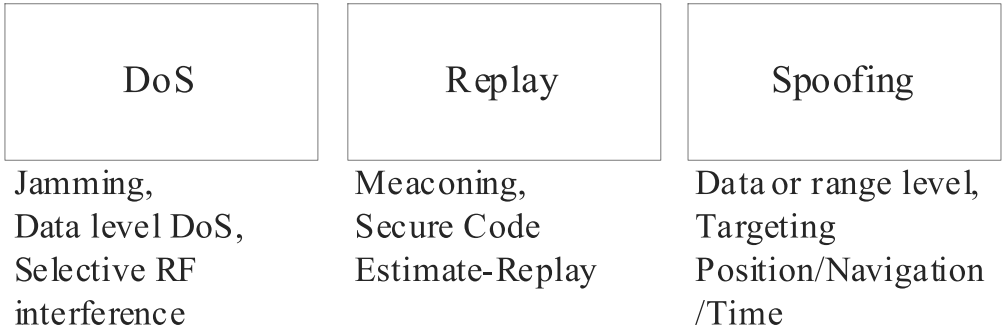
- Qascom is an Aerospace and Defence company based in North Italy

- The Advanced Navigation Systems division studies new attacks and robust PNT and GNSS authentication strategies targeting different applications, from space to mass-market.
  - At receiver level: interference & spoofing detection and mitigation
  - At system level: new signals or payloads (contributing to the definition of Galileo signals and services, including OSNMA)

GNSS threats for smartphones

- MIJI (Meaconing, Intrusion, Jamming, and Interference)
  - Degrade, disrupt, obstruct or limit the effective navigation performance
  - Performed by outsider or untrusted users targeting a trusted/untrusted device
  - Intentional or unintentional
  - At different level (e.g. radio frequency, navigation, application, HW&SW tampering)

- Main GNSS attacks



INTRODUCTION

GNSS threats in the real World

POKEMON GO HACK! Pokemon GO GPS Spoofing With Joystick & Teleport...

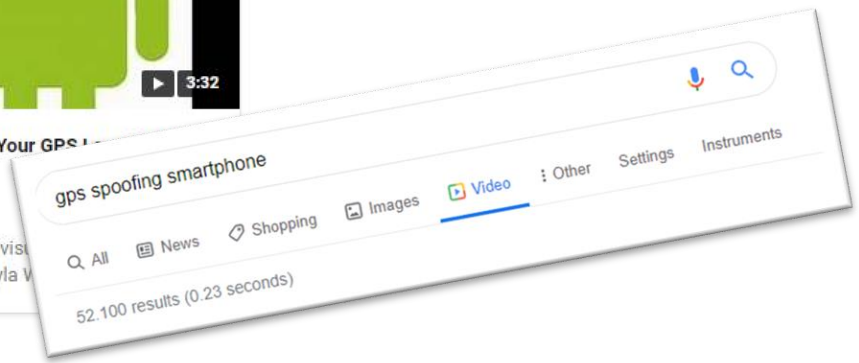
14 migliaia di visualizzazioni · 2 mesi ...
YouTube › princeumar20.09

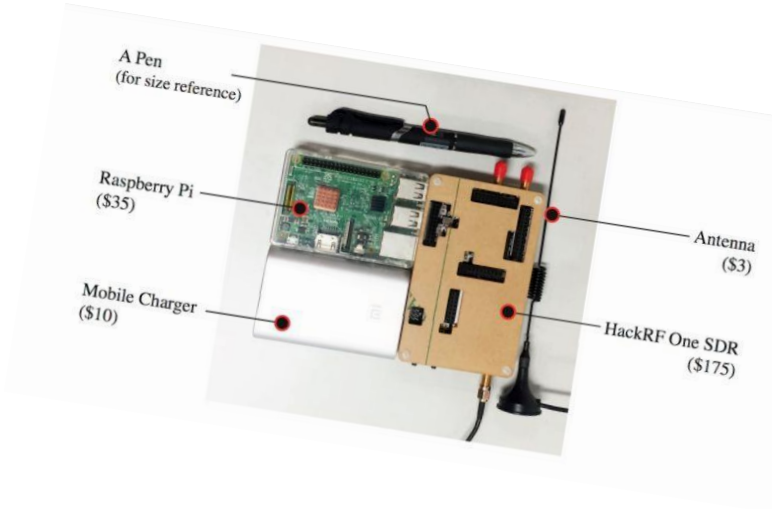
GPS Spoofing With The HackRF On Windows

24 migliaia di visualizzazioni · 4 mesi ...
YouTube › Tech Minds

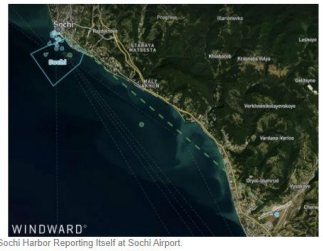
How To Fake Your GPS L... Android!!

33 migliaia di vis...
YouTube › Cayla W...





GPS Spoofing Patterns Discovered



Vessel at Sochi Harbor Reporting Itself at Sochi Airport.
BY THE MARITIME EXECUTIVE 09-27-2017 02:30:06

Examination of global ship tracking data for the last two years has shown several instances of multiple vessels reporting their locations as being on land at airports far from where the ships were operating off shore.

"We first became interested in this problem in June when a vessel master in the Black Sea reported his GPS showing him to be at the Gelendzhik airport, about 25 miles from his real location," said Dana A. Goward, President of the non-profit Resilient Navigation and Timing Foundation. "He provided photographs of equipment and other information that convinced experts his GPS receiver was

GNSS threats

- Risk (R) is normally derived by the likelihood that an event will occur (L) multiplied by the impact that would create I. Likelihood of occurrence (L) is obtained multiplying the probability that an attacker will start the event (also known as Likelihood of initiation, L_i) with the probability that it will succeed, given that it started the attack (Likelihood of success, L_s).

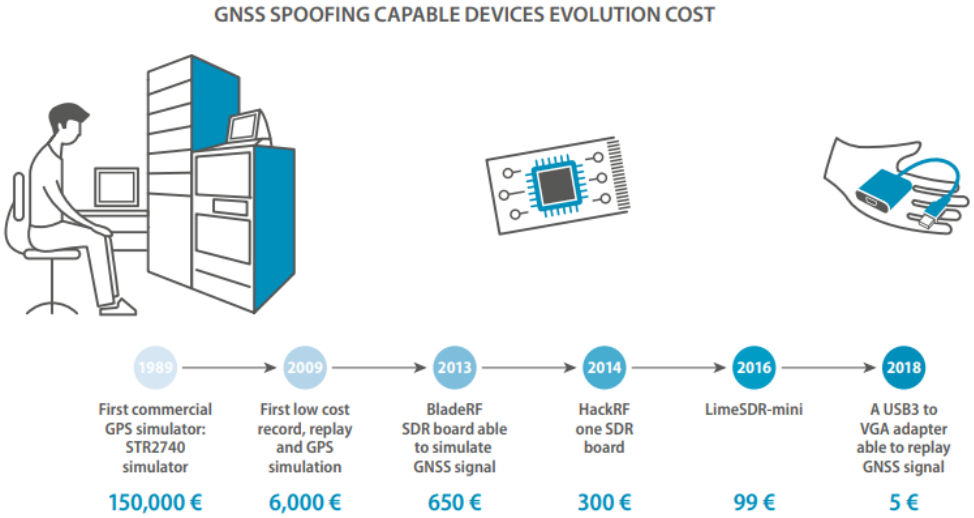
$$
\begin{aligned}
R &= L \cdot I \\
R &= L_i \cdot L_s \cdot I \\
R &= P\left(attack_{initiated}\right) \cdot P\left(attack_{successful} \mid attack_{initiated}\right) \cdot I \\
R &= P\left(attack_{initiated} \cap attack_{successful}\right) \cdot I
\end{aligned}
\qquad (1\text{-}1)
$$

- L_s generally increases if the attacker is the owner of the device
- L_s can be considerably decreased with NMA (almost removed for simplistic attacks with high L_i and low L_s)

- Countermeasures and barriers shall be defined considering the target specific application

Navigation threats

- Likelihood (L_i) of Meaconing and Simple Spoofing events is rapidly increasing.
  - Spoofing: based on RF simulation and broadcasting or use of applications the falsify the position. Navigation messages are generally auto-generated.
  - Replay: record (even of real GNSS signal) and playback.
  - Simple spoofing and meaconing can be achieved with <1K EUR (or 5-10 EUR by reducing signal quality) with L_i depending if the attacker is the owner of the device.
  - Being successful as an outsider attacker, using a 5 EUR, is not so easy. In general, only simplistic attack are cheaper.



GSA, GNSS User Technology Report (Issue 2, 2018)

What comes next …

- OSNMA will be available soon and it will be a game changer
- Free for all users, available on single frequency, not requiring specific GNSS hardware changes
- Giving the opportunity to fill the gap an develop cost-effective solutions

- OSNMA scheme is based on the transmission of crypto material providing time-constrained authentication of the navigation messages.

1. OSNMA data is transmitted every 2 seconds and it includes bits (generated with crypto functions) changing in an unpredictable way
   - Once received they can be verified but they cannot be easily guessed before they are transmitted (this makes spoofing very unpractical)
   - The transmission of false data leads to authentication errors
   - Several unsuccessful authentication events identify an attack
2. It requires loosely synchronized trusted time reference
   - Use of a trusted time ref. is one of the simpler ways to detect meaconing
   - Meaconing with several seconds delay can be recognized

Summary

- OSNMA targets the protection of the navigation data
- But it also allows to detect some spoofing attacks
- Time reference allows to detect some meaconing attacks
- As a result, although navigation is available from external sources, OSNMA can be used to increase resilience against GNSS attacks.

- OSNMA is well-suited to be complemented by additional integrity checks based on raw measurements (time jumps, pseudoranges, RAIM, C/N0)
- Other integrity checks specific to the application should also be considered (information from cellular network, use of mock location providers)

- OSNMA
- RAW MEAS AND TIME CHECKS
- CHECKS AT APPLICATION / OS LEVEL
- CHECK MOCK LOCATION

Summary

- The complexity of an attack considers the quality of the simulated signal and data, including time synchronization accuracy (which for advanced attack might be at tens-hundred nanoseconds level), capability of changing navigation messages, capability of compensate for relative dynamics, etc…
- The following tables also considers intentional events assuming the smartphone is under attack.

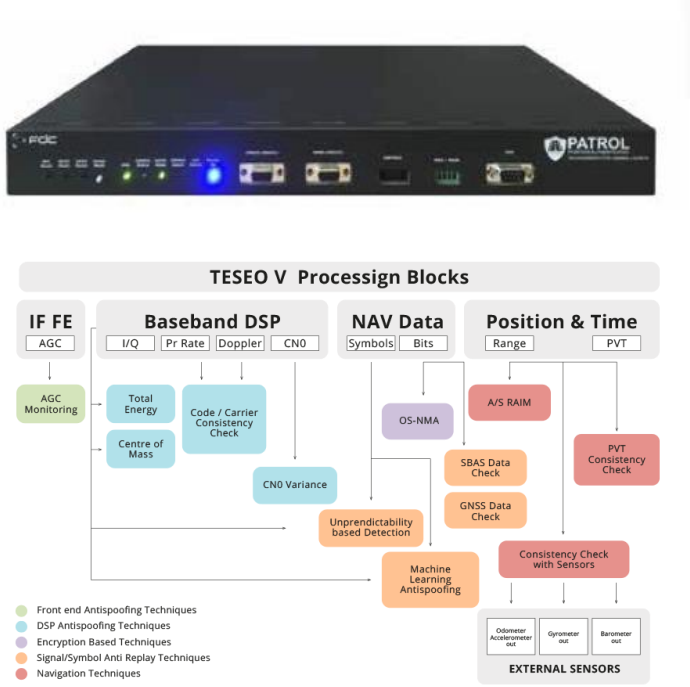
P. Initiated \ P. Success	Very Unlikely	Unlikely	Possible	Likely	Almost Certain
Almost certain					
Likely				Meaconing	
Possible				Simplistic Spoofing	
Unlikely				Data level spoofing,	Advanced meaconing
Very Unlikely					Advanced spoofing

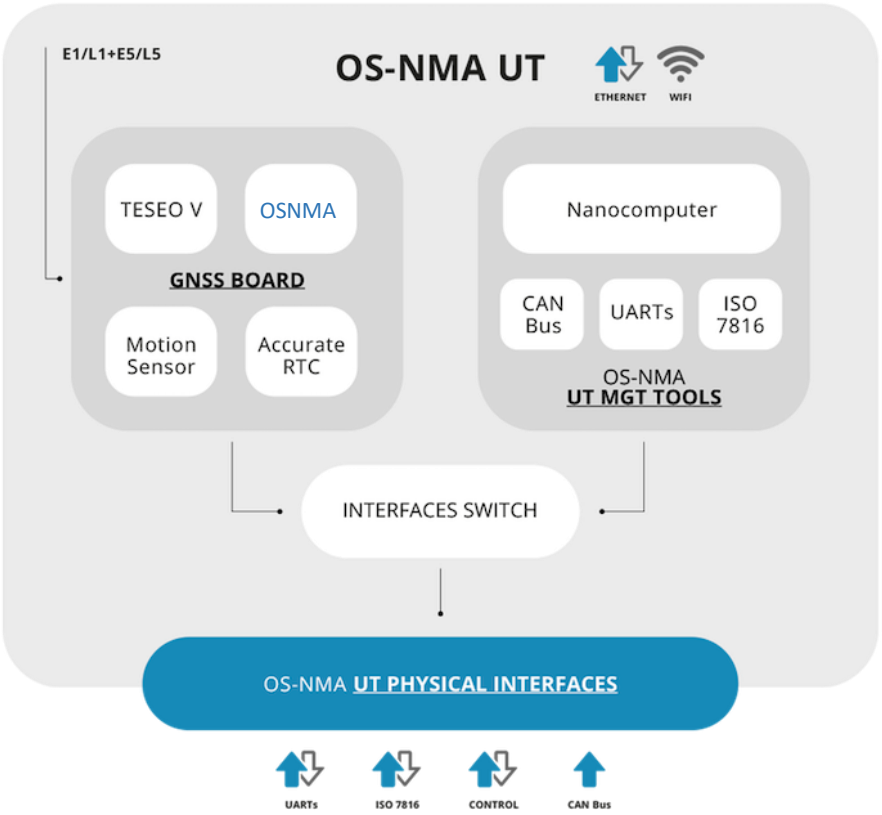
- OSNMA and the previously identified countermeasures considerably decrease the risk

P. Initiated \ P. Success	Very Unlikely	Unlikely	Possible	Likely	Almost Certain
Almost certain					
Likely	Meaconing				
Possible		Simplistic Spoofing			
Unlikely	Data level spoofing, Advanced meaconing				
Very Unlikely		Advanced spoofing,			

Detection and mitigation

- PATROL[1] project implementing OSNMA in a mass-market (automotive) receiver
  - In conjunction with state-of-the-art spoofing detection and mitigation techniques





1) https://www.patrol-osnma.eu/, https://www.gsa.europa.eu/newsroom/news/new-generation-os-nma-user-terminals

Countermeasures

- Specific features for smartphone were developed already in 2013 – STON[2] project (security technologies based on location)

Implementing signal authenticity based on **observables statistics**, checks for use of **simulated location provider** and remotely updated **app black list** of location spoofing applications. Compatible with 2020 smartphones, implementing **secure location based access control**.

2) https://www.gsa.europa.eu/security-technologies-based-location

Smartphones

- Smartphones are a good candidate platform for OSNMA
  - They can obtain time reference from a variety of sources
  - They are connected and can obtain OSNMA data to speed up the start-up and decrease the computational complexity
  - Other location/positioning sources are available
- Smartphones have power constraints
  - Need for ad-hoc OSNMA receiver implementation
- While connected, a continuous navigation messages stream is not necessarily needed
  - The cryptographic material transmitted over OSNMA can be used to implement a variety of strategies not requiring a continuous stream
  - On demand request (e.g. 2-4 seconds of data) would be sufficient for a snapshot OSNMA processing
  - OSNMA checks requested just before a critical task (time/date adjustment, payment, etc.)

WAY-FORWARD

- Ongoing implementation of OSNMA SDK for Android
- Ideally, the security of some functions would benefit if implemented at operating system level.
  - Collaboration with Google on how to best leverage OSNMA at OS level
  - Evaluate needs of available raw measurements SDK to cope with OSNMA development/experimentation

Thank you!

Carlo Sarto
carlo.sarto@qascom.it