Multi-Layer Satellite Navigation Security: Signal in Space Authentication and Receiver Interfaces Hardening

A Data Management Plan created using DMPonline.be

Creator: Aleix Galan

Affiliation: KU Leuven (KUL)

Funder: Fonds voor Wetenschappelijk Onderzoek - Research Foundation Flanders (FWO)

Template: FWO DMP (Flemish Standard DMP)

Principal Investigator: Aleix Galan

Data Manager: Aleix Galan

Grant number / URL: 1SH9424N

ID: 204120

Start date: 01-11-2023

End date: 01-11-2027

Project abstract:

Global Navigation Satellite System (GNSS) are the cornerstone of several modern systems: from smartphones to autonomous cars to low Earth orbit satellites; providing precise positioning and timing. However, GNSS is only useful as long as it is reliable and secure. One source of unreliability is spoofing, when a forged signal is transmitted to induce on affected receivers an arbitrary position and time. Multiple authentication protocols, such as the novel watermark techniques, are being embedded into the GNSS signal structure to protect against spoofing. Yet, when deployed in real scenarios, they require certain trade-offs from the already resource-constrained GNSS receivers. Additionally, signal vulnerabilities are only one side of the story as GNSS modules have multiple connections and interfaces. There is no need to counterfeit a radiofrequency signal if the receiver can be controlled through its connections. These connections have been overlooked even if they are used by many positioning protocols. Therefore, this research aims to evaluate the security of GNSS from the plane of the space signal and the receiver module. We will analyse, secure and benchmark multiple designs of state-of-the-art signal authentication protocols under common receiver constraints, propose solutions to mitigate spoofing attacks, and characterize the interface security of GNSS receivers.

Last modified: 14-05-2024

Questionnaire

Describe the datatypes (surveys, sequences, manuscripts, objects …) the research will collect and/or generate and /or (re)use. (use up to 700 characters)

1. Computer Code (Matlab, Python, C) of the software used to interact with SDR and simulate a receiver, generate a watermark signal, and evaluate attacks and mitigations.
2. Logs of how the signal features evaluated respond to multiple scenarios and parameters.
3. Manuscripts (Latex, Word) containing the knowledge and results obtained in a summarized manner. Also, manuscripts containing journals and articles and the thesis itself.
4. List of vulnerabilities found in Global Navigation Satellite Systems receivers.
5. Proposals of techniques to harden the navigation signal and/or the GNSS receiver communications.

Specify in which way the following provisions are in place in order to preserve the data during and at least 5 years after the end of the research? Motivate your answer. (use up to 700 characters)

The promotor of this project, Prof. Sofie Pollin, will be the main responsible person for data preservation.
To ensure the proper conservation and security of the data, we will use private cloud storage services such as Google Drive and also academic cloud service available at the host institution KU Leuven. To keep track of and manage the code development, we will use Gitlab repositories in the KU Leuven network. When writing Latex manuscripts, we will use the online service Overleaf which automatically keeps track of changes and has cloud storage. We will perform periodical external, offline backups. Both the cloud and the offline
backups are foreseen to be preserved for up to 5 years after the end of the research.

What's the reason why you wish to deviate from the principle of preservation of data and of the minimum preservation term of 5 years? (max. 700 characters)

N/A

Are there issues concerning research data indicated in the ethics questionnaire of this application form? Which specific security measures do those data require? (use up to 700 characters)

To prevent information about vulnerabilities or the code for spoofing attacks from being made publicly available before a responsible disclosure process has taken place, any cloud service or git used will be in private instances.

Which other issues related to the data management are relevant to mention? (use up to 700 characters)

N/A

Multi-Layer Satellite Navigation Security: Signal in Space Authentication and Receiver Interfaces Hardening
FWO DMP (Flemish Standard DMP)

1. Research Data Summary

List and describe all datasets or research materials that you plan to generate/collect or reuse during your research project. For each dataset or data type (observational, experimental etc.), provide a short name & description (sufficient for yourself to know what data it is about), indicate whether the data are newly generated/collected or reused, digital or physical, also indicate the type of the data (the kind of content), its technical format (file extension), and an estimate of the upper limit of the volume of the data.

				Only for digital data	Only for digital data	Only for digital data	Only for physical data
Dataset Name	Description	New or reused	Digital or Physical	Digital Data Type	Digital Data format	Digital data volume (MB/GB/TB)	Physical volume
GNSS recordings walking in Brussels	I will walk around Brussels with a Septentrio GNSS receiver and collect logs in SBF format to be used in the research.	Generate new data	Digital	Observational	.sbf	<1GB	
RF Recordings	IQ recordings done with an SDR for the implementation and test of defenses.	Generate new data	Digital	Experimental	IQ binary files	<100GB	
OSNMAlib: Open-source OSNMA library	I will extend my existing library with new optimizations and ideas.	Reuse existing data	Digital	Software	Computational scripts.	<100MB	
Watermark codes implementation	Part of the research requires to create a new software framework to simulate the watermark codes in GNSS signals	Generate new data	Digital	Software	Computational scripts.	<100MB	
Vulnerability exploitation scripts	When performing cybersecurity assessments on GNSS receivers several vulnerability exploitation scripts will be generated.	Generate new data	Digital	Software	Computational scripts.	<100MB	

If you reuse existing data, please specify the source, preferably by using a persistent identifier (e.g. DOI, Handle, URL etc.) per dataset or data type:

Reusing OSNMAlib library from previous projects: 10.1109/NAVITEC53682.2022.9847548 (https://github.com/Algafix/OSNMA)

Are there any ethical issues concerning the creation and/or use of the data (e.g. experiments on humans or animals, dual use)? Describe these issues in the comment section. Please refer to specific datasets or data types when appropriate.

- Yes, dual use

Yes, the vulnerability exploit scripts fall under the dual-use umbrella. We requested an ethical evaluation to the Ethics Committee for “Dual use, military use & misuse of research” and got it approved (E-2023-4486).

Will you process personal data? If so, briefly describe the kind of personal data you will use in the comment section. Please refer to specific datasets or data types when appropriate.

- No

Does your work have potential for commercial valorization (e.g. tech transfer, for example spin-offs, commercial exploitation, …)? If so, please comment per dataset or data type where appropriate.

- No

Do existing 3rd party agreements restrict exploitation or dissemination of the data you (re)use (e.g. Material/Data transfer agreements/ research collaboration agreements)? If so, please explain in the comment section to what data they relate and what restrictions are in place.

- Yes

Are there any other legal issues, such as intellectual property rights and ownership, to be managed related to the data you (re)use? If so, please explain in the comment section to what data they relate and which restrictions will be asserted.

- No

2. Documentation and Metadata

Clearly describe what approach will be followed to capture the accompanying information necessary to keep data understandable and usable, for yourself and others, now and in the future (e.g., in terms of documentation levels and types required, procedures used, Electronic Lab Notebooks, README.txt files, Codebook.tsv etc. where this information is recorded).

For the RF data recorded, we will use the Signal Metadata Format (SigMF) standard to document the contents of the binary files.
The recorded logging files in proprietary format will be accompanied by the manual for their interpretation and parsing scripts if needed.
The code developed by the project will always have documentation in the code in a similar approach to Docstring for Python code and README files, including how to execute and interpret them.

Will a metadata standard be used to make it easier to find and reuse the data? If so, please specify (where appropriate per dataset or data type) which metadata standard will be used. If not, please specify (where appropriate per dataset or data type) which metadata will be created to make the data easier to find and reuse.

- Yes

For the RF data the Signal Metadata Format will be used.
https://github.com/sigmf/SigMF/blob/main/sigmf-spec.md

3. Data storage & back-up during the research project

Where will the data be stored?

The KU Leuven Gitlab repository will be used to store and keep versions of the code.
I will use Overleaf to work and store the manuscripts written in LaTeX since they are stored in the cloud. However, backups to the

KU Leuven OneDrive will be done periodically.

For general documents and data, I will use the KU Leuven OneDrive and, sporadically, the personal Google Drive storage since OneDrive is not available natively on Linux. However, the important files will be backed to OneDrive at least once a month.

How will the data be backed up?

ICTS periodically backs up the backup solutions provided by KU Leuven, which performs full backup in non-Microsoft data centers.

The cloud services used during the projects that are not managed by KU Leuven will always be configured to have a local copy. Moreover, I perform bi-annual offline air-gapped backups of the hard drive of my local machine.

Important physical documents used during the project will be scanned to prevent their loss.

Is there currently sufficient storage & backup capacity during the project? If yes, specify concisely.
If no or insufficient storage or backup capacities are available, then explain how this will be taken care of.

- Yes

As a KU Leuven student, I have more than 2 TB of storage available in OneDrive. The data generated by the project is expected to be less than 200 GB.

How will you ensure that the data are securely stored and not accessed or modified by unauthorized persons?

The data stored in the university's secured environment is protected by the experienced IT team at KU Leuven. The data in personal accounts always has 2FA, and I use a password manager. The room where I work at the university and store my personal machine and documents requires badge access.

What are the expected costs for data storage and backup during the research project? How will these costs be covered?

The price of the OneDrive cloud storage is free for KU Leuven students and staff. The GitLab server cost and the Overleaf account are also covered by KU Leuven.

4. Data preservation after the end of the research project

Which data will be retained for at least five years (or longer, in agreement with other retention policies that are applicable) after the end of the project? In case some data cannot be preserved, clearly state the reasons for this (e.g. legal or contractual restrictions, storage/budget issues, institutional policies...).

After the research, all recorded datasets, manuscripts, code, and generated data will be stored on ESAT central network drives. Following KU Leuven's RDM policy, research datasets will be kept for 10 years. Limited data of high value may be made available for longer in deemed appropriate during the project.

Where will these data be archived (stored and curated for the long-term)?

The data will be stored on ESAT central network drives (with automatic backup procedures) for at least 10 years, conform the KU Leuven RDM policy.

What are the expected costs for data preservation during the expected retention period? How will these costs be covered?

Given the size of the expected dataset (<200 GB), the estimated cost for the storage drive expansion is 40 EUR.

5. Data sharing and reuse

Will the data (or part of the data) be made available for reuse after/during the project? In the comment section please explain per dataset or data type which data will be made available.

- Yes, in an Open Access repository

The GNSS recordings may be helpful for other researchers and, therefore, will be made available. The codes to test defenses against spoofing attacks will be made available.

If access is restricted, please specify who will be able to access the data and under what conditions.

NA

Are there any factors that restrict or prevent the sharing of (some of) the data (e.g. as defined in an agreement with a 3rd party, legal restrictions)? Please explain in the comment section per dataset or data type where appropriate.

- Yes, Aspects of dual-use

The scripts to exploit vulnerabilities will only be made available if needed after the manufacturer has fixed the vulnerability.

Where will the data be made available? If already known, please provide a repository per dataset or data type.

Some candidates to host data are:
https://rdr.kuleuven.be/
https://ieee-dataport.org/

When will the data be made available?

Upon acceptance or publication of research results, depending on the case.

Which data usage licenses are you going to provide? If none, please explain why.

The preferred license will be a CC-BY license. Therefore, it will be available to anyone for any purpose, provided that they give appropriate credit to the creators

Do you intend to add a PID/DOI/accession number to your dataset(s)? If already available, you have the option to provide it in the comment section.

- Yes

What are the expected costs for data sharing? How will these costs be covered?

If the chosen repository is not free of cost, the FWO fellowship grant may be used.

6. Responsibilities

Who will manage data documentation and metadata during the research project?

The PI, Aleix Galan, bears the responsibility for the data documentation and metadata.

Who will manage data storage and backup during the research project?

The PI, Aleix Galan, bears the responsibility for the data storage and back up during the project.

Who will manage data preservation and sharing?

The PI, Aleix Galan, and his supervisor, Prof. Sofie Pollin, share the responsibility for ensuring data preservation and sharing.

Who will update and implement this DMP?

The PI, Aleix Galan, bears the end responsibility of updating & implementing this DMP.