INFORMED CONSENT FORM

Study title

Security Pointers Inside Open-Source Software Projects

Principal investigator

[redacted]

Sponsor

[redacted]

Project

Privacy and Data Protection in Social Coding Platforms

PARTICIPANT INFORMATION SHEET

1. Introduction

Thank you for your interest!

This online survey is part of an empirical study conducted by the [redacted]. The goal of this study is to gain insights into the security practices of software developers in Open-Source Software (OSS) projects. Particularly, regarding the incorporation of security pointers inside software artifacts such as commit messages, pull requests, issue reports, and code comments. It consists of a set of questions and scenarios that you must assess and should take around 10 minutes.

Please read the Participant Information Sheet before starting with the survey. The sheet can be accessed via this link: https://cloud.tuhh.de/index.php/s/dtGA6WZfazGzj44

For any questions or inquiries please contact [redacted]

IMPORTANT: To participate in this study, you must (i) be at least 18 years old, (ii) have prior experience working in OSS projects, and (iii) pass the technical screening, consisting of 3 generic questions about programming.

If you do not meet any of these conditions, you will be excluded from participating.

If you would like to proceed to the technical screening and take this survey, please answer the following questions by placing a check mark accordingly:

☐ I am age 18 or older.

☐ I am an active user of Social Coding Platforms.

☐ I have read and understood the Participant Information Sheet.

☐ I agree to participate in this research and I want to continue with the survey.

2. Purpose of the research

The study of Technical Debt (TD) has received special attention in the last decades due to its implications for software maintenance and evolution. At its core, TD encompasses a wide array of sub-optimal design and implementation choices that can compromise, to a great extent, the quality of a software system, not to mention its security. A large part of TD is explicitly reported through "self-admissions", namely by developers in software artefacts such as code comments and commit messages. These reports have helped identify and manage different TD types including requirements and testing. However, they can also be deemed as dreadful sources of information on potentially exploitable vulnerabilities and security flaws.

This study seeks to gain insights into the security practices of software developers in Open-Source Software (OSS) projects through an online survey. Particularly, regarding the incorporation of security pointers inside software artifacts such as commit messages, pull requests, issue reports, and code comments. The survey consists of an assessment of developers' tendencies to disclose security pointers inside SATS instances and their motivations for doing so. Additionally, it elicits their perceptions of risk regarding these practices. That is, whether they believe explicit references to security vulnerabilities inside commit messages, pull requests, issue reports, and code comments can compromise the availability, integrity, and confidentiality of an OSS project.

3. Type of research intervention

This research will involve your participation in an online survey.

4. Participant selection

Pre-screened in Prolific based on (i) self-reported knowledge of software development techniques, and (ii) self-reported computer programming skills. We aim to collect around 150 responses from a pre-screened Prolific sample of about 9.000 users.

5. Voluntary participation

Participation in the scientific research project is voluntary; if you do not participate, you will not suffer any disadvantages. Once the survey is started, you will need to complete it in one go.

You do not have to answer any question you do not want to answer (mandatory questions will have an N/A option). If at any time and for any reason, you would prefer not to participate in this study, please feel free not to.

You also have the possibility to assert the following rights at any time:

- **Right of access** about the personal data processed concerning you (art. 15 GDPR),
- **Right to rectification** of inaccurate personal data concerning you (art. 16 GDPR),
- **Right to erasure** of personal data concerning you (art. 17 GDPR),
- **Right to restriction** of processing of personal data concerning you (art. 18 GDPR),
- **Right to object** the processing of personal data concerning you (art. 21 GDPR),
- You also have the right to lodge a **complaint** with a **data protection supervisory authority** about the processing of personal data by us concerning you (art. 77 GDPR),
- If you have consented to the processing of your data, you have the right to **withdraw** this consent at any time for the future (art. 7 paragraph 3 GDPR). In this case, all personal data must either be deleted or made anonymous.

Your rights must always be asserted in writing to the person responsible for data processing.

6. Duration of the study

The online survey will take approximately 10 minutes.

7. Recording

We may quote your remarks in presentations or articles resulting from this work, However, no personal data of yours will be mentioned, i.e. the research results are published without reference to you personally. Interviews are only quoted in excerpts to ensure to third parties that the resulting overall context of events cannot lead to an identification of your person.

8. Risks

There are no risks or hazards to yourself when participating in this survey beyond those associated with basic computer tasks (e.g., boredom, fatigue, or mild stress). As with all research, there is a chance that confidentiality of the information we collect from you could be breached – we will take steps to minimize this risk, as discussed in more detail below in this form.

9. Benefits

While we cannot guarantee that the outcomes of this research will generate any benefits for yourself personally beyond the learning experience from participating in a research study. The benefit to society is the contribution to scientific knowledge.

10. Reimbursements

By participating in the scientific research project no additional costs are incurred.

Participants that produce a valid submission will be paid through Prolific a rate of £1.25 for a completed survey.

Claims for further remuneration, royalties or other participations in financial benefits and profits, that may be achieved on the basis of the research results, are excluded.

11. Confidentiality

Your personal data will be handled as confidentially as possible adhering to all pertinent international, European and national legislation. Whenever results of this study are published or presented, individual names and other personally identifiable information will not be used; i.e. the data will be anonymized.

- Personal data are collected on a need-to-know basis only.
- Withdrawal rights and oblivion rights made compulsory by the European Court of Justice in 2014 are guaranteed.
- The merger of datasets containing personal data will be avoided in order to prevent any unforeseen personal information disclosure. Data may be made available for reuse by other researchers only if personal data has been anonymized or erased from the dataset.

12. Data collection and processing

In the context of the scientific research project the following data will be collected from you:

- **contact data**: your Prolific ID.
- **project data**: This is the information about you produced in the context of the scientific research project, in particular your answers to the survey's questions.

The produced **project data** will be evaluated by project members. Your **contact data** will be marked with a project data identifier and stored separately from the project data in different locations to which only authorized employees of the scientific research project and authorized scientists have access.

Access to your data is restricted to employees of the scientific research project as well as authorized scientists. These persons are obliged to observe the data protection requirements. The data is protected against unauthorized access.

13. Data storage

The original data or -records are kept for at least 10 years in accordance with the guidelines for handling research data of the German Research Foundation for safeguarding good research practice and are deleted afterwards, unless legal requirements stipulate longer archiving obligations.

After the completion of the scientific research project, your contact data will be automatically deleted, unless you expressly agree to the further storage of your contact data for future topic related scientific research projects. In this case, scientists would be provided with the data on request so that they can contact you and ask whether you are available to participate in a scientific research project.

Such participation is of course voluntary and you can refuse it without giving reasons. You can of course object to a longer storage at any time; your contact data will then be deleted.

14. Sharing the results

We aim to disseminate outcomes of this research through academic venues, targeting software engineering conferences and journals with a security/privacy inclination, or from the broad area of software engineering. Examples are FSE, TOSEM, TSE and Usenix. Data sets not containing any personal data may be shared via repository called Zenodo. All confidential information will remain confidential.

15. Right to refuse or withdraw

You may stop participating at any time by closing the browser window. Partial data will not be analyzed. You will not be penalized in any way for deciding to stop participating.

16. Who to contact

The scientific research ro ect will be carried out b [redacted]. Responsible for the data rocessin is [redacted]

If ou have further uestions regarding the scientific research project, please contact [redacted]:

- **Address**: [redacted].
- **Phone**: [redacted]

- **E-Mail**: [redacted]

If you have any questions re ardin data rotection law, please contact the data protection officer at [redacted]:

- **Address**: [redacted]
- **Phone**: [redacted]
- **E-Mail**: [redacted]