Pushed by Accident: A Mixed-Methods Study on Strategies of Handling Secret Information in Source Code Repositories

Alexander Krause, *CISPA Helmholtz Center for Information Security;*
Jan H. Klemmer and Nicolas Huaman, *Leibniz University Hannover;*
Dominik Wermke, *CISPA Helmholtz Center for Information Security;*
Yasemin Acar, *Paderborn University, George Washington University;*
Sascha Fahl, *CISPA Helmholtz Center for Information Security*

https://www.usenix.org/conference/usenixsecurity23/presentation/krause

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 32nd USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Artifact Appendices to the Proceedings of the 32nd USENIX Security Symposium is sponsored by USENIX.

USENIX'23 Artifact Appendix: Pushed by Accident: A Mixed-Methods Study on Strategies of Handling Secret Information in Source Code Repositories

Alexander Krause, CISPA Helmholtz Center for Information Security

A Artifact Appendix

A.1 Abstract

Our paper contains a mixed-methods study, a survey with developers on their experiences handling secrets in source code, and an interview study with developers that experienced code secret leakage in the past. In order to support our paper and make it more useful for the readers, we provide all the necessary artifacts available in a replication package. The replication package includes: 1. The full survey and interview recruitment materials (including Upwork post and invitation, as well as GitHub invite messages). 2. The survey screening questions and interview pre-survey questionnaire. 3. The survey and interview consent form. 4. The survey questionnaire and interview guide. 5. The survey and interview codebook. 6. The background section on version control.

A.2 Description & Requirements

In this section, we provide the descriptions of all the applicable subsections for our use case (i.e., "artifacts available" badge).

A.2.1 Security, privacy, and ethical concerns

The data we provide is not harmful to viewers. All data we provide has been anonymized to protect our participants' privacy.

A.2.2 How to access

Our artifact can be accessed using the following URL: https://doi.org/10.25835/xfc2h3pg.

The complete replication package can be downloaded as a .zip file through the provided link. This replication package is hosted on the Research Data Repository of our university (data.uni-hannover.de).

A.2.3 Hardware dependencies

None

A.2.4 Software dependencies

None

A.2.5 Benchmarks

None

A.3 Set-up

Our artifacts can be downloaded as a .zip file from the URL we provided in the section A.2.2. The file contains the following seven .pdf files:

1. **README.md** This .md file contains a list of all provided resources.
2. **index.html** This .html file is used to render the replication package as a website.
3. **background.md** This .md file contains an additional background section on version control, source code platforms, and secret information.
4. **interviews/codebook.txt:** This .txt file contains the high level codebook, including counts of the codes that we assigned to participants' answers.
5. **interviews/consentform.html:** This .pdf file contains the consent form we used in the pre-survey.
6. **interviews/Interview_Guide.pdf** This .pdf file contains the semi-structured interview guide we used in our interview study.
7. **interviews/invite_mail.md** This .md file contains our recruitment material. We sent this invite mail text to developers from GitHub.
8. **interview/pre-survey.md** This .md file contains the pre-survey we used to collect demographics and screen participants.
9. **survey/codebook.md** This .md file contains the high level codes that emerged from the survey to identify code secret leakage prevention and remediation approaches.

10. **survey/consentform.html** This .html file contains the consent forms used for participants recruited from Upwork and GitHub.
11. **survey/github_invite_mail.md** This .md file contains our recruitment material. We sent this invite mail text to developers from GitHub.
12. **survey/survey.md** This .md file contains the survey questionnaire.
13. **survey/survey-matrix.png** This .png file contains the survey question on participants' threat models because it could not be displayed in a .md file.
14. **survey/upwork_recruitment_material.md** This .md file contains all recruitment materials used to recruit developers from Upwork.

A.3.1 Installation

N/A

A.3.2 Basic Test

N/A

A.4 Notes on Reusability

To replicate the study, we suggest using the survey questionnaire excluding the open-ended questions that did not work well; we detailed on that in the paper). When replicating the interview study, we suggest using our template of the interview guide that we provide within this artifact.

A.5 Version

Based on the LaTeX template for Artifact Evaluation V20220926. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2023/.