Everyone for Themselves?

A Qualitative Study about Individual Security Setups of Open Source Software Contributors

Sabrina Amft[C], Sandra Höltervennhoff[L], Rebecca Panskus[R], Karola Marky[R,] Sascha Fahl[C]

[C] CISPA Helmholtz Center for Information Security; [L] Leibniz University Hannover;
[R] Ruhr University Bochum

Motivation

Companies typically offer various guidelines and rules for employees, including liability clauses.

This is generally not the case for open source (OS) projects: While highly relevant in the software supply chain, there are no contracts or mandatory policies.

We are therefore interested in which security measures OS developers take.

Research Questions

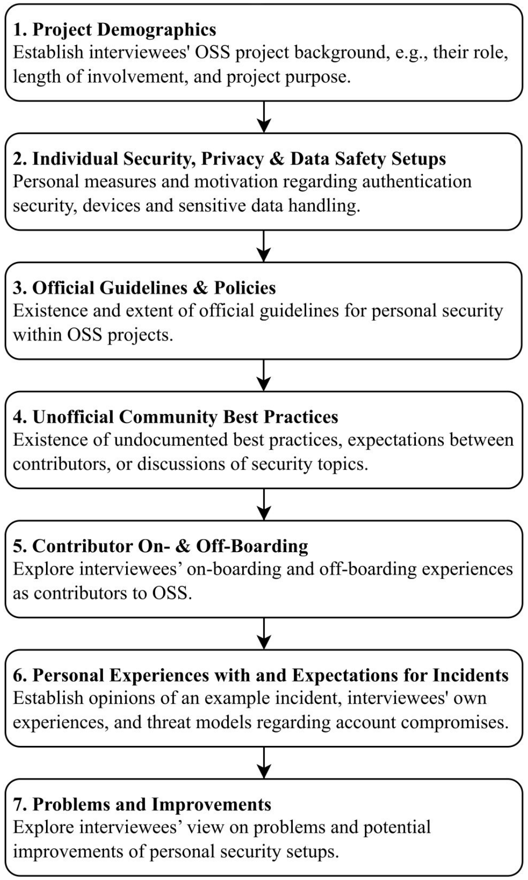
RQ1. Which technologies and practices do open source contributors deploy for their open-source related individual security setups?

RQ2. What are common challenges of securing open source contributors' individual security setups?

RQ3. How can open source contributors be better supported in maintaining their individual security setups?

Methodology

- 20 Semi-structured online interviews with OS developers of projects that were:
  - active: >40 commits, >20 contributors
  - critical: dependency counts, stars+forks
- Analysis: descriptive and inductive coding with 3 coders



1. Project Demographics
Establish interviewees' OSS project background, e.g., their role, length of involvement, and project purpose.

2. Individual Security, Privacy & Data Safety Setups
Personal measures and motivation regarding authentication security, devices and sensitive data handling.

3. Official Guidelines & Policies
Existence and extent of official guidelines for personal security within OSS projects.

4. Unofficial Community Best Practices
Existence of undocumented best practices, expectations between contributors, or discussions of security topics.

5. Contributor On- & Off-Boarding
Explore interviewees' on-boarding and off-boarding experiences as contributors to OSS.

6. Personal Experiences with and Expectations for Incidents
Establish opinions of an example incident, interviewees' own experiences, and threat models regarding account compromises.

7. Problems and Improvements
Explore interviewees' view on problems and potential improvements of personal security setups.

Selected Challenges

Social Cues: *"I don't want to come across as a paranoid person all the time. You'll talk about it less [...]"*

Security is Rarely Communicated: *"Because I'm the person who presses merge on pull requests [...], I don't need to communicate the guidelines to anyone else."*

Ease of Trust: *"I got an email that I'm now the owner of <project>. That was a surprise for me, I didn't know him, but he trusted me a lot."*

Recommendations

Platform-Enforced Measures can circumvent social obstacles by enforcing, e.g., MFA through technical means, not other developers.

Manage Hierarchies and Access Rights to limit attack surfaces, as only selected individuals can deploy or access secrets.

Provide Basic Guidance on a project level, ideally by creating a basic template that can be easily copied and shared.

Published at S&P 2024
https://research.teamusec.de/2023-oss-contributors/