Codebook

V1.4 (Anonymized)

Changelog

- V1.4 | Added 3rd round codes
- V1.3 | Added 2nd round codes
- V1.2 | Updated some IDs to match Interview Guide
- V1.1 | Additional codes from interviews + data analysis plan
- V1 | Initial version

Overview

Setup codes in this codebook have the following structure:

Ex	Worries
(This is an example) **Description:** General code for worries expressed in questions Q3, Q4, and Q5. **Subcodes** include currently: - worries-1: security - worries-2: privacy (see Code 1.3 for an additional sub coding) - worries-3: usability You **may** extend this list if you identify a new worry. **Buzzwords:** “I worry about …”, “I fear …”, “I feel bad about …" **Examples:** - “I often worry about my privacy, especially if I use an app with many ads." → worries-2: privacy - “I dislike using these apps, because I feel like a hacker could easily hack them." → worries-1: security **Coding:** Add the corresponding subcode(s). Remember to also assign Code 1.3 if the worries include privacy.	

C1 Project Demographics

Get additional demographics such as contributor count etc. directly from repositories.

C1.1	Project Type

Description: General code for project type(s) of the participant.
Subcodes include currently:

- C1.1-1: Operating System
- C1.1-2: Library
- C1.1-3: Virtualization/containers
- C1.1-4: Code analysis
- C1.1-5: Hybrid engineering
- C1.1-6: WebApp/Backend
- C1.1-7: Parser/Serialization/Deserialization
- C1.1-8: Shared libraries
- C1.1-9: Version Control System
- C1.1-10: UI Tool
- C1.1-11: Orchestration:
- C1.1-12: Network Monitoring
- C1.1-13: Scientific simulations
- C1.1-14: Decentralized exchange (crypto)
- C1.1-15: CLI Tool
- C1.1-16: Network Protocol

You **may** extend this list if you identify a new project type.
Buzzwords: *"I work on X, a library for ..."*
Coding: Add corresponding subcodes for each project mentioned.

C1.2	Project Age

Description: Age of the project.
Coding: Code (if) estimated by participant + enhance with actual repo age if available

C1.3	Contributor Count

Description: Number of (regular) contributors to the project.
Coding: Code (if) estimated by participant + enhance with actual repo data if available

C1.4	Contributor Connections

Description: How the contributors are connected to each other.

Coding: Add corresponding subcodes, when in doubt: likely random "Contributors"

C1.5	Contributor Distribution

Description: How the contributors are distributed.
Coding: Add corresponding subcodes, when in doubt: likely "Global"

C1.6	Participant Position

Description: Rough estimate of our participant's position within the project (estimate from project data if not mentioned by participant).
Subcodes include currently (roughly ordered by rank):

- C1.6-1: Founder or Owner (or equiv.)
- C1.6-2: Team Lead (or equiv.)
- C1.6-3: Maintainer (or equiv.)
- C1.6-4: Regular contributor

You **may** extend this list if you identify a new position.
Coding: Add corresponding subcodes.

C2 Incidents

C2.1	Security Challenges

Description: If/What security challenges the project faced.
Subcodes include currently:

- C2.1-1: None
- C2.1-2: Suspicious/Low Quality Commits (but no obvious attack)
- C2.1-3: Social Engineering
- C2.1-4: Vuln in dependency
- C2.1-5: Other
- C2.1-6: Full disclosure of vulnerabilities
- C2.1-7: Unsafe user input
- C2.1-8: Loss of credentials

You **may** extend this list if you identify a new incident type.
Coding: Add corresponding subcodes

C2.2	Incident Aware

Description: If the participants were aware of the incident.
Subcodes include currently:

- C2.2-1 Aware: No
- C2.2-2 Aware: Yes

Coding: Add corresponding subcodes

C2.3	Incident Opinion

Description: What opinion the participant had of the research approach mentioned in the incident.
Subcodes include currently:

- C2.3-1 Opinion: No opinion / Refuse to answer
- C2.3-2 Opinion: Negative
- C2.3-3 Opinion: Neutral / Mixed
- C2.3-4 Opinion: Positive

Coding: Add corresponding subcodes

C3 Guidance

C3.1	Guidance Types

Description: If/what type of guidance the project(s) provide.
Subcodes include currently:

- C3.1-1: None
- C3.1-2: Language (e.g. style)
- C3.1-3: Security
- C3.1-4: Crypto-specific
- C3.1-5: Infrastructure
- C3.1-6: General (contributing)
- C3.1-7: Test-specific

You **may** extend this list if you identify a new type.
Coding: Add corresponding subcodes

C4 Security Policies

C4.1	Policies Content

Description: If/what type of security policies the project(s) provide.
Subcodes include currently:

- C4.1-1: None
- C4.1-2: Mandatory 2FA
- C4.1-3: Security contact/team
- C4.1-4: Bug bounty program
- C4.1-5: Limited scope
- C4.1-6: Air gapping

You **may** extend this list if you identify a new type.
Coding: Add corresponding subcodes

C4.2	Disclosure Policies

Description: If/what type of disclosure policies the project(s) follow.
Coding: Add corresponding subcodes

C4.3	Incident Playbooks

Description: If/what type of incident playbooks the project(s) follow.
Subcodes include currently:
Coding: Add corresponding subcodes

C4.4	Security Testing

Description: If/what type of security testing does the project(s) perform.
Subcodes include currently:
Coding: Add corresponding subcodes

C4.5	Security Reviews

Description: If/what type of security reviews does the project(s) perform.
Subcodes include currently:
Coding: Add corresponding subcodes, see also **C5.3 - Pull Requests**.

C4.6	Threat Modeling

Description: If threat modeling is mentioned by the participant (exact match only?).
Subcodes include currently:
Coding: Add corresponding subcodes

C5 Project Structure

C5.1	Project Stage
Description: What does the setup of the project look like? Which stages does the project have? **Examples:** Code → Commit → PRs → Review → CI for tests and Build → Deployment **Coding:** Code mentions of stage-relevant parts.	

C5.2	Stage Control
Description: Who controls the different stages. **Coding:** Add corresponding subcodes	

C5.3	Pull Requests/Patches
Description: How are pull requests (or patches if mailing list ist used) handled? **Coding:** Add corresponding subcodes	

C5.4	Secret Management
Description: How are (CI/CD) secrets handled **Coding:** Add corresponding subcodes	

C5.5	Commit Signing
Description: Whether/Why commits are signed **Coding:** Add corresponding subcodes	

C5.6	Supply Chain

Description: What does the software supply chain look like?
Subcodes include currently:

- C5.6-1: Private package repo used
- C5.6-2: Vulnerability checking with tools
- C5.6-3: Vulnerability checking manual
- C5.6-4: Decision Criteria
- C5.6-5: Frequent updates of dependencies
- C5.6-6: Pinning of package versions
- C5.6-7: Optional dependencies
- C5.6-8: Link against OS libs

You **may** extend this list if you identify a new type.
Buzzwords: Third Party Libraries, Package Manager, APIs, External projects
Coding: Add corresponding subcodes

C5.7	Other Infrastructure

Description: Does the project have additional infrastructure such as a project website or chat tools?
Subcodes include currently:

- C5.7-1: None
- C5.7-2: Access (who controls this infrastructure?)

Coding: Add corresponding subcodes

C6 Release and Updates

C6.1	Release Decision
Description: Who makes the decision to release an update? **Coding:** Add corresponding subcodes	

C6.2	Release Deprecation
Description: How are releases deprecated? **Coding:** Add corresponding subcodes	

C6.3	Release Announcement
Description: How are (security) releases announced? **Coding:** Add corresponding subcodes	

C6.4	Release Distribution
Description: If/how releases are actually distributed. **Coding:** Add corresponding subcodes	

C6.5	Release Signing
Description: If/how releases are signed. **Coding:** Add corresponding subcodes	

C7 Roles and Responsibilities

C7.1	Hierarchy
Description: What does the trust hierarchy look like **Coding:** Add corresponding subcodes	

C7.2	Security-specific roles
Description: Are there security-specific roles within the project? **Buzzwords:** security team, sysadmins **Coding:** Add corresponding subcodes	

C8 Trusting Contributors

C8.1	Gaining Trust
Description: What are ways to gain trust as a new contributor **Coding:** Add corresponding subcodes	

C8.2	Identity Check
Description: Does the project(s) check the identity of contributors **Coding:** Add corresponding subcodes	

C8.3	Contributor License Agreement
Description: Does the project(s) have a CLA? **Subcodes** include currently: - C8.3-1 None **Coding:** Add corresponding subcodes	

C8.4	Public List of Contributors
Description: Does the project(s) maintain a public list of contributors **Coding:** Add corresponding subcodes	

C9 Untrustworthy Contributors

C9.1	Trust Incidents
Description: Did the project(s) have trust incidents **Coding:** Add corresponding subcodes	

C9.2	Trust Strategy
Description: What are the project(s) strategies for dealing with trust incidents **Coding:** Add corresponding subcodes	

C9.3	Commit Removal
Description: If/how the project(s) removed affected commits **Coding:** Add corresponding subcodes	

C10 Problems and Improvements

C10.1	Reputation
Description: What does the participant think about the reputation of their project(s) **Coding:** Add corresponding subcodes	

C10.2	Improvements
Description: Areas that the participant wants to improve **Coding:** Add corresponding subcodes	