Guide for the report

Discussion

Consider the **security mechanism** that is studied in this project, and that consists of:

1. Statically retrieving the potentially vulnerable program slices by means of a taint analysis;
2. Discarding the slices where input is considered to have been validated, as defined and implemented in the experimental part.

Given the intrinsic limitations of the static analysis problem, the above mechanism is necessarily imprecise. It can be **unsound** (produce false negatives), **incomplete** (produce false positives) or **both**.

Define and discuss **what the resulting mechanism is able to achieve**, while answering the following questions:

- Explain **what are the imprecisions that are built into the proposed mechanism**. Have in mind that they can originate at different levels, for instance:
    - Imprecise tracking of information flows
        - Are all illegal information flows captured by the adopted slicing technique?
        - Are there flows that are unduly reported?
    - Imprecise endorsement of input validation
        - Are there sanitization functions that could be ill-used and not properly validate the input?
        - Are all possible validation procedures detected by the tool?

- **For each of the identified imprecisions that lead to**:
    - undetected vulnerabilities (false negatives)
        - Can these vulnerabilities be exploited? If yes, how (give concrete examples)?
    - reporting non-vulnerabilities (false positives)
        - Can you think of how they could be avoided?

Propose one way of making the tool more precise, and predict what would be the tradeoffs (efficiency, precision) involved in this change.

Format

Report:

- describe briefly the experimental part (maximum 2 pages)
- discuss the **guarantees** provided by the tool, as well as its **limitations**, in light of the state of the art for the proposed problem.

The first part should present the design of the tool, the main design options, and the output of the tool for a few examples. The document should have no more than 4 pages (excluding references and appendices.)

Evaluation

Criteria:

- **Quality of writing** - structure of the report, clarity of the ideas, language
- **Content** - relevance and value of the ideas that are conveyed
- **Depth** - understanding of the state of the art, connection with experimental work
- **Originality** - detachment from words used in cited papers, references that are cited beyond the suggested ones, own ideas

All sources should be adequately cited.