

Know vulnerabilities oss libraries

Ronaldo Canesqui
Southern Adventist University
ronaldocanesqui@southern.edu

Abstract—The abstract should describe the basic message of the paper, including: the problem, why your solution should be of interest, some notion that your solution is effective, and a teaser about how it has been evaluated. Cover all of this using between 75 and 150 words. The abstract is thus the hardest part to write. Sometimes I try to write it first, but the final version is usually composed of items drawn from the introduction, and then condensed, as the last step of writing the paper.

I. INTRODUCTION

The problem we have solved:

The use of open-source libraries is a factual reality in the software industry. Their usage has increased exponentially during the last decade and proportionally the number of security vulnerabilities that are introduced with them. How to leverage the power of open source libraries and still manage the risk of vulnerabilities they carry is a problem that either remain ignored by many software engineers or present considerable challenges to them.

Why the problem is not already solved or other solutions are ineffective in one or more important ways

During this paper important studies related to dependencies management will be presented along with the most recent studies about how to identify known vulnerabilities in open source libraries.

A 2014 study from Sonatype determined that over 6% of the download requests from the Maven Central Repository were for component versions that included known vulnerabilities. In their review of over 1,500 applications, each of them had an average of 24 severe or critical flaws inherited from their components.¹ A white paper produced by Contrast security, stated that over 25% of all libraries download from Maven Central Repository has vulnerability. Only one vulnerable version of the Java GWT package was downloaded 17,666,703 times [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?]. This is the place to provide a succinct description of the problem context giving enough information to support the claim that a problem exists, made in the preceding problem declaration.

Why our solution is worth considering and why is it effective in some way that others are not

A succinct statement of *why* the reader should care enough to read the rest of the paper.

This should include a statement about the characteristics of your solution to the problem which 1) make it a solution, and 2) make it superior to other solutions to the same problem.

How the rest of the paper is structured The short statement below is often all you need, but you should change

it when your paper has a different structure, or when more information is *required* to describe what a given section contains. If it isn't *required* then you don't want to say it here.

The rest of this paper first discusses related work in II, and then describes our implementation in III. IV describes how we evaluated our system and presents the results. V presents our conclusions and describes future work.

II. RELATED WORK

Other efforts that exist to solve this problem and why are they less effective than our method

Resist the urge to point out only flaws in other work. Do your best to point out both the strengths and weaknesses to provide as well rounded a view of how your idea relates to other work as possible

In a social and political sense, it is *very smart* as well as ethical to say good things, which are true, about other people's work. A major motivation for this is that editors and program committee members have to get a set of reviews for your paper. The easiest way for them to decide who should review it is to look at the set of references to *related work* to find people who are likely to be competent to review your paper. The people whose work you talk about are thus likely to be reading what you say about *their* work while deciding what to say about *your* work.

Clear enough? Speak the truth, say what you have to say, but be generous to the efforts of others.

Other efforts that exist to solve related problems that are relevant, how are they relevant, and why are they less effective than our solution for this problem

Many times no one has solved your exact problem before, but others have solved closely related problems or problems with aspects that are strongly analogous to aspects of your problem

III. IMPLEMENTATION

What we (will do | did): Our Solution Another way to look at this section is as a paper, within a paper, describing your implementation. That viewpoint makes this the introduction to the subordinate paper, which should describe the overall structure of your implementation and how it is designed to address the problem effectively.

Then, describe the structure of the rest of this section, and what each subsection describes.

How our solution (will | does) work This is the body of the subordinate paper describing your solution. It may be

¹Report published January 02, 2015 at <http://goo.gl/i8J1Zq>.

divided into several subsections as required by the nature of your implementation.

The level of detail about how the solution works is determined by what is appropriate to the type of paper (conference, journal, technical report)

This section can be fairly short for conference papers, fairly long for journal papers, or *quite* long in technical reports. It all depends on the purpose of the paper and the target audience

Proposals are necessarily a good deal more vague in this section since you have to convince someone you know enough to have a good chance of building a solution, but that you have not *already* done so.

REFERENCES

IV. EVALUATION

How we tested our solution

- Performance metrics
- Performance parameters
- Experimental design

How our solution performed, how its performance compared to that of other solutions mentioned in related work, and how these results show that our solution is effective:

- Presentation and Interpretation
- Why, how, and to what degree our solution is better
- Why the reader should be impressed with our solution
- Comments

Context and limitations of our solution as required for summation: State what the results *do* and *do not* say.

V. CONCLUSIONS AND FUTURE WORK

The problem we have solved: The most succinct statement of the problem in the paper. Ideally one sentence. More realistically two or three. Remember that you simply state it without argument. If you have written a good paper you are simply reminding the reader of what they now believe and of how much they agree with you.

Our solution to the problem: again, a succinct statement of the presented solution. Sometimes it works well to leave it at that and not even describe your solution here. If you do, then again state your solution in one or two sentences taking the rhetorical stance that this is all obvious. If you have a good solution and have written an effective paper, then the reader already agrees with you.

Why our solution is worthwhile in some significant way: Again, a succinct restatement in just a few sentences of why your solution is worthwhile assuming the reader already agrees with you.

Why the reader should be impressed and/or pleased to have read the paper: A few sentences about why your solution is valuable, and thus why the reader should be glad to have read the paper and why they should be glad you did this work.

What we will (or could) do next

- Improve our solution
- Apply our solution to harder or more realistic versions of this problem
- Apply our solution or a related solution to a related problem