Secure Programming: Group Project

Christophe Petit
University of Birmingham

November 15, 2019

The purpose of this project is to expand your knowledge and understanding of Secure Programming techniques beyond what is covered in the lecture slides and the labs, in a direction of your choice. The assignment counts for 20% of the overall mark for the course.

You are requested to form a small group, choose a research problem related to the course and a research paper addressing that question, study that paper and write a report on your findings. The remaining of this document describes the successive tasks associated to this project.

A research project? For this project you will have to study at least one research paper published in the literature. This will involve verifying the arguments and results presented in the paper, often by writing your own code or running your own tests on existing code. To be clear, it is not expected that you will produce new scientific results of a publishable level here, but instead that you use your knowledge, judgment and skills to evaluate previous work.

1 Build your Group (deadline Monday Week 2)

The majority of groups must have 6 students. For practical reasons it may make sense to group students from the same program together, but as far as I am concerned you can really group yourselves as you wish. You may also want to group yourselves according to your interests (see next section).

Assignment. You should register your group before the deadline on the appropriate section of the Canvas webpage: `canvas.bham.ac.uk/courses/38504/groups#tab-14333`.

2 Choose a project (deadline Thursday Week 3)

Once you have formed a group, you should identify a topic of interest and at least one (good) research paper that relates to it. The topic must of course be related to Secure Programming.

How to identify good research papers? Good papers tend to be published at good venues, be written by authors from recognized institutions, have a high number of citations (relative to their age) and a high editorial quality.

I would suggest that you either start from a question of interest to you and search for good papers related to it, or that you browse the program of some top security conferences (CCS, Usenix, etc) to identify topics of interest to you.

Rankings such as `http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm` can be helpful at identifying good venues.

Assignment. You are asked to submit a one-page description of your project by the deadline on Canvas. The description must include the topic description, why it is an important secure programming question and why you chose it. It should also include a tentative workplan, describing the work you will do and how it will be organized during the term and distributed to the group members. It should of course clearly reference the research paper(s) that you will be focusing on to address your problem, as well as any other source used.

Priority claims and early feedback. All groups must have clearly distinct projects. Your group can claim priority for a particular project by proposing it ahead of the submission deadline on the relevant discussion page on Canvas `canvas.bham.ac.uk/courses/38504/discussion_topics/531864`. In case of conflict, the first group to post their idea on this page will get the priority on the project, and the other group will have to find a new project.

Evaluation. The assignment does not count towards the final mark, but a penalty of up to 5% of the project mark can be applied if you do not submit your project proposal by the deadline.

3 Study the paper

Some questions you may want to consider when reading a research paper:

- What is the problem considered? How important is it? Does it relate to other more important problems? What is the evidence that the problem is important?
- How much work had been done previously on that problem? What were the limitations in previous works? Is the paper providing a fair description of the state-of-the-art?
- Have the papers cited appeared in good venues?
- What is exactly the gap that the paper aims to fill in? Judging from the abstract, introduction and conclusion, does it succeed in doing that?
- What is the most important idea in the paper?

- What is the methodology employed in the paper? Is this methodology sound? Had it been used before?
- Does the paper make any assumption or restrict the context? How realistic are those assumptions and restrictions?
- Are the results impressive? Should they be complemented with more results to provide definitive evidence? What are the main weaknesses of the results?
- Are the weakness fundamental, are they due to the methodology? could they be avoided using other techniques?
- Can you reproduce the results? If not then why is is not possible? Could you improve the results?
- Are there other papers citing this one? how do they describe its contributions? do they agree with the overall conclusions? Do they identify further weaknesses? do they improve it?
- Will the paper become/remain influential in the field, or will it be quickly forgotten?

These questions are only examples to guide your critical thought process. Not every question is necessarily relevant for every project, and you may want to consider other questions as well.

Often you will not be able to verify all the authors' claims only by reading the paper and other literature items, in which case you may want to write your own code, or run your own tests on existing code to verify certain assumptions and results.

4 Draft report (deadline Thursday Week 7)

Assignment. You are asked to submit a draft report of your project by the deadline on Canvas. Guidelines on the report are provided in Section 7 below.

Evaluation. The assignment does not count towards the final mark, but a penalty of up to 5% of the project mark can be applied if you do not submit your report by the deadline.

Feedback. Feedback will be provided aimed at improving the final report.

5 Submit slides (deadline Thursday Week 8)

Assignment. You are asked to submit slides for a presentation to the class. You will have 12 minutes to present, and the number of slides and their content should be tuned accordingly.

The slides should be well-structured, well-written and their technical content must be correct.

The slides should be targeted at an audience of computer science students who have taken an introductory course on Secure Programming. You won't have the time to present all your findings in your presentation. The goal for your presentation is "to encourage the audience to read the report". That usually implies clearly presenting the problem, hinting at the main technical contributions, and discussing results.

Guidance on how to write effective slides can be found at many places online, for example on this youtube video: `www.youtube.com/watch?v=meBXuTIPJQk`

Evaluation. The assignment does not count towards the final mark, but a penalty of up to 5% of the project mark can be applied if you do not submit your slides by the deadline.

Feedback. Feedback will be provided aimed at improving the final report.

6 Present your work in front of the class

Assignment. You are asked to present your work in front of the class. The presentations will be followed by a short discussion.

Presentations are expected to take place in Weeks 10-11.

Evaluation. The assignment does not count towards the final mark, but a penalty of up to 5% of the project mark can be applied if you do not present.

Feedback. Feedback will be provided aimed at improving the final report.

7 Submit final report (deadline Wednesday Week 11)

Assignment. You are asked to submit your final report by the deadline on Canvas. The report must be at most eight pages including references and appendices. The code you have written can be shortly described in the report and provided as an external link.

The report should summarize the question you are considering and how the paper(s) contribute to it.

It should start with an introduction explaining what the problem is and why it is important. It can then go on describing the paper's main contribution(s), explaining their assumptions, methodology, main ideas and results. When appropriate, the report can then describe your own attempts at reproducing (part of) their findings. Finally, it should put the results in perspective, explain why they are important and what are their current limitations, and possibly compare

the paper(s) to other approaches in the literature. It should of course reference any source you have used.

Be critical: not every paper published at a good conference will completely solve a major open problem, and very often you will find that they have crucial limitations. You may find that authors tend to downplay the limits of their papers and highlight their advantages; in this case you should of course be more critical and justify your claims.

Attention should be paid to the editorial quality, including the overall structure, English language quality, and the proper use of scientific conventions.

The University takes plagiarism issues very seriously. See `intranet.birmingham.ac.uk/as/studentservices/conduct/plagiarism/guidance-students.aspx`

Evaluation. The report counts for 90% of the project mark, with 50% allocated to technical content, 20% on the investigation effort and 20% on the editorial quality.

8 Submit individual report (deadline Friday Week 11)

Assignment. Every student must submit an individual report by the deadline on Canvas. The report should be no longer than one page. It should summarize the project and explain how the work was distributed between the group members.

Evaluation. The report counts for 10% of the project mark. The mark will be based on your individual understanding of the project and the editorial quality of your report.

9 Contribution-based adjustments

Every group member is expected to contribute fairly to the project. This will be evaluated from the individual reports and from personal observations from the teaching staff. The evaluation could result in individual adjustments to the individual project marks. Under normal circumstances these adjustments will be limited to a 10% bonus or penalty on individual marks.

A note on team working Working in groups can be very stimulating and rewarding, but it can sometimes also present significant challenges. Useful advise in that respect is provided here: `www.uq.edu.au/student-services/learning/problems-associated-group-work` Please talk to me if you are experiencing a significant problem of this nature, which you are not able to solve within the group.