OPPOSITION FOR MASTER'S PROJECT

The duties of an opponent are to:

Critically review the report in question

Pay particular attention to the problem approach, the methodology chosen and to the interpretation/evaluation of results

Make annotations on the report of clerical errors, other minor errors, incomprehensible or ambiguous text

Complete this Opponent Record (use a computer or black ink)

In advance – at the time stipulated – give this record to the persons stipulated in the instructions for your exjobb subject.

Orally present your general opinion of and comments on the work during about 5 minutes after the author's presentation of the work

Put questions to the author of the report following his/her presentation: you may put forward the questions set down in the Opponent Record, or some of these questions, but it is also reasonable to expect the presentation to generate new questions.

Give the Opponent Record and the annotated report to the author at the conclusion of the seminar

You may contact the person responsible for the degree project, e.g. to test programs.

The Opponent Record can be completed either using a computer or manually. If writing by hand, use red or black ink and write distinctly. The Record copies must be legible but not necessarily aesthetically pleasing.

Master's projects vary considerably. Consequently, at times not all of the questions will be relevant to the project you are opposing. It can be appropriate to rephrase the questions to fit the project. You may also introduce one or two additional questions.

Attempt to answer the questions in the Opponent Record in relative detail. Answers such as **Yes** and **Good** are insufficient.

OPPONENT RECORD

Thesis compiled by

Fredrik Lilkaer & Christopher Tejlstedt

Title of thesis:

RB-PoW: A reputation based approach to cryptographic mitigation of denial-of-service attacks

Opponent:

Fredrik Bystam (bystam@kth.se)

Was it easy to understand the underlying purpose of the project? Comments.

That depends somewhat. The abstract does not in any way explain what Proof of Work (PoW) is. It also seems to suggest that the project was done in order to prove that PoW works rather than researching whether it actually does or does not. The rest of the report seems to deal with the latter.

The introduction contains a precise description of Proof of Work. Sadly, I found the explanation to be rather difficult, at least too difficult for me to understand right away. I had to do a google search and read up on PoW before I could continue. A simple example would have been perfect.

This particular version of PoW, RB(Reputation Based)-PoW is never explained explicitly in the introduction. That makes you feel a little lost from the start.

Do you consider that the report title justly reflects the contents of the report?

Yes, the title does describe the purpose of the report, and nothing else. It clearly states that the RB-PoW is a way to defend against DOS-attacks. RB-PoW should perhaps not have been abbreviated, though.

How did the author describe the project background? Was there an introduction and general survey of this area?

Yes, there is an explanation of the field and in what ways it has been implemented. Examples are given where PoW has been attempted both successfully and unsuccessfully. It is also explained what differs this project from previous work.

Still, though, the "reputation based" part of RB-PoW is not explained anywhere in the introduction. It is only mentioned.

To what degree did the author justify his/her choice of method of tackling the problem?

It is explained very precisely. It is clear what the purpose of the implementation is, and in what

way it is to be measured. The measurements are to be made using a testing suite, which is also mentioned briefly in the introduction.

It is also explained in what further ways the problem can be treated, but why these methods have been excluded from the study.

Did the author discuss the extent to which the prerequisites for the application of such a method are fulfilled?

There is an exhaustive assumptions section that precisely describes the environment in which these implementations are meant to work.

The authors describe how the scope of the project affects the assumptions. For example; the testing and solutions attempted in the project all affect the application layer of the OSI-model. It is explained how this evolves into specific prerequisites and assumptions regarding the attackers.

Is the method adequately described?

The method is throughly described, but it feels like it is spread across several headlines. There is no concise description of the actual approach from start to finish, but rather separate headlines describing the different pieces of this project (System architecture, simulation experiments etc..).

I found it difficult both the first and the second time I read the report to get a really good grip on how this study was to be performed and how the resulting data was to be compiled to come to a conclusion.

Algorithms used for these PoW puzzles are explained in great detail mathematically, but one can easily be lost amidst the rows of all the formulas. This is in the opening of section 2. The term sub puzzle is introduced as a way to normalise running times, but not explained how. One can guess what a sub puzzle is, but not in what way they would normalise run times.

There is only one piece of illustration present in the report. There is definitely room for some drawings explaining the most complex parts.

Has the author set out his/her results clearly and concisely?

Concisely, yes, but it would probably have been better with a description and an example that puts some piece of the result into perspective. In the current version, it's difficult to determine what the numbers mean with their very brief column descriptions.

Do you consider the author’s conclusions to be credible?

Given that the "Lessons learned"-section is equal to the author's conclusions, I do find the conclusions to be credible. Although, I am not sure I find all of them to be motivated in writing. Some conclusions feel like they are speculations rather than based on results.

What is your opinion of the bibliography? What types of literature are included? Do you feel they are relevant?

I find the bibliography to be very relevant. There are articles both supporting the thesis, as well as contradicting it, which gives the area more flavour and makes it more interesting.

Which sections of the report were difficult to understand?

The introduction comes to mind. Fundamental things such as RB-PoW are not described at all before it is described in detail in section 2.1. I found myself quite uncertain about what the study was about until I read the detailed description.

Also, the parts regarding algorithms in the methods are described in great mathematical detail, which in the long run comes down to looking very foggy. These parts could be described in different layers of abstraction so that you can dig deeper and understand more and more gradually.

Other comments on the report and its structure.

The headlines presented seem to me to be rather confusing. Section 1 is called "Introduction" and speaks for itself, but section 2, "Adapting Proof of Work", should perhaps have been called "Method" containing subsections describing how this project is to be performed.

The information is divided in logical pieces, but it is hard to keep track of what it is you are reading about.

What are the stronger features of the work/report?

It is very precise and exhaustive. I find it to be a very professional problem statement and conclusion. It is clear that this is a difficult subject that has been researched by two very appropriate authors. It is clear that this project has been performed in great scientific manner.

What are the weaker features of the work/report?

Since the subject is very difficult, it is also very difficult to follow. When some critical part is being described in a less than very evident way, one can easily get lost.

One reason for this is the lack of an intuitive report structure (Introduction, background, method…).

What is your estimation of the news value of the work?

According to the introduction, there have been articles written about the fact that Proof of Work does not work, which the author's seem to have proven wrong. In that sense, it feels a lot like high valued news.

On the other hand, the context and prerequisites in which this study has been performed in could mean that it becomes of less important in the general case.

Summarize the work in a few lines.

This study treated a very complex area, and did so using very sophisticated methods. It is evident that the authors are very competent people and that they have successfully tackled a subject very cutting edge relative to their current level of education.

The complexity of the project comes somewhat as an issue in the written presentation (the report), though. One can easily understand that the work has required some heavy thinking and problem solving. Understanding the exact methods is sadly rather difficult when reading it afterwards. Most people would probably need an oral explanation to get a grip of the exact work flow.

All in all, it is very scientific, but rather poorly explained.

Questions to author:

1. Do you find these methods to be as complex as I did?

2. How does the limitations of the project scope affect the news value in your opinion? Does the fact that only the application layer of the OSI has been analysed render this study less useful?

3. Is there any particular reason for this unique report structure?

4. How did you find out about conclusions like

"A non-linear diffculty model could potentially be more effective against large scale flooding type of denial-of-service attacks"

and

"The protocol could be improved by using bit-strings instead of byte-strings to make the diffculty levels more fine grained"?

5.

6.

Kerstin Frenckner, tel 08–790 9754, e-mail:. kfrenck@csc.kth.se2

February 12, 2009