KTH Computer Science
and Communication

Kerstin Frenckner, tel 08–790 9754, e-mail:. kfrenck@csc.kth.se2 February 12, 2009

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 Teljstedt

Title of thesis:

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

Opponent:

Thomas Sjöholm

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

The concept of *Reputation Based – Proof of Work* (RB-PoW) and the purpose of the concept was easy to understand. Presents the problem of DoS attacks and then how the RB-PoW acts to protect from such attacks.

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

The title reflects the content well without being to long or abstract. Summarize the contents accurately.

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

The introduction is clear, describing why DoS attacks can be a problem and what PoW is. After that the introduction to RB-PoW is presented. General survey of the area is presented in a nice way.

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

The justification of using RB-PoW is done smoothly by having the problem described and criticise the PoW solution to the problem and then presents the RB-PoW solution.

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

The prerequisites of the method is done nicely in the 2.2 assumptions chapter. In that chapter they presents prerequisites of the method in a clear way.

Is the method adequately described?

The method of the experiment is adequately described in the Simulation Experiments chapter. The RB-PoW implementation is definitively not good enough described.

With the information in this report it is possible to replicate the results provided that you have the software they used. The description of a puzzle, a concept very central to this report, is not adequately described. Puzzles are some sort of hash solving, but other then that it is very unclear.

Several functions, variables and operators are not adequately defined. Some undefined functions, variables and operators are the following:

P (without index; set of puzzles?),

$H(S_i \| P_i)$ (Some function of a hash? The h is equal to this function and later h is also sha2(x) for some x meaning that this is a sha2 hash? What does the "||" mean? Boolean "or"? Bitwize "or"?),

g(t, x) (the output is a puzzle, so it is a string? the t is undefined? The x is a random value between what values? How does g work?)

How does the difficulty integer d impact the hash? Does it impact the hash? Cannot see it as a parameter to any of the functions/hashes...

α in the $b_i = \alpha * \delta + (1 - \alpha) b_{i-1}$ formula is never defined and the ß in the $B_i = ß * \delta + (1 - ß) B_{i-1}$ formula is never defined.

The code blocks pasted needs to be more defined. What is the Param p in the function rp_scale_model? How is the cpu threshold cpu_thres defined/adapted? The code needs more description otherwise the code have no purpose.

The RB-PoW communication protocol is not defined, define it or remove the operation code numbers.

How and when the RB-PoW system interacts with the request is not adequately described. Maybe add that to the background?

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

The results is clear and concise in tables with good descriptive text.

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

The authors conclusions in the conclusions chapter are referring to the data presented in the tables in the result chapter to discuss the data. The conclusion is credible, discussing the result with the current implementation of the RB-PoW, the lessons learnt and future research in a sober way.

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

The bibliography is adequate. The types of literature includes: Lecture notes, conference papers, tech reports, official documents on large websites, workshop notes, standards from standard institutes, programming language website and books. The bibliography seem relevant.

Which sections of the report were difficult to understand?

The *2 Adapting Proof of Work* chapter was the most difficult to understand, specially the first part before the *2.1 RB-PoW Protocol* section. It contained lots of formulas that were not that good described and were in-text formulas, making the text harder to understand.

Other comments on the report and its structure.

The method were lacking to such degree that it is impossible to replicate the experiment, greatly making the report to suffer. Other than that it is a good report with good strutcutre.

What are the stronger features of the work/report?

- The language of the report is correct and mostly clear.
- The introduction, simulation experiment, result and conclusions were clear and easy to understand.

What are the weaker features of the work/report?

- The method
- Needs to be more precise in some contexts
- The use of letters as a concept is sometimes destroying the flow of the text as one have to check each letter several times before remembering what each letter is describing.

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

Basically saying the same thing as the work of Jeff Green et al. “Reconstructing hash reversal based proof of work schemes” from 2011 rendering the news value of this work to null.

Summarize the work in a few lines.

It is about an adaptive variant of PoW, a requirement of calculating some hash before the server handles the request. It is adaptive in the difficulty of the hash calculation required based on the global average frequency of these requests. The higher the frequency, the harder the hash problem and it is based on the global average.

This protection against DoS is better than non-adaptive proof-of-work. Reputation based scaling is a viable adaptive proof-of-work approach.

The report is adequate, lacking in the method but otherwise good, clear and precise.

Questions to author:

1.

Does the server store the service request during the solving of the puzzle? Does that make the server more vulnerable to request flooding attacks making the server store lots of requests and the adversary drop the puzzles and makes another request?

2.

How would you say that servers would protect themselves against attacks such as the *Server Draining Attacks* as it defeats the core concept of RB-PoW?

3.

How does servers protect themselves against DoS attacks today? Do they try at all?

4.

How come that the legitimate users on the PoW *Server Flooding Attack* have both longer solving and service times?

5.

6.