Review to the seminar paper ”Extending a universally composable cryptographic library” by Long Ngo.

Dan Bogdanov

April 16th, 2008

1 General evaluation

<table>
<thead>
<tr>
<th>Evaluation criterion</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>The paper is well readable</td>
<td>Rather yes than no</td>
</tr>
<tr>
<td>Language used in the paper is correct</td>
<td>More or less</td>
</tr>
<tr>
<td>The paper is logical and well structured</td>
<td>Yes</td>
</tr>
<tr>
<td>The general typeset of the paper is correct</td>
<td>Rather yes than no</td>
</tr>
<tr>
<td>The paper was interesting to read</td>
<td>Rather yes than no</td>
</tr>
<tr>
<td>The paper gives a good overview of the topic</td>
<td>Rather no than yes</td>
</tr>
<tr>
<td></td>
<td>(preliminaries are missing)</td>
</tr>
<tr>
<td>The material in the paper is mathematically correct</td>
<td>Rather yes than no</td>
</tr>
<tr>
<td>References to the external sources are presented correctly</td>
<td>Yes</td>
</tr>
<tr>
<td>All the relevant references are present</td>
<td>Yes</td>
</tr>
<tr>
<td>The formulae are typed correctly</td>
<td>Rather yes than no</td>
</tr>
</tbody>
</table>

2 Content evaluation

1. The seminar paper represents part of the author’s masters thesis. The topic is of interest to me as it is related to connections between theoretical and practical security.

2. The paper is structured as a description of the proposed library. Since the paper is still in its early stages, several parts are missing.
3. The paper is based on a few key articles with references to related papers. Given the topic of the paper, this is a justified decision. The missing parts will, no doubt, be added to the final version of the paper or the actual thesis.

4. The paper is typeset using \LaTeX. There are a few typesetting mistakes, like underscores which should be underscores, but are interpreted as subscripts (example page 9, gennonce).

5. I got an idea about the structure of the universally composable cryptographic library.

6. Since I did not know much about the universally composable cryptographic library, I really missed the preliminaries. Also I would have like to see at least a hint about the security proof for the extensions.

3 Propositions for improvement

1. The paper contains a number of misprints. The following list is not exhaustive:
   - page 1 - indistinguishability
   - page 7, in the definition of ports for the user - userporst\text{stan}
   - page 8 - idea system vs ideal system
   - page 11, three times - adversarial
   - pages 13 and 14, a copy-paste errors in section titles - encryption

   A speller would have found most of them and will probably find more.

2. The paper contains numerous style and grammar errors. There are too many to explicitly list. I list here the types of issues with an example:
   - Word compatibility. "Protocol verification is an essential work to guarantee the security of a certain protocol." vs "Protocol verification is an essential tool for guaranteeing the security of a certain protocol." "...must has..." vs "...must have...".
   - Time. "For a long time there are two methods for this job: formal and computational methods." vs "For a long time there were two methods for this job: formal and computational methods."
   - Word order. "Cryptographic protocol analysis is a hot research topic recently." vs "Cryptographic protocol analysis has recently been a hot research topic."
3. There were no mathematical errors, as there wasn’t a lot of math to begin with.

4. There are some typesetting errors:
   - Non-italicized variables, message $m$ on page 3
   - In the description of the library, some names cross the page margin.
   - Badly typeset underscore for gen_nonce on page 9.
   - Missing space on the top of page 15—"where $d_s, cvk..."

5. The article would be more readable if the language used was correct. Also, the lack of preliminaries makes it harder to understand.

6. The articles is missing preliminaries, proofs and several details. But the author acknowledges that in the paper.

7. Although the paper is too long for a seminar paper, I won’t suggest to remove anything, as the text is the basis for a thesis. However, I suggest that in the future the author focuses a seminar paper better.