On 25/04/18 22:33, Ben O'Neill wrote:

> I’ve attached the PDF. I’ve been working on this for quite some time,

> so it would be good to have some input from a fresh pair of eyes.

Some random comments while skimming through it:

Stylistic hints:

- somewhat erratic use of uppercase vs lowercase letters

("Asymmetric Cryptography, also referred to a Public-key cryptography")

- just general proof-reading, e.g. p12: "unlimited doors" -> unlimited number of doors"?

- Avoid the use of passive voice, especially at places where it would likely be

of interest \*who\* did something (i.e., you or someone else)

"Initially, the OpenCard framework was identified ..." ->

"Initially, I identified the OpenCard framework ...", etc.

Questions (that the dissertation perhaps ought to answer):

- Can you show some example dump of a protocol exchange, to give readers an idea

of how this looks like on the interface (i.e., number of bytes exchanged),

initially and with PB?

There should ideally be some example machine-generated program output

in the evaluation section or appendix, possibly even with timestamps,

along with all the related data needed to reproduce the result,

e.g. the keys you used in the examples.

Overall, it is clearly heading in the right directions, but still quite a number

of unfinished bits and sections that read more like bullet items then like

a finished report.

> Do you think there are any sections that don’t really need to be

> included, or that go into far too much depth?

Parts of the evaluation section repeat things that

you said already several times before. I would replace these with

hard data, e.g. program traces, timing measurements, code fragments,

protocol packets, etc.

As a rule of thumb, good editing should be able to remove about

30% of the words of a first draft, just by saying the same

with fewer words, cutting accidental repetition, and cutting

material that is not essential to enabling the reader to

follow and reproduce your work.

I certainly recall several sentence that merely said what

I had already read just a minute ago.

Reread the entire dissertation, mark with a green pen

on the margin paragraphs that are dense in technical information

(function names, protocol steps, crypto parameters,

command-line arguments, etc.), and with a red pen sections that

are far more handwavy and vague. Then focus on pruning/condensing

these red sections. You have plenty of both.

The best dissertations are usually well below the word limit.

> Incidentally, do you know if appendices count to the overall word

> length of the dissertation? I was thinking I could cut down the

> effective length of the dissertation by moving some parts that are

> only tangentially related (like the MIFARE problems) to an appendix

> section to reduce the length.

There are such rules, but I would first try to get along without them.

Markus