Master's thesis title: An Internet of Things Software and Firmware Update Architecture Based on the SUIT Specification
Master's thesis author: Simon Carlson
Reviewing student: Samuel Lindemer, lindemer@kth.se
Opposition date: May 23, 2019

Overall assessment

It's clear to the reader that you have good understanding of the necessary background and have made insights into what the possible solutions to the problems are. Your proof-of-concept experiment looks appropriate and seems to back up your claims. There is, however, a lot of repeated concepts and explanations throughout the paper that can easily be removed. Overall, the content is all there, but it's hard to parse in its current format. Additionally, I do think there should be some discussion of other software update mechanisms that currently exist (outside IoT), what works and what doesn't, and how, if at all, they impacted your design decisions. Why did you decide to follow SUIT? Since you also place a lot of emphasis on security from the start of the work, I think you should have a correspondingly strong analysis of the vulnerabilities in your own protocol.

Abstract

The abstract should be about half the length that it is currently. Try to be very concise and simply answer three questions: *What is the problem? Why is it a problem? How did you solve it?*

Introduction

The content here is good but there is a lot of repeated information from subsection to subsection, as well as some copying and pasting from the abstract, which I noted in my hand-written markup of the thesis. The ethics and sustainability section could be more concise and focused on the impact of your specific thesis work.

Subject area

I think there is more detail in the background than needed. For example, protothreads and EST-coaps are only tangentially related to your work, so they can probably be left out. Try to explain everything in the context of how it directly impacts the decisions you make in your methods. I think the background could be reorganized into three main categories: SUIT, CoAPs, and OSCORE. Restructuring it in this way and starting each section with "____ is relevant to this work because ____" would help the reader follow your thought process. It would also be helpful to briefly mention some approaches to the problem which you did not pursue, and why you did not pursue them. This would strengthen your argument and make your work sound more trustworthy.

Problem discussion

There is a lot of repeated information throughout the thesis; I think it's important that each heading only contains new information rather than saying "as previously discussed" and re-explaining. I get the impression that the thesis was written so that someone can read any individual section without needing to read the preceding sections for context. This makes reading the entire document through sequentially feel repetitive at times. Your figures make the text much easier to understand, and I think presenting those as early in the document as possible would help the reader a lot. Figure 2.1 nicely illustrates CoAPs but there is no illustration of OSCORE. I think the difference between the two is difficult to explain in writing, so an illustration would be helpful.

Boundaries

A discussion of the delimations of the work appears to be missing. As I was reading the work, I was anticipating some work regarding the actual local operations of a software update because of the title. It wasn't clear to me that this was purely about the actual downloading of an update and not the installation until about halfway through. I really think this needs to be clear from the beginning.

Methods

Your approach seems solid and compelling, but I think the presentation of what you did vs. what is background could be a lot clearer. For example, Table 2.1 shows the SUIT requirements and Table 4.1 shows what you decided to do. These look very similar but if you presented it as some sort of side-by-side or illustration, it would be much easier to understand. I found the thesis easiest to follow where you used bullet points and tables, but sections spanning four or five paragraphs feel somewhat unfocused.

There were a couple concepts that seem important but were not thoroughly explained. I am unclear on what you mean by an update “breaking” a certificate, or what “introspection” means in the context of your work.

Data collection

Again, just some organizational issues here. Page 62 is the first time that you are doing 30 executions for each test, but the experimental setup should be separated from the actual results. Why did you decide to present only the average times without standard deviations? It may also be worth pointing out that you work in an office with many people running experiments on these frequencies, so wireless interference is actually quite high. You might want to be more clear that your experiment is mainly a proof of concept that a design like yours can be implemented, and that there are many revision steps from a concept such as this to an IETF standard. Can you give the reader some idea of how much energy other tasks require so they have something to compare the results to?

Discussion

I think there should be a stronger focus on the security implications of your protocol. Throughout the paper, generalized references to the impact of an attack on an update system are discussed, but I think these may be fairly obvious to most readers. The abstract, introduction and background make it clear that security is one of the most important aspects of any solution to the problem you described, so your solution should have a correspondingly strong defense of why it is secure in its own section. What are the threats facing existing software update technologies? Are these threats present in your solution or are they fixed somehow?

Language

(See handwritten marked-up copy for thorough comments.)