Posudek *oponenta* diplomové práce

Jméno a příjmení autora posudku: Jan Kofroň

Jméno a příjmení autora práce: Martin Mašek

Název práce: Privacy issues of the Internet of Things

Vlastní text (sem prosím napište text posudku, délka textu posudku není omezena):

The goal of the thesis is to explore the privacy issues in the context of Internet of Things and provide a set of practices and approaches to both prevent privacy breaches and mitigate the impacts of privacy incidents in the sense of providing as few pieces of information as possible.

In the first part, the author describes the context of IoT and explains the principles of privacy. Then, he lists particular privacy protection methods and sketches simple scenarios, where they could be used. The scenarios often look artificial and unreal to me, which is unfortunate as there are many other, more realistic use cases (e.g., a device monitoring the movies a user watches and the temperature at his home at the same time). At several places, the author mentions the option of client-side computation. This is, however, a generally advantageous concept assuring the privacy, whatever information the data carries. Why this is mentioned just in some special cases (e.g. position)?

In the second part, the author describes usage of particular methods to protect private information and to avoid third parties to collect and, to some extent, deduce additional, unneeded information about users. The author introduces a simple library developed in the scope of the thesis that should help IoT designers to design and simulate scenarios and analyze privacy issues. He also provides two simple demonstration scenarios (including implementation) using the library. Here, I would expect much more elaborated demonstration than simple command line applications, since those are the only runnable results of the thesis.

The text of the thesis is written in English. Despite quite frequent language issues (cf. the list below), it is readable and usually easy to comprehend. A thing I do not like is overusing the bullet style, which makes the text hard to read.

Generally, except for the list of privacy protection methods, which are, however, not developed by the author of the thesis, I do not see a significant contribution; the implementation of the library (basically implementing the methods), however useful, comprises around 2kloc and just implements the (simple) methods protecting privacy of data described earlier. I would call it a simplistic implementation.

Overall, the contribution of the thesis is not significant, making it, together with the aforementioned issues, a border case. However, I still think that it should be defended as a master thesis.

Detailed issues (not a complete list, skipping some language issues):

Pg. 9: “This is will be helpful later…”

Pg. 10: “…number of devices is increasing form year to year…”

Pg. 10: “…getting rid of bottlenecks in real-time location of containers leading to inefficiencies…”? What kind of containers? What is the real-time location? What inefficiencies?

Pg. 18.: “We would like to what degree the method is deterministic…”

Pg. 19: Hashing – time is not a good salt – it changes over time and so the same data are hashed to different hashes. What is the reason then, to send the hash of the identity if it carries no information? Also, I do not understand the example…

Pg. 23: “A case in which we get dynamically generated data, know nothing about distribution and have no idea of origin of data is unlikely.” I am not able to parse this…

Pg. 35: Delay – the position example is not a good one: Either the position is close even after tens of second (I am in a city seeking for a restaurant) and then the delay does not help much, or the position changes quickly (traveling by car/train) and then the delay in request makes the response useless.

Pg. 46: “The purpose of measuring is to bill the households appropriately.” I do not think it is necessary to provide the data online for billing.

Pg. 46: Why forecasting is needed? The demonstration example should be described in much more detail as it looked artificial and ad-hoc as it is.

Pg. 48: “If the positional data are provided for a given interval, the first patter” – incomplete sentence?

Pg. 49: “…having an information that…”

Throughout the text: “…way how to…”

Doporučení k obhajobě:

Z výše uvedených důvodů práci *doporučuji / ~~nedoporučuji~~** k obhajobě.

Vynikající práce vhodná pro soutěž studentských prací	ANO ☐

Seznam soutěží studentských prací, viz http://www.mff.cuni.cz/studium/bcmgr/prace/

Pokud jste výše zaškrtli ANO, zdůvodněte prosím svůj návrh, případně uveďte konkrétní soutěž, pro kterou je práce vhodná (rámeček lze nechat prázdný, pokud za dostatečné zdůvodnění považujete text posudku):

V Praze dne: 1. 6. 2016

Podpis:**

** nehodící se škrtněte (vymažte)*
*** do SISu vkládejte formulář nepodepsaný (ve formátu PDF), podpis je potřeba doplnit až na vytištěný posudek.*