Summaries

Lakshay Badlani

May 8, 2015

Abstract

I read one research paper, based around Fab a content based, collaborative response based program and attended a research seminar hosted by Tamara Denning who works for the group known as TRUST. Here are summaries of both, including an explanation of a new concept, two insights and an oversight.

0.1 Fab

This paper, written by Marko Balabanovic and Yoav Shohman, is about a program designed to suggest articles to readers depending on specific criteria such as user interests, trending articles and similarity of material already read. One new concept that was introduced was how to combine two distinct systems (collaborative response and contest based systems specifically) in order to attain both of their relative strengths whilst also using one system to combat the others weaknesses and vice versa. For example the paper suggests that we create profiles based off content read and then compare it to others in order to connect similar profiles thus setting the stage for collaborative response. An insight made by the author are that many previous systems designed to suggest readings to a user are too simplistic in the sense that they rely on a singular criteria; for instance a purely content based approach doesnt appreciate other qualities of the documents namely aesthetics and "network factors such as loading time." Another insight made by myself is how important a program like this is especially given the time we live in with the amount of information constantly being uploaded to the Internet and how quickly tastes can change. However the oversight made by the authors concerns the features of the program, namely it doesnt support randomization. By this I mean that the users dont have the ability to read a randomly selected article so they are confined to their comfort zone and thus lose the chance to widen their reading horizons.

0.2 Trust Security Seminar

The talk was obviously focused on security with the particular emphasis given on “prevalent and emerging technologies” as it is these that are becoming more common in our everyday lives. As a result security breaches in these technologies might have very serious negative consequences for the person using them. One concept that was explained was the actual usage of pacemakers and their convenience. I learnt about how researchers were attempting build long-range WiFi capabilities into pacemakers so patients dont have to visit the hospital for checkups as regularly and about all the non-obvious drawbacks that come with this. This leads us on to the first insight made by the speaker: many of these implantable devices contain private information about the patient, their settings can be changed and the therapies they hold can be toggled on or off posing a threat to the wearers life. Thus there is a need for individualized security to make these devices more secure. Another insight that was made was that security is about tradeoffs; we cant maximally protect assets because of the associated costs such as time used to develop the machine and money spent on research towards to it. As a result it is a weigh up between the cost of security solutions and the value of human assets. Lastly an oversight made by the speaker regarding robots and their vulnerabilities is that many people dont have robots in their home just yet hence at the current moment their vulnerabilities may not pose as big of a threat as security breaches in medical devices such as pacemakers.