Willy Husted

10/16/14

CMSI 370

1. Introduction

Ubiquitous computing—also known by the colloquial term “The Internet of Things” (IoT)—refers to the vision of connecting any and everything from the physical world to the digital world of the Internet. The idea is that everything *not* currently connected to the Internet will one day be connected. IoT would involve devices and sensors of all different varieties placed on and in physical things, from tree roots to thermostats to human hearts. Phones were some of the first devices titled as “smart”; ubiquitous computing promises that label will reach to *all* things. Beyond the physical issues that will come with ubiquitous computing—such as the energy consumption of thousands of devices—there are several usability questions accompanying the rise of IoT. In this paper, I will be looking at ubiquitous computing with regards to new interaction paradigms, as well as privacy and authentication.

1. Background/Prior Work/Literature Review

Many academic articles have been published on ubiquitous computing, and a small percentage of those deal directly with privacy, authorization, and safety. In A Device-Centric Approach to a Safer Internet of Things, authors Chao Chen and Sumi Helal address the issue of more and more devices causing failures as they all connect to each other. They point to four categories of risk factors that leave devices vulnerable: hostile environment, interference, misuse, and internal failures (Chen and Helal 2). Interference deals with the issue of pervasive devices getting in the way of one another. They cite as an example that “airplanes ban the use of cell phones to avoid interferences to avionic devices” (Chen and Helal 2). This modern example speaks to a broader issue that Chen and Helal believe will gain importance as more and more devices become available via ubiquitous computing.

In IoT, communication and consistency among devices is essential to ensure the usability of the system. Chen and Helal address security and safety issues in their article, stating that there “are rules pre-defined or hardcoded in the application logic” to perform context-driven tasks like an alarm going off when a house is broken into. They believe this approach will not work in IoT because “asking users and programmers to specify rules for each and every potential risk scenarios is not a scalable approach” (Chen and Helal 2).

1. Methods

In *Some Computer Science Issues in Ubiquitous Computing*, author Mark Weiser addresses several usability issues for IoT, specifically interaction between users and varying screen sizes. One in particular is a speculation on how we will interact with large displays; he believes a pen will be the proper device. Weiser states: “we needed pens that would work over a large area (at least 60"x40"), not require a tether, and work with back projection” (Weiser 1993). He goes on to say that pens and their corresponding large displays would need to be suited for “casual use, no training, naturalness, multiple people at once” (Weiser 1993).

In IoT, computers (and therefore screens) will be everywhere. Mark Weiser discusses the issue of interacting with different sized screens, dividing the issue between two new device paradigms: pads (tablets) and Liveboards (large screens). He begins with the issues that arise from pads, saying “pads have a tiny interaction area -- too small for a keyboard, too small even for standard handprinting recognition” (Weiser 8). In this section, Weiser acknowledges the usability issue of inputing data into a device that is too small for a keyboard. He addresses this issue by explaining a new “method of touch-printing that uses only a tiny area and does not require looking. As drawbacks, our method requires a new printing alphabet to be memorized, and reaches only half the speed of a fast typist” (Weiser 8). This is a clear learnability issue for the ubiquity of pads; a new alphabet must be learned and then memorized. Once that occurs, Weiser notes the problem with another interaction metric: efficiency. After overcoming the difficulty of learning a new way to input data to a computer, Weiser admits that even an efficient user will only reach half the speed of a proficient typist. In Weiser’s vision of IoT, pads/tablets will be ubiquitous; however, he does not offer a viable way to input data from the user onto these various devices.

The second device that Weiser anticipates will dominate in IoT is a “Liveboard”, essentially just a very large screen. The immediate usability concern voiced by Weiser is the spatial issue of an enormous screen. He notes that current interaction principles may need to change, saying: “using conventional pulldown or popup menus might require walking across the room to the appropriate button” (Weiser 8). Weiser is justifiably concerned about applications not adapting properly to increasing screen sizes, and thus losing their usability. For example, a responsive web app would be difficult to interact with if menus and dropdowns merely grew to fit the screen. Instead, Weiser indicates that a shift in the way we interact with large screens—and therefore how we develop for large screens—needs to occur alongside the growth of ubiquitous computing. Furthermore, Weiser’s concern of having to walk across a room to achieve proper interaction contends with one of Bruce Tognazinni’s first principles of interaction design: Fitt’s Law (site asktog.com). Fitt’s Law, according to Tognazinni, states that “The time to acquire a target is a function of the distance to and size of the target” (**asktog citation**). While the size of a dropdown menu would be very large on a big screen, the distance would be so great that it would take a significant amount of time to access. Without developing a new way to interact with large screens, Weiser predicts that the usability metric of efficiency would decrease.

1. Discussion
2. Conclusions