Willy Husted

10/16/14

CMSI 370

1. Introduction

Ubiquitous computing—also known as “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, authentication, and security.

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, and how these notions affect usability. 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 across devices are 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. It would be more desirable for systems to automatically enact devices to mitigate and eliminate risky context” (Chen and Helal 2). To solve this issue, they believe devices ought to become more autonomous. In a smart home, for example, they state: “when a door is left open at night, a system should be intelligent enough to discover the door actuator and invoke the device to close the door” (Chen and Helal 2). This point illustrates the need for expedient communication between devices in order to remove risky context in IoT.

Another article that deals with privacy, authorization, and safety, in ubiquitous computing (and how these notions affect usability) is *Internet of Things and Privacy Preserving Technologies* by Vladimir Oleshchuk. Location privacy is one of the primary issues that Oleshchuk addresses. He states that “location is an important characteristic of almost any ubiquitous application since it is often considered as a contextual parameter that decision making in such applications is based on” (Oleshchuk 3). A user benefits from her device knowing her location, so that she may receive context-aware information. However, conflict arises because she “would prefer not to disclose her location to protect her against tracking” (Oleshchuk 3). The solution, according to Oleshchuk, is to “use secure multi-party computations and…3-way authentication” (3). Using cryptography and advanced authentication, Oleshchuk believes that location privacy can be preserved in the IoT.

Furthermore, Oleshchuk addresses the essential issue of access control with regards to ubiquitous computing. In a world filled with devices—some of which we may interact with only a handful of times—it is imperative that each device can make personalized decisions based on a user’s identity. Oleshchuk introduces a new approach to access control “called privacy preserving attribute-based access control” which “protects user identity and enforce access control where access is based on attributes” (Oleshchuk 4). In other words, a user must be the sole possessor of certain attributes in order to gain access to the desired system.

1. Methods

Of the articles I researched on ubiquitous computing with regards to privacy, authorization, and security, Vladimir Oleshchuk’s *Internet of Things and Privacy Preserving Technologies* is the most relevant and important for my paper. Oleshchuk addresses the issue of location privacy, a current concern with the increasing ubiquity of mobile phones. I agree with Oleshchuk when he determines that the issue of location privacy will only become more and more apparent as IoT progresses.

Regarding location privacy and mobile phones, authors Bastian Könings and Florian Schaub express their concerns in *Territorial Privacy in Ubiquitous Computing.* They begin by describing territorial privacy as a new method to “provide a more user centered approach [to privacy]”, a paradigm shift away from “an information centered approach where privacy is controlled by protecting particular information” (Könings and Schaub 2).s

1. Discussion
2. Conclusions