Usability and Security in Ubiquitous Computing

Willy Husted

10/21/14

Abstract: This paper addresses usability issues in the world of ubiquitous computing with regards to security, authorization, and privacy. Ubiquitous computing (or "The Internet of Things") promises to connect everything—and everyone—to the Internet. In this paper, I argue that ubiquitous computing will initiate a paradigm shift in the way users interact with devices. Machine learning will advance to a state in which a device's effectiveness is measured by its level of autonomy. As shared devices become more prevalent, authorization will simultaneously grow in importance. Current proposed methods of better authorization will harm the usability metrics of efficiency and satisfaction. No perfect method of authentication exists; however, it is necessary that a more secure and reliable method than text passwords be invented alongside the rise of ubiquitous computing.

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.