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.

2 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 [1]. 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" [1]. This modern example speaks to the broader issue of devices interference that Chen and Helal believe will gain importance as more and more devices become available in IoT.

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" [1]. 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" [1]. 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: "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" [2]. 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" [2]. The solution, according to Oleshchuk, is to "use secure multi-party computations and... 3-way authentication" [2]. 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" [2]. In other words, a user must be the sole possessor of certain attributes in order to gain access to the desired system.

3 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 smartphones. 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 smartphones, 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" [3]. The authors see smartphones as a sign of what is to come for ubiquitous computing: constant location tracking. They believe that the current issues of information privacy will not be nearly as important as personal privacy in the world of IoT, or "being in 'a state in which one is not observed or disturbed by others"' [3]. In a world full of devices and sensors, will there even be the opportunity to be by oneself? Or will technology always be there with us? While my paper centers on the issue of information privacy and security in IoT, Könings and Schaub address a more philosophical potential problem of "alone time".

Another article I consulted is *Some Computer Science Issues in Ubiquitous Computing* by Mark Weiser, an article based more on general usability issues than security, authentication, and privacy. 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" [4]. 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" [4].

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" [4]. In this section, Weiser acknowledges the usability issue of inputting 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" [4]. 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" [4]. 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 [5]. 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" [5]. 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.

4 Discussion

In Chen and Helal's article, they acknowledge that communication and consistency across devices will become more important in IoT. I agree with their observations in the article and can see the same issues of communication and consistency pointed out by the authors. I can imagine that, for example, all devices in a smart home should communicate effectively. When a person wakes up, the lights come on in his or her closet, which communicates to the kitchen floor to begin heating, and the coffee maker to begin brewing.

An interesting result of expedient communication is that, in a fully autonomous system, devices in IoT are at their best when we interact with them very little. In the early stages of owning a device, interaction will have to be frequent and detailed; but as machine learning becomes more and more accurate, I will be required to provide minimal information and my device will know what I want. It will learn my likes and dislikes, and my habits, both good and bad. I anticipate a drastic shift away from current interaction paradigms in which I have to tell my device—through keyboard input or my voice—what I desire; instead, by communicating with thousands of other devices and sensors recording information and exchanging data, my device will work autonomously for my benefit.

The issue of security, authorization, and privacy in ubiquitous computing is addressed in Vladimir Oleshchuk's article, and I agree with his call for secure multi-party computation

and multiple levels of authentication; however, I would like to take his thought one step further to point out possible usability issues.

In IoT, we will potentially interact directly with dozens of devices every day; indirectly, we may interact with hundreds of devices. A major challenge for this system lies in authenticating each person so that personalized information can be transmitted. Currently, there is no flawless method of authentication. Both hardware and software have no perfect way of confirming whether a user is in fact who she says she is. In *Comparing the Proof by Knowledge Authentication Techniques*, authors Stamati Gkarafli and Anastasios A. Economides from the University of Macedonia state that "text passwords represent the authentication method that is mainly used by all users today" [6]. While it is the most popular form of authentication, "text passwords are very vulnerable to 'dictionary attacks' (automated attacks using tools that can crack the passwords that are common words, names or dates)" [6]. Perfect authentication—knowing with certainty if a user is who she says she is—remains impossible; however, the current method of choice for authentication (text passwords) is far too insecure. Additional steps in authentication such as security questions provide greater security, but they come at the cost of usability.

In Oleshchuk's proposed model of 3-way authentication, the user must take numerous steps before he or she can properly interact with a device. Authentication is currently a usability issue; in general, the longer it takes for a user to be authenticated, the less happy he or she is with the interaction. Therefore, increased security measures via multi-step authentication will harm the usability metrics of efficiency and satisfaction. Even an advanced user can do little to expedite authentication, so the overall efficiency of the system will be downgraded. Furthermore, if it takes several seconds—or even minutes—to authenticate in the world of ubiquitous computing, users will be less satisfied with the experience. Authentication is already seen as a barrier of entry to engaging users with software. I anticipate that, if security remains a crucial aspect of technology, expedient methods of authentication must be implemented to achieve high efficiency and satisfaction.

5 Conclusions

The Internet of Things promises a world in which computing is ubiquitous. Both seen and unseen sensors and devices will constantly be gathering data, transferring data across devices, and presenting data to users. In this shared world of computing, communication without interference is necessary for users to properly interact with devices. Chao Chen and Sumi Helal present this idea in *A Device-Centric Approach to a Safer Internet of Things*. Vladimir Oleshchuk's *Internet of Things and Privacy Preserving Technologies* addresses security, authentication, and privacy in IoT. He cites cryptography and advanced forms of 3-way authentication as reliable methods for ubiquitous computing. In this paper, I extended his research to bring to light usability issues in terms of authentication; specifically, how the metrics of efficiency and satisfaction will be harmed by multi-step au-

thentication. *Territorial Privacy in Ubiquitous Computing* by Bastian Könings and Florian Schaub addresses personal privacy in a philosophical light: will alone time exist in a world overrun by sensors and ever-present devices? With the help of other sources on usability in IoT, I conclude that a paradigm shift in interaction will occur. Emphasis will be placed on minimizing interaction time with a device, with the focus on autonomous computing via machine learning. From a security, authorization, and privacy viewpoint, I am able to conclude that the current method of authorization—text passwords—is too insecure to be a viable option in IoT.

References

[1] Chao Chen and Sumi Helal, *A Device-Centric Approach to a Safer Internet of Things*. ACM, New York, NY, 2011.

[2] Vladimir Oleshchuk, *A Device-Centric Approach to a Safer Internet of Things*. IEEE, New York, NY, 2009.

[3] Bastian Könings and Florian Schaub, *Territorial Privacy in Ubiquitous Computing*. IEEE, New York, NY, 2009.

[4] Mark Weiser, *Some Computer Science Issues in Ubiquitous Computing*. ACM, New York, NY, 1993.

[5] Bruce Tognazinni, *First Principles of Interaction Design (Revised and Expanded)*. askTog, 2014.

[6] Stamati Gkarafli and Anastasios A. Economides, *Comparing the Proof by Knowledge Authentication Techniques*. International Journal of Computer Science and Security, 2010.