

Privacy and Information Integrity in Wearable Computing and Ubiquitous Computing

Jennica Falk and Staffan Björk

PLAY research group, The Interactive Institute
c/o Viktoria Institute, Box 620, 405 30 Göteborg, SWEDEN
<http://viktoria.informatik.gu.se/groups/play/>
{jennica.falk,staffan.bjork}@interactiveinstitute.se

ABSTRACT

Wearable and ubiquitous computing are two computing paradigms with different views on privacy and information integrity. We present terms that help provide a framework for understanding these, and describe a prototype device that combines attributes from both, challenging presumptions about these paradigms. By looking at narrow application areas, we argue that it is possible to find applications that merge wearable computing and ubiquitous computing.

Keywords

computing paradigms, privacy, information integrity, wearable computing, ubiquitous computing, hybrid systems

INTRODUCTION: TRANSFORMING THE PC

A number of computing paradigms have emerged that transform the personal computer (PC) in general and the desktop PC in particular. While they differ in approach and terminology, they essentially promise the same thing - to free the user from the boundaries of the desktop and from the limitations of the PC user interface. The *ubiquitous computing* (ubicom) [8] paradigm offers invisible and omnipresent computers in our surroundings, which we effortlessly can access wherever we are. The *wearable computing* [3] paradigm aims to turn the PC into a piece of clothing, to function as an extension of our body and mind.

To distinguish between the paradigms, one could say that when wanting to transform the PC to fit new situations, one can take either one of two approaches. Either we move the PC closer to the user, or even make it a part of the user. Or, we move it into the environment, away from the desktop, hiding it from the user. The wearable computing advocates take the first approach, to create the 'truly personal computer.' Ubiomp advocates take the second approach, to make the personal computer less personal. The two paradigms take different approaches regarding computer design, as well as how these computer systems handle issues of privacy and information integrity.

This paper presents some terms that help provide a framework for understanding and describing wearable computers and ubiquitous computing environments. This is important both because it is useful to be clear on terminology, and because such a framework can aid the design and description of hybrid systems, or systems that belong in one paradigm but has features from the other.

PROBLEM: THE INTEGRITY OF INFORMATION

If information has *integrity*, it is not being misused, abused or otherwise used in a way that its owner could disagree with. This is related to, but different from the term privacy,

which involves the concealment of information, to completely remove it from public view. One of the prime challenges for computer systems involve maintaining this integrity of information. Ubiomp environments have given rise to concern about keeping sensitive information (e.g. information about user's location or activities) on centralized systems. Similarly, the encapsulating [3] property of wearable computers, i.e. that it hides the user's actions, intentions, and recordings, have made people uneasy about wearable computers as well.

When the capture or distribution of information is always initiated or controlled by the owners of that information [cf. 4], the problem of information integrity is mitigated. However, if users need to make explicit statements or requests to ubiomp systems (e.g. regarding location or actions), the desired invisibility of ubiomp is difficult to achieve. Similarly, if a wearable computer user needs explicit permission from a subject each time he or she wants to collect or recall information about that subject, the empowering functionality of a wearable computer is lost. Thus, if owners must maintain control of their information, the functionality of both approaches is greatly restricted.

In order to suggest a solution to these problems, we introduce some terms that highlight connotations associated with the paradigms. In the following, the systems we discuss are assumed to be general-purpose systems, hence not dedicated to one narrowly specified area of use.

Ubiquitous computing: *communal and public*

In a ubiomp environment, users share the same computational resources. Hence, these resources are *communal*, in the sense that no specific person can claim ownership. But, the fact that all computation and information is contained in the environment causes concerns about information integrity. Therefore, it makes sense to organize and distribute information that is *public*, i.e. pertains to more people than one. Examples can be found in "smart room" applications used to support for instance collaboration. This is manifested in a number of systems [cf. 6], suggesting the connotation that communal systems should provide public information or services.

Wearable computing: *personal and private*

Wearable computers are single-user systems. They encapsulate the user, thus making them highly *personal* devices. Because outsiders can not interact with the system, the information can not be shared. Therefore, it makes sense to store and present information that is *private*. Examples of such private information are e-mail or personal notes. Many wearable computing applications [cf. 5, 3] are designed to

© Copyright on this material is held by
the author(s).

host private information, suggesting the connotation that systems and devices that are personal should handle private information or services.

SOLUTION: BREAKING THE CONNOTATIONS

By looking at narrow application areas, we argue that one can find instances which break the personal-private and communal-public links between technology and information, while mitigating inherent information integrity issues.

Our prototype, the *BubbleBadge* [2] is designed to illustrate this point. It is a wearable computational device designed as a brooch with an embedded display. Due to its design, it effectively turns the concept of a wearable computer inside-out, transforming the wearable computer's private display into a public one, with the effect that the visual interaction with the device is shifted from the wearer to the viewer. This interaction takes place in face-to-face situations.

The *BubbleBadge* is equipped with an infrared (IR) eye that detects other *BubbleBadges* in its line-of-sight. When two badges detect each other, each collects information from a server using wireless communication, which is then displayed on the other device. The information may be addressable to a specific person but is non-sensitive. Therefore, it does not have to be private. To explore such an information space, we have developed two services:

The first service checks the *BubbleBadge* wearer's mailbox for new e-mail. If there is a new message, the *BubbleBadge* sends a notification message to the *BubbleBadge* within its line-of-sight. It does not send the e-mail message, only a standardized 'You have NEW e-mail!' message. In this aspect, the information that the *BubbleBadges* handle, is represented by abstract notification messages, rather than the information itself. Thus, no sensitive information is contained within the communication. In addition, the information is displayed only in face-to-face situations. The second service involves public announcements broadcasted from the server. In this case, the receiving *BubbleBadges* displays messages even if no other *BubbleBadges* are within line-of-sight. Because the information in this case is public, and does not address to a specific person, it can be displayed on all *BubbleBadges* within the server's range. In addition, people who are not wearing *BubbleBadges* can in this can take part of the public message.

The *BubbleBadge* is wearable, and thus personal, because it is worn by a person and that it continually performs computation for that person. However, it does not display information to its wearer, but instead to its viewers. This implies that if a person wants to view the results of his or her *BubbleBadge*'s computations, he or she needs to find another device. Secondly, *BubbleBadges* utilize human mobility to make themselves ubiquitous, or rather, components of ubicomp environments. They proactively collect and display information without violating their wearers' integrity.

RELATED WORK

The *Meme Tag* [1] is a wearable display device worn around the neck and like the *BubbleBadge*, its display faces a viewer rather than its wearer. The *Meme Tags* host text messages that can propagate over a "network" of *Meme Tags*. The tags exchange information and if one *Meme Tag* has a

message that the other does not have, the wearer of that other device is offered to accept a transfer of that message. The *Meme Tag* is proactive in that it initiates communication with other *Meme Tags* without explicit user action, but ultimately the user authorizes the message transfer by explicitly pressing a button. Hence, no messages can propagate over the "network" unless users specifically agree to host them and, in fact, this is the main idea behind the *Meme Tag* application.

The *Active Badge* [7] is a ubicomp application for locating people within a physical environment. People wear badges equipped with IR transmitters that communicate their wearers' presence to IR beacons mounted throughout the physical space. This location information is made available on displays where name and location of *Active Badge* wearers are presented. The *Active Badge* is related to our discussion because it deals with a narrow application area, i.e. providing location information. However, location information is private and can be considered sensitive, and because this information is made public, the system may give rise to concern about integrity of information.

CONCLUSION

Wearable and ubiquitous computing are two fundamentally different approaches to computing beyond the desktop. They are different not just in how they transform the PC ("closer to the user" or "away from the user") but also in how they handle the integrity of information. However, some of the theoretical assumptions about the differences between ubiquitous and wearable computing are possible to override in practice. As we have shown, there are applications and devices that challenge the traditional presumptions about wearable and ubiquitous computing. We claim, given a narrow application area, that it is possible to create new systems, applications and devices that belong to one of the computing paradigm but that include features traditionally associated with the other. We have distinguished between personal-private and communal-public and believe that by breaking these connotations, the design space of computing beyond the PC can be further expanded and explored.

REFERENCES

1. Borovoy, R., et.al. *Meme Tags and Community Mirrors: Moving from Conferences to Collaboration*. In *Proc. of CSCW '98*, ACM Press, 1998.
2. Falk, J. and Björk S. *The BubbleBadge: A Public Wearable Display*. In *Extended Abstracts of CHI '99*, ACM Press, 1999.
3. Mann, S. *Wearable Computing as Means for Personal Empowerment. Keynote Address at ICWC '98*, 1998. Available at: <http://wearcam.org/icwckeynote.html>. Last visited: 09/12/99.
4. Moran, T. P., et.al. *Design and Technology for Collaborative: Collaborative Collages of Information on Physical Walls*. In *Proc. of UIST '99*, ACM Press, 1999.
5. Rhodes, B. *The wearable remembrance agent: a system for augmented memory*. In *Proc. of ISWC '97*, IEEE Computer Society, 1997.
6. Streitz, N., et.al. *i-Land: An interactive Landscape for Creativity and Innovation*. In *Proc. of CHI '99*, ACM Press, 1999.
7. Want, R., et.al. *The Active Badge Location System*. In *Transactions on Information Systems*, Vol. 10, No. 1, pp. 91-102, ACM Press, 1992.
8. Weiser, M. *The Computer for the 21st Century*. *Scientific American*, Vol. 265, No. 3, pp. 94-104, 1991.