Analysis of Privacy Threats in Ubicomp Applications

Manas Kumar Yogi[1] Lakshmi Pavani Cherla[2]
[1]Assistant Professor [2]B.Tech Student
[1,2]Department of Computer Science and Engineering
[1,2]Pragati Engineering College, Kakinada, Andhra Pradesh, India

Abstract— Ubiquitous computing (ubicomp) is a post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities. In the course of ordinary activities, someone "using" ubiquitous computing engages many computational devices and systems simultaneously, and may not necessarily even be aware that they are doing so. This model is usually considered advancement from the desktop paradigm. More formally Ubiquitous computing is defined as "machines that fit the human environment instead of forcing humans to enter theirs."This paradigm is also described as pervasive computing, ambient intelligence, where each term emphasizes slightly different aspects. This paper presents the environment present in ubiquitous computing, its design features, security considerations and tradeoffs while implementing such features.

Key words: Ubiquitous, Privacy, Mobile, Ad-hoc, Social

I. INTRODUCTION

Ubiquitous computing (Ubicomp) is a concept in software engineering and computer science where computing is made to appear everywhere and anywhere. In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. The underlying technologies to support ubiquitous computing include Internet, advanced middleware, operating system, mobile code, sensors, microprocessors, new I/O and user interfaces, networks, mobile protocols, location and positioning and new material. Over the last few decades there has been tremendous growth in the area of pervasive and ubiquitous computing. During this era, various portable devices have been invented which are capable of performing various complex operations while keeping in view of the needs of users. These devices are being used in wide varieties of applications such as health monitoring and diagnostic systems, safety alarms, intelligent transport systems and environment monitoring.

But as these devices are vulnerable to various types of attacks (inside and outside) and threats, secure communication between them is of paramount concern in the pervasive and ubiquitous computing environment. This is mainly because of the direct interaction of these devices with the Internet, which is an open environment for information dissemination using these devices. Additionally, because to the lack of pre-deployment infrastructure due to resource constraints in these devices, the research community faces new security challenges to provide efficient solutions for secure communication with practical aspects.

The success of Ubicomp development requires the understanding of possible problems, however, and safeguarding against them, including safeguarding against possible privacy implications. There is no doubt that the notion of privacy alters with time , technology , innovations .There are very important differences between past and future technologies, however, which could change our lives more quickly than we could possibly adapt our understanding of the world, human behavior , ethics and laws to the new technologies:

(1) Past technologies were largely controlled by a human, whereas future technologies will be capable of automatic actions.

(2) Large-scale accumulation of data in a digital form will no longer require manual (slow) human work in order to connect information from different sources, so that it may be easier to assemble the full life story of a person in the future than it was to find scattered pieces of information in the past.

(3) Modern devices are smaller in size, more reliable and move closer to the human body than was the case in the past, and it is proposed that these could be embedded into clothes, watches or jewelry.

Ubiquitous computing applications are often proposed without considering privacy issues, whereas existing privacy enhancing technologies mainly have been developed form networked applications and, thus, are not always applicable to emerging applications for smart spaces and personal devices, especially because the users and their data are not spatially separated in such applications. The success of Ubicomp development also requires the understanding of possible problems, however, and safeguarding against them, including safeguarding against possible privacy implications.

Ubiquitous computing is about networked microprocessors embedded in everyday objects: not just cellphones and home appliances but also books, bookshelves, bus stops and hotels--all entities interacting to each other over wireless links. Hundreds of internet-enabled computers per human being, none of them resembling a conventional keyboard-and-monitor machine. This future is closer than we might imagine.The insecurity of networked PCs is notorious. If the ubicomp systems we deploy in our homes, offices, shops and vehicles are as vulnerable as today's PCs, the risks for society will be catastrophic. In this paper we analyze the threats to privacy, depending on real world application settings and the choice of technology; and present few design guidelines for the choice and development of technological safeguards against privacy threats.

II. CHARACTERISTICS OF PRIVACY FEATURE IN PHYSICAL WORLD

Privacy protection requires an understanding of how new technologies change the ways that have developed in the physical world, where personal privacy is protected by the following borders:

All rights reserved by www.ijsrd.com

A. Natural Borders:

A natural border is a physical border shielding the true feelings of a person such as walls, clothing, darkness, facial expression.

B. Social Borders:

This refers to trust and expectations with regard to confidentiality in certain social groups, such as family members, doctors and lawyers.

C. Spatial Or Temporal Borders:

This border includes expectations by people that parts of their lives can exist in isolation from other parts, both spatially and temporally.

1) Borders Due To Creation Of Interfaces Or Transitory Effects:

This contains expectations that certain action or spontaneous utterances will soon be forgotten or simply unnoticed because of limitations on people's attention and memory. These borders are bi-directional, that is, people expect these borders not only to protect the person's feelings, appearance, actions, and so forth from the outside world, but also to protect the person from intrusions by the outside world. Physical borders are perhaps perceived as most reliable. Concerning social and spatial borders, people perceive them as not so strong. In general terms, the stronger is the personal belief that a certain border is reliable, the more difficult it will be to adapt to its violation by a new technology. Recent experiments in the research area of computer-supported collaborative work suggest that adaptation is difficult.

III. ISSUES IN PRIVACY PROVISION

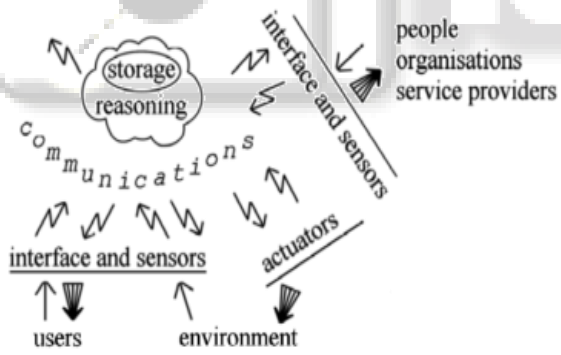

Fig. 1: Interfaces involved in Ubicomp

Privacy problems essentially fall into three major groups, the best-known of which concerns problems associated with information flow from the user, that is, due to the acquisition, transmission, and storage of personal data in large quantities. Most privacy-enhancing technologies are being developed for the protection of personal data in networked applications, but new Ubicomp applications present new challenges.Memory aids and recordings of work meetings imply the storage of raw video data, which violates personal expectations regarding the limits of human's attention and memory. There are two reasons for these problems.First, as work in the computer-supported cooperative activity domain has shown, humans are not used to environments full of sensors, and continue to behave according to their expectations regarding their privacy in the real world. The second reason is the blurring of boundaries between "traditional" application domains. The second group of privacy problems concerns those caused by linkages between different kinds of data . For example, it has been proposed that a personal memory aid should not record everything, but instead, it should measure the personal arousal level via skin conductivity sensors and other physiological sensors and record only the exciting scenes .The third group of privacy problems are those caused by information flow towards the users, either because technology-initiated communication intrudes into personal life, because the content of the information can disclose private information,or because actuators fail . Intrusions of technology into personal life can happen when an application interacts with people or when an application does not allow people to escape communication with others. Currently, it is easy for a person to say that he missed a phone call because the battery in his mobile phone was empty, or because of street noise, and so forth, but will it be as easy to avoid undesirable communications in the future, when communication is embedded in clothes and battery life is longer? This group of problems is the least studied of all, and Privacy Enhancing Technologies dealing with these problems are almost non-existent. What is also important about this group of problems is that technology-initiated communications can reduce user acceptance or act as a hindrance to personal development.

IV. TRADE OFFS IN PRIVACY ENABLED TECHNOLOGIES

We suggest that the most important safeguards are the following:

A. Intelligent Reasoning Capabilities:

Advanced artificial intelligence algorithms capable of recognizing sensitive data in order to avoid recording or publishing it, for example, algorithms capable of intelligent online summarizing of audio recordings (online conversion of a meeting audio stream into a text document, including only working discussions), algorithms capable of detecting that persons in a video or photo are naked or kissing, algorithms capable of adaptation to the user's ethics and culture (a photo of a Muslim woman with her head uncovered is private, while for the majority of Finnish women this would be nothing special) and so on. To some extent these capabilities can be implemented as common-sense rules, such as "if a person is alone, or if there are only two persons in a room, the probability of discovering confidential data is higher than if there are a larger number of people." In addition, algorithms for detecting unusual patterns of copying and processing of personal data are needed (e.g., if a new back-up is made soon after the previous back-up it may indicate data theft, and an alarm should be given), because these would also be of help when a person authorized to work with the data is dishonest, unlike other access control methods, which work mainly against outsiders.

B. User-Friendly Security:

Advanced access control and security methods, such as frequent unobtrusive context-aware authentication of users. Different user verification methods should be chosen, for example, depending on the application that a user wants to access, or on the user's location and behaviour; access to a

All rights reserved by *www.ijsrd.com*

calculator application should not require user effort , whereas access to personal memory aid data should be allowed only to the data owner. Thus, the current "once and forever" password-based user verification on mobile phones, which facilitates unauthorized use when the owner is in another room, for instance, should be replaced with continuous unobtrusive user verification, for example, based on user behavior or voice recognition, and on stronger authentication methods if unobtrusive authentication fails but access to sensitive data continues to be requested. In general terms, we suggest that security should be a fairly effortless matter for users and should be enforced. We suggest this by analogy with control over technical conditions in personal cars and the security enforced with regard to financial operations, because future Ubicomp scenarios envision personal devices that perform life-critical tasks. A malfunctioning personal device could fail to notice a health crisis on the part of the device owner, or fail to communicate this to the doctors, for example, and it could also create threats to other people; for instance, if it sends a lot of spam and malware to surrounding personal devices it can significantly slow down their operation and hinder their performing of the tasks required of them. Work on user-friendly authentication is an emerging research area. Current work is mainly concerned with biometrics, which is not a perfect solution, because of possibility of spoofing biometric sensors. Thus, we suggest that biometric modalities which carry a high danger of identity theft should be used cautiously and only with aliveness detection, and that a fusion of several not so privacy-threatening biometric modalities should be used as a primary or complementary means of authentication.

C. Communication Protocols Which Do Not Use Unique Device Identifiers:

It is easy to link a device ID or a smart object ID to a user and to track the user's actions. Communication protocols which hide the very fact of communication would be an ideal case, because a lot of information can be acquired by tracking who communicates with whom. For example, it can be concluded from the fact that a person has started to visit the Web page of a certain bank that that person has opened an account at this bank, and a false request to update a recently created account in this particular bank has higher chances of succeeding than when sent to an established client of the bank, or to a client of another bank.This safeguard has the drawback that it would hinder the discovery of users with malicious intentions or with malfunctioning personal devices sending out spam and viruses, but this problem can be partially solved by means of good firewalls and anti-virus software, which would protect against malware (see "user-friendly security" bullet). In cases where the detection of users' IDs is important, these communication protocols cannot be used (e.g., some applications can require the using of IDs in communication protocols), but their usage should not be a common practice because large-scale logging of everybody's actions is not likely to improve security in society, as pointed out by few security experts.

D. Secure.AD-Hoc Communications:

If a device owner enables ad-hoc Bluetooth communications, for example, the sending of a large number of requests to this device can slow down its operation or even exhaust the battery. This is not a direct threat to privacy, but it might engender privacy if the encryption of personal data becomes delayed, and it is definitely a violation of the "right to be left alone" in cases where the user cannot simply ignore incoming spam because he is expecting an important message.

E. Encryption For Untrustworthy Platforms:

It is not all functions can be executed in encrypted form. Instead, it is common to decrypt the code and the data before execution, which allows spying.

F. Unified, Concise User Interface Methods of Maintaining User Awareness:

About the functionality of the application and its privacy threats, possibly in graphical form (e.g., similar to road signs). A warning about video cameras is currently placed on the doors of shops (although with no information as to whether video data is stored or not, or for how long), but other Ubicomp technologies would require similar icons.

G. More Detailed Transparency Tools For Awareness In Average Non-Technical Users:

Regarding security risks, the correct usage of anti-virus and firewall applications, the dangers of data collection and the accepting of ad-hoc messages from unknown devices, and so on. Since users do not want to spend much time on security education, these tools and their user interfaces should be really intelligent and work "just in time." Currently, it is too easy for users to make mistakes (it is often too easy to ignore important questions that all look the same, and click yes without even reading a security-related question). For example, the current practice of asking users whether they agree to "accept temporarily, for this session," a security certificate regarding a certain Web site is not really helpful, because the same question is used for all Web sites, and it is not linked to other data regarding the website in question.

H. Recovery Means:

First, if somebody's personal data was compromised (e.g., a fingerprint was forged), it is necessary to switch quickly and easily to a new authentication procedure in all applications (home, work, smart car, banking, etc.), unlike the current situation, in which recovery from an identity theft requires significant efforts on the part of the victim and can harm that person's reputation. Second, if a personal device is lost, the personal data contained in it can be protected from strangers by security measures such as data encryption and strict access control. However, it is important that the user does not need to spend time customizing and training a new device (so that denial of service does not occur). Instead, the new device should itself load user preferences, contacts, favourite music, and so forth, from a back-up service, probably a home server. We suggest that ways be developed to synchronize data in personal devices with a back-up server in a way that is secure and requires minimal effort from the user.

All rights reserved by *www.ijsrd.com*

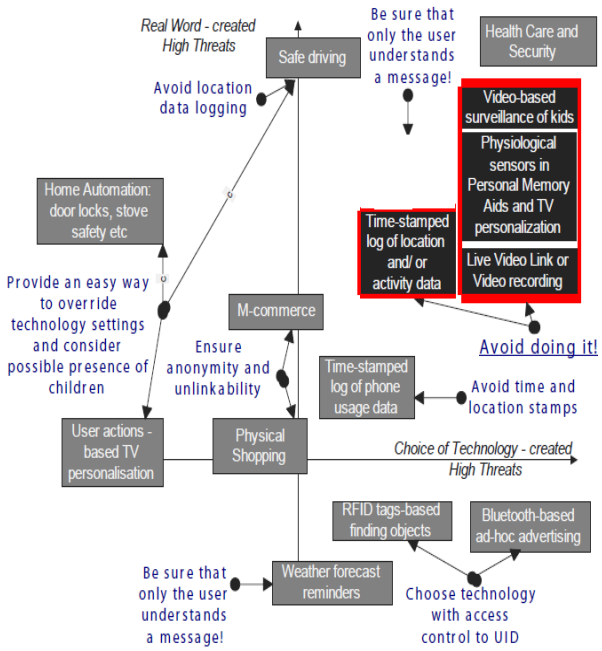

Fig. 2: Examples of levels of privacy threats in ubiquitous computing

V. CONCLUSION

In this paper we have analyzed the privacy threats in an operational ubiquitous computing environment. Characteristics of interfaces to be designed for an ubiquitous computing environment are also considered with relevant discussion on their merits and demerits. A discussion on security aspects in such environment is also discussed with considerable threats in each interface environment.

VI. REFERENCES

[1] Bellotti, V., & Sellen, A. (1993). Design for privacy in Ubiquitous Computing environments.Proceedings of the The Third European Conference on Computer Supported Cooperative Work (ECSCW'93) (pp. 77-92).

[2] Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., & Rohs, M.(2005). Social,economic, and ethical implications of Ambient Intelligence and Ubiquitous Computing. In W. Weber, J. Rabaey, E. Aarts (Eds.), Ambient Intelligence (pp.5-29). London: Springer-Verlag.

[3] HiSPEC project (2002), Privacy enhancing technologies: state of the art review,version 1. HiSPEC Report. Retrieved on March 1, 2006.

[4] Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., & Burgelman, J.-C. (2001).Scenarios for Ambient Intelligence in 2010. Institute for Prospective Technological Studies (IPTS), EC-JRC, Sevilla.

All rights reserved by *www.ijsrd.com*