International Journal of Innovative Research & Growth
A Peer Reviewed Journal
ISSN: 2455-1848
Journal homepage: http://www.ijirg.com/ijirg/
Volume: 12 Issue: 2, April 2023

Security challenges and requirements in ubiquitous computing

Sandeep Kumar Tiwari[1*], R. P. Sarang[2]
[1,2,3]Vikrant University, M.P., India
E-mail: sandeep72128@gmail.com
* Corresponding Author

Article Info
Received 12 February 2023
Received in revised form 15 March 2023
Accepted for publication 20 April 2023
DOI: 10.26671/IJIRG.2023.2.12.101
Citation:
Tiwari, S. K., Sarang, R. P. (2023). Security challenges and requirements in ubiquitous computing. *Int J Innovat Res Growth*, 12, 11-16.

Abstract
Pervasive computing environments with their interconnected devices and services promise seamless integration of digital infrastructure into our everyday lives. While the focus of current research is on how to connect new devices and build useful applications to improve functionality, the security and privacy issues in such environments have not been explored in any depth. While traditional distributed computing research attempts to abstract away physical location of users and resources, pervasive computing applications often exploit physical location and other context information about users and resources to enhance the user experience. The need to share resources and collaborate introduces new types of interaction among users as well as between the virtual and physical worlds. In this context, it becomes difficult to separate physical security from digital security. Existing policies and mechanisms may not provide adequate guarantees to deal with new exposures and vulnerabilities introduced by the pervasive computing paradigm. In this paper we explore the challenges for building security and privacy into pervasive computing environments, describe our prototype implementation that addresses some of these issues, and propose some directions for future work.
Keywords:- Pervasive Computing, Trust, Privacy, Security, context-awareness, transparency, unobtrusiveness, scalability, authentication, access control, smart spaces, scalability, interoperability, heterogeneity

1. Introduction

We are witnessing the birth of a revolutionary computing paradigm that promises to have a profound effect on the way we interact with computers, devices, physical spaces, and other people. This new technology envisions a world where embedded processors, computers, sensors, and digital communications are inexpensive commodities that are available everywhere. This eliminates time and place barriers by making services available to users anytime and anywhere.
Pervasive computing will surround users with a comfortable and convenient information environment that merges physical and computational infrastructures into an integrated habitat. This habitat will feature a proliferation of hundreds or thousands of computing devices and sensors that will provide new functionality, offer specialized services, and boost productivity and interaction. Context-awareness will allow this habitat to take on the responsibility of serving users, by tailoring itself to their preferences as well as performing tasks and group activities according to the nature of the physical space. We term this dynamic, information-rich habitat an “active space.” Within this space, individuals may interact with flexible applications that may follow the user, define and control the function of the space, or collaborate with remote users and applications. With growing concern about privacy in pervasive computing environments, considerable research has been conducted focusing on various aspects. Solutions and models put forth by this research address specific challenges of the problem. In this paper, the discussion will focus on the characteristics of the problem and how the works done in this field addresses these challenges.
The realization of this computing paradigm is not farfetched. An average person today already owns vast numbers of consumer devices, electronic gadgets, and gizmos that already have processors, microcontrollers, and memory chips embedded into them, like VCRs, TVs, washers and dryers. The vehicles we use on daily basis already have a large number of embedded computers handling different subsystems of the vehicle, like ABS (Anti-lock Braking System) and ESP (Electronic Stability Program). Technologies like Bluetooth [1] and Wi-Fi [2] make it possible to embed networking capabilities into any small devices without hassle. In effect, these technologies help make networking much more general and achievable even on elementary devices, like toasters and paperclips.

In Section 2 we explore the salient features of pervasive computing, Section 3, and 4 we describe the challenges and requirement for building security, privacy into pervasive computing environments. In Section 5 list some challenges for protecting privacy in pervasive computing and Section 6 we propose some directions for future work and conclude.

1.1 The Problem

Current research in pervasive computing focuses on building infrastructures for managing active spaces, connecting new devices, or building useful applications to improve functionality. Security and privacy issues in such environments, however, have not been explored in depth. Indeed, several researchers and practitioners have admitted that security and privacy in this new computing paradigm are real problems. Langheinrich [3, 4] warns us about the possibility of an Orwellian nightmare in which current pervasive computing research continues on without considering privacy in the system. Stajano [5] notices that while researchers are busy thinking about the killer applications for pervasive computing, cyber-criminals and computer villains are already considering new, ingenious attacks that are not possible in traditional computing environments. Kagal [6, 7] admit that securing pervasive computing environments presents challenges at many levels. The very same features that make pervasive computing environments convenient and powerful make them vulnerable to new security and privacy threats. Traditional security mechanisms and policies may not provide adequate guarantees to deal with the new exposures and vulnerabilities. In this paper we address some of these issues as follows.

2. Pervasive Computing Abstractions

To have a better understanding of the challenges associated with securing pervasive computing environments, it is important to list the salient features of pervasive computing. These include the following.

2.1 Creating Smart and Sentient Spaces

A dust of invisible embedded devices and sensors are incorporated to turn physical spaces into active, smart surroundings that can sense, “see,” and “hear,” effectively, making the space sentient and adaptable. Ultimately, the space should become intelligent enough to understand users’ intent and become an integral part of users’ everyday life.

2.2 Invisibility and Non-Intrusiveness

In current computing models, computers are still the focus of attention. In effect, people have to change some of their behavior and the way they perform tasks so that these tasks can be computerized. To boost productivity, it is important that computing machinery disappear and leave the spotlight. Computers should blend in the background allowing people to perform their duties without having machines at the centre of their focus.

2.3 Extending Computing Boundaries

While traditional computing encompassed hardware and software entities, pervasive computing extends the boundaries of computing to include physical spaces, building infrastructures, and the devices contained within. This aims to transform dull spaces into interactive, dynamic, and programmable spaces that are coordinated through a software infrastructure and populated with a large number of mobile users and devices.

2.4 Context Awareness

A pervasive computing environment should be able to capture the different context and situational information and integrate them with users and devices. This allows the active space to take on the responsibility of serving users and automatically tailoring itself to meet their expectations and preferences.

2.5 Mobility and Adaptability

To be truly omnipresent, the pervasive computing environment should be as mobile as its users. It should be able to adapt itself to environments with scarce resources, while being able to evolve and extend once more resources become available.

3. Challenges

As mentioned before, the additional features and the extended functionality that pervasive computing offers make it prone to additional vulnerabilities and exposures. Below, we mention these features that add extra burden to the security subsystem.

3.1 User Interaction Issues

One of the main characteristics of pervasive applications is a richer user-interface for interaction between users and the space. A variety of multimedia mechanisms are used for input and output, and to control the physical aspects of the space. At any point of time, the set of users in the space affects the security properties of the space. Because of the nature of these interactions, users in the space cannot easily be prevented from seeing and hearing things happening in it, so this has to be taken into account while designing access control mechanisms. We believe that the access control mechanisms should allow groups of users and devices to use the space in a manner that facilitates collaboration, while enforcing the appropriate access control policies and preventing unauthorized use. Thus the physical and “virtual” aspects of access control for such spaces have to be considered together.

3.2 Privacy Issues

The physical outreach of pervasive computing makes preserving users' privacy a much more difficult task. Augmenting active spaces with active sensors and actuators enables the construction of more intelligent spaces and computing capabilities that are truly omnipresent. Through various sensors and embedded devices, active spaces can automatically be tailored to users' preferences and can capture and utilize context information fully. Unfortunately, this very feature could threaten the privacy of users severely. For instance, this capability can be exploited by intruders, malicious insiders, or even curious system administrators to track or electronically stalk particular users. The entire system now becomes a distributed surveillance system that can capture too much information about users. In some environments, like homes and clinics, there is usually an abundance of sensitive and personal information that must be secured. Moreover, there are certain situations when people do not want to be tracked.

3.3 The Extended Computing Boundary

Traditional computing is confined to the virtual computing world where data and programs reside. Current distributed computing research tends to abstract away physical locations of users and resources. Pervasive computing, however, extends its reach beyond the computational infrastructure and attempts to encompass the surrounding physical spaces as well. Pervasive computing applications often exploit physical location and other context information about users and resources to enhance the user experience. Under such scenarios, information and physical security become interdependent. As a result, such environments become prone to more severe security threats that can threaten people and equipment in the physical world as much as they can threaten their data and programs in the virtual world. Therefore, traditional mechanisms that focus merely on digital security become inadequate

3.4 Security Policies

It is important in pervasive computing to have a flexible and convenient method for defining and managing security policies in a dynamic and flexible fashion. Policy Management tools provide administrators the ability to specify, implements, and enforces rules to exercise greater control over the behavior of entities in their systems. Currently, most network policies are implemented by systems administrators using tools based on scripting applications [8, 9] that iterate through lists of low-level interfaces and change values of entity-specific system variables. The policy management software maintains an exhaustive database of corresponding device and resource interfaces. With the proliferation of heterogeneous device-specific and vendor-specific interfaces, these tools may need to be updated frequently to accommodate new hardware or software, and the system typically becomes difficult to manage. As a result, general purpose low-level management tools are limited in their functionality, and are forced to implement only generic or coarse-grained policies [10]. Since most policy management tools deal with these low-level interfaces, administrators may not have a clear picture of the ramifications of their policy management actions. Dependencies among objects can lead to unexpected side effects and undesirable behavior [11]. Further, the disclosure of security policies may be a breach of security. For example, knowing whether the system is on the lookout for an intruder could actually be a secret. Thus, unauthorized personnel should not be able to know what the security policy might become under a certain circumstance.

3.5 Info Operations

There is a great deal of concern over new types of threats, namely, Information Operations (info ops) and cyber-terrorism, which are natural consequences of the increasing importance of electronic information and the heavy reliance on digital communication networks in most civilian and military activities. Info ops, which can be defined as "actions taken that affect adversary information and information systems while defending one's own information and information systems," [12] is a serious concern in today's networks. In such a scenario, cyber-terrorists and other techno-villains can exploit computer networks, inject misleading information, steal electronic assets, or disrupt critical services. Pervasive computing gives extreme leverage and adds much more capabilities to the arsenal of info warriors, making info ops a much more severe threat.

4. Security Requirements

To deal with the new vulnerabilities introduced by pervasive computing, security and privacy guarantees in pervasive computing environments should be specified and drafted early into the design process rather than being considered as add-ons or afterthoughts. Previous efforts in retrofitting security [21] and anonymity into existing systems have proved to be inefficient and ineffective. The Internet and Wi-Fi are two such examples both of which still suffer from inadequate security. In this section, we briefly mention the important requirements needed for a security subsystem for pervasive computing environments.

4.1 Transparency and Unobtrusiveness

The focal point of pervasive computing is to transform users into first class entities, who no longer need to exert much of their attention to computing machinery. Therefore, even the security subsystem should be transparent to some level, blending into the background without distracting users too much.

4.2 Multilevel

When it comes to security, one size does not fit all. Hence, the security architecture deployed should be able to provide different levels of security services based on system policy, context information, environmental situations, temporal circumstances, available resources, etc. In some instances, this may go against the previous point. Scenarios which require a higher-level of assurance or greater security may require users to interact with the security subsystem explicitly by, say, authenticating themselves using a variety of means to boost system's confidence.

4.3 Context-Awareness

Traditional security is somewhat static and context insensitive. Pervasive computing integrates context and situational information, transforming the computing environment into a sentient space. The security aspects of it are no exceptions. Security services should make extensive use of context information available. For example, access control decisions may depend on time or special circumstances. Context data can provide valuable information for intrusion detection mechanisms. The principal of "need to know" should be applied on temporal and situational basis. For instance, security policies should be able to change dynamically to limit the permissions to the times or situations when they are needed. However, viewing what the security policy might become in a particular time or under a particular situation should not be possible. In addition, there is a need to verify the authenticity and integrity of the context information acquired. This is sometimes necessary in order to thwart false context information obtained from rogue or malfunctioning sensors.

4.4 Flexibility and Customizability

The security subsystem should be flexible, adaptable, and customizable. It must be able to adapt to environments with extreme conditions and scarce resources, yet, it is able to evolve and provide additional functionality when more resources become available. Tools for defining and managing policies should be as dynamic as the environment itself.

4.5 Interoperability

With many different security technologies surfacing and being deployed, the assumption that a particular security mechanism will eventually prevail is flawed. For that reason, it is necessary to support multiple security mechanisms and negotiate security requirements.

4.6 Extended Boundaries

While traditional security was restricted to the virtual world, security now should incorporate some aspects of the physical world, e.g. preventing intruders from accessing physical spaces. In essence, virtual and physical security becomes interdependent.

4.7 Scalability

Pervasive computing environments can host hundreds or thousands of diverse devices. The security services should be able to scale to the "dust" of mobile and embedded devices available at some particular instance of time [13]. In addition, the security services need to be able to support huge numbers of users with different roles and privileges, under different situational information.

5. Challenges to Privacy Protection

Privacy appears as a major issue for pervasive computing applications. Several models have been proposed to address privacy challenges. Successful design requires knowledge of the technology's users and that their desires and concerns are understood. This is difficult as few experiential researches exist about potential pervasive users that designers can use. Complicating design further is the fact that pervasive systems are typically embedded or invisible, making it difficult for users to know when these devices are present and collecting data. As users have a limited understanding of the technology several privacy, design, and safety issues are raised [13-17]. We discuss how privacy might be preserved in a pervasive computing environment. It presents some research developments in these areas to address privacy concerns. Open issues and challenges are also examined. With the enhance of handheld devices and wireless networks, pervasive computing has become integral part of our life. A pervasive computing environment unobtrusively and transparently supports the human beings with its embedded computation and communication. This embedding ensures transparent interaction of the devices with the users. Privacy can be defined as "the privilege of users to determine for themselves when, how, and to what extent information about them is communicated to others". Thus privacy in pervasive computing can be perceived as an entitlement of users for control over collection and dissemination of information related to them. These users can be individuals, groups, or organizations.

To protect privacy [20] a user can be notified of requests for information. But for pervasive technology to become truly ubiquitous, it should merge into the background and become a part of everyday life. Users' inability to see a technology makes it difficult for them to understand how it might affect their privacy. Unobtrusiveness however is a reasonable and required goal because pervasive systems should minimize the demands on users. Location privacy is a particular type of information privacy that can be defined as "the ability to prevent other parties from learning one's current or past location". Until recently the concept of location privacy was unknown as reliable and timely information about the exact location of others was not available. Most people did not perceive any privacy implications in revealing their location except in certain situations but with pervasive computing the scale of the problem has changed considerably. It is a major concern if someone can inspect the history of all past movements of a user that has been recorded continuously. This "change in scale

of several orders of magnitude is often qualitative as well as quantitative and is a recurring problem in pervasive computing". With increase in location-based applications protecting personal location information has become a major challenge. To address this challenge a mechanism is required that lets users control their location information automatically.

5.1 Unobtrusiveness

The goal of pervasive computing is to be unobtrusive. For this purpose, technology is embedded into everyday objects that transmit and receive information. This "embedding" reduces the visibility of the pervasive computing environment surrounding the user and makes the technology more friendly and acceptable. Ironically, the same characteristic makes it possible to invade the privacy of the user without the user realizing it. This leaves the users with limited control over their own privacy and also adds the responsibility that they do not intrude on privacy of others. This invasion and responsibility cannot be managed or imposed through social and organizational controls. There is a need to find a balance between usability and privacy. Traditional models requiring explicit user input have to be replaced with models that can sense information securely and automatically from the context and environment, and exchange it seamlessly with communicating devices and users. A single sign on feature to enable single-step authentication to multiple applications can be a solution. The extension of such models to truly pervasive environments still remains a challenge.

5.2 Location Dependency

Pervasive computing applications make use of location information to provide services including local information access (traffic reports, news, navigation maps) and nearest-neighbor services [13]. To utilize these location-based services, the users have to make their location known to the service provider. The access to location information about a user can provide opportunity for its misuse. Location is privacy-sensitive information that is available readily making its protection a challenge. There is also the added requirement for the services to be flexible enough to support different location privacy policies based on situation. For example a user might want location privacy but change this need in case of an emergency to pinpoint and communicate the exact location.

5.3 Context Dependency

Pervasive computing applications also depend on context information. This information can include the type of wireless device used by the application, GPS coordinates, user profiles, user preferences, current time, etc. The ability to use contextual information to enhance traditional user attributes is important for making privacy protection less intrusive. Providing sufficient protection for context information is difficult as context-aware systems deal with sets of information that might have different privacy requirements due to variance in sensitivity and user preference. However there is a lack of protocols and infrastructure for securely collecting, validating, and using contextual information.

5.4 Amount of Data Collection

Compared to current computing technology, pervasive computing implementation relies on an increased amount, quality, and accuracy of data generated and collected. This is also enhanced by increasing capabilities to process and analyze the data. This sheer amount of data collection and processing leads to users frequently ignoring or being deprived from the decision of release of personal data. In addition, pervasive computing environments have a majority of wireless devices [19]. These devices have limitations for processing power, bandwidth, throughput, memory etc. These factors put a resource limitation on elaborate models and protocols for privacy protection that might depend on extensive use of these resources.

5.5 Role of Service Provider

The role of the service provider as maintainer and preserver of the privacy sensitive data is critical. There are numerous opportunities for misuse of data passing through the devices of the service provider. The Platform for Privacy Preferences (P3P) of the World Wide Web Consortium (W3C)[18] provides a specification that can be used to ensure that each data request by the service providers also specifies purpose, retention, and recipients of the data. In the real-world ensuring that all service providers follow the rules is difficult.

5.6 Lack of Ownership

Resources in a traditional computing system have ownership and access control. On the other hand pervasive computing environments "permit looser and more dynamic couplings between people and resources, thereby invalidating the usual approaches to ownership and control of resources". For example a user has no control over a camera recording activities in a room where the user is. It is difficult to implement privacy control when ownership cannot be easily determined.

6. Conclusion and Future Directions

The shift to the pervasive computing paradigm brings forth new challenges to security and privacy, which cannot be addressed by mere adaptation of existing security and privacy mechanisms. Unless security concerns are accommodated early in the design phase, pervasive computing environments will be rife with vulnerabilities and exposures. In this paper, the various aspects of privacy preservation in pervasive computing have been discussed. This is an area that had not been given much attention earlier but recent research has addressed some of the challenges. We also presented some solutions in

our prototype implementation. The construction of complete, integrated pervasive environments and their real-life deployments are still things of the future. Security in pervasive computing is expected to be an integral part of the whole system, which is not realized yet. It should be noted, however, that there is no single "magical" protocol or mechanism that can address all the security issues and meet the requirements and expectations of secure pervasive computing. Moreover, security itself consists of a variety of different and broad aspects each of which requires detailed research and customized solutions. For these reasons, our prototype implementations are not meant to be a solution for all problems. Instead, they represent milestones towards the construction of a full-fledged security subsystem. Promising future directions include the development of formal specifications of desirable behavior in the form of security and privacy properties in pervasive computing. Access control, information flow, availability, and secure protocols for authentication, non-repudiation, confidentiality and integrity can be specified in terms of system properties such as safety and live ness. It is also promising to incorporate intelligence and automated reasoning into the security architecture.

This "intelligent" security system would be able to make judgments and give assistance in securing the environment without too much intervention by users or administrators. Therefore, we are exploring the possibility of incorporating automated reasoning and learning into the active spaces security architecture, enabling it to perform intelligent inferences under different contexts despite the uncertainties that arise as a result of bridging the physical and virtual worlds. We are also looking into the development of several middleware reflective object-oriented patterns that can support the different aspects of security, including authentication, access control, anonymity, and policy management, as well as how to instantiate them with diverse mechanisms. Finally, because it is difficult to develop security models that involve people and physical spaces, more studies on integrating virtual and physical security need to be considered.

Conflict of Interest

In this manuscript the authors declare that there is no conflict of interest.

References

i. Bluetooth." http://www.bluetooth.com/.

ii. Smith, J. R. et al. (2006). A Wirelessly Powered Platform for Sensing and Computation. *Proc. 8th Int'l Conf. Ubiquitous Computing, Springer Verlag*, 495–506.

iii. Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *ACM Ubi Comp Atlanta*, GA, 2001.

iv. Langheinrich, M. (2002). A Privacy Awareness System for Ubiquitous Computing Environments. *In: Borriello, G., Holmquist, L.E. (eds) UbiComp 2002: Ubiquitous Computing. UbiComp 2002*. Lecture Notes in Computer Science, 2498. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45809-3_19

v. Stajano, F. (2002). Security for ubiquitous computing. 1. Chichester: Wiley.

vi. Kagal, L., Finin, T. and Joshi, A. (2001). Trust-based security in pervasive computing environments. *Computer*, 34, 154-157. doi: 10.1109/2.970591.

vii. Kagal, L., Undercoffer, J., Perich, F., Joshi, A., and Finin, T. (2002). Vigil: Enforcing Security in Ubiquitous Environments. *Grace Hopper Celebration of Women in Computing 2002*.

viii. Boyle, J., et al. (1999). The COPS Protocol. *Internet Draft*, Feb. 24, 1999.

ix. Mundy, R., Partain, D., and Stewart, B. (1999). Introduction to SNMPv3. *RFC 2570*, April 1999.

x. Stevens, M., et al. (1999). Policy Framework. *IETF draft*, September 1999.

xi. Loscocco, P. and Smalley, S. (2001). Integrating Flexible Support for Security Policies into the Linux Operating System. *Proceedings of the FREENIX Track of the 2001 USENIX*, 2001.

xii. Luiijf, E. A. M. (1999). Information Assurance and the Information Society. *EICAR Best Paper Proceedings*, 1999.

xiii. Beresford, A. R., Stajano, F. (2003). Location Privacy in Pervasive Computing. *Pervasive Computing, IEEE*, 2, 46-55.

xiv. Haque, M. and Ahamed, S. I. (2006). Security in Pervasive Computing: Current Status and Open Issues. *International Journal of Network Security*, 3, 203–214.

xv. . Seigneur, J, Jensen, C. D. (2004). Ubiquitous computing (UC):Trust enhanced ubiquitous payment without too much privacy loss. *Proceedings of the 2004 ACM symposium on Applied computing*, March 2004.

xvi. Hong, J. I., and Landay, J. A. (2004). Support for location: An architecture for privacy-sensitive ubiquitous computing. *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, June 2004.

xvii. Beckwith, R. (2003). Designing for ubiquity: the perception of privacy. *Pervasive Computing, IEEE*, 2, 40-46.

xviii. Want, R. (2009). When Cell Phones Become Computers. *IEEE Pervasive Computing*, 8, 2-5. doi: 10.1109/MPRV.2009.40.

xix. Shen, D.Z. (2006). Open Tag—Privacy Control Methods in RFID, master's thesis, *Massachusetts Institute of Technology*, Dept .Electrical Engineering and Computer Science, 2006.

xx. Holtzman, H., Lee, S. ,and Shen, D. (2009). Open Tag: Privacy Protection for RFID IEEE 1536-1268/ 2009

xxi. Ahamed, S. I., Li, H., Talukder, N., Monjur, M., Chowdhury, S. H. (2009). Design and implementation of S-MARKS: A secure middleware for pervasive computing applications. *The Journal of Systems and Software. New York*: 82, 1657 Oct 2009.