ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

Analytical Study of Ubiquitous Computing

Nitin Jain
Research Scholar
Punjab Technical University
Kapurthala, Punjab

Dr. S N Panda
Professor & Principal
RIMT, Mandi Gobindgarh
Punjab, India

Dr. H C Agrawal
Professor
RIMT, Mandi Gobindgarh
Punjab, India

Abstract: ***Aim of ubiquitous computing is to support the users in their daily life by making services available to users anytime, any network and anywhere. Users would exchange data with the other users or the service providers and these interactions must be secure enough regardless of the context in which device is used to access the services. In order to suit the requirements of ubiquitous computing, traditional security mechanisms have to be changed as these are context-insensitive. In ubiquitous environment security policies must change according to the change in context means security policies must be dynamic. System architecture of a ubiquitous computing environment consists of entities like mobile devices/users, services/service providers and authentication servers along with underlying wired and wireless communication infrastructures. This paper explores the security aspect of ubiquitous computing generally based on privacy and authentication.***

Keywords: **Ubiquitous Computing, Authentication, Privacy.**

I. INTRODUCTION

Ubiquitous computing means a rapid increase in large number of computing devices, sensors and embedded processors, all in background and invisible to the user to provide a new kind of functionality, offer specialized services, increase productivity, and facilitate seamless interaction with the surrounding environment and available resources. Ubiquitous computing is networked microprocessors embedded [3] in everyday objects not just mobile phones and home appliances but also pen, books, bookshelves, bus stops and vehicles--all talking to each other over some form of links. . Thus the concept of Ubiquitous Computing doesn't mean just that there are lots of computers in the environment, they also must collect data by monitoring natural human activity and be able to interact with other computing devices. The features of ubiquitous computing include Invisibility, non-intrusiveness, Context awareness, Mobility, Adaptability and extended computing boundaries. Ubiquitous environment is very different from traditional computing environment .It consists of different homogeneous as well as heterogeneous networks having diverse client nodes with minimal or no user involvement. Communication between devices is blended into the environment without distracting users. Ubiquitous Computing combines context and situational information to provide services to the user in active space. Ubiquitous computing environments raise complex security and privacy issues, which require altogether a different security mechanism to deal with the ubiquity, context awareness and authentication. Traditional security mechanisms have to be changed to be suited to ubiquitous environment as these security methods are static, non-adaptable, and context-insensitive. Security policies have to be dynamic in ubiquitous environment. Security will have to be provided at different levels based on system policy, services, context information, and available resources.

II. ISSUES FOR UBIQUITOUS COMPUTING

A. Social Issues

Ubiquitous computing environment is of the idea of making it easier for computation to sense, understand, and react to phenomenon in the physical world and to record those phenomena. These enabling technologies carry with them a lot of dangers, e.g., making it too easy for people to build systems that effectively spies on others without any controlling authority. Researchers would have to undertake their work by understanding these issues. However, the fear of wrong-doing is not a call to close down all work in this area, but to work toward technological, design, and social solutions to address these concerns. Another problem for the users is the lack of knowledge of what the computing system/ device is doing behind their backs [4]. The original idea of ubiquitous computing described computing as disappearing into the physical environment, this "invisibility" is counter to informing users about how they are being sensed. To tone down that fear, design solutions can be employed to make this information visible. For example, systems that sense physical phenomena and capture live situations should provide clear indicators that this sensing or recording is occurring [5]. As these sensing and recording capabilities are more commonly found, one challenge for everyday computing is to enable people to be aware of how they are being sensed? The next step is to allow those being sensed or recorded to have control to either stop this activity or to at least control the distribution and use of the information

.

B. Privacy Issues

Technology is not privacy neutral. Mark Weiser, also known as father of ubiquitous computing already identified privacy as one of its biggest challenges: "Perhaps key among the social issues that embodied virtuality will engender is privacy: hundreds of computers in every room, all capable of sensing people near them and linked by high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy." [1]. The deployment of ubiquitous computing

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

technology will make it difficult to differentiate between public and private actions and can have a dramatic effect on the level of privacy enjoyed by the users of the system. The privacy implications [14] of ubiquitous computing implementations must always be accorded the most careful consideration. Data collection and processing are the core components of ubiquitous computing. Privacy issues [2] are thus of utmost importance in ubiquitous environment. As ubiquitous computing tries to hide the use of technology by making computing invisible, the level of awareness for such electronic transactions will drop drastically and hence invisible nature of such systems threatens users' privacy. Without powerful standards surrounding user privacy, the world of ubiquitous computing may very well shift from one of ease and convenience to one where each of us has an inescapable sense of being watched, at best, and no control over our personal information, at worst. Such prospects are clearly far from desirable. We have to protect user privacy not only from external world but also from service providers who are serving the user. Much of the current research into the protection of location privacy for ubiquitous computing has concentrated on defining mechanisms that allow users to control access to their location information; however, explicit and detailed configuration of access parameters runs counter to the aims of ubiquitous computing. Privacy can be enabled by anonymsing all data released to a third-party. Anonymisation has several advantages over access control: users may prefer to remain anonymous; configuration of access control parameters can be difficult and error-prone; and anonymised location data means location-aware applications do not have to be trusted, thus increasing confidence in the protection of location privacy.

C. Authentication Issues

Authentication verifies whether the identification of this entity is correct. Ubiquitous computing requires approaches to authentication in which traditional authentication mechanisms need to be tailored and adapted to ubiquitous environments in such a way that preserves the environment's ubiquity and unobtrusiveness. Different authentication & cryptographic mechanisms suiting the requirements of ubiquitous environment will have to be developed which combine different identification and authentication mechanisms to build up confidence among the computing devices. Traditional authentication mechanisms require too much user intervention in the form of manual logins and logouts. In ubiquitous environment devices join and leave the environment very frequently making impractical for users to manually log in and log out each time they enter and leave network. In ubiquitous computing environments not only people but computer systems, mobile devices, PDAs need to be authenticated. As new authentication mechanisms and devices keep evolving, different authentication & cryptographic mechanisms suiting the requirements of ubiquitous computing will have to be developed which combine different identification and authentication mechanisms to build up confidence among the computing devices. Some of the attributes of traditional authentication protocols need to be improved in order to specifically suit for ubiquitous computing environment. Zakiuddin et al. [6] discuss a revolutionized authentication mechanism for pervasive computing environments, which is not only concerned with the "name attribute" of an entity, but it takes into account other attributes, like location, type, and trust level. J.Al-Muhtadi et al [7] suggested to use many wearable and embedded devices like smart jewelries; smart watches and active badges etc those contains an ID for authentication, but the problem is that the user should carry the device wherever he goes. Colouris [8] reckons that because of volatile environment of ubiquitous computing as compared to the existing computing environment, there is a need for a special authentication and authorization protocol. In a ubiquitous environment, heterogeneous devices may come in the network at any time and could start interacting with each other and also may suddenly leave the network [9].The dynamicity and volatility of mobile devices in a ubiquitous computing environment could contribute to the fluctuating usage environment like user's location, device's context and user's activity that varies randomly. Due to this reason, many of the current rigid authentication protocol that relied on certification authorities to confirm the identity of the entity involved will not be sufficient for a volatile ubiquitous environment like smart environment as described by Nixon [10].Certifying Authority (CA) concept for authentication, was used by C. Lesniewski et al [11] in which the user have to register his devices and maintain his certificate on a regular basis. OpenID, one of the authentication protocol enables users to choose their preferred identity providers for the creation of their accounts. By using the Users can only sign in that application which acknowledges by authentication of those accounts. OpenID is also susceptible to phishing attacks in such a way that a user is believed to enter his credentials into the real authentication page but actually it is a fake authentication page. Unauthorized person controlling the page now can use these entered credentials to access the user's account and then log on to any application associate with that particular user's OpenID as mentioned in [12]. Wenjuan Liu et al [13] have used information hiding concept of TCP/IP packets. This method can be used only for trustworthy authentication of fire walls like security devices. The information whether sensitive or non-sensitive will be en-capsulated. Because of this reason computational and transmission overhead will be high in this method.

To conclude, security framework of ubiquitous computing has to interface with other security solutions and negotiate security requirements. Framework has to be

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 12, June 2013

flexible, adaptable and need to preserve the privacy of users of ubiquitous computing technologies. It should provide support for plugging in new devices, mechanisms or reconfiguration to existing ubiquitous applications and services. The security services should be able to scale to wide variety of mobile and embedded devices.

REFERENCES

[1] Weiser, Mark, "The Computer for the 21st Century" in Scientific American 265(3), 94-104 (Sept. 1991).

[2] Langheinrich, Marc, "Privacy in Ubiquitous Computing", Chapman & Hall / CRC Press, Sep. 2009. ISBN: 9781420093605.

[3] Jain, N., Panda, S. N., & Kumar, A. Future Scintillation of Ubiquitous Computing. International Journal of Computing and Business Research. Vol 3, Sept 2012.

[4] Gregory D. Abrod, Elizabeth D. Mynatt, "Past, Present and Future Research in Ubiquitous Computing, ACM Transactions on Computer-Human Interaction, Vol 7 No. 1, March 2000, Pages 29-58.

[5] Dourish, P. (2004): What we talk about when we talk about context-Personal & Ubiquitous Computing.

[6] I. Zakiuddin, S. Creese, B. Roscoe, and M. Goldsmith, "Authentication in Pervasive Computing, Position Paper," presented at PAMPAS '02 - Workshop on Requirements for Mobile Privacy & Security Royal Holloway, University of London, 2002.

[7] Al-Muhtadi, J., Ranganathan, A., Campbell, R., & Mickunas, M.(2002) A flexible, privacy preserving authentication framework for ubiquitous computing environments. In Distributed Computing Systems Workshops, 2002.Proceedings.22nd International Conference on (pp. 771-776). IEEE.

[8] G.Coulouris, "Mobile & Ubiquitous Computing, Distributed Systems," Concepts and Design 4th ed., Addison-Wesley, Reading, MA: Addison-Wesley, ch.16, pp. 683-704, (2005).

[9] J.Bardram, A.Friday, "Ubiquitous Computing Systems, Ubiquitous Computing Fundamentals," J.Krumm, Ed. Redmond, Washington, and U.S.A: CRC Press, ch. 2, pp. 39-41, (2010).

[10] P.Nixon, W.Wagealla, C.English, & S.Terzis, "Privacy, Security & Trust Issues in Smart Environments," In Smart Environments: Technology, Protocols and Applications. Wiley, London, UK, pp. 220-240. ISBN 978-0-471-54448-7, (2004).

[11] Lesniewski-Laas, C., Ford, B., Strauss, J., Morris, R., & Kaashoek, M. F. (2007, October). Alpaca: extensible authorization for distributed services. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 432-444). ACM.

[12] Rehman, R. U. (2008). OpenID Protocol: Miscellaneous Topics Get Ready for OpenID. Conformix Technologies Inc, 205-207.

[13] Liu, W., Fu, X., Ouyang, S., Lin, J., & Teng, S. (2009, December). Information hiding for pervasive trusted authentication. In Pervasive Computing (JCPC), 2009 Joint Conferences on (pp. 653-656). IEEE.

[14] http://www.siop.org/tip/backissues/ papr02/07 weiss.aspx.