ENABLING SECURITY FOR SERVICE DISCOVERY IN PERVASIVE COMPUTING ENVIRONMENTS

MAHDI SHARIFI

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Centre for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

MARCH 2009

ABSTRACT

Nowadays, the digital world is witnessing the birth of a revolutionary computing paradigm that promises to have a profound effect on the way users interact with computers, devices, physical spaces, and other users. Pervasive or ubiquitous computing is a new technology introduced to computer science and digital world and has been investigated since 1993. Since the beginning of the new millennium, this concept has been actualized more than in the past and became more realistic than a dream. Making the computer disappear from the eyes of the people, in a way that people cannot feel the presence of computers is the other aim of pervasive computing. In a broad sense, pervasive computing includes four major areas: mobile computing, wireless networks, embedded computing and context-aware sensor networks. Furthermore, the presence of service discovery in pervasive environments is an unavoidable principle considering the fact that the number of available services is increasing on the fly in such environments. Meanwhile, providing security for processes in pervasive computing environments to maintain communicating information securely and reliable is a demanding task. This study aims to analyze security requirements raised in service discovery in pervasive computing environments and proposes a secure framework to enable service discovery to adapt with security issues, in particular authentication, in pervasive computing environments in order to obtain secure pervasive computing envisions. Moreover, in order to demonstrate the proposed framework design, the prototype applying a case study is illustrated.

ABSTRAK

Kini dunia digital sedang menyaksikan kelahiran satu revolusi paradigm perkomputeran yang menjanjikan perubahan besar ke atas cara pengguna berinteraksi dengan komputer, peralatan, ruang fizikal, dan pengguna lain. Perkomputeran merata atau sentiasa ada merupakan teknologi baru yang diperkenalkan kepada sains komputer dan dunia digital dan ia dikaji sejak tahun 1993. Semenjak bermulanya millennium baru, konsep ini lebih direalisasikan berbanding dahulu dan menjadi lebih nyata, bukan hanya impian. Mewujudkan keadaan di mana manusia tidak lagi meyedari kehadiran komputer adalah matlamat perkomputeran merata. Secara amnya, perkomputeran merata merangkumi empat perkara utama: perkomputeran mudah alih, jaringan tanpa wayar, perkomputeran terbenam dan jaringan sensor sedar konteks. Selanjutnya, kewujudan penemuan perkhidmatan dalam persekitaran yang merata ialah prinsip yang tidak dapat dielakkan memandangkan pertambahan bilangan perkhidmatan pada kadar yang cepat dalam persekitaran tersebut. Sementara itu, penyediaan sekuriti perkomputeran bagi proses di dalam persekitaran perkomputeran merata agar penyampaian maklumat selamat merupakan tugas yang berat. Kajian ini menganalisis keperluan keselamatan yang wujud bagi perkhidmatan penemuan dalam persekitaran pengkomputeran merata dan mencadangkan satu rangka kerja keselamatan agar perkhidmatan penemuan dapat disesuaikan dengan isu-isu keselamatan, khususnya pengesahan dalam persekitaran perkomputeran merata bagi membolehkan perkomputeran merata yang selamat. Tambahan dari itu, reka bentuk cadangan rangka kerja telah digubal, satu prototaip menggunakan kes kajian dipaparkan.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Regards to the advances in technology, pervasive computing has become a hot and animate field of computer science. Pervasive computing, also called ubiquitous computing, emphasizes particularly on the amalgamation of computing capability and human's living conditions [55]. Furthermore, the paradigm of pervasive computing represents ubiquitous computing environments which make available anytime and anywhere access to information services while making the presence of the system invisible to the user. Pervasive computing envisioned by Mark Weiser emerged at the conjunction of research and development in a number of areas which include embedded devices and systems, wireless communications, and distributed, mobile and context-aware computing [9].

In this chapter an introduction to research is provided. Initially, the background of the problem is presented. Following this, problem statement described. After that, project objective, aim and scope mentioned respectively. Finally, significant of the study is stated.

1.1. Background of the Problem

Recently, digital world move toward pervasive computing environments where great number of networked computing devices which range from tiny sensors to extremely dynamic and powerful devices are integrated with people and their ambient environments. For instance, a room may be saturated with numerous number

of devices which may provide people with information without needing their active attention. Further, a user in next room can reach and communicate with devices in that room as same as user in other side of the world who connected to Internet. Therefore, to achieve such sophistication in these environments, service discovery can be essential that enables devices and services to properly discover, configure, and then communicate with each other.

As it is quoted in [28], service discovery in pervasive computing environments facilitates users to access network services by automating tedious manual configurations, otherwise user should waste their precious time to finding services and manually configuring devices and programs. Kindberg T. and Fox A. mentioned that “Perhaps the most distinguishing characteristics of service discovery in pervasive computing environments are the integrations of computing devices with people and their ambient environments. Extremely dynamic environments and computing resources, mobility, and a wide range of heterogeneous devices, protocols, and platforms are also crucial issues and should be addressed” [49].

Several researches on these hot issues have been conducted in both industry and academia and as a result, many products and standards have emerged. However, privacy and security issues have been neglected and challenged when services may be used or discovered. Subsequently, a motivated scenario mentioned in[20] which can be helpful to understand and address this problem.

The scenario is about a physician, Bob; wants to discover different services at different locations. In his house, there are various wired and wireless computing devices that he shares with his family members. As usual, he puts his cell phone, PDA, and MP3 player in his handbag and a Bluetooth earphone in his pocket, and then travels to his office. On the way to his office, he may wear his Bluetooth earphone and use it to discover his Bluetooth, MP3 player, and listen to songs. Nonetheless, he does not want others to know what is in his bag. In his office, he uses his computer, cell phone, and MP3 player. When he goes to Alice's office, through the office's wireless LAN, they look at a document on the office file server simultaneously with their respective laptops. The devices within his pocket, however,

should not be able to discover and use Alice's personal services on the devices in her purse, and vice versa. This process cannot be completed unless Alice provides a user name and a password for him to access later. Bob also volunteers to help patients at public places such as at a train station in case of emergencies. If a medical emergency happens and Bob is in the vicinity, he is notified of the patient's position. To find it, Bob may follow the directions on a map shown on his PDA and moves towards the patient. At the place, Bob reads the medical information from a medical device that the patient wears. When Bob is in an airport and he has an hour before his flight leaves, he turns on his PDA and finds that there is an available wireless LAN. After Bob makes the connection, he receives an email that includes an attached document. Then, he uses his PDA to search for a nearby printer to print the document so he can read it during his flight. Moreover, when he goes away, he wants to check his office using intelligent CCTVs which are connected together via sensor networks.

It can be deduced with respect of above scenario, following information is sensitive and should be protected during service discovery:

- At the service owners' side, service information, owners' identities, and presence information.
- At the users' side, identities used for authentication, user's presence information, and service query information.

In pervasive computing environments, achieving these two goals is challenging in consideration that there are some reasons included: First, in a place coexisting services may belong to different owners. For instance, in Bob's work place, services belong to Bob, Alice, or the office. Second, the available domains and services change dramatically with respect to user and service mobility. For example, different services are available in Bob's house and on his way to the office. Bob carries his mobile devices, and the services on them move with Bob. Third, in view of the fact that users can act in many different roles, they can use different identities for different administrative domains. Considering above scenario, Bob uses one user name to access his office PC and another user name for his PDA. Fourth, sensitive

information should be discovered, accessed, and exposed only when it is necessary, such as a medicate device that one wears in mentioned situation on that scenario.

In conclusion, in order to provide secure service discovery framework for authorized users, considering pervasive computing environments for adapting them with security solutions is become an important issue.

1.2. Statement of the Problem

As it quoted in [28], in traditional secure network service accesses, a user explicitly specifies a service's network address and supplies a credential (a user name and password pair or a certificate) to authenticate with a service provider. The user has a priori knowledge of the service, the service provider, the credential, and the relation among them. Nevertheless, within pervasive computing environments, network services become ubiquitous and embedded within users' personal belongings, homes, and offices. In addition, every person may become both, a service provider and a user and the number of services and service providers which a user interacts with them increased dramatically.

As a consequence, two new challenges emerge. First, since the increasing number of services, manual efforts to configure devices for potential communications and maintain availability of services become overwhelming. Second, memorizing the relation between services, service providers, and credentials becomes burdensome in consideration of the number of service providers increases.

Therefore, for purpose of service access and sharing in pervasive computing, service discovery as an essential element has been widely accepted. Most existing service discovery protocols provide well-designed solutions to meet the first challenge [51]. However, designing a service discovery protocol which support protection to sensitive information for both users and service providers is challenging[28]. As it mentioned before, the challenges can be viewed different since

there two different points of views. From users' point of view, authentication and exposing service requests is prudent to only necessary service providers, yet, the necessary service providers can be identified if users recognize the current existing services and service providers and their relations. In an ideal world, if service providers expose their existence and service information first, users can choose only necessary service providers to contact.

On the other hand, from the service providers' point of view, when a request is from an illegitimate user or the requested service is not offered, it is not sensible to response .The act of hiding by not replying, saves computation power and energy as well as protects the presence information of a service provider. Ideally, a service provider can easily make an accurate decision if users expose their credentials and service requests firstly. Consequently, both users and service providers prefer that the other party exposes information firstly. The conflict between a service provider and a user becomes the chicken-and-egg problem.

In fact, the general research question this research plans to response can be declared as follows:

How to propose a secure framework enabling service discovery to adapt with security issues, in particular authentication, in pervasive computing environments in order to obtain secure pervasive computing envisions?

Moreover, with the intention of being able to answer this question, a set of research questions that deal with the problem in detail are defined, as follows:

i. **RQ1:** What does pervasive computing concept mean and why pervasive environments and traditional environments should be distinguished?
   - ✓ What are the features and characteristics of pervasive computing environments?

ii. **RQ2:** What is the role of the service discovery in ubiquitous computing environments?

- ✓ What is the service discovery concept itself?
- ✓ How can it help to facilitate users to make benefits services which pervasive environments offer them?

iii. **RQ3:** What security solutions can be feasible and helpful to employ in pervasive environments taking into consideration their features?

- ✓ How to infer suitable authentication mechanisms as a security baseline with respect to pervasive computing concept?

iv. **RQ4:** How to apply security concepts which affect on service discovery process to protect sensitive data and information?

- ✓ How to assure authentication provide reasonable security defense to user and service provider information against unauthorized exposure and disclosure?

1.3. Project Aim

The aim of this project is to develop a framework for secure service discovery in pervasive computing environments using state-of-the-art technologies which has been proposed in ubiquitous computing.

1.4. Objectives of the Study

The research objectives are mentioned based on the problem statement, as follows:

i. To investigate the current security problems and breaks in service discovery in pervasive computing environments

ii. To study and analyze of current solutions and models regarding the problems

iii. To design a secure framework with respect to authentication in order to support service discovery in pervasive computing

iv. To develop a prototype based on the design

v. To validate the prototype applying one case study

1.5. Scope of the Study

Obviously, pervasive computing is a broad and wide area in computer science. So far, different knowledge and experience apply together to make pervasive environments such as mobile ad hoc network, wireless sensor networks and the like. In addition, as it stated previously, service discovery is an essential part of pervasive environments regarding dramatic increasing number of services and heterogeneous devices offered to users to make pervasive computing envisions real. It can be seen in accordance with subject of study, three research directions were inspired consist of pervasive computing environment, service discovery and security concepts, as following:

- This study tries to design and develop a secure framework in service discovery in pervasive environments but does not go to the concept of technologies like mobile Ad hoc and wireless sensor networks. Indeed, this research concentrates on a basic pervasive computing which may have wireless network, mobile devices and PCs. Therefore, implementation on the enterprise and perfect pervasive environment is beyond the scope of this project and the implementation is limited to prototype.
- Furthermore, according to second study direction, the goal of research is emphasized on using secure service discovery in ubiquitous spaces and not on service discovery itself.

- ❖ After that, with respect to third direction of the study, security concepts are too wide and implementing all these security requirements in such pervasive environments is impossible, even there are lots of unsolved challenges in pervasive computing due to security issues. Therefore, it is decided to choose and focus on authentication as first basic level security model.

Consequently, the intent of this study is to propose and develop a secure framework for service discovery in pervasive computing environments in terms of the state-of-the-art technologies in ubiquitous computing environments.

1.6. Significance of the Study

Currently, the environments change and taking into consideration this fact, directly applying existing solutions and mechanisms have not been had any useful points and efficiency yet. Likewise, as it mentioned in [32], using current security solutions may fail with respect to changing environments.

Besides, the shift to the pervasive computing paradigm brings new challenges regarding to security and privacy that cannot be addressed by mere adaptation of existing security and privacy mechanisms [5].

Furthermore, envision that within pervasive environments, dozens to hundreds of devices and services may surround a user. Over the time, he or she may utilize thousands of services at different places; meanwhile, the user may be the owner of some services. When discovering services in such environments, much information is sensitive and should be exposed with prudence [20].

Regarding this issue, service discovery is extensively accepted as an essential element in pervasive computing environments. Much research on service discovery

has been conducted, but privacy and security have been ignored and may be sacrificed [20]. While it is vital that legitimate users should be able to discover services, it is also necessary that services be hidden from illegitimate users. In view of the fact that service information, service provider's information, service requests, user presence information, and user's identities may be sensitive, it is needed to maintain them private during service discovery processes.

As a result, the complexity related to this issue, in general, comes from the following considerations:

- First, the nature of pervasive computing environments itself which makes different such environments in comparison traditional ones completely.
- Second, the number of available services and devices encompassed users in ubiquitous environments is increasing on the fly.
- Third, security challenges which pervasive computing dealing with them are protecting sensitive information against exposure and leakage to unauthorized users.

REFERENCES

[1] Mark Weiser, The Computer for the 21st Century, Scientific American , September 1991, 265 (3):94 – 104.

[2] M. Weiser, Hot topics-ubiquitous computing, Computer, 1993, 26 (10):71–72.

[3] Hua Wang, Yanchun Zhang and Jinil Cao, Access control management for ubiquitous computing, ScienceDirect Future Generation Computer Systems 870-878,August 2007.

[4] Roshan K. Thomas and Ravi Sandhu, Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions, Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), 2004.

[5] Roy Campbell, Jalal Al-Muhtadi, Prasad Naldurg Geetanjali Sampemane, M. Dennis Mickunas, Towards Security and Privacy for Pervasive Computing, Springer LNCS 2609 1-15,2003.

[6] Reddy, Y.V., Pervasive Computing: Implications, Opportunities and Challenges for the Society, West Virginia University, Morgantown, WV 26508, USA,2006.

[7] Boukerche A. and Ren Y., A trust-based security system for ubiquitous and pervasive computing environments, Computer Communication, Elsevier, 2008.

[8] Robert, G., et al., A system architecture for pervasive computing, in Proceedings of the 9th workshop on ACM SIGOPS European workshop: beyond the PC: new challenges for the operating system. 2000, Kolding, Denmark: ACM.

[9] Stan Kurkovsky, Pervasive computing: past, present and future, ITI 5th International Conference, 16-18 Dec. 2007, 65-71.

[10] Thompson M.S. and Midkiff, S.F., Service description for pervasive service discovery, 25th IEEE International Conference on Distributed Computing Systems Workshops, 6-10 June 2005, 273-279.

[11] Pfleeger C.P. and Pfleeger S.L., Security in Computing, Fourth edition, Prentice Hall, 2006.

[12] Harris S., All-In-One, CISSP Certification, Third edition, McGraw-Hill, Sep.2005.

[13] Stewart J. M., Tittel E. and Chaaple M., Certified Information Systems Security Professional, Third edition, SEBEX, 2005.

[14] The network authentication protocol, available online on: www.web.mit.edu/kerberos.

[15] The network authentication in IBM's network security program, available online on: www.zurich.ibm.com/security/past-projects/kryptoknight.

[16] Thompson M.S., Service discovery in pervasive computing environments, PhD thesis, Virginia Polytechnic Institute and State University, 2006.

[17] Alan Colman, Minh Tran and Jun Han, An Adaptive Architecture for Context-Aware Interaction in Pervasive Applications, Centre for Information Technology Research (CITR) Swinburne University of Technology, Melbourne, Victoria, Australia, 2007.

[18] Zhu F., Mutka M.W., and Ni L.M, service discovery in pervasive computing environments, IEEE Pervasive Computing, Oct.-Dec. 2005, 4(4): 81 – 90.

[19] Matsumiya K., Aoki S., Murase M. and Tokuda H., Active Authentication for pervasive computing environments, Springer LNCS 2609. 28-41, 2003.

[20] Zhu F., Mutka M.W., and Ni L.M, A private, secure, and user-centric information exposure model for service discovery protocols, IEEE Transactions on Mobile Computing, April 2006, 5(4): 418 – 429.

[21] R. Anderson, F. Bergadano, B. Crispo, J.-H. Lee, C. Manifavas, and R. Needham, A New Family of Authentication Protocols, Operating Systems Review, 1998.

[22] Zakiuddin, S. Creese, B. Roscoe, and M. Goldsmith, Authentication in Pervasive Computing: Position Paper, 1st International Conference on Security in Pervasive Computing, Boppard, Germany, 2003.

[23] M. Burnside, D. Clarke, T. Mills, S. Devadas, and R. Rivest, Proxy-Based Security Protocols in Networked Mobile Devices, 17th ACM Symposium on Applied Computing, Madrid, Spain, 2002.

[24] M. Langheinrich, A Privacy Awareness System for Ubiquitous Computing Environments; UbiComp 2002, GOTEBORG, SWEDEN, 2002.

[25] K. Zhang and T. Kindberg, An Authorization Infrastructure for Nomadic Computing, HP Labs, HPL-2001-228, 2001.

[26] M. Abadi and C. Fournet, Private Authentication, Theoretical Computer Science, vol. September 427-476, 2004.

[27] F. Stajano, Security for Ubiquitous Computing: John Wiley & Sons, LTD, 2002.

[28] Zhu F., Zhu W., Mutka M. W. and Ni L., Expose or not? A progressive exposure approach for service discovery in pervasive computing environments, Third IEEE International Conference on Pervasive Computing and Communications (PerCom 2005), 8-12 March 2005, 225 – 234.

[29] Stajano F. and Anderson R., The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, 7th International Workshop on Security protocols, Cambridge, UK, 1999.

[30] Stajano F. and Anderson R., The Resurrecting Duckling -- what next?, 8th International Workshop on Security protocols, Cambridge, UK, 2000.

[31] Balfanz D., Smelters D. K., Stewart P., and Wong H. C., Talking to Strangers: Authentication in Ad-Hoc Wireless Networks, 9th Annual Network and Distributed System Security Symposium, San Diego, CA, 2002.

[32] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.

[33] Bluetooth SIG, "Specification of the Bluetooth System -- Core", 2004, Available online: www.bluetooth.org.

[34] Sun Microsystems, Jini™Technology Core Platform Specification, Version 2.0, Sun Microsystem, 2003.

[35] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan, and J. Lilley, The design and implementation of an intentional naming system, 17th ACM Symposium on Operating Systems Principles (SOSP '99), Kiawah Island, SC, 1999.

[36] M. Balazinska, H. Balakrishnan, and D. Karger, INS/Twine: A Scalable Peer-to-Peer Architecture for Intentional Resource Discovery, International Conference on Pervasive Computing, Zurich, Switzerland, 2002.

[37] B. A. Miller, T. Nixon, C. Tai, and M. D. Wood, Home Networking with Universal Plug and Play, IEEE Communications Magazine, 2001, 104-109.

[38] M. Nidd, "Service Discovery in DEAPspace, IEEE Personal Communications, 2001, 39-45.

[39] E. Guttman, C. Perkins, J. Veizades, and M. Day, Service Location Protocol, Version 2, 1999, Available online: http://www.ietf.org/rfclrfc2608.txt .

[40] S. Czerwinski, B. Y. Zhao, T. Hodes, A. Joseph, and R. Katz, An Architecture for a Secure Service Discovery Service, Fifth Annual International Conference on Mobile Computing and Networks (MobiCom '99), Seattle, WA, 1999.

[41] Salutation Consortium, Salutation Architecture Specification, 1999, Available online: ftp://ftp.salutation.orgJsalute/sa20ela21.ps.

[42] S. Cheshire, Discovering Named Instances of Abstract Services using DNS, Apple Computer, 2002, Available online: http://files.dns-sd.orgldraft-cheshire-dnsext~dns-sd.txt

[43] Apple Computer Inc, Rendezvous Web Site, 2003, Available online: http://developer.apple.com/macosx/rendezvousJ.

[44] Bluetooth SIG Security Expert Group, Bluetooth Security White Paper, 2002,Availabe online: http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security Paper.pdf

[45] C. Ellison, "UPnP™ Security Ceremonies VI.O," Intel Co., Oct. 3 2003, Available online: http://www.upnp.orgldownioad/standardizeddcps/UPnPSecurityCeremonies _1_ Osecure.pdf.

[46] F. Sommers, Jini Starter Kit 2.0 tightens Jini's security framework, Java World, 2003.

[47] James E. Mauch and Namgi Park , Guide to the Successful Thesis and Dissertation A Handbook for Students and Faculty, Fifth Edition, University of Pittsburgh, Pittsburgh, Pennsylvania, U.S.A, 2003.

[48] Cooper D.R. and Schindler P.S., Business Research Methods, Tenth Edition, McGraw-Hill, 2008.

[49] T. Kindberg and A. Fox, System Software for Ubiquitous Computing, IEEE Pervasive Computing, 2002, 70-81.

[50] UPnP. Forum, Universal Plug and Play Device Architecture 1.0, Available online: http://www.upnp.org/resources/documents/CleanUPnPDA101 - 20031202s.pdf, 2003.

[51] F. Zhu, M. Mutka, and L. Ni, Classification of Service Discovery in Pervasive Computing Environments, Michigan State University, East Lansing MSU-CSE-02- 24, Available online: http://www.cse.msu.edu/~zhufeng/ServiceDiscoverySurvey.pdf, 2002.

[52] Yi Liu, Feng Li, PCA: A Reference Architecture for Pervasive Computing, 1st International Symposium on Pervasive Computing and Applications, 2006.

[53] J. Cook and Sajal K. Das, Smart Environments: Technologies, protocols, and applications, New Jersey: John Wiley & Sons Inc., 2005.

[54] James E. Mauch, Guide to the Successful Thesis and Dissertation A Handbook for Students and Faculty, Fifth Edition, Pittsburgh, Pennsylvania, U.S.A.: MARCEL DEKKER, INC., 2003.

[55] W. Xu, Y. Xin and G. Lu, A System Architecture for Pervasive Computing, Third International Conference on Natural Computation (ICNC 2007) Volume 5 : 772 – 776, 24-27 Aug. 2007.

[56] I. Constantinescu, W. Binder and B. Faltings, Service Composition with Directories, SC 2006, Springer LNCS 4089. 163–177, 2006.

[57] C. Preist, A Conceptual Architecture for Semantic Web Services, In Proceedings of the International Semantic Web Conference 2004 (ISWC 2004), November 2004.

[58] Park K., Lim S. and Park K., Computationally Efficient PKI-Based Single Sign-On Protocol, PKASSO for Mobile Devices, IEEE Transactions, 57(6): 821 – 834, June 2008.

[59] Zhu F., Mutka M. and Ni L., "Splendor: A secure, private, and location-aware service discovery protocol supporting mobile services", Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom 2003), 23-26 March 2003, 235 – 242.

[60] S. Lloyd, C. Adams, and S. Kent, Understanding Public-Key Infrastructure: Concept, Standards, and deployment considerations, New Riders, 1999.

[61] Kulkarni D. and Tripathi A., Context-aware Role-based Access Control, (SACMAT08) ACM, June 2008.

[62] Imamura T., Dillaway B. and Simon Ed., XML Encryption Syntax and Processing, 2002.

[63] Bartel M., Boyer J., Fox B., LaMacchia B. and Simon Ed., XML-Signature Syntax and Processing, 2002.

[64] Myatt A., Pro NetBeans IDE 5.5 Enterprise Edition, Apress, 2007.

[65] Ahamed Sh., Sharmin M., A Trusted-based Secure Service Discovery (TSSD) model for pervasive computing, Computer Communication Journal, Elsevier, August 2008.

[66] K. Minami, D. Kotz, Secure context-sensitive authorization, Third International Conference on Pervasive Computing and Communications Workshops (PerCom 2005), Hawaii, March 2005, 257–268.

[67] F. Almenarez, C. Campo, SPDP: a secure service discovery protocol for ad-hoc networks, 9th Open European Summer School and IFIP Workshop on Next Generation Networks (EUNICE 2003), Hungary, September 2003.

[68] N. Shankar, W. Arbaugh, On trust for ubiquitous computing, Workshop on Security in Ubiquitous Computing (UBICOMP 2002), Gteborg, Sweden.

[69] A. Tripathi, T. Ahmed, D. Kulkarni, R. Kumar, K. Kashiramka, Context-based secure resource access in pervasive computing environments, Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, vol. 00, FL, USA, 2004, 159.

[70] J. Basu, V. Callaghan, Towards a trust based approach to security and user confidence in pervasive computing systems, The IEEE International Workshop, Intelligent Environments 2005 (IE05), UK, June 2005.

[71] H. Kopp, U. Lucke, D. Tavangarian, Security architecture for service-based mobile environment, Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05),Washington, DC, USA, March 2005, 199–203.

[72] S. Pearson, How trusted computers can enhance privacy preserving mobile applications, Proceedings of the Sixth International IEEE Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), Taormina, June 2005, 609–613.

[73] P. Robinson, H. Vogt, W. Wagealla, Some research challenges in pervasive computing, Post Workshop at the Second International Conference on Pervasive Computing, Vienna, Austria , April 18–23 2004, 1–16.