UNIVERSITI PUTRA MALAYSIA

XML-BASED PRIVACY MODEL IN PERVASIVE COMPUTING

ALI DEHGHANTANHA

FSKTM 2008 2

XML-BASED PRIVACY MODEL IN PERVASIVE COMPUTING

ALI DEHGHANTANHA

MASTER OF SCIENCE

UNIVERSITI PUTRA MALAYSIA

2008

XML-BASED PRIVACY MODEL IN PERVASIVE COMPUTING

By

ALI DEHGHANTANHA

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirement for the Degree of Master of Science

February 2008

Dedication

To my family in Iran for their patience, encouragement, and support

To my friends in Malaysia for their standing with me all the time

Abstract of theses presented to the senate of University Putra Malaysia in fulfillment of the requirement for the Master of Science

XML-BASED PRIVACY MODEL IN PERVASIVE COMPUTING

By

ALI DEHGHANTANHA

February 2008

Chairman: Associate Professor Ali B.Mamat, PhD

Faculty: Computer Science and Information Technology

The years coming promise to bring new area of information technology, transferring it from scientists minds into reality, on one hand a new paradigm known as pervasive calm, ubiquitous computing, or pervasive computing has the ability to overcome a lot of insufficiencies of the current information systems while on the other hand central blocks of pervasive computing are in direct conflicts with privacy protection fundamentals. Considerable efforts have been taken to cope with this problem but each one had its own shortage. Some just provide one privacy type like location privacy or just identity privacy, some of them were not platform independence, and some resulted to a lot of privacy alarms.

In this thesis we proposed a new privacy model in pervasive computing that provides all four privacy types (ID, Location, Time, and content) for the user with high control over

private information (User Control over Private Information) and as less privacy warnings as possible (Unobtrusiveness of Privacy Mechanism). To complete the proposed model we showed model privacy policies with XML tags and distributed decision making processes in different layers to provide high scalability.

To validate the model, through implementation we showed that model provides “Privacy Policy Expressiveness” with supporting mandatory and discretionary rules, uncertainty handling and conflict resolution. We showed model unobtrusiveness with experimenting and measuring the time user wastes on dealing with privacy sub-system. We showed that our model provides content, identity, location and time privacy that leads to a high level of user control over private information. The model scalability would be granted by using XML as a platform independent format to describe privacy policies with addition of distributed decision making processes.

The validation results confirmed that the model supports all four metrics of “expressiveness of privacy policies”, all four metrics of “user control over private information”, and both factors of “scalability”, with less than 10% “unobtrusiveness”.

Abstrak tesis yang dibentangkan kepada senat Universiti Putra Malaysia dalam memenuhi keperluan untuk ijazah Master Sains

MODEL PERSENDIRIAN BERASASKAN XML UNTUK KOMPUTER SERATA

Oleh

ALI DEHGHANTANHA

February 2008

Pengerusi : Professor Madya Ali B.Mamat, PhD

Fakulti : Sains Komputer dan Teknologi Maklumat

Tahun-tahun yang mendatang menjanjikan satu era teknologi maklumat yang baru, pemindahan dari pemikiran seorang saintis kepada satu realiti, dari satu segi, paradigma baru dikenali sebagai pengkomputeran *ubiquitous*, atau pengkamputeran serata yang membolehkan kita mengatasi banyak kekurangan di dalam sistem maklumat yang terkini, sementara dari segi yang lain pula, pengkamputeran serata adalah bertentangan secara langsung dengan asas perlindungan kebersendirian. Banyak usaha telah dilakukan bagi mengatasi masalah ini tetapi setiap satunya mempunyai kekurangan tersendiri. Sesetengah penyelesaian menyediakan hanya satu aspek kebersendirian seperti kebersendirian lokasi atau kebersendirian pengenalan, setengah daripada mereka adalah bukan tak bersandar tapak (*platform independence*), dan setengahnya pula menghasilkan banyak isyarat kebersendirian kepada pengguna.

Dalam tesis ini kami mencadangkan model kebersendirian baru dalam pengkomputeran serata yang menyediakan semua empat jenis kebersendirian (pengenalan, lokasi, masa, dan kandungan) untuk pengguna dengan kawalan ketat ke atas maklumat persendirian dan sedikit amaran kebersendirian yang mungkin. Untuk melengkapkan model cadangan, kami tunjukkan polisi kebersendirian model dengan tag XML dan agihkan proses pembuatan keputusan dalam lapisan berlainan demi menyediakan keskalaan tinggi.

Untuk mengesahkan model ini, kami telah tunjukkan menerusi pelaksanaan bahwa model menyediakan "Kebolehungkapan Polisi Kebersendirian" dengan sokongan peraturan-peraturan mandatori dan budi bicara, pengendalian ketidakpastian dan resolusi konflik. Kami telah tunjukkan sifat *unobtrusiveness* dengan pelaksanaan dan pengukuran masa yang pengguna buang dalam berurusan dengan subsistem kebersendirian. Kami juga telah tunjukkan bahawa model kami menyediakan kebersendirian kandungan, pengenalan *(identity)*, lokasi dan waktu yang membawa kepada kawalan pengguna paras tinggi terhadap maklumat persendirian. Keskalaan model dapat diperoleh melalui penggunaan XML sebagai format tak bersandar tapak untuk memerihalkan polisi kebersendirian dengan tambahan proses pembuatan keputusan teragih.

Keputusan mengesahkan bahawa model yang dicadangkan menyokong kesemua empat metrik kebolehungkapan polisi kebersendirian, empat metrik kawalan pengguna terhadap maklumat persendirian, juga kedua-dua faktor keskalaan dan *unobtrusiveness* dengan ukuran kurang daripada 10%

AKNOWLEDGEMENTS

It is a great opportunity to thank Dr. Ali B.Mamat and Dr. Ramlan B.Mahmod for their great help on this thesis and for their supporting guidance, ideas, and materials.

I would also like to express my thanks to the Faculty of Computer Science and Technology, especially the ICT unit, for providing general help and assistance. Also, I'd like to thank the Library and the School of Graduate Studies for helpfully fulfilling my every request.

Special thanks to my friends and colleagues at the Faculty of Computer Science and Information Technology for their support and advice. Your help will not be forgotten.

Finally, I would like to thank my family for giving me the motivation and moral support needed to complete this thesis. Only Allah can truly reward what they have done.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the Master degree. The members of the Supervisory Committee were as follows:

Ali B.Mamat, PhD
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Ramlan B.Mahmmod, PhD
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

AINI EDRIS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 12 June 2008

DECLARATION

I declared that the thesis is my original work except for quotations and citations, which have been duly acknowledge. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at UPM or at any other institutions.

ALI DEHGHANTANHA

Date: 24 June 2008

TABLE OF CONTENTS

LIST OF TABELS

LIST OF FIGURES

TERMS AND ABBRIVIATIONS

ECC Algorithms	ElliptiC Curve Algorithms
XML	eXtended Markup Language
APL	Authentication Precision Level
Ubiquitous Computing	Another name for pervasive computing systems
N/A	Not Applicable

CHAPTER 1

INTRODUCTION

1.1 Background

Mark Wiser (Wiser, 1995) for the first time described environments that devices weave themselves to user's daily life, they enable users to work in any environment, anytime at anywhere. He called this environment "Ubiquitous Computing" or "Pervasive Computing" environment.

A lot of research projects attempt to reach to this idea. Aura project (Carnegie Mellon University, 2002) was a wireless umbrella that pervasively connects different devices in Carnegie Mellon University campus. Oxygen project (MIT University Computer Science and Artificial Intelligence Laboratory, 2006) aims to build a pervasive environment that devices weave themselves as oxygen to users life. The Gaia project (University of Illinois, 2006) was an effort to build a middle-ware for traditional devices to work and join to the pervasive environments. Microsoft Easy Living project (Microsoft, 2007) brings intelligent, computational devices to the people daily life.

A pervasive computing environment consists of mobile devices, sensors and wireless antenna and WAP gateways (Dapos, Ambrogio, & Iazeolla, 2005). Architecture of this environment is shown in Figure 1.1.

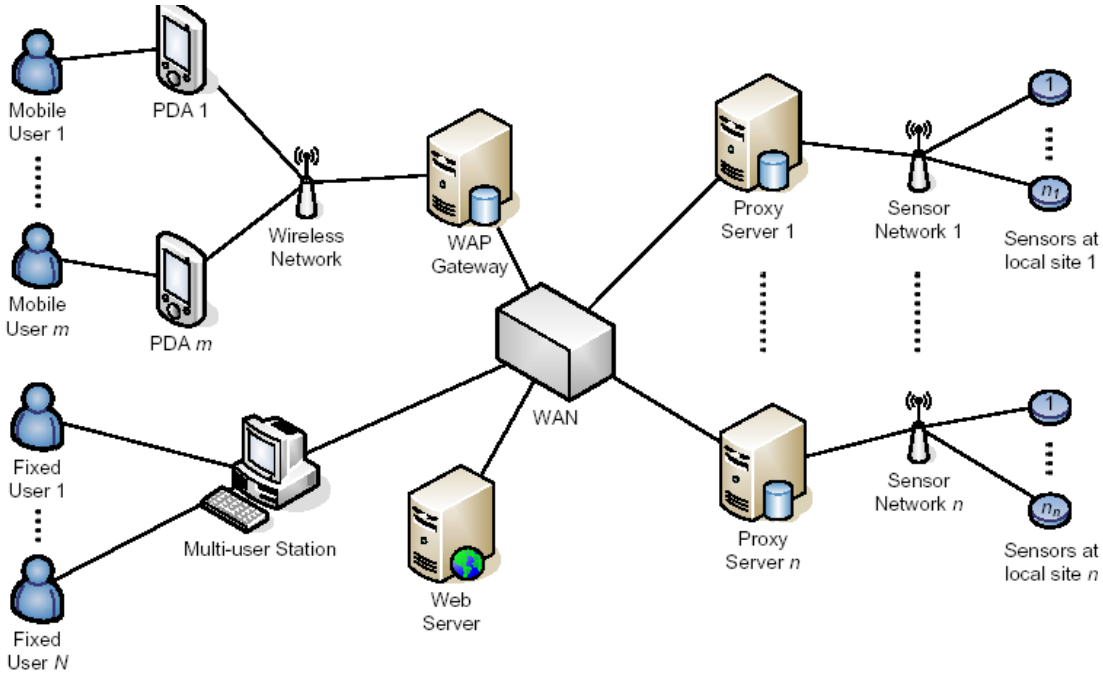

Figure 1.1: Pervasive Computing Architecture

The most noticeable characteristics of pervasive environments are (Lahlou, Langheinrich, & Rocker, 2005; Russell, Streitz, & Winograd, 2005):

1. Ubiquity: Environmental services are everywhere for every user.
2. Invisibility: Services invisibly weave themselves to the environment.
3. Sensing: The invisible and ubiquitous devices can sense and detect environmental information.
4. Inter connection and co-operation between devices: The sensitive, invisible, and ubiquitous devices cooperate and connect to each other for providing pervasive services.
5. Memory amplification: The cooperative, sensitive, invisible, and ubiquitous devices increase environmental storage ability and amplify memory.

The above characteristics make privacy as an inevitable need for all pervasive environments. There are privacy principals based on well known Fair Information Practices (Organization for Economic Co-operation and Development (OECD), 1980) as listed below (Lahlou & Jegou, 2004):

- Notice*:* Users always should be aware of gathering their personal data.
- Choice and Consent*:* Users should always have choice to carrying out their personal data or not.
- Proximity and Locality*:* Gathering of data should always happen in an environment that user is present (proximity) and the processing of the data should be in the space that the data has been gathered (locality).
- Anonymity and Pseudonymity*:* Whenever user identity is not required or user did not consent, pseudonymity and anonymity mechanisms should be used.
- Access to Resources: Access to the user resources should only be allowed to the authorize parties.

As it is clear the pervasive environment characteristics are in direct conflict with privacy principals. The most profound privacy risks in pervasive systems are (Dritsas, Gritzalis, & Lambrinoudakis, 2005):

a. Pervasive devices exist everywhere and with the enhancements in their saving capacities and little size they can invisibly gather a lot of user private information.
b. The communication between pervasive devices should be held by their own so they might reveal user private information in communication with each other.

Beside the above risks we have to consider that in most countries privacy regulations are in their begging steps. All the above reasons clarify the need for privacy models in pervasive environments.

1.2 Problem Statement

From the early time of pervasive computing the researchers proposed different privacy models. The early models focus was on providing different types of private information (content, identity, location, and time privacy) for the user. The “Privacy Mirror Model” (Nguyan & Mynatt, 2000) supported time and content privacy, the “Identity Management Model” (Rennhard & Plattner, 2003) supported identity privacy, the “Mist Protocol” (Al-Muhtadi, Ranganathan, Campbell, & Mickunas, 2002) supported location privacy, the “Unified Privacy Tagging” (Jiang & Landay, 2002) supported content privacy, and “Mix Zones” (Beresford & Stajano, 2004) model supported location privacy.

The recent privacy models like Loc Serve (Myles, Friday, & Davies, 2003), Context Model for Privacy (Henricksen, Wishart, McFadden, & Indulska, 2005), PSIUM and Anonymity Enhancer (Cheng, Zhang, & Tan, 2005), Tachyon (Iwai & Tokuda, 2005), IDRSC (Xinyi, Susilo, Yi, & Futai, 2005), and Loom Model (Imada, Ohta, & Yamaguchi, 2006) support all four types of private information (content, identity, location, and time) while increasing the expressiveness of privacy policies with supporting mandatory and discretionary rules, reflect context sensitive information, handle uncertain situations and resolve conflict situations. These models attempt to

increase their scalability with providing a common communication platform and distributing decision making processes. Finally these models decrease the unobtrusiveness of their privacy mechanisms (percent of time that user wastes on dealing with privacy sub-system). Table 1.1 shows the current privacy models with their supporting features.

Table 1.1: The current privacy models supported features

MODEL	EXPRESIVNESS OF PRIVACY POLICIES LIST OF SUPPORTED FEATURES	USER CONTROL OVER PRIVATE INFORMATION	UNOBTRUSIVENESS OF PRIVACY POLICIES	PLATFORM INDEPENDENCY, LIST OF SUPPORTED FEATURES
Loc Serve (Myles et al., 2003)	Support for mandatory and discretionary rules.	Identity, location, time privacy	Less than 10%	XML as common platform
Context Model for Privacy (Henricks et al., 2005)	Context sensitivity, uncertainty handling, conflict resolution	Identity, location privacy	More than 40% and less than 70%	Not scalable
PSIUM and Anonymity Enhancer (Cheng et al., 2005)	No privacy policy support.	Content, identity, location privacy	More than 40% and less than 70%	Not scalable
Tachyon (Iwai & Tokuda, 2005)	Support for mandatory and discretionary rules.	Location privacy	Less than 10%	XML as common platform, no centralized server

IDRSC (Xinyi et al., 2005)	No privacy policy support	Content, and identity privacy	Less than 10%	Not scalable
Loom Model (Imada et al., 2006)	No privacy policy support	Content, identity, location, and time privacy	More than 10% and less than 40%	Not scalable

Previous evaluations on privacy models in pervasive computing systems (Blaine, et al, 2004; Dritsas et al., 2005; Ranganathan et al., 2005) and our investigation show that none of previous privacy models could preserve all types of information privacy, with expressive privacy policies with less than 10% of unobtrusiveness and high scalability.

This research problem is to seek for a privacy model that supports all four types of information privacy (content, location, identity, and time) while its privacy policies are expressive and the model should be scalable with less than 10% of unobtrusiveness.

1.3 Research Objective

This research objective is to provide a privacy model with the following characteristics:

a. The privacy policies should be expressive to support mandatory and discretionary rules, context sensitivity, uncertainty handling, and conflict resolution.