Dieter Hutter
Günter Müller
Werner Stephan
Markus Ullmann (Eds.)

LNCS 2802

# Security in Pervasive Computing

First International Conference
Boppard, Germany, March 2003
Revised Papers

Springer

Dieter Hutter Günter Müller
Werner Stephan Markus Ullmann (Eds.)

# Security in Pervasive Computing

First International Conference
Boppard, Germany, March 12-14, 2003
Revised Papers

Springer

Volume Editors

Dieter Hutter
Werner Stephan
German Research Centre for Artificial Intelligence, DFKI
Stuhlsatzenhausweg 3, 66123 Saarbrücken, Germany
E-mail: {hutter,stephan}@dfki.de

Günter Müller
University of Freiburg, Institute for Computer Science
Friedrichstrasse 50, 79098 Freiburg, Germany
E-mail: mueller@iig.uni-freiburg.de

Markus Ullmann
BSI
Godesberger Allee 183, 53175 Bonn, Germany
E-mail: Markus.Ullmann@bsi.bund.de

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): C.2, D.2, D.4.6, H.5, K.4.1, K.4.4, K.6.5

ISSN 0302-9743
ISBN 3-540-20887-9 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 10980521 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 2802
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
*Berlin*
*Heidelberg*
*New York*
*Hong Kong*
*London*
*Milan*
*Paris*
*Tokyo*

# Preface

The ongoing compression of computing facilities into small and mobile devices like handhelds, portables or even wearable computers will enhance ubiquitous information processing. The basic paradigm of such pervasive computing is the combination of strongly decentralized and distributed computing with the help of diversified devices allowing for spontaneous connectivity via the Internet. Computers will become invisible to the user, and exchange of information between devices will effectively be beyond the user's control.

Assuming a broad usage of more powerful tools and more effective ways to use them the quality of everyday life will be strongly influenced by the dependability of the new technology. Information stored, processed, and transmitted by the various devices is one of the most critical resources. Threats exploiting vulnerabilities of new kinds of user interfaces, displays, operating systems, networks, and wireless communications will cause new risks of losing confidentiality, integrity, and availability. Can these risks be reduced by countermeasures to an acceptable level or do we have to redefine political and social demands.

The objective of this 1st International Conference on Security in Pervasive Computing was to develop new security concepts for complex application scenarios based on systems like handhelds, phones, smartcards, and smart labels hand in hand with the emerging technology of ubiquitous and pervasive computing. Particular subjects were methods and technology concerning the identification of risks, the definition of security policies, and the development of security measures that are related to the specific aspects of ubiquitous and pervasive computing like mobility, communication, and secure hardware/software platforms.

We received 51 submissions. Each submission was reviewed by three independent reviewers and an electronic program committee meeting was held via the Internet. We are very grateful to the program committee members for their efficency in processing the work within four weeks and also for the quality of their reviews and discussions. Finally the program committee decided to accept 19 papers. We are also very grateful to the four invited speakers for their vivid and stimulating talks.

Apart from the program committee, we would like to thank also the other persons who contributed to the success of this conference: the additional referees for reviewing the papers, the authors for submitting the papers, and the local organizers, and in particular Hans-Peter Wagner, for a smooth and pleasant stay in Boppard.

June 2003

Dieter Hutter, Günter Müller,
Werner Stephan, Markus Ullmann
Program Co-chairs SPC 2003

# Organization

SPC 2003 was organized by the German Research Center for Artificial Intelligence in Saarbrücken and the German Bundesamt für Sicherheit in der Informationstechnik in Bonn.

## Executive Committee

| | |
|---|---|
| Program Co-chairs | Dieter Hutter (DFKI GmbH, Germany)<br>Günter Müller (University of Freiburg, Germany)<br>Werner Stephan (DFKI GmbH, Germany)<br>Markus Ullmann (BSI, Germany) |
| Local Arrangements | Hans-Peter Wagner (BSI, Germany) |

## Program Committee

| | |
|---|---|
| Michael Beigl | University of Karlsruhe, Germany |
| Joshua Guttman | MITRE, USA |
| Dieter Hutter | DFKI Saarbrücken, Germany |
| Paul Karger | IBM Watson Research, USA |
| Friedemann Mattern | ETH Zürich, Switzerland |
| Catherine Meadows | Naval Research Lab, USA |
| Guenter Mueller | University of Freiburg, Germany |
| Joachim Posegga | SAP, Germany |
| Kai Rannenberg | University of Frankfurt, Germany |
| Kurt Rothermel | University of Stuttgart, Germany |
| Ryoichi Sasaki | Tokyo Denki University, Japan |
| Frank Stajano | Cambridge University, UK |
| Werner Stephan | DFKI Saarbrücken, Germany |
| Moriyasu Takashi | Hitachi Ltd., Japan |
| Seiji Tomita | NTT Information Platform Laboratories, Japan |
| Markus Ullmann | BSI, Bonn, Germany |

## Invited Speakers

| | |
|---|---|
| Friedemann Mattern | ETH Zürich, Switzerland |
| Hideyuki Nakashima | Cyber Assist Research Center, AIST, Japan |
| Frank Stajano | Cambridge University, UK |
| Markus Luidolt | Philips Semiconductors, Austria |
| Paul Karger | IBM Watson Research, USA |

## Additional Referees

L. Fritsch
P. Girard
J. Hähner
T. Heiber
R. Kilian-Kehr
M. Kinateder
D. Kügler
M. Langheinrich
P. Robinson
M. Rohs
H. Rossnagel
H. Vogt
S. Wittmann

## Sponsoring Institutions

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Saarbrücken, Germany
Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany

# Lecture Notes in Computer Science

## For information about Vols. 1–2849 please contact your bookseller or Springer-Verlag

Vol. 2802: D. Hutter, G. Müller, W. Stephan, M, Ullmann (Eds.), Security in Pervasive Computing. Proceedings, 2003. XI, 291 pages. 2004.

Vol. 2850: M.Y. Vardi, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. Proceedings, 2003. XIII, 437 pages. 2003. (Subseries LNAI)

Vol. 2851: C. Boyd, W. Mao (Eds.), Information Security. Proceedings, 2003. XI, 443 pages. 2003.

Vol. 2852: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. Proceedings, 2003. VIII, 509 pages. 2003.

Vol. 2853: M. Jeckle, L.-J. Zhang (Eds.), Web Services – ICWS-Europe 2003. Proceedings, 2003. VIII, 227 pages. 2003.

Vol. 2854: J. Hoffmann, Utilizing Problem Structure in Planning. XIII, 251 pages. 2003. (Subseries LNAI)

Vol. 2855: R. Alur, I. Lee (Eds.), Embedded Software. Proceedings, 2003. X, 373 pages. 2003.

Vol. 2856: M. Smirnov, E. Biersack, C. Blondia, O. Bonaventure, O. Casals, G. Karlsson, George Pavlou, B. Quoitin, J. Roberts, I. Stavrakakis, B. Stiller, P. Trimintzios, P. Van Mieghem (Eds.), Quality of Future Internet Services. IX, 293 pages. 2003.

Vol. 2857: M.A. Nascimento, E.S. de Moura, A.L. Oliveira (Eds.), String Processing and Information Retrieval. Proceedings, 2003. XI, 379 pages. 2003.

Vol. 2858: A. Veidenbaum, K. Joe, H. Amano, H. Aiso (Eds.), High Performance Computing. Proceedings, 2003. XV, 566 pages. 2003.

Vol. 2859: B. Apolloni, M. Marinaro, R. Tagliaferri (Eds.), Neural Nets. Proceedings, 2003. X, 376 pages. 2003.

Vol. 2860: D. Geist, E. Tronci (Eds.), Correct Hardware Design and Verification Methods. Proceedings, 2003. XII, 426 pages. 2003.

Vol. 2861: C. Bliek, C. Jermann, A. Neumaier (Eds.), Global Optimization and Constraint Satisfaction. Proceedings, 2002. XII, 239 pages. 2003.

Vol. 2862: D. Feitelson, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. Proceedings, 2003. VII, 269 pages. 2003.

Vol. 2863: P. Stevens, J. Whittle, G. Booch (Eds.), «UML» 2003 – The Unified Modeling Language. Proceedings, 2003. XIV, 415 pages. 2003.

Vol. 2864: A.K. Dey, A. Schmidt, J.F. McCarthy (Eds.), UbiComp 2003: Ubiquitous Computing. Proceedings, 2003. XVII, 368 pages. 2003.

Vol. 2865: S. Pierre, M. Barbeau, E. Kranakis (Eds.), Ad-Hoc, Mobile, and Wireless Networks. Proceedings, 2003. X, 293 pages. 2003.

Vol. 2866: J. Akiyama, M. Kano (Eds.), Discrete and Computational Geometry. Proceedings, 2002. VIII, 285 pages. 2003.

Vol. 2867: M. Brunner, A. Keller (Eds.), Self-Managing Distributed Systems. Proceedings, 2003. XIII, 274 pages. 2003.

Vol. 2868: P. Perner, R. Brause, H.-G. Holzhütter (Eds.), Medical Data Analysis. Proceedings, 2003. VIII, 127 pages. 2003.

Vol. 2869: A. Yazici, C. Şener (Eds.), Computer and Information Sciences – ISCIS 2003. Proceedings, 2003. XIX, 1110 pages. 2003.

Vol. 2870: D. Fensel, K. Sycara, J. Mylopoulos (Eds.), The Semantic Web - ISWC 2003. Proceedings, 2003. XV, 931 pages. 2003.

Vol. 2871: N. Zhong, Z.W. Raś, S. Tsumoto, E. Suzuki (Eds.), Foundations of Intelligent Systems. Proceedings, 2003. XV, 697 pages. 2003. (Subseries LNAI)

Vol. 2873: J. Lawry, J. Shanahan, A. Ralescu (Eds.), Modelling with Words. XIII, 229 pages. 2003. (Subseries LNAI)

Vol. 2874: C. Priami (Ed.), Global Computing. Proceedings, 2003. XIX, 255 pages. 2003.

Vol. 2875: E. Aarts, R. Collier, E. van Loenen, B. de Ruyter (Eds.), Ambient Intelligence. Proceedings, 2003. XI, 432 pages. 2003.

Vol. 2876: M. Schroeder, G. Wagner (Eds.), Rules and Rule Markup Languages for the Semantic Web. Proceedings, 2003. VII, 173 pages. 2003.

Vol. 2877: T. Böhme, G. Heyer, H. Unger (Eds.), Innovative Internet Community Systems. Proceedings, 2003. VIII, 263 pages. 2003.

Vol. 2878: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. Part I. Proceedings, 2003. XXXIII, 819 pages. 2003.

Vol. 2879: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. Part II. Proceedings, 2003. XXXIV, 1003 pages. 2003.

Vol. 2880: H.L. Bodlaender (Ed.), Graph-Theoretic Concepts in Computer Science. Proceedings, 2003. XI, 386 pages. 2003.

Vol. 2881: E. Horlait, T. Magedanz, R.H. Glitho (Eds.), Mobile Agents for Telecommunication Applications. Proceedings, 2003. IX, 297 pages. 2003.

Vol. 2882: D. Veit, Matchmaking in Electronic Markets. XV, 180 pages. 2003. (Subseries LNAI)

Vol. 2883: J. Schaeffer, M. Müller, Y. Björnsson (Eds.), Computers and Games. Proceedings, 2002. XI, 431 pages. 2003.

Vol. 2884: E. Najm, U. Nestmann, P. Stevens (Eds.), Formal Methods for Open Object-Based Distributed Systems. Proceedings, 2003. X, 293 pages. 2003.

Vol. 2885: J.S. Dong, J. Woodcock (Eds.), Formal Methods and Software Engineering. Proceedings, 2003. XI, 683 pages. 2003.

Vol. 2886: I. Nyström, G. Sanniti di Baja, S. Svensson (Eds.), Discrete Geometry for Computer Imagery. Proceedings, 2003. XII, 556 pages. 2003.

Vol. 2887: T. Johansson (Ed.), Fast Software Encryption. Proceedings, 2003. IX, 397 pages. 2003.

Vol. 2888: R. Meersman, Zahir Tari, D.C. Schmidt et al. (Eds.), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. Proceedings, 2003. XXI, 1546 pages. 2003.

Vol. 2889: Robert Meersman, Zahir Tari et al. (Eds.), On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops. Proceedings, 2003. XXI, 1096 pages. 2003.

Vol. 2890: M. Broy, A.V. Zamulin (Eds.), Perspectives of System Informatics. Proceedings, 2003. XV, 572 pages. 2003.

Vol. 2891: J. Lee, M. Barley (Eds.), Intelligent Agents and Multi-Agent Systems. Proceedings, 2003. X, 215 pages. 2003. (Subseries LNAI)

Vol. 2892: F. Dau, The Logic System of Concept Graphs with Negation. XI, 213 pages. 2003. (Subseries LNAI)

Vol. 2893: J.-B. Stefani, I. Demeure, D. Hagimont (Eds.), Distributed Applications and Interoperable Systems. Proceedings, 2003. XIII, 311 pages. 2003.

Vol. 2894: C.S. Laih (Ed.), Advances in Cryptology - ASIACRYPT 2003. Proceedings, 2003. XIII, 543 pages. 2003.

Vol. 2895: A. Ohori (Ed.), Programming Languages and Systems. Proceedings, 2003. XIII, 427 pages. 2003.

Vol. 2896: V.A. Saraswat (Ed.), Advances in Computing Science – ASIAN 2003. Proceedings, 2003. VIII, 305 pages. 2003.

Vol. 2897: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. Proceedings, 2003. XI, 240 pages. 2003.

Vol. 2898: K.G. Paterson (Ed.), Cryptography and Coding. Proceedings, 2003. IX, 385 pages. 2003.

Vol. 2899: G. Ventre, R. Canonico (Eds.), Interactive Multimedia on Next Generation Networks. Proceedings, 2003. XIV, 420 pages. 2003.

Vol. 2900: M. Bidoit, P.D. Mosses, CASL User Manual. XIII, 240 pages. 2004.

Vol. 2901: F. Bry, N. Henze, J. Maluszyński (Eds.), Principles and Practice of Semantic Web Reasoning. Proceedings, 2003. X, 209 pages. 2003.

Vol. 2902: F. Moura Pires, S. Abreu (Eds.), Progress in Artificial Intelligence. Proceedings, 2003. XV, 504 pages. 2003. (Subseries LNAI).

Vol. 2903: T.D. Gedeon, L.C.C. Fung (Eds.), AI 2003: Advances in Artificial Intelligence. Proceedings, 2003. XVI, 1075 pages. 2003. (Subseries LNAI).

Vol. 2904: T. Johansson, S. Maitra (Eds.), Progress in Cryptology – INDOCRYPT 2003. Proceedings, 2003. XI, 431 pages. 2003.

Vol. 2905: A. Sanfeliu, J. Ruiz-Shulcloper (Eds.), Progress in Pattern Recognition, Speech and Image Analysis. Proceedings, 2003. XVII, 693 pages. 2003.

Vol. 2906: T. Ibaraki, N. Katoh, H. Ono (Eds.), Algorithms and Computation. Proceedings, 2003. XVII, 748 pages. 2003.

Vol. 2908: K. Chae, M. Yung (Eds.), Information Security Applications. Proceedings, 2003. XII, 506 pages. 2004.

Vol. 2910: M.E. Orlowska, S. Weerawarana, M.P. Papazoglou, J. Yang (Eds.), Service-Oriented Computing – ICSOC 2003. Proceedings, 2003. XIV, 576 pages. 2003.

Vol. 2911: T.M.T. Sembok, H.B. Zaman, H. Chen, S.R. Urs, S.H.Myaeng (Eds.), Digital Libraries: Technology and Management of Indigenous Knowledge for Global Access. Proceedings, 2003. XX, 703 pages. 2003.

Vol. 2912: G. Liotta (Ed.), Graph Drawing. Proceedings, 2003. XV, 542 pages. 2004.

Vol. 2913: T.M. Pinkston, V.K. Prasanna (Eds.), High Performance Computing – HiPC 2003. Proceedings, 2003. XX, 512 pages. 2003.

Vol. 2914: P.K. Pandya, J. Radhakrishnan (Eds.), FST TCS 2003: Foundations of Software Technology and Theoretical Computer Science. Proceedings, 2003. XIII, 446 pages. 2003.

Vol. 2916: C. Palamidessi (Ed.), Logic Programming. Proceedings, 2003. XII, 520 pages. 2003.

Vol. 2918: S.R. Das, S.K. Das (Eds.), Distributed Computing – IWDC 2003. Proceedings, 2003. XIV, 394 pages. 2003.

Vol. 2919: E. Giunchiglia, A. Tacchella (Eds.), Theory and Applications of Satisfiability Testing. Proceedings, 2003. XI, 530 pages. 2004.

Vol. 2920: H. Karl, A. Willig, A. Wolisz (Eds.), Wireless Sensor Networks. Proceedings, 2004. XIV, 365 pages. 2004.

Vol. 2921: G. Lausen, D. Suciu (Eds.), Database Programming Languages. Proceedings, 2003. X, 279 pages. 2004.

Vol. 2922: F. Dignum (Ed.), Advances in Agent Communication. Proceedings, 2003. X, 403 pages. 2004. (Subseries LNAI).

Vol. 2923: V. Lifschitz, I. Niemelä (Eds.), Logic Programming and Nonmonotonic Reasoning. Proceedings, 2004. IX, 365 pages. 2004. (Subseries LNAI).

Vol. 2924: J. Callan, F. Crestani, M. Sanderson (Eds.), Distributed Multimedia Information Retrieval. Proceedings, 2003. XII, 173 pages. 2004.

Vol. 2926: L. van Elst, V. Dignum, A. Abecker (Eds.), Agent-Mediated Knowledge Management. Proceedings, 2003. XI, 428 pages. 2004. (Subseries LNAI).

Vol. 2927: D. Hales, B. Edmonds, E. Norling, J. Rouchier (Eds.), Multi-Agent-Based Simulation III. Proceedings, 2003. X, 209 pages. 2003. (Subseries LNAI).

Vol. 2928: R. Battiti, M. Conti, R. Lo Cigno (Eds.), Wireless On-Demand Network Systems. Proceedings, 2004. XIV, 402 pages. 2004.

Vol. 2929: H. de Swart, E. Orlowska, G. Schmidt, M. Roubens (Eds.), Theory and Applications of Relational Structures as Knowledge Instruments. Proceedings. VII, 273 pages. 2003.

Vol. 2932: P. Van Emde Boas, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2004: Theory and Practice of Computer Science. Proceedings, 2004. XIII, 385 pages. 2004.

Vol. 2935: P. Giorgini, J.P. Müller, J. Odell (Eds.), Agent-Oriented Software Engineering IV. Proceedings, 2003. X, 247 pages. 2004.

Vol. 2937: B. Steffen, G. Levi (Eds.), Verification, Model Checking, and Abstract Interpretation. Proceedings, 2004. XI, 325 pages. 2004.

Vol. 2950: N. Jonoska, G. Păun, G. Rozenberg (Eds.), Aspects of Molecular Computing. XI, 391 pages. 2004.

# Table of Contents

## Invited Talks (Abstracts)

## Location Privacy

## Security Requirements

## Security Policies and Protection

## Authentication and Trust

## Secure Infrastructures

## Smart Labels

## Verification

## Hardware Architectures

## Workshop

# The Age of Pervasive Computing – Everything Smart, Everything Connected?
## (Abstract of Invited Talk)

Friedemann Mattern

Institute for Pervasive Computing
ETH Zurich, Switzerland
mattern@inf.ethz.ch

**Abstract.** Given the continuing technical progress in computing and communication, it seems that we are heading towards an all-encompassing use of networks and computing power, a new era commonly termed "Pervasive Computing". Its vision is grounded in the firm belief amongst the scientific community that Moore's Law (i.e. the observation that the computer power available on a chip approximately doubles every eighteen months) will hold true for at least another 10 years. This means that in the next few years, microprocessors will become so small and inexpensive that they can be embedded in almost everything – not only electrical devices, cars, household appliances, toys, and tools, but also such mundane things as pencils (e.g. to digitize everything we draw) and clothes. All these devices will be interwoven and connected together by wireless networks. In fact, technology is expected to make further dramatic improvements, which means that eventually billions of tiny and mobile processors will occupy the environment and be incorporated into many objects of the physical world.

Together with powerful and cheap sensors (and thus the ability to sense the environment), this progress in processor and communication technology will render everyday objects "smart" – they know where they are, and they may adapt to the environment and provide useful services in addition to their original purpose. These smart objects may form spontaneous networks, giving rise to a world-wide distributed system several orders of magnitude larger than today's Internet.

It is clear that we are moving only gradually towards the ultimate vision of Pervasive Computing. Much progress in computer science, communication engineering, and material science is necessary to render the vision economically feasible and to overcome current technological hurdles. However, the prospects of a world of things that virtually talk to each other are fascinating: many new services would then be possible that transform the huge amount of information gathered by the smart devices into value for the human user, and an entire industry may be set up to establish and run the underlying infrastructure for the smart and networked objects.

Clearly, there are also many issues on the political, legal, and social level to consider. Privacy is certainly a primary concern when devices or smart everyday objects can be localized and traced, and when various objects we use daily report their state and sensor information to other objects. The repercussions of such an extensive integration of computer technology into our everyday lives as Pervasive Computing advocates it, are difficult to predict and only time will tell whether this technology does contribute to a better and more enjoyable world or, on the contrary, promote a more totalitarian regime.

D. Hutter et al. (Eds.): Security in Pervasive Computing 2003, LNCS 2802, p. 1, 2004.

# Cyber Assist Project and Its Security Requirement (Abstract of Invited Talk)

Hideyuki Nakashima

Cyber Assist Research Center
AIST Tokyo Waterfront, 2-41-6 Aomi,
Koto-ku, Tokyo 135-0064, Japan
h.nakashima@aist.go.jp

## 1 Introduction

The Goal of the Cyber Assist Project is realization of a ubiquitous, or pervasive, information society in which all can benefit from assistance of information processing technology (IT hereafter) in all situations of daily life.

Traditional IT is accessible only through computers sitting on a desktop. Its accessibility is broadening recently with the spread of mobile devices including mobile phones with i-mode. Nevertheless, such technology is used only by a small portion of people in rather limited scenarios of their everyday lives. IT should be able to support human in every aspect of everyday life with information processing units embedded in the environment which communicate with portable or wearable personal devices. Keywords are “here, now and me”. IT will be able to help human daily life by automatically booking a seat in a train according to an individual schedule, by guiding a user through a shopping mall while providing necessary information about goods, or automatically calling a taxi or requesting bus service when needed. Through this technology, we believe that IT can boost the quality of life in economy, politics, culture, and education.

To widen the range of opportunity for receiving assistance from IT, computers should be able to share the semantics of tasks with humans. We must pull computers from their digital world into our physical world by providing various sensors and visual and acoustic recognition technologies. For instance, if a mobile phone can understand that its holder has a visitor and is discussing an important issue, it may be able to automatically forward incoming calls to a secretary.

We need new network architecture to support the technology. It must be capable of dynamic reconfiguration and connection with very low latency, creating “responsive” network technology.

Another technology necessary for semantic sharing is worldwide document processing with tagging, ontology, and semantic search as proposed in the SemanticWeb project. We cooperate with that movement and will develop “intelligent content” technologies.

D. Hutter et al. (Eds.): Security in Pervasive Computing 2003, LNCS 2802, pp. 2–5, 2004.

## 2 Cyber Assist Project

Our project is classified as follows. We have two main targets:

1. Situated information support
2. Privacy protection

We also have two main approaches:

1. Location-based communications
2. Intelligent contents

The four cross-sections yield the following research issues:

### 2.1 Semantic Structuring

A major cause of information overload and the 'digital divide' is the semantic gap between humans and computers; humans are adapted to dealing with deep meaning, while machines excel at processing explicit syntax. The only feasible way to fill this gap systematically is to make the semantic structure of information content explicit so that machines can manage them too. [Hasida 2000]

### 2.2 Non-ID Communication

There exist two global communication networks: the telephone network and the Internet. Telephone systems use a phone number as a global ID to reach each telephone in the world. Communication over the Internet is based on IP-addresses, which are also a global ID for each processing unit connected to the network. When communication is overheard, it is easy to connect content to recipients using those global IDs. In a ubiquitous computing environment, the majority of communication is computer to computer: frequency is much larger in magnitude. If ubiquitous computing follows this tradition, it may endanger privacy protection. For instance, if someone discovers the IP address of a TV set, all programs a user watches may be monitored. It is therefore recommended to use locally- resolved IDs wherever possible. It is even better to use no IDs at all.

One candidate for non-ID communication is to use physical location as a target address of communication. We call this location-based communication. We are testing various methods for location-based communication using optical and radio connections.

### 2.3 Location-Based Services

The main (positive) target of our project is situated information support. If a server knows the user's situation, it can provide more fine-tuned information support without querying the user's selections. There may be many keys to this; we regard location as a most prominent physical property.

One form of location-based service is to provide information only to a certain area of 3D space. For example, in a museum, detailed information of an entry is broadcast to the area in front of an exhibition, but only to those facing it.

As a communication device to receive such information, we developed a very simple compact battery-less information terminal called CoBIT [Nishimura 2002]. In our design, devices embedded in the environment play many important roles. CoBIT is equipped with a reflective sheet whose location can be identified easily from cameras mounted in the environment. Then an infrared beam is projected toward the direction from a LED scanner that is capable of tracking CoBIT movement . Note that there is no need for any ID to establish communication. Physical location of the terminal is an essential and unique key of the device. The infrared signal is modulated using a sound wave; CoBIT replays it as auditory information. The infrared beam itself is the power source of CoBIT; thus, there is no need to have any internal power supply. Cameras in the environment will see the reflection from the reflective sheet of CoBIT to know its location, direction and movement (gesture). Therefore, CoBIT functions as a two way communication terminal even without its own internal power source.

In ubiquitous computing, many devices in the vicinity of the user are used. How does one know which devices are near to the user, and free to use? The location of user may be given by the name of the building, or longitude and latitude of GPS positioning. Those must be converted from one to another. Multiagent architecture plays important roles for access control of those devices. We are developing location identification (including conversion between coordinates and names) and access control architecture called Consorts [Kurumatani 2003].

### 2.4 Tally Method

In old movies, there were plots employing a map of hidden treasure split into two and possessed by two participants. Two of them must get together to unveil the location. We are seeking a digital version of similar technology. Double encryption is an obvious candidate. But once data is decoded, it is plain data and both participants can copy it freely. What we seek is protected data that can be used only when both of tally holders are present.

These days, a customer's personal data may be gathered by each individual service provider. For instance: a mail order company has a customer's record of purchase; a mobile phone company has a record of outgoing and incoming phone calls as well as history of the trajectory of the mobile phone device with accuracy of cellular area of its connection station; a hospital has a record of a patient's past treatment and medical examinations. If those data are gathered into a single database, it may contain a large amount of personal information. Such accumulation itself is dangerous from the perspective of privacy protection. On the other hand, if those data are used for the benefit of the individual only, they may constitute a valuable personal database. We are seeking a solution to this problem. We seek to protect privacy information while using all data for the sake of the individual. One compromise is that those data be used only when the target person, or their software agent, is present.